Patrick Legand

sans tabou

Préface de **Benjamin Arnault (HSC)**

Sécuriser *enfin* son PC

Réflexes et techniques contre les virus, spams, phishing, vols et pertes de données

EYROLLES

Préface

Qu'est-ce que la sécurité ? A priori, c'est le sentiment, à tort ou à raison, d'être à l'abri de tout danger. Cependant doit-on se limiter à cette définition ? Assurément non. Bien qu'elle présente un postulat de départ satisfaisant, il ne faut pas s'y arrêter. Une autre formulation plus adaptée au contexte des systèmes d'information pourrait être la suivante : protéger l'intégrité, assurer la disponibilité et garantir la confidentialité des biens.

La sécurité informatique a toujours été vue comme le parent pauvre du domaine des technologies de l'information numérique. Elle constitue pour beaucoup une contrainte et un investissement en temps, ressources et argent. Longtemps, les utilisateurs et administrateurs n'ont pas bien vu la nécessité d'entreprendre des actions de sécurisation et les décideurs n'ont pas eu d'idée concrète du retour sur investissement qu'elles impliquaient. Aujourd'hui, les directeurs ont pris le tournant de la sécurité des systèmes d'information. Elle est progressivement devenue une préoccupation majeure s'intégrant dans les définitions de politiques de gestion des risques, motivées par le sentiment latent d'insécurité.

Avec 85 % du marché des systèmes d'exploitation, Windows est aujourd'hui incontournable. Quel que soit le pays, des plus petites entreprises aux multinationales, mais aussi chez les particuliers, le système d'exploitation de Microsoft est présent, dominant le marché. Succès indubitable depuis son parent MS-DOS, il a su s'imposer aussi bien au niveau des postes de travail que des serveurs, grâce à la puissance commerciale et marketing de la firme de Redmond.

Vis-à-vis de la sécurité, Windows a connu une histoire mouvementée, et une réputation d'instabilité chronique a collé aux anciens systèmes Windows 95, 98 et ME (qui n'a jamais rencontré les tristement célèbres « écrans bleus » ?). Par la suite, avec l'arrivée des systèmes

Précision

Puissance commerciale de Microsoft

La firme de Redmond a annoncé un budget de 900 millions de dollars pour la promotion de Windows Vista et Office 2007.

Windows 2000 et XP et la généralisation du noyau NT à tous les postes, de nouveaux défis pour les administrateurs sont apparus avec le développement des réseaux, l'ouverture sur Internet et plus récemment l'apparition d'infrastructures spontanées.

Les défaillances logicielles ne sont plus alors de simples nuisances pour l'utilisateur, mais des failles majeures qui profitent aux virus, chevaux de Troie, spammeurs et autres pirates informatiques. Armes de la cybercriminalité, certaines de ces menaces peuvent aussi, indirectement, conduire à d'importants dommages financiers. Ainsi, bien qu'il soit relativement difficile de les estimer, des sommes de l'ordre de plusieurs milliards de dollars ont été avancées suite à des dommages causés par des programmes malveillants comme le ver Code Red affectant le serveur web IIS de Windows NT 4.0 et 2000. Dès lors, Microsoft a pris la sécurité beaucoup plus au sérieux et a développé de nouveaux moyens de protection pour ses systèmes et applicatifs. Cependant, chacun de ces ajouts était motivé par l'apparition de codes malveillants qui exploitaient des failles du système.

C'est avec la forte croissance du développement des vers comme Blaster, Sasser ou Nimda que Microsoft s'est réellement engagé en définissant une politique de sécurité s'appliquant à tous ses produits. La sécurité a été clairement introduite dans le cycle de vie des logiciels et son suivi a été structuré avec l'apparition des bulletins mensuels. Avec Windows XP Service Pack 2 et Windows 2003, la firme de Redmond a fait un pas dans la bonne direction grâce à l'ajout de fonctionnalités intéressantes comme le pare-feu et le mécanisme de protection de la pile (réduisant les possibilités d'exploitation des débordements de tampon). Après de nombreuses vulnérabilités affectant les fonctionnalités réseau depuis 2003, Windows connaît actuellement un grand nombre de failles de sécurité sur la suite Office, dévoilées pour la plupart dès leur découverte (en *0-day*), ne laissant pas le temps à Microsoft de proposer un correctif. Comme les personnes malveillantes cherchent à atteindre le plus de machines possible, ce nombre important de failles connues est en particulier lié au fait que Windows est le plus déployé des systèmes d'exploitation.

PRÉCISION Utilisateurs des autres sytèmes

Si ce livre traite spécifiquement de Windows, il expose des principes concernant la nécessité de sauvegarder et les attaques réseau qui touchent tous les systèmes d'exploitation (Mac et Unix/Linux).

Ce tableau est pessimiste... Cependant, l'utilisateur de Windows a les moyens de rendre son système d'exploitation robuste contre les menaces existantes. Microsoft a implémenté dans la famille au noyau NT un modèle de sécurité complet, mais complexe. De nombreuses possibilités de sécurisation du système sont proposées, malheureusement elles ne sont la plupart du temps pas toutes employées efficacement. La configuration par défaut de Windows n'est pas encore un parfait exemple de sécurité (on pourra ici citer OpenBSD qui s'en approche). C'est pour-

quoi sa sécurisation nécessite un minimum de sensibilisation pour configurer correctement le système. La difficulté réside ici dans l'exhaustivité de l'application de ces mesures. En effet, si la sécurité est une chaîne, sa solidité est égale à celle du plus faible de ses maillons. Par exemple, utiliser EFS pour chiffrer ses données est une bonne pratique, mais associer cela à un mot de passe faible pour le compte Administrateur compromet grandement les chances d'obtenir un système sûr.

L'apprentissage de la sécurisation d'un système est une tâche comme les autres et, comme lorsqu'on apprend à faire du vélo, il est nécessaire de pratiquer : rien ne remplace l'expérience ! Sachez prendre du recul vis-à-vis des possibilités offertes. Persévérance, sérieux et précision permettent de protéger un système tout en conservant tout son potentiel fonctionnel.

Quelles sont les perspectives pour le système de Microsoft ? Si les annonces concernant la sécurité de Windows Vista ont été nombreuses, la réécriture de grandes parties du système soulève plusieurs questions, en particulier en ce qui concerne l'implémentation de nouvelles fonctionnalités de sécurité (seront-elles exemptes de failles ?). À l'aube de l'année 2007 et de Vista, l'utilisateur de systèmes Windows ne sait pas encore ce que lui réserve l'avenir. Voilà une raison de plus pour s'intéresser de près à la sécurité de son ordinateur.

Un dernier conseil : n'oubliez pas d'être curieux et ouvert. Toutefois, il n'est pas nécessaire d'insister sur ce point : vous vous êtes déjà emparé de ce livre !

Benjamin Arnault
Hervé Schauer Consultants

Avant-propos

Félicitations ! Si vous avez ouvert ce livre, c'est que vous faites partie des rares personnes pour qui « sécurité » ne rime pas tout de suite avec « calamité » ! Sauf, bien sûr, si vous l'avez malencontreusement fait tomber du rayon et si en le ramassant, vous l'avez ouvert fortuitement sur cette page. Si tel est votre cas, attendez encore un peu avant de le refermer : la sécurité informatique vous concerne directement. Non seulement vous allez découvrir un sujet passionnant, parfois même ludique, mais en plus, vous tenez entre vos mains le guide qui vous aidera à préserver votre poste informatique et vos données personnelles contre vous-même (la terrible négligence !) et contre les fâcheux en tous genres et en grand nombre qui se servent d'Internet pour vous causer du tort.

Tous les professionnels de la sécurité font actuellement un constat absolument effarant : l'incroyable degré de technicité des attaques informatiques – très au delà d'ailleurs du niveau de conscience de la plupart des informaticiens professionnels en la matière ! – face à l'ignorance et au mépris quasi généraux de la menace !

Aujourd'hui, voler des données personnelles, comme des identités et des numéros de cartes bancaires, voler des données professionnelles à caractère stratégique, infiltrer un poste pour le transformer – à l'insu de l'utilisateur – en un agent de piratage, espionner des faits et gestes, semer la pagaille sur une machine ou paralyser une infrastructure informatique, est devenu presque banal et parfaitement maîtrisé par les pirates avertis. Si certaines mesures de sécurité bien pensées ne sont pas mises en œuvre, le poste, qu'il soit situé chez le particulier ou au cœur d'un réseau d'entreprise, devient tôt ou tard l'agent sous contrôle d'une entité extérieure, rendant ainsi les autres composants de sécurité, comme l'antivirus et le pare-feu, à peu près inefficaces !

Bien sûr, il n'est pas très difficile de mettre en place une barrière de protection robuste pour renvoyer la très grande majorité des agresseurs dans leurs pénates. Toutefois, pour cela, il faut un guide. C'est l'ambition de cet ouvrage : vous aider à comprendre comment les attaquants s'y prennent pour infiltrer votre machine, comment vous perdez ou vous faites voler des données précieuses, afin de vous faire mieux percevoir les subtilités d'une architecture réellement sécurisée, et éviter ainsi les situations catastrophiques.

À qui s'adresse cet ouvrage ?

Cet ouvrage est consacré à la sécurité sous Windows, qui est de loin le système d'exploitation le plus déployé dans le monde. Il s'adresse à toutes les personnes qui souhaitent enfin comprendre les problèmes de sécurité de leur ordinateur, afin de mieux appréhender la façon de se protéger. Il s'agit donc essentiellement d'utilisateurs non informaticiens, mais qui abordent le sujet de la sécurité en profondeur. C'est pourquoi nous nous sommes efforcés d'employer des mots simples pour expliquer des concepts qui, parfois, se révèlent fort complexes.

Cependant, ce livre s'adresse aussi aux entreprises. En effet, situé au cœur du réseau de l'entreprise, donc au-delà du pare-feu ou du système de prévention d'intrusions, le poste utilisateur représente le moyen idéal pour infiltrer l'infrastructure informatique et véhiculer des flux malveillants, que les composants de sécurité auront de bonnes chances de considérer comme valides. Malheureusement, derrière les banales attaques informatiques et les problèmes de sécurité en général, se cachent souvent pour l'entreprise des enjeux autrement plus stratégiques, comme l'espionnage ou l'atteinte à l'intégrité ou à la disponibilité de son principal outil de travail.

Il est très préoccupant à l'heure actuelle de constater à quel point les utilisateurs, particuliers et entreprises réunis, considèrent bénéficier d'une réelle protection dès lors qu'ils ont installé sur leur site un antivirus et un pare-feu. Comme nous allons le voir au cours des chapitres qui suivent, la réalité est beaucoup plus sournoise, et nous allons tenter de la démystifier.

En nous basant sur de nombreux exemples d'attaques connues, nous tenterons de faire découvrir au lecteur l'état d'esprit qui agite le pirate, afin qu'il puisse mieux cerner les trous dans sa cuirasse. Nous expliquerons notamment comment beaucoup de barrières de protection se révèlent inefficaces, comment un virus réussit à infecter une machine, ou comment un intrus parvient à prendre le contrôle d'un ordinateur à distance, malgré la présence du pare-feu.

Nous aborderons la problématique des pare-feux du point de vue de l'assaillant, et donnerons les pistes pour construire un rempart efficace, y compris dans un environnement hostile.

L'un des points capitaux évoqués dans cet ouvrage concerne la sécurité des applications. Nous montrerons qu'aujourd'hui, et probablement aussi dans le futur, aucun pare-feu ne sait – et ne saura – filtrer de façon pertinente les couches de protocoles applicatifs, qui se révèlent de plus en plus sophistiquées et diversifiées. Nous parlerons du problème délicat des codes mobiles et expliquerons comment l'insertion d'un cheval de Troie sur le poste situé au sein de n'importe quel réseau peut se faire en toute tranquillité, et avec la bénédiction du pare-feu. Nous évoquerons bien sûr les contre-mesures efficaces pour éviter ces attaques.

Avec l'utilisation croissante de la messagerie chiffrée et des transactions électroniques, l'utilisateur est de plus en plus confronté aux problèmes techniques liés à la cryptologie et à la gestion des clés publiques et des certificats qui s'y rapportent. Malgré leur complexité et quelques petites connaissances mathématiques nécessaires, il nous a semblé important d'expliquer les principes de fonctionnement des mécanismes de chiffrement et de signature. À l'aide d'exemples concrets et très simples, nous présenterons les grands principes de la cryptologie à clés publiques, la problématique des certificats, et présenterons un aperçu des limites de la robustesse de certaines solutions employées couramment.

Enfin, à la lumière de tout ce que nous aurons expliqué concernant les mécanismes de sécurité, nous tâcherons d'éclairer le lecteur sur les évolutions proposées en la matière par Vista, la future version de Windows.

Dans cet ouvrage, nous avons donc cherché à démystifier la sécurité, à l'expliquer le mieux et le plus complètement possible. Toutefois, avant de rentrer tête baissée dans une lecture approfondie de l'ouvrage, le lecteur devrait savoir qu'en combattant sa propre négligence, il évitera une bonne partie de ses soucis. C'est pourquoi la lecture du premier chapitre, qui aborde ce point précis, est absolument fondamentale !

À RETENIR **Et les autres systèmes ?**

Cet ouvrage est consacré à la sécurité sous Windows. Cependant, sachez que les concepts et principes de sécurité décrits tout au long des chapitres restent pour la plupart valables avec Unix, Linux, ou Mac OS.

Structure de l'ouvrage

Tout d'abord, l'informatique étant avant tout une affaire de bon sens, le **chapitre 1** vous éclairera sur les conséquences de la négligence et vous invitera à acquérir quelques réflexes salutaires, notamment à sauvegarder systématiquement vos données et à savoir les restaurer en cas de problème. Quelques pistes pour réparer un système endommagé seront également proposées.

Le **chapitre 2** s'intéressera quant à lui à l'élément de base de votre architecture logicielle : le système d'exploitation. Vous y découvrirez comment configurer le système de fichiers, restreindre les accès à la machine, au registre et aux applications, partager des informations sur un réseau et chiffrer les fichiers et les dossiers les plus importants.

Lorsque l'on parle de sécurité informatique, tout le monde pense invariablement aux virus. Le **chapitre 3** détaillera ce que sont et ce que font ces codes malveillants et expliquera comment choisir, installer et utiliser un antivirus.

Les protocoles réseau sont également sources de nombreux risques. Le **chapitre 4** décrira leurs différents rôles à l'aide du modèle OSI et précisera comment les pirates s'en servent pour prendre le contrôle de votre machine. Une section sera spécialement consacrée aux réseaux Wi-Fi, points d'entrée de nombreuses attaques. Le **chapitre 5** expliquera concrètement comment sécuriser tous ces protocoles par la mise en place d'un pare-feu et la définition de règles de filtrage. La distinction sera faite entre pare-feux matériels et pare-feux applicatifs et les sondes de détection d'intrusion seront également présentées.

Le **chapitre 6** expliquera comment les certificats X.509 signés par des autorités reconnues permettent de garantir l'authenticité d'un acteur sur Internet et l'intégrité des messages qu'il vous transmet. L'accent sera mis sur l'organisation des réseaux de confiance basés sur les certificats et leurs listes de révocation. Nous appuyant sur ce chapitre-clé, nous aborderons ensuite la sécurisation des cibles privilégiées des pirates, à savoir le navigateur Internet, la messagerie électronique et les transactions Internet.

La sécurisation du navigateur, qui fera l'objet du **chapitre 7**, passe par l'authentification et/ou le filtrage des codes mobiles et des cookies, ainsi que par une gestion vigilante des certificats. Tous ces aspects seront détaillés.

Vous apprendrez ensuite au **chapitre 8** comment lutter contre les messages non sollicités (spam) et réduire les risques d'infection virale via la messagerie. Une grosse section sera par ailleurs consacrée à l'échange de courriers signés et/ou chiffrés, que ce soit par le biais des certificats ou à l'aide d'OpenPGP.

Le **chapitre 9** sera consacré aux transactions électroniques sur Internet. Tous les aspects pratiques et juridiques des connexions sécurisées seront abordés et nous expliquerons sur un cas pratique comment utiliser les certificats pour garder l'esprit tranquille au moment de divulguer des informations confidentielles sur Internet.

Le **chapitre 10** dressera une courte analyse des évolutions technologiques proposées par la future version de Windows, Vista. Nous y verrons que le noyau du système sera effectivement mieux protégé, mais aussi comment les mécanismes d'authentification et de signature risquent d'être détournés, non pas au profit d'un pirate « classique », mais de quelques majors de l'industrie du logiciel, au détriment de l'utilisateur.

Deux annexes enfin serviront de références tout au long de l'ouvrage. L'**annexe A**, tout d'abord, fournira les notions de base de cryptologie nécessaires pour une bonne compréhension des chapitres 2 et 6 à 9. L'**annexe B**, quant à elle, dressera une liste de tous les types d'attaques cités dans le texte.

Remerciements

Je souhaite tout d'abord saluer le courage de ma femme, Nathalie Barbary, qui a effectué sur cet ouvrage un travail admirable. Lisant mes premiers textes, je crois que, très vite, elle a eu pitié du lecteur. Avec une obstination qui ne l'a jamais quittée durant de longs mois, elle a relu, allégé, remanié, supprimé, reformulé mes écrits, afin de donner à ce texte une allure enfin décente. Son talent est décidément inimitable pour traduire l'Ours en français.

Je souhaite bien évidemment dire un grand merci à Laurence Richard, qui est à l'origine de ce livre, et qui a su employer des trésors de persuasion pour me convaincre de me lancer dans une telle aventure, en dépit de mon emploi du temps très chargé. Je lui dois de nombreux week-ends et de nombreuses nuits en osmose complète avec mon traitement de texte. Merci Laurence.

Un grand merci à toute l'équipe Eyrolles, et notamment mon éditrice, qui m'a fait entièrement confiance durant toute la réalisation de ce projet, et qui a été d'une patience infinie, malgré la lenteur maladive de ma production ! Merci de m'avoir laissé le temps de travailler, et d'avoir rendu cette collaboration si sympathique. Enfin, je souhaite aussi remercier Anne Bougnoux, pour la qualité de son travail de relecture et la pertinence de ses remarques. Elles ont incontestablement contribué à enrichir le contenu de cet ouvrage.

Patrick Legand
http://blog.patrick-legand.com
livre@patrick-legand.com

Table des matières

1. Votre principal ennemi : la négligence 1
Un problème malheureusement classique • 2
Causes possibles à la perte des données électroniques • 3
Arrêt brutal du système • 3
Obésité du système de fichiers • 4
Système corrompu • 5
Noms de fichiers à rallonge • 5
Bogues des logiciels • 6
Méthode simple et efficace pour lutter contre la perte des données • 7
Sauvegarder des données • 7
Activer et paramétrer l'enregistrement automatique des documents • 7
Ce qu'il faut sauvegarder • 8
Supports de sauvegarde et d'archivage • 10
Sauvegarde manuelle • 11
Sauvegarder la messagerie • 11
Sauvegarder le carnet d'adresses personnel • 13
Sauvegarder le bureau et les favoris • 14
Sauvegarde automatique • 14
Sauvegarde normale, incrémentielle, différentielle ou quotidienne • 16
Planifier une sauvegarde automatique • 17
Vérifier si une sauvegarde s'est bien passée • 19
Restaurer des données • 21
Restaurer un document de bureautique • 21
Restaurer un document supprimé par inadvertance • 21
Restaurer la messagerie • 21
Restaurer les données avec l'utilitaire de sauvegarde • 23
Quand le système ne démarre plus… • 24
Identifier la panne • 25
Se préparer à une panne du processus de démarrage • 25
Réparer un système gravement endommagé par un virus • 26
Réactiver la dernière bonne configuration connue • 26
Le mode sans échec • 27
Réparer une installation endommagée • 28
Récapitulatif : les dix commandements à l'usage de l'utilisateur • 28

2. Configurer son système de façon sécurisée ... 31
Configurer le système d'exploitation • 33
Windows, un système sécurisé ? • 33
Étapes essentielles d'une configuration sécurisée • 34
Configuration de base : formater les disques en NTFS • 34
Convertir une partition en NTFS • 35
Formater une partition en NTFS • 36
Sécuriser le Registre • 37
Risques encourus • 37
Modifier les permissions du Registre • 37
Restreindre l'accès aux applications • 39
Créer un compte restreint • 39
Choisir les programmes accessibles par le menu Démarrer • 40
Protéger l'accès à votre machine • 41
Définir un mot de passe utilisateur • 41
Fiabilité des mots de passe Windows • 42
Choisir un mot de passe robuste • 43
Protéger votre machine lorsque vous vous absentez : écran de veille et mot de passe • 43
Partager des informations sur un réseau • 45
Visualiser les partages présents sur votre ordinateur • 45
Régler les autorisations d'un partage • 46
Mettre fin au partage d'un dossier • 47
Partages « fantômes » • 47
Petites mesures anodines… • 49

Vider la liste Mes documents récents • 49
Vider les historiques et paramètres sensibles du navigateur • 51
Rendre les fichiers « invisibles » • 53
Le plus : préserver la confidentialité des fichiers par chiffrement • 54
Chiffrer une information • 54
Chiffrer des fichiers sur son ordinateur • 56
Chiffrer un fichier ou un volume sous Windows 2000/XP avec EFS (Encrypted File System) • 58
Limites des solutions natives de chiffrement fournies par Windows • 60
Alternatives possibles pour un chiffrement plus robuste • 61
Mettre en œuvre et utiliser GnuPG pour chiffrer fichiers et répertoires • 62
Récapitulatif • 67

3. Se protéger contre les virus et autres codes malveillants.....69
Connaître son ennemi • 71
Qu'est-ce qu'un virus ? • 71
Principaux types de virus • 71
Virus • 71
Vers • 72
Chevaux de Troie ou troyens • 72
Autres formes de malveillances • 73
Agissements des virus • 73
S'installer discrètement sur votre ordinateur • 73
Pervertir votre système • 74
Ouvrir toutes grandes les portes de votre PC • 74
Lancer des attaques de grande envergure • 75
Agissements des logiciels espions • 75
Infection de la machine • 79
Clic sur une pièce jointe infectée • 79
Exploitation d'une faille logicielle • 79
Image piégée • 80
Macro infectée • 80
Propagation des virus • 81
Périodicité d'apparition de nouveaux virus • 82
Auteurs des virus • 82
Comprendre le fonctionnement d'un logiciel antivirus • 84
Fichier de définitions de virus • 84
Détection des menaces • 85
Détection par reconnaissance de la signature d'un virus • 85
Détection par vérification de l'intégrité des fichiers • 85
Surveillance du comportement des processus de l'ordinateur • 86
Méthode heuristique • 86
Fonctionnalités importantes d'un logiciel antivirus • 87
Principaux antivirus du marché • 88
Choisir un antivirus • 89
F-Secure Antivirus • 90
Kaspersky Anti-Virus • 92
BitDefender • 93
McAfee VirusScan • 94
Panda Antivirus • 95
PC-cillin Internet Security • 95
Norton Antivirus • 97
AntiVir Personal Edition Classic • 99
Sophos antivirus • 100
Installer un nouveau logiciel antivirus • 101
Mise à jour et première analyse • 102
Configurer le logiciel antivirus • 107
Optimiser au quotidien la protection de votre ordinateur • 109
Procéder à une analyse complète du système • 110
Éradiquer un virus • 112
Code malveillant reconnu par l'antivirus • 112
Nettoyer une machine contaminée • 113
Votre machine ne démarre plus • 113
Votre antivirus propose une fonction de démarrage à partir du support d'installation • 113
Votre antivirus ne propose pas de fonction de démarrage à partir du support d'installation • 114
Votre machine démarre encore • 114
Mettez à jour votre antivirus • 114
C'est un nouveau virus • 114
Votre antivirus ne sait pas éradiquer le virus • 114
Vous n'avez pas d'antivirus • 115
Créer un jeu de disquettes d'urgence • 116
Mesures complémentaires à prévoir pour éviter l'infection par un virus • 117
Peut-on se passer d'un antivirus ? • 118
Expulser les logiciels espions • 118
Récapitulatif • 121

4. Les réseaux, autoroutes de l'intrusion 123
Messagerie, forums ou navigation sur Internet : les risques induits par les protocoles de transmission • 125
Rôle majeur des protocoles « IP » dans les communications sur Internet • 125
Adressage IP • 125
Transmission d'informations avec le protocole IP • 126
Réseau IP • 127

Protocole TCP • 128
Couches fonctionnelles : modèle OSI • 129
Couches 1 (physique) et 2 (liaison) • 130
Couche 3 (réseau) • 130
Couche 4 (transport) • 131
Couche 7 (application) • 131
Modèle simplifié TCP/IP • 131
Protocoles UDP et ICMP • 132
Comment l'attaquant perçoit-il un protocole de communication ? • 134
Attaques perpétrées via les protocoles réseau • 134
Derrière leur apparente innocence, les protocoles IP sont de redoutables vecteurs d'intrusion • 134
TCP, UDP ou ICMP : des protocoles bien utiles aux pirates pour analyser une installation à distance • 135
Exploitation de ICMP • 135
Ouverture de session TCP • 136
Balayage de ports • 136
Exploitation du TTL • 138
Telnet, FTP, TFTP et SNMP, facteurs de risque • 139
Telnet • 139
TFTP • 140
SNMP • 141
Les protocoles NetBIOS : une pièce maîtresse de Windows très apréciée des pirates • 141
Attaques perpétrées via les protocoles applicatifs • 143
En quoi HTTP, le protocole du Web est-il dangereux ? • 143
Encapsulation de protocole • 144
Téléchargement de codes mobiles • 144
Détournement des flux chiffrés • 145
Piratage par courrier électronique • 145
Risques liés aux applications sur Internet • 147
Applications sur Internet : des vecteurs potentiels d'intrusion • 147
Se protéger des attaques dirigées contre les applications • 149
Mention spéciale pour le Wi-Fi • 150
Risques liés au Wi-Fi • 151
Localisation des points d'accès • 152
Intrusion au cœur de votre système • 152
Mesures de protection • 153
Installez un pare-feu personnel • 153
Utilisez WPA, voire WPA2 • 153
Activez la traduction d'adresse (NAT) • 154
Masquez le SSID • 154
Ayez recours aux tunnels VPN • 154
Désactivez le Wi-Fi lorsque vous vous raccordez au réseau filaire • 155
Récapitulatif • 155

5. INSTALLER ET CONFIGURER SON PARE-FEU PERSONNEL 157
Notions générales sur les pare-feux • 159
Qu'est-ce qu'un pare-feu ? • 159
Antivirus et pare-feu • 160
Cible du pare-feu • 161
Différents types de pare-feux • 161
Pare-feux de niveau 4, dits « stateful inspection » • 162
Pare-feux applicatifs • 163
Fonctionnement d'un pare-feu • 163
Limites des pare-feux • 165
Choisir un type de pare-feu • 165
Pare-feux logiciels disponibles gratuitement ou dans le commerce • 167
Choisir un pare-feu logiciel • 168
Sécurité assurée par les fournisseurs d'accès • 168
Configurer son pare-feu personnel • 170
Installer un pare-feu logiciel • 170
Définir la politique de filtrage des flux d'information • 170
Principales règles de filtrage protocolaire proposées par les pare-feux logiciels • 172
Filtrage du trafic ICMP • 174
Politique de filtrage des protocoles du Web et de la messagerie • 175
Politique de filtrage des ports TCP et UDP • 176
Filtrer les applications avec un pare-feu • 176
Traduction d'adresses • 181
Créer ses propres règles de filtrage • 184
Réagir aux alertes affichées par les pare-feux • 187
Journaux du pare-feu • 188
Trouver le juste équilibre entre le niveau de protection délivré par un pare-feu et la facilité d'emploi • 190
Protéger l'accès aux fonctions d'administration du pare-feu • 191
Les pare-feux matériels • 191
Nécessité d'un pare-feu matériel • 191
Emplacement du pare-feu matériel • 192
Avantages d'un pare-feu matériel par rapport à un pare-feu logiciel • 192
Principaux pare-feux matériels disponibles sur le marché • 194
Cyberguard Firewall (US) • 194
Arkoon Network Security (France) • 195
Netasq (France) • 196
Check Point (Israël) • 197
Choisir un pare-feu matériel • 197

Détection et prévention d'intrusion • 199
Détecter une tentative d'intrusion • 199
Apport d'un logiciel spécifique de détection et de prévention d'intrusion en complément du pare-feu • 200
Principales sondes en matière de détection et de prévention d'intrusion • 201
Règles natives des IDPS • 201
Écrire une règle de détection d'intrusion avec Snort • 202
Type d'action • 202
Type de protocole • 202
Adresses IP, ports source et destination • 203
Opérateur de direction • 203
Options • 203
Récapitulatif • 204

6. Reconnaître l'authenticité sur Internet avec les certificats 207
Certifier une clé publique • 209
Certificat, signature et autorité de certification • 210
Déchiffrer un certificat • 211
Exemple concret • 211
Processus d'authentification d'un correspondant • 212
Principe de confiance • 214
Réseaux de confiance • 214
Infrastructures centralisées X.509 • 215
Organismes habilités à établir un certificat • 215
Autorité de certification racine • 215
Chaîne de certification • 216
Modèle réel composé de nombreuses autorités de certification • 218
Listes de révocation • 220
Récapitulatif • 220

7. Configurer son navigateur Internet de façon sécurisée 223
Un pare-feu et un antivirus ne sont pas suffisants • 224
Risques liés aux navigateurs • 225
Codes mobiles présents dans les pages web • 225
Contrôles ActiveX • 226
Protection par Authenticode • 228
Contrôle ActiveX reconnu sûr pour l'écriture de scripts • 231
Les applets Java sont-elles sûres ? • 231
Autres formes de risques liés aux contenus exécutables • 233
Modules externes ou plug-ins • 234
Scripts • 234
Cookies • 235
Fonctions de sécurité offertes par les navigateurs • 236
Sécuriser Internet Explorer • 237
Zones de sécurité prédéfinies • 238
Paramètres de sécurité affectés à chaque zone • 240
Affecter un site web à une zone de sécurité • 244
Paramètres de « confidentialité » • 244
Sécuriser Netscape Navigator • 246
Préférences concernant les cookies • 246
Préférences concernant les scripts et plug-ins • 248
Préférences liées à l'interprétation des pages web • 248
Préférences concernant les scripts • 249
Sécuriser Mozilla Firefox • 250
La gestion des cookies • 251
Gestion des mots de passe de sites web • 252
Paramètres de sécurité liés aux fonctionnalités web • 252
Gérer les certificats • 254
Afficher la liste des certificats stockés dans votre navigateur • 255
Sous Internet Explorer • 255
Sous Netscape • 255
Sous Firefox • 256
Modifier la liste des certificats présents par défaut dans le navigateur • 257
Attitude à adopter lorsqu'un certificat ne peut être vérifié • 258
Déterminer si le certificat d'une nouvelle autorité de certification est fiable • 260
Gérer les listes de révocation • 262
Sous Internet Explorer • 262
Sous Netscape Navigator • 262
Sous Firefox • 266
Récapitulatif • 266

8. Sécuriser son courrier électronique 269
Lutter contre les messages non sollicités • 270
Le spam • 270
Divulgation de votre adresse de courrier électronique • 272
Protéger son adresse électronique contre le spam : quelques mesures simples • 272
Un compte public et un compte privé • 272
Une adresse résistant au spam • 274
Un domaine peu usité • 274
Plutôt l'image que le texte • 274
Le phishing • 276
Éviter de se faire piéger avec le phishing • 277
Filtrer les messages indésirables • 277

Mode opératoire d'un filtre antispam • 277
Services proposés par les clients de messagerie pour filtrer les spams • 278
Bloquez ou déplacez les indésirables • 278
Règles de filtrage des messages • 279
Installer un filtre antispam additionnel • 281
Principaux filtres antispam disponibles actuellement • 281
Configurer un filtre antispam • 281
Une solution simple pour une protection efficace • 284
Réduire les risques d'infection virale ou de pénétration via la messagerie • 284
Optimiser la configuration de son antivirus vis-à-vis de la messagerie électronique • 285
Bloquer images et contenus externes dans les messages HTML • 285
Préserver la confidentialité et garantir l'authenticité d'un message électronique • 286
Principes de fonctionnement des échanges sécurisés • 287
Chiffrement d'un message • 287
Signature d'un message • 289
Chiffrer et signer à l'aide des certificats • 291
Échanger des messages signés et/ou chiffrés avec un correspondant • 291
Obtenir un certificat et l'intégrer dans votre client de messagerie • 292
Diffuser votre certificat à vos interlocuteurs • 295
Récupérer et intégrer le certificat d'un correspondant • 296
Signer ou chiffrer un message • 298
Lire un message chiffré par votre correspondant • 300
Vérifier la signature et donc l'authenticité d'un message • 300
Authentification de l'expéditeur via un certificat • 302
Niveau de protection réel délivré • 304
Problème de la fiabilité des clés secrètes et privées • 305
Renforcer la sécurité des échanges par voie de messagerie électronique • 307
Valeur juridique de la signature d'un message électronique • 308
Sécuriser son courrier sous Thunderbird avec OpenPGP • 308
Modèle de confiance d'OpenPGP • 308
Réseau de confiance • 308
Niveaux de confiance • 310
Installer les extensions de sécurité • 313
Configurer Enigmail • 314
Diffuser votre clé publique OpenPGP • 317
Obtenir la clé OpenPGP d'un correspondant • 318
Signer ou chiffrer un message avec OpenPGP • 318
Récapitulatif • 320

9. Transactions électroniques et paiement sur Internet 323
Acheter et payer sur Internet • 325
Principes mis en œuvre au cours d'une transaction électronique sécurisée • 325
Déroulement d'une transaction électronique sécurisée • 326
Niveau de sécurité réel offert au consommateur lors d'une transaction SSL • 329
Moyens mis à votre disposition pour rendre vos transactions plus sûres • 331
Vigilance • 331
Législation française favorable au consommateur en ligne • 331
Modèle de transaction avec tiers • 332
Étude de cas : la sécurité dans le cadre de la déclaration des revenus sur Internet • 334
Obtenir votre certificat • 335
Vérifier le certificat • 336
Importer les certificats des AC signataires • 339
Utiliser les services sécurisés • 340
Récapitulatif • 342

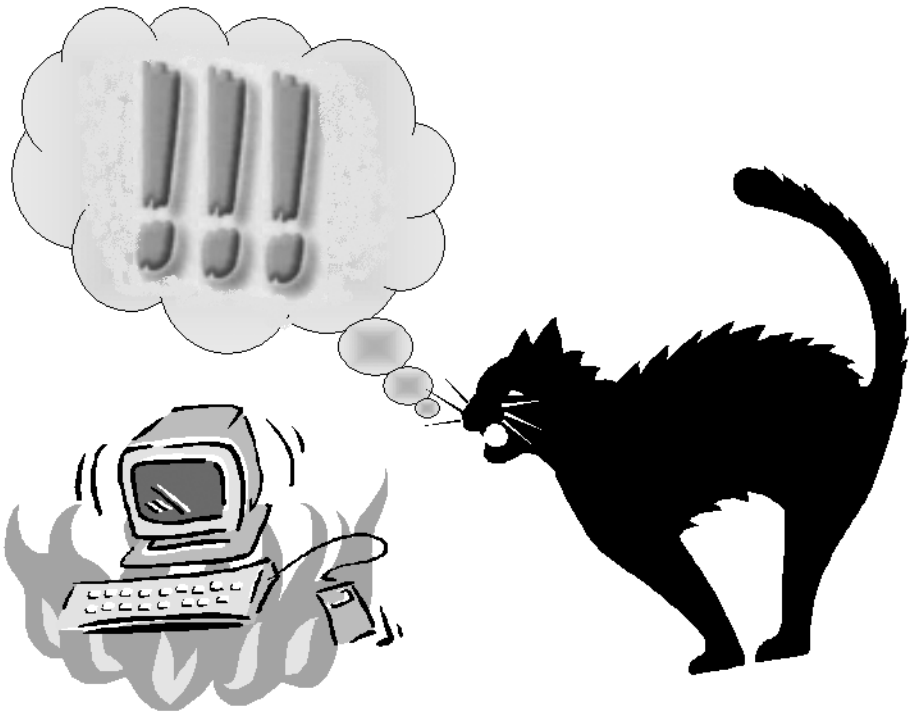
10. Et Windows Vista ? 345
Conséquences du contrôle d'accès généralisé aux contenus • 346
Signature des pilotes et des exécutables • 348
Dépendance vis-à-vis du fournisseur • 349
Dépendance technologique et absence d'interopérabilité • 350
TCPA, Palladium et NGSCB • 350
La sécurité, je fais tout seul • 353
Améliorations de la sécurité du système • 354
Vista, forteresse imprenable ? • 356
Faut-il migrer ? • 356

A. Notions de cryptologie 357

B. Récapitulatif des principaux risques encourus ... 377

Index 395

chapitre 1



Votre principal ennemi : la négligence

Combien d'entre nous ne se sont décidés à sauvegarder leurs données importantes qu'après avoir perdu bêtement de nombreuses heures de travail ?

SOMMAIRE

- Perdre ses données par négligence
- Sauvegarder son travail
- Restaurer des fichiers
- Vérifier et réparer le système d'exploitation

MOTS-CLÉS

- Sauvegarder
- Restaurer un fichier
- Restaurer le système

Un problème malheureusement classique

Imaginez : vous êtes invité chez un brillant écrivain et attendez pour passer à table que l'homme de lettres en pleine inspiration achève de rédiger. Hélas ! c'est en état de choc qu'il arrive enfin : sa machine vient de « planter » et tout ce qu'il a écrit depuis le matin s'est semble-t-il volatilisé. À la question « avez-vous pensé à enregistrer régulièrement votre travail ? », vous lisez dans son regard étonné et désemparé que cette notion lui est complètement étrangère. Si l'informatique était née plus tôt, combien de trésors littéraires auraient ainsi été sacrifiés sur l'autel de la négligence ?

Autre scenario : un de vos clients vous appelle, catastrophé. En train d'éditer sur sa clé USB une base Access qu'il développait tranquillement depuis cinq ans, il arrache sa clé dans la précipitation, éteint sa machine et, conscient qu'il n'a peut-être pas fait les choses dans le bon ordre, rallume son PC, branche sa clé et… constate que le fichier a disparu : il n'est ni sur la clé, ni sur le PC. Access n'a pas pu refermer ce fichier proprement et ne le reconnaît plus ! À la première question : « Disposez-vous d'une sauvegarde récente de ce fichier ? », il vous répond, dépité, que la seule sauvegarde exploitable date de plusieurs mois, et encore, il ne sait plus très bien où elle se trouve.

Encore un exemple de négligence… qui apparaît ici à deux niveaux. Tout d'abord, une clé USB n'est pas un support de travail, mais de stockage. Ensuite (surtout dans le cas d'une base de données), il faut toujours conserver plusieurs versions d'un travail sur des supports faciles à retrouver, et à partir desquels il faut être sûr de pouvoir récupérer les fichiers.

À la lumière de ces deux exemples, vous serez sans doute convaincu de la très grande importance des notions de sauvegarde et de restauration. Lorsqu'on parle de sécurité informatique, ces sujets sont à aborder en priorité. Vous avez tout à fait le droit de penser que la sécurité informatique est un sujet qui vous ennuie profondément, mais vous devez être conscient que l'informatique n'est pas un outil fiable et que vous pouvez perdre des quantités de données précieuses du jour au lendemain. Voici donc le message le plus important de ce livre : même si vous choisissez d'ignorer la sécurité de votre PC, prenez la décision, dès aujourd'hui, de ne plus jamais faire l'impasse sur les sauvegardes.

Causes possibles à la perte des données électroniques

Avant d'aborder la sauvegarde, essayons d'identifier les erreurs commises le plus souvent par les utilisateurs et qui peuvent conduire bêtement à la perte d'informations. Savoir éviter ces erreurs et connaître les gestes qui sauvent vous rendront certainement beaucoup plus pacifiques avec votre ordinateur.

Sachez tout d'abord qu'une information qui n'est pas dupliquée disparaîtra tôt ou tard, d'une façon ou d'une autre. C'est inéluctable, vous n'y pouvez rien. Donc, avant toute chose, interrompez tout de suite la lecture de ce livre, et allez dupliquer toutes vos données précieuses. Nous nous reverrons après.

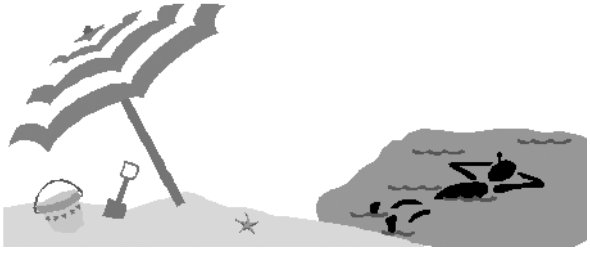


Figure 1–1
L'auteur fait une pause.

Arrêt brutal du système

Au cours de vos manipulations quotidiennes, ayez toujours à l'esprit que l'informatique est un outil fragile : il faut éviter de le malmener systématiquement. N'oubliez pas qu'un « simple » traitement de texte ou une messagerie met en œuvre de nombreux composants matériels et des centaines de milliers de lignes de code. Même si ces outils savent aller assez loin dans la gestion des situations extrêmes, comme des arrêts brutaux, on ne peut pas leur demander l'impossible.

Une application ou un système d'exploitation a besoin de refermer des fichiers, de sauvegarder des données stockées en mémoire vive, ou d'assurer la cohérence de l'ensemble avant de s'arrêter. À la suite d'un arrêt brutal, qui peut prédire l'état dans lequel se trouve le système ? Lorsque ce dernier redémarre, il doit gérer une situation incohérente. Or, il est impossible de demander aux concepteurs de programmes aussi complexes de savoir gérer l'imprévisible en toute circonstance, et sans erreur. Pour cette raison, il ne faut **jamais** interrompre un processus ou une application en cours d'exécution, ni arrêter brutalement un système d'exploitation. S'il le faut, n'hésitez pas à perdre quelques minutes pour donner une chance à un processus, bloqué en apparence, de se terminer

proprement. Évitant peut-être un « plantage » grave, vous gagnerez un temps précieux et éviterez de perdre des informations.

Si vraiment le processus semble irrémédiablement « dans les choux », vous n'avez peut-être plus d'autre choix que de tenter l'arrêt brutal. Attention toutefois ! N'en abusez pas. Dans sa grande bienveillance, Windows déploie des trésors d'artifices pour retomber sur ses pieds après un arrêt brutal et vous redonner ainsi la main sur la machine, mais ne tentez pas le diable : si vous adoptez régulièrement cette manière de procéder, vous finirez par endommager votre application ou votre système, et, à terme, vous perdrez à coup sûr du temps et des données importantes.

Astuce **Fermeture incomplète de Windows**

Il arrive, et c'est là l'un des nombreux mystères de l'informatique, que le processus de fermeture de Windows reste indéfiniment dans un état proche de l'arrêt complet, sans toutefois arriver à son terme. Essayez une légère impulsion sur le bouton marche/arrêt de la machine : cela redonne une petite claque au processus, qui s'achève proprement quelques secondes après.

Conseil **Allégez vos profils itinérants**

Si vous travaillez en réseau et si vous disposez d'un profil itinérant, lorsque vous arrêtez l'ordinateur, Windows synchronise le profil itinérant, stocké sur le serveur, avec la copie locale de ce profil, située sur votre poste. Si vous avez la malencontreuse idée de déposer sur votre bureau tous vos documents en cours, votre profil peut devenir très lourd (nous avons déjà vu des profils supérieurs à 1 Go !). Dans ce cas, l'opération de synchronisation – et par conséquent de fermeture – devient très longue, pour peu que votre réseau local 10/100 Mb/s fonctionne réellement à 10 Mb/s (câbles réseau de mauvaise qualité) et que vous subissiez de surcroît une attaque par déni de service (ce que nous avons déjà vu aussi !). Pour éviter ce problème, et donc la tentation de couper sauvagement le courant pour en finir, allégez plutôt votre profil : ne déposez jamais vos documents sur le bureau, mais seulement les raccourcis !

Obésité du système de fichiers

Il faut penser régulièrement à faire le ménage. Même si l'espace de stockage d'une machine dépasse aujourd'hui plusieurs dizaines de Go, les disques se remplissent à une vitesse effrayante. Certains utilisateurs atteignent sans ambages des taux de remplissage supérieurs à 80 %. Si c'est votre cas, vous flirtez dangereusement avec l'incident car un disque trop plein gêne, voire compromet sérieusement le bon fonctionnement de l'ordinateur ; lorsque le système se met à mal fonctionner et qu'il met trois heures à ouvrir un fichier, vous jurez, mais un peu tard, qu'on ne vous y prendra plus.

Conseil
Archivez régulièrement vos messages

La boîte de réception des courriers électroniques doit garder une taille raisonnable pour rester utilisable.

De même, un chef d'entreprise vous appelle un jour, catastrophé : il n'arrive plus à accéder à sa messagerie, outil ô combien stratégique de son activité bien remplie. La raison ? Fichier corrompu, selon le client de messagerie. Et pour cause ! Sa boîte de réception Outlook atteint les 2,3 Go alors que Microsoft indique clairement que ce fichier ne doit pas dépasser les 2 Go (ce qui est déjà énorme !). Les boîtes de réception ont une fâcheuse tendance à grossir, et il est impératif d'archiver régulière-

ment vos messages ; soyez raisonnable, il faut plusieurs années pour atteindre 2Go, alors archivez au moins une fois l'an !

Plus le temps passe, plus on installe d'applications sur sa machine et, en conséquence, plus les risques de conflits entre elles augmente ; pensez à désinstaller les applications dont vous ne vous servez plus. Archivez, faites maigrir, déblayez, bazardez, allégez, et vous verrez comme votre poste se portera mieux.

Système corrompu

En informatique, il faut proscrire la négligence. Si votre machine affiche systématiquement un message d'erreur (au démarrage par exemple), cela doit vous alerter. Même si ce message est indigeste, documentez-vous, demandez à un ami qui connaît l'informatique, ou faites appel à un administrateur, mais ne restez pas sans réagir. Si c'est un message système (on reconnaît facilement un tel message : il est encore plus incompréhensible que les autres), il se peut que la configuration de la machine ait été altérée, symptôme d'une intrusion (presque) réussie, que le système ait été endommagé, ou que vous ayiez été contaminé par un cheval de Troie (nous en reparlerons au chapitre 3). Faites disparaître le problème, sinon vous risquez de mauvaises surprises.

Noms de fichiers à rallonge

Lorsque vous enregistrez pour la première fois un document Word que vous venez de créer, ce logiciel de traitement de texte vous propose un titre par défaut : la première phrase de votre document. Si vous ne prenez pas la peine de définir vous-même un titre raisonnable, vous risquez d'avoir des fichiers dotés d'un nom à rallonge, comme « *Vous trouverez en annexe le rapport suite à notre discussion avec le Comité Consultatif des Problématiques Possibles au Ministère ce jeudi matin.doc* ». La figure 1-2 en présente un exemple flagrant, dû au simple enregistrement d'une page HTML.

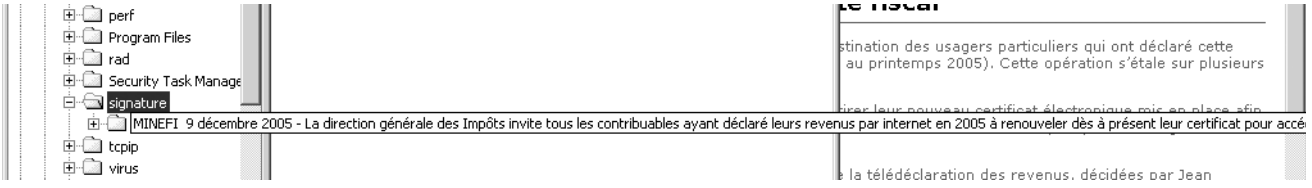


Figure 1–2 Attention aux noms à rallonge

Pour peu que ces fichiers soient stockés au fin fond d'une arborescence dont les répertoires ont eux aussi des noms interminables, Windows se révèlera incapable de les copier sur un autre support, donc de les sauvegarder. Dans sa grande bienveillance, Windows peut vous alerter en cas d'erreur (figure 1-3), mais ce ne sera pas toujours le cas.

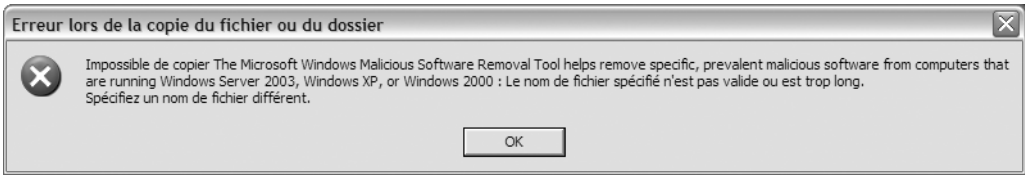


Figure 1–3
Windows ne sait pas bien gérer les fichiers dont les noms sont trop longs.

Bogues des logiciels

Faites toujours preuve de lucidité. Les outils informatiques ne viennent jamais sans leur ration de bogues et sont susceptibles d'engendrer des erreurs (les développeurs professionnels disent souvent que le système tombe en marche !). Aussi, lorsque vous réalisez une tâche mettant en jeu des données vitales, assurez-vous toujours de son bon déroulement. Par exemple :

- Lorsque vous ouvrez ou créez un document, commencez donc par l'enregistrer, et enregistrez-le régulièrement. Il arrive parfois que la fonction d'enregistrement ne fonctionne plus normalement… autant ne pas s'en apercevoir en fin de journée, alors que tout le travail effectué va être irrémédiablement perdu !
- Lorsque vous archivez, ou lorsque vous transférez en masse des fichiers à travers un réseau, inspectez le contenu de l'arborescence cible après coup. Conservez l'arborescence d'origine quelque temps, on ne sait jamais. Ne croyez jamais que l'informatique viendra pallier vos propres erreurs.
- Ne forcez pas les logiciels à effectuer des tâches « tordues ». Plus vous cherchez la complexité, plus vous risquez d'exécuter des parties du logiciel qui n'auront pas été suffisamment testées ou de mettre celui-ci face à des situations qu'il ne sait pas bien gérer. N'oubliez pas que l'informatique est un outil d'une puissance colossale destiné à accomplir des tâches simples.

Il ne s'agit là que de quelques recommandations simples parmi des dizaines d'autres. Nous ne pouvons pas en énoncer la liste exhaustive dans cet ouvrage. Restez toujours vigilant, méfiez-vous de l'informatique qui peut vous jouer des tours, et ne faites confiance qu'à vous-même.

Méthode simple et efficace pour lutter contre la perte des données

Il existe un moyen simple et très efficace de se protéger contre la perte des données : la redondance. Il faut conserver plusieurs copies des données importantes. La sauvegarde (multiple) est la seule méthode fiable qui vous préserve à coup sûr de la perte malencontreuse d'informations.

- Sauvegardez vos données vitales sur un support amovible : sur CD-Rom, réinscriptible ou non, ou sur bande. Vous pouvez aussi investir dans un disque dur externe sur lequel vous pourrez très facilement obtenir une copie très complète de vos données.
- Dans votre profession, si votre administrateur vous a alloué un espace de travail sur le serveur de l'entreprise, n'hésitez pas non plus à conserver une image de vos données vitales sur le disque local de votre ordinateur.
- Aujourd'hui, tout le monde possède sa propre clé USB. Utilisez cet espace pour stocker les données les plus récentes (entre deux sauvegardes). Si vous vous déplacez fréquemment avec votre ordinateur portable, ne rangez pas la clé USB dans la housse de l'ordinateur ! Mettez-la dans votre poche.
- Archivez les données sur un support non réinscriptible (CD-Rom par exemple). Fabriquez deux jeux d'archives que vous ne stockerez pas physiquement au même endroit.

Sauvegarder des données

Activer et paramétrer l'enregistrement automatique des documents

Si vous utilisez Microsoft Office, vous pouvez configurer Word, Excel et Powerpoint afin que ceux-ci enregistrent régulièrement une copie de sauvegarde des documents en cours d'édition. Dans Word par exemple, déroulez le menu *Outils*, sélectionnez *Options*, puis cliquez sur l'onglet *Enregistrement* (figure 1-4).

En cas de panne secteur ou d'extinction intempestive de votre machine, vous pourrez restaurer votre travail. Pour cela, cochez la case *Enregistrer les infos de récupération automatique toutes les :* et conservez la valeur par défaut (10 minutes) ou choisissez une valeur à votre convenance.

Alternative Open Source OpenOffice.org

La suite OpenOffice.org propose elle aussi ce mode de sauvegarde et de récupération automatique des données : menu *Outils>Options>Chargement/enregistrement>Général*, section *Enregistrement*.

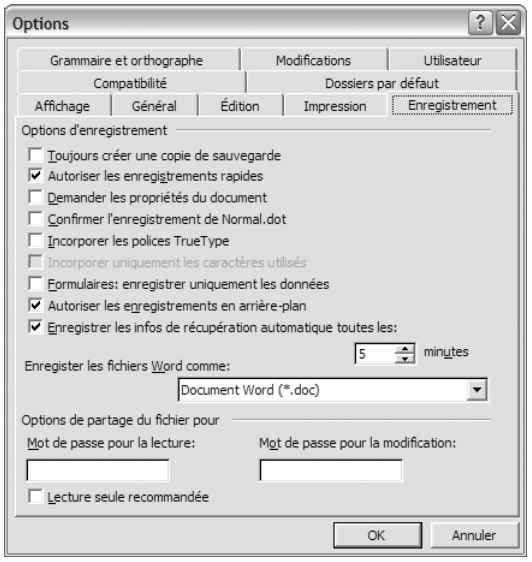


Figure 1–4
Paramétrer les options d'enregistrement automatique

Ce qu'il faut sauvegarder

En premier lieu, il faut bien entendu sauvegarder vos données personnelles (documents, photos, etc.). Étant donné que vous gérez le plus souvent vous-même l'emplacement de ces fichiers, il est rare que vous oubliiez ces éléments.

Il existe en revanche un élément essentiel auquel, paradoxalement, vous ne pensez pas toujours : la messagerie. Après un incident, un sinistre ou un reformatage du disque, beaucoup de personnes – y compris des informaticiens professionnels ! – prennent conscience de la catastrophe lorsqu'ils s'aperçoivent qu'ils ont tout bonnement oublié de sauvegarder leur messagerie. Il est vrai que cette opération ne coule pas de source et que, souvent, vous ne savez pas très bien où elle se trouve et quels fichiers il faut sauvegarder. Nous verrons plus loin comment procéder.

Parmi les données utilisateur à sauvegarder, n'oubliez pas non plus tous vos mots de passe (notamment ceux que l'on ne saisit jamais, comme le mot de passe permettant d'accéder aux ressources réseau), le ou les numéros de téléphone de votre fournisseur d'accès, vos favoris et votre bureau.

À la rigueur, il peut être utile de sauvegarder les paramètres complets de votre système ; cela vous permettra de récupérer plus rapidement votre configuration opérationnelle en cas de panne majeure et de réinstallation du système d'exploitation. Dans le menu *Démarrer*, choisissez *Tous les programmes*, sélectionnez *Accessoires*, puis *Outils système* et cliquez sur *Informations système*. Dans le menu *Fichier*, cliquez sur *Enregistrer* (figure 1-5).

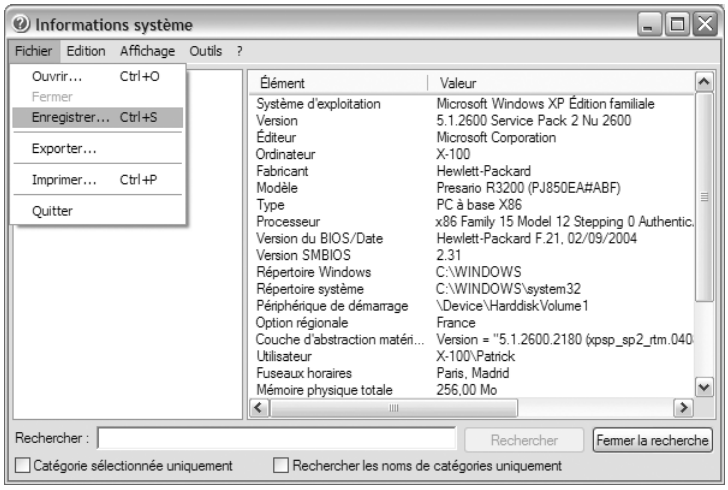


Figure 1–5
Enregistrez vos paramètres système.

En revanche, il est capital que vous gardiez sous le coude les paramètres de votre compte de messagerie (ils apparaissent dans les propriétés du compte, voir figure 1-6) :

- le nom du compte (par exemple David Vincent) ;
- l'adresse de messagerie (par exemple david.vincent@mars-telecom.fr) ;
- le mot de passe ;
- l'adresse des serveurs POP3, SMTP, IMAP4.

Ces paramètres ne nécessitent nullement une sauvegarde électronique. Contentez-vous de les noter sur un papier que vous rangerez soigneusement. Avec Outlook Express par exemple, vous trouverez ces paramètres dans le menu *Outils*, sous-menu *Comptes*, article *Propriétés*.

ALTERNATIVE OPEN SOURCE Thunderbird

Si vous utilisez sous Windows le logiciel Open Source Mozilla Thunderbird, les paramètres de courrier se trouvent dans le menu *Outils*, sous-menu *Paramètres des comptes*, articles *Paramètres serveur* et *Serveur sortant (SMTP)*.

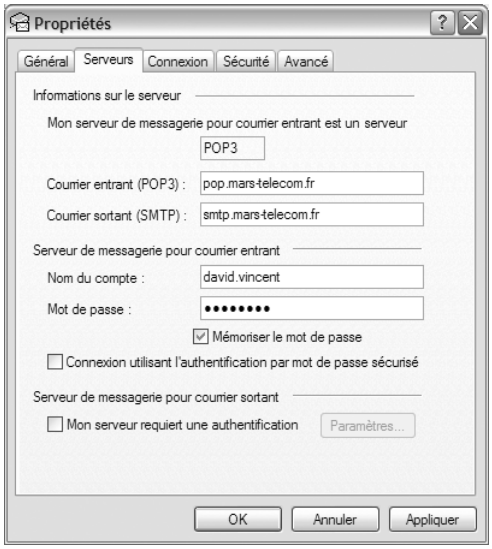


Figure 1–6
Paramètres de votre compte de messagerie

TECHNOLOGIE **La disquette, un support suranné ?**

Même si ce type de support revêt de nos jours un caractère un peu désuet, les disquettes restent toujours très fiables pour sauvegarder les fichiers de taille modeste. Nombreux sont les utilisateurs qui manipulent toujours des petits fichiers (par exemple, les fichiers Excel qui servent à calculer vos impôts sont beaucoup plus légers que l'impôt lui-même !). Certaines petites entreprises utilisent même depuis des années la disquette comme principal moyen de sauvegarde, sans que cela leur ait porté préjudice.

Supports de sauvegarde et d'archivage

Il faut bien reconnaître qu'avec le multimédia, l'unité de volume de la donnée a « explosé ». Étant donné que les machines récentes sont toutes livrées avec, au minimum, un graveur de CD-Rom intégré (voire un graveur de DVD), on peut considérer que le CD-Rom est actuellement le support le mieux adapté aux besoins des particuliers. Sauvegardez sur disques réinscriptibles toutes vos données « en cours », susceptibles d'être modifiées, et archivez définitivement sur CD-Rom non réinscriptibles les données figées. Si ces données sont vitales, créez deux jeux de sauvegardes ou d'archives, que vous entreposerez physiquement dans deux lieux différents.

La clé USB représente aussi un espace de stockage intéressant. Toutefois, ne la considérez pas comme un support de sauvegarde à part entière : elle est trop volatile pour constituer une référence stable et peut être facilement égarée. En revanche, vous pouvez très bien vous en servir comme élément de sauvegarde temporaire pour stocker les fichiers modifiés depuis la dernière sauvegarde sur CD-Rom.

En raison de ses capacités de stockage élevées, de sa rapidité d'accès et de son faible coût, le disque dur externe représente une autre alternative au stockage des sauvegardes. Il est particulièrement indiqué lorsqu'il s'agit de sauvegarder plusieurs dizaines de Go. Le disque dur externe vous sauvera la mise en cas de crash (annoncé !) de votre disque interne ou de la machine. Cependant, n'oubliez pas qu'un disque externe peut lui-même subir des défaillances graves et, tant qu'il est relié à votre machine, ne vous sera d'aucun secours en cas de sinistre, tel qu'un incendie ou une inondation. Si vous utilisez un disque externe, veillez tout de même à sauvegarder vos données importantes sur CD-Rom.

Pour les entreprises, même modestes, le meilleur support est incontestablement la bande magnétique. Dotée de grandes capacités (plusieurs dizaines, voire centaines de Go), elle permet de sauvegarder quotidiennement l'intégralité des données stockées sur votre serveur, limitant ainsi considérablement les risques de perte. Si la mise en route d'un système de sauvegarde sur bandes nécessite peut-être l'intervention d'un spécialiste, une fois que la procédure fonctionne, toutes les sauvegardes, incrémentielles ou totales, se dérouleront automatiquement et indéfiniment, sans que vous ayiez à faire quoi que ce soit. Votre seule astreinte sera d'introduire une nouvelle bande dans le lecteur, une fois la sauvegarde précédente terminée. Étant donnée la taille réduite d'une bande, vous pouvez très facilement la loger dans votre serviette afin de l'entreposer dans un espace différent de celui du lieu de travail. Par ailleurs, son faible coût vous incitera à vous approvisionner en nombre suffisant, afin de pouvoir conserver les sauvegardes quotidiennes pendant plusieurs semaines et les sauvegardes mensuelles pendant plusieurs mois.

Sauvegarde manuelle

Réaliser une sauvegarde manuelle sur CD-Rom est très simple. Ouvrez l'explorateur Windows, sélectionnez les répertoires à sauvegarder et faites-les glisser sur le *Lecteur DVD/CD-RW (D:)* (la lettre du lecteur peut varier suivant votre installation). Veillez toutefois à ce que le volume total de ces fichiers ne dépasse pas la capacité d'un CD-Rom (de l'ordre de 700 Mo). Windows vous affiche lui-même la marche à suivre (figure 1-7).

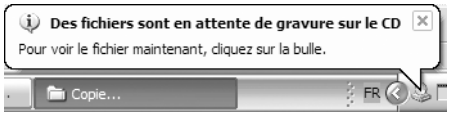


Figure 1–7
Pour graver le CD-Rom, cliquez sur la bulle et suivez les instructions.

Une autre possibilité consiste à cliquer sur le lecteur DVD/CD-RW, puis sur *Graver ces fichiers sur le CD-ROM* (figure 1-8).

Figure 1–8
Cliquez sur Graver ces fichiers sur le CD-Rom.

Sauvegarder la messagerie

Il suffit de sauvegarder les fichiers qui contiennent la messagerie, exactement comme n'importe quels autres fichiers. La seule différence est qu'ils ne sont pas gérés par vous, mais par votre application. Le problème est donc de savoir les localiser.

Si vous utilisez Outlook, tous vos messages, ainsi que vos contacts, tâches et journaux, se trouvent regroupés dans un unique fichier .pst (le plus souvent nommé outlook.pst), situé par défaut dans le répertoire `C:\Documents and Settings\nom_utilisateur\Local Settings\Application Data\Microsoft\Outlook`. Pour accéder à ce répertoire, vous serez obligé d'activer l'affichage des fichiers et dossiers cachés : à partir de l'explorateur Windows, dans le menu *Outils*, sélectionnez *Options des dossiers*,

CONSEIL Avant tout, sachez retrouver l'emplacement physique de vos fichiers de données

La sauvegarde en elle-même n'est pas une opération délicate. Ce qui pose problème, c'est de savoir localiser les répertoires et fichiers à l'intérieur desquels les applications stockent vos données, et qui constituent les éléments à sauvegarder. Il n'existe malheureusement aucune règle générale permettant de connaître l'emplacement physique de tels éléments : chaque application gère les données selon son propre modèle. Suivez donc attentivement ce conseil : avant de définir votre politique de sauvegarde, acceptez de passer du temps à bien comprendre comment vos applications gèrent et stockent les données que vous leur confiez. Souvent, un rapide coup d'œil à l'aide en ligne ou un clic droit sur une donnée (une photo, un fichier musical...) vous donne la réponse.

cliquez sur l'onglet *Affichage*, puis choisissez *Afficher les fichiers et dossiers cachés*. Si votre courrier est stocké ailleurs, vous visualisez l'emplacement exact du fichier en cliquant droit sur votre boîte de messagerie puis sur *Propriétés* (figure 1-9).

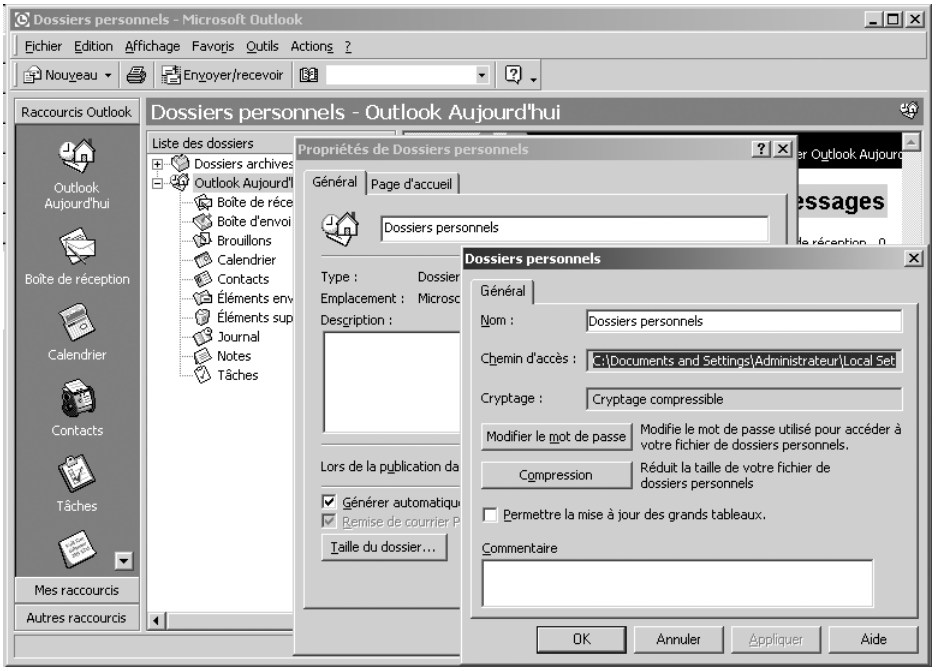


Figure 1–9
Localisation des fichiers Outlook à sauvegarder

Avec Outlook Express en revanche, chaque dossier de courrier électronique fait l'objet d'un fichier `.dbx` à part entière. Pour localiser ces fichiers, à partir de la fenêtre *Dossiers*, cliquez droit sur le dossier correspondant (par exemple, sur *Boîte de réception*), et choisissez *Propriétés*. Sous l'intitulé *Ce dossier est stocké dans le fichier suivant*, vous verrez apparaître le chemin d'accès, qui peut ressembler à :

```
C:\Documents and Settings\Patrick\Local Settings\Application
Data\Identities\{460DE967-20DE-4CA5-A36D-CC2FBAA42CAC}\
Microsoft\Outlook Express\Boîte de réception.dbx
```

Convivial, n'est-ce pas ?

Si vous allez dans le répertoire indiqué, vous visualiserez les fichiers `.dbx` correspondant à vos dossiers de courrier (figure 1-10).

Pour sauvegarder ces fichiers, **fermez d'abord votre application de messagerie**. Suivez ensuite la procédure exposée précédemment.

ALTERNATIVE OPEN SOURCE **Thunderbird**

Thunderbird stocke toutes vos informations (messages, filtres, adresses, paramètres des comptes...) dans un seul dossier, créé par défaut à l'emplacement suivant :

`c:\Documents and Settings\`
`nom_utilisateur``\Application Data\`
`Thunderbird\Profiles\`
`XXXXXXXX``.default`

C'est ce dossier que vous devez sauvegarder.

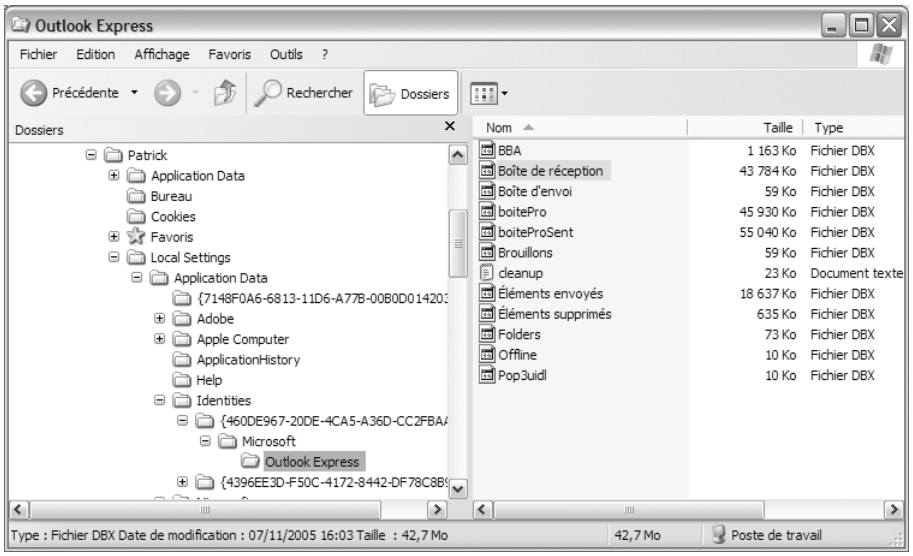


Figure 1–10
Fichiers Outlook Express à sauvegarder

Sauvegarder le carnet d'adresses personnel

Avec Outlook, le carnet d'adresses est inclus dans le fichier de vos messages (`outlook.pst`). Si ce fichier est sauvegardé, vos contacts le seront donc aussi.

Vous avez également la possibilité d'exporter votre carnet d'adresses. Avec Outlook Express, dans le menu *Fichier*, choisissez *Exporter*, puis sélectionnez *Carnet d'adresses* (figure 1-11)

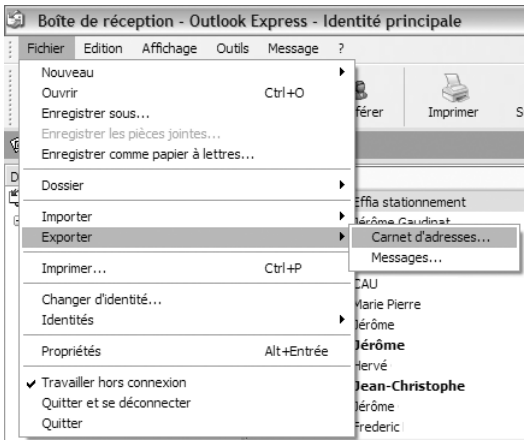


Figure 1–11
Exportez votre carnet d'adresses avec Outlook Express.

Suivez les instructions et vous obtiendrez un nouveau fichier `.WAB` (par exemple `carnetAdresses.WAB`) contenant la liste de vos contacts. Vous pourrez le sauvegarder au même titre que tout autre fichier.

Alternative Open Source **Thunderbird**

La procédure est exactement la même avec Thunderbird : ouvrez votre carnet d'adresses, sélectionnez *Outils*, puis *Exporter*. Spécifiez ensuite le nom du fichier.

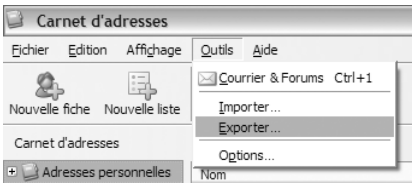


Figure 1–12 Exportez votre carnet d'adresses avec Thunderbird.

Sauvegarder le bureau et les favoris

Sous Windows 2000 ou XP, les éléments du bureau sont gérés par le système et situés à l'intérieur des répertoires `C:\Documents and Settings\`*`nom utilisateur`*`\bureau` et `C:\Documents and Settings\All Users\bureau`.

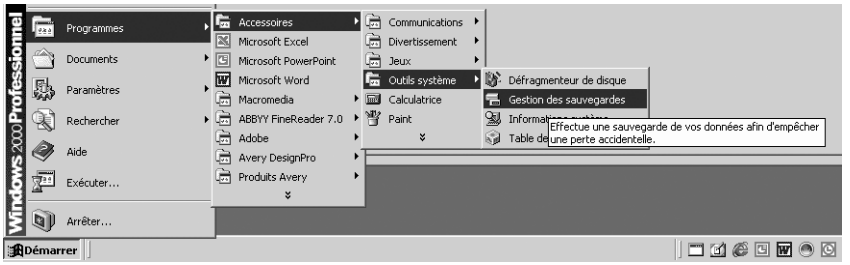
Quant aux favoris d'Internet Explorer, vous les trouverez dans le répertoire `C:\Documents and Settings\`*`nom utilisateur`*`\favoris`.

Pour sauvegarder bureau et favoris, il vous suffit de sauvegarder les fichiers ou les répertoires correspondants.

Sauvegarde automatique

Si vous disposez de supports suffisamment volumineux pour contenir l'intégralité des informations à sauvegarder (un disque externe, une bande), vous vous simplifierez considérablement la vie en rendant cette procédure automatique.

Windows XP Pro est livré avec un programme de Gestion des sauvegardes, que vous trouvez dans la section *Outils système* du dossier *Accessoires*.



Ouvrez cette application. L'assistant vous demande si vous souhaitez effectuer une *Sauvegarde* ou une *Restauration*. Choisissez la sauvegarde.

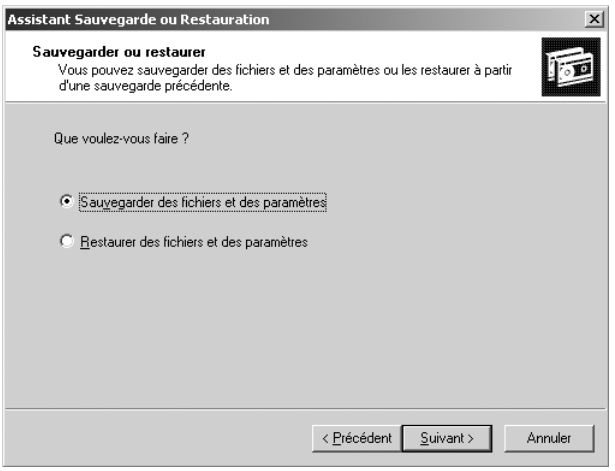


Figure 1–15
Sauvegardez ou restaurez vos données avec l'utilitaire de Windows.

ALTERNATIVE OPEN SOURCE Firefox

Avec Firefox, vous pouvez très facilement exporter vos favoris dans un seul fichier : dans le menu *Marque-pages*, choisissez *Gérer les marque-pages*. Sélectionnez *Fichier*, puis *Exporter*, et spécifiez le nom de votre fichier de marque-pages.

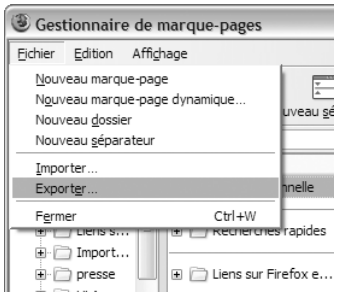


Figure 1–13 Enregistrez vos favoris Firefox dans un fichier.

Figure 1–14
Emplacement de l'utilitaire de gestion des sauvegardes

Choisissez ensuite les données que vous voulez sauvegarder ; parcourez votre arborescence et cochez les cases correspondant aux fichiers et dossiers importants.

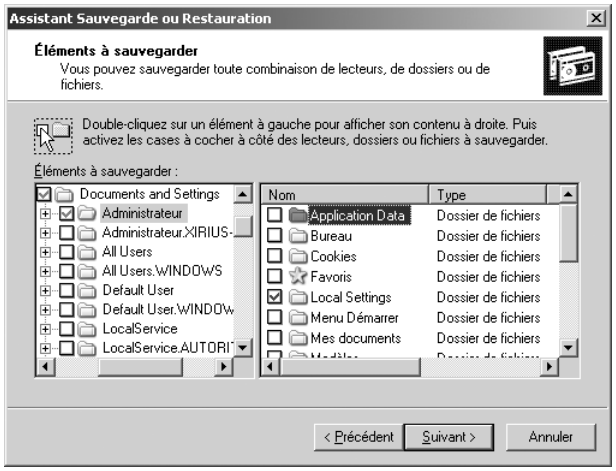


Figure 1–16
Choisissez les éléments à sauvegarder.

Ensuite, choisissez un emplacement pour le fichier de sauvegarde (`.bkf`). Par défaut, ce dernier se nomme `Backup.bkf` et est créé dans le dossier `Mes Documents` de la personne effectuant la sauvegarde. Toutefois, vous pouvez cliquer sur le bouton *Parcourir* pour choisir un autre emplacement. Ce choix doit être effectué dès la première exécution du programme de sauvegarde.

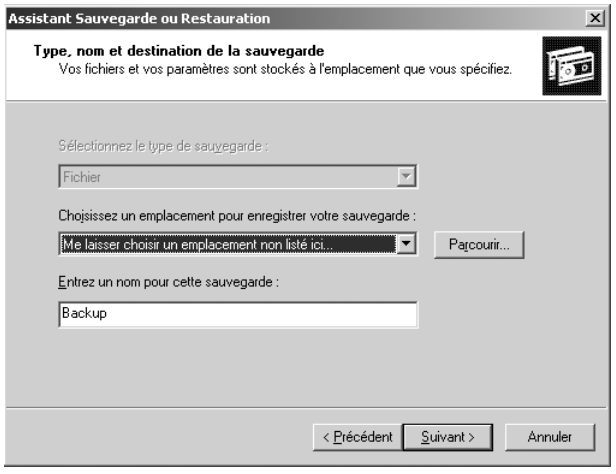


Figure 1–17
Choisissez un emplacement pour la sauvegarde.

Il vous suffit ensuite de cliquer sur le bouton *Terminer* pour lancer une sauvegarde élémentaire.

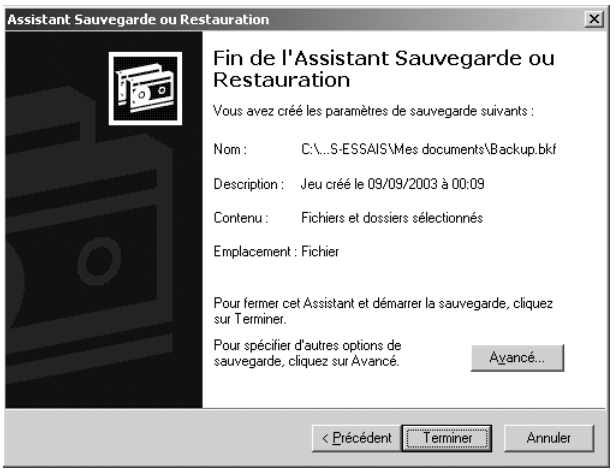


Figure 1–18
Lancez la sauvegarde.

Vous pouvez de plus agir sur d'autres paramètres de contrôle du processus de sauvegarde, comme spécifier le type de sauvegarde (normale, incrémentielle, différentielle ou quotidienne), ou demander la vérification des données copiées. Cliquez pour cela sur le bouton *Avancé* et sélectionnez les paramètres adéquats.

Sauvegarde normale, incrémentielle, différentielle ou quotidienne

Vous serez concerné par ce paramètre uniquement si vous réalisez de gros archivages. Dans la majorité des cas (au moins en ce qui concerne les particuliers), une **sauvegarde normale** – ou sauvegarde complète – sera amplement suffisante : elle copie les fichiers sélectionnés et les marque comme sauvegardés.

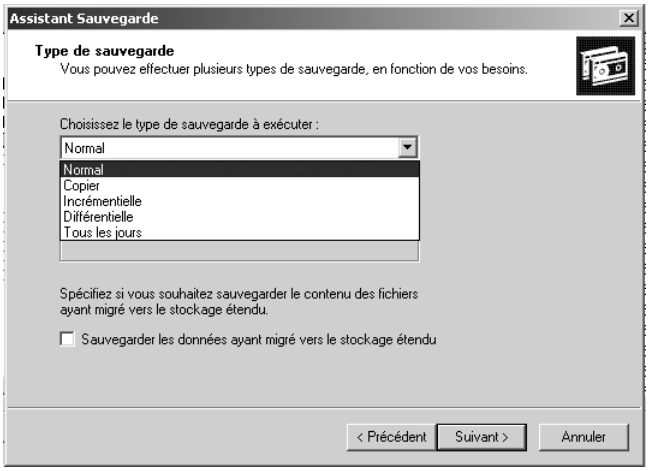


Figure 1–19
Types de sauvegardes

Si vous gérez d'importants volumes de données, et selon l'espace disponible pour le stockage, la **sauvegarde incrémentielle** optimise considérablement le processus : elle sauvegarde les fichiers sélectionnés seulement s'ils ont été créés ou modifiés depuis la dernière sauvegarde.

Une **sauvegarde différentielle** enregistre les fichiers sélectionnés seulement s'ils ont été créés ou modifiés depuis la dernière sauvegarde mais n'ont pas été marqués comme sauvegardés.

Une sauvegarde différentielle fait une copie de tous les fichiers modifiés depuis la dernière sauvegarde complète, tandis qu'une sauvegarde incrémentielle copie tous les fichiers modifiés depuis la dernière sauvegarde. L'une et l'autre fonctionnent très bien en complément d'une sauvegarde complète régulière. Les sauvegardes différentielles sont plus faciles à effectuer et à utiliser : la restauration d'une situation revient à utiliser la sauvegarde complète la plus récente avec la dernière sauvegarde différentielle. L'utilisation de sauvegardes incrémentielles est un processus plus lent. Vous devez d'abord restaurer individuellement chaque sauvegarde incrémentielle réalisée depuis la dernière sauvegarde complète. Néanmoins, les sauvegardes incrémentielles sont plus rapides à effectuer que les différentielles.

Une **sauvegarde quotidienne** ne copie que les fichiers sélectionnés qui ont été créés ou modifiés le jour même. Elle ne sert pas vraiment à préserver les données mais vous aide plutôt à trouver rapidement les fichiers que vous êtes en train d'utiliser pour les transférer sur un autre média.

La **copie** enregistre les fichiers sélectionnés mais ne les marque pas comme sauvegardés. Cette fonction est utile si vous voulez créer une copie complète de tous les fichiers sélectionnés, sans réinitialiser le bit d'archive pris en compte par la sauvegarde incrémentielle.

Planifier une sauvegarde automatique

Le bouton *Avancé* de l'utilitaire de gestion des sauvegardes (figure 1-20) propose une suite d'options, parmi lesquelles les paramètres de planification.

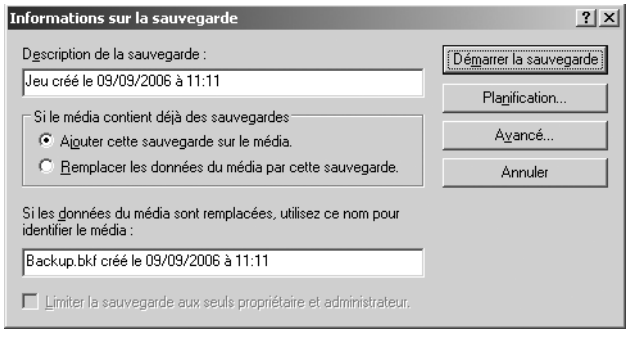


Figure 1–20
Vous pouvez démarrer immédiatement ou planifier la sauvegarde.

Si vous cliquez sur *Planification*, un calendrier mensuel apparaît (figure 1-21). Vous pouvez accéder directement à cet écran lorsque vous démarrez l'utilitaire de gestion des sauvegardes en mode *Avancé* (onglet *Planifier les travaux*).

Pour créer et planifier une sauvegarde à partir de cet onglet, cliquez sur le bouton *Ajouter une opération*, dans le coin inférieur droit de l'écran. Vous lancez alors un assistant de sauvegarde qui vous guide dans le choix des différentes options.

Figure 1–21
Onglet *Planifier les travaux* de l'utilitaire de gestion des sauvegardes

Figure 1–22
Choisissez une heure et une fréquence pour la sauvegarde.

L'une de ces options propose d'exécuter la sauvegarde maintenant ou ultérieurement, l'heure par défaut d'une sauvegarde planifiée étant minuit au jour où vous définissez l'opération de sauvegarde. Pour planifier une opération, sélectionnez *Ultérieurement* et cliquez sur le bouton *Planification*.

Choisissez la fréquence d'exécution de la sauvegarde (tous les jours, une seule fois, toutes les semaines, tous les mois, au démarrage du système, en cas de connexion, ou lorsque l'ordinateur est inactif), ainsi que la date et l'heure de début (figure 1–22).

Vérifier si une sauvegarde s'est bien passée

Cela peut paraître une évidence, mais il faut toujours s'assurer qu'une sauvegarde s'est bien déroulée. Il n'y a pas plus rageant que de s'apercevoir après un « plantage » qu'une sauvegarde est inexploitable !

Dans le cas d'une sauvegarde manuelle, une possibilité efficace est de surveiller vous-même le bon déroulement des opérations. Prenez la peine de vérifier après coup le contenu du support de sauvegarde, vérifiez que vous accédez normalement aux fichiers copiés et effectuez le cas échéant (au moins au début) quelques restaurations. Vérifiez toujours que ce que vous avez copié correspond bien à ce que vous vouliez réellement sauvegarder !

Dans le cas d'une sauvegarde automatique, ayez le réflexe de consulter régulièrement les journaux système. Ouvrez pour cela la console *Gestion de l'ordinateur* : dans le menu *Démarrer*, cliquez droit sur *Poste de travail* et sélectionnez *Gérer* (figure 1–23).

AVANCÉ **Console Gestion de l'ordinateur**

- *Démarrer>Poste de travail>Gérer*
- *Outils d'administration>Gestion de l'ordinateur*
- Clic droit sur l'icône *Poste de travail* du bureau, puis *Gérer*

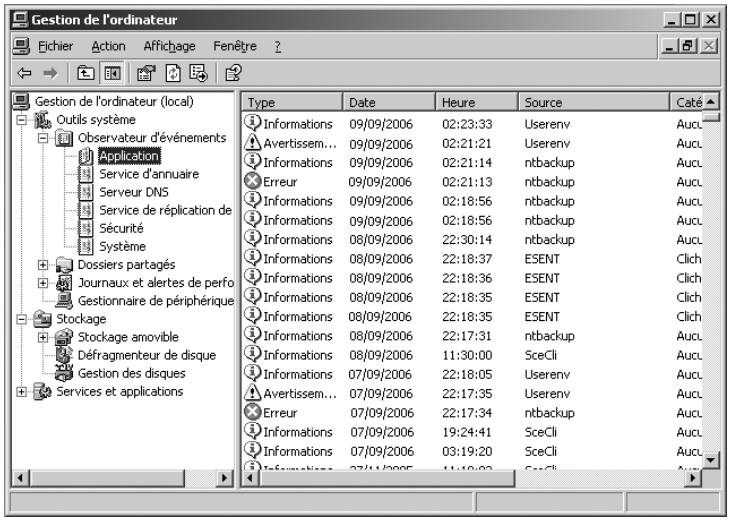


Figure 1–23
Consultez la présence éventuelle d'événements système relatifs au déroulement de la sauvegarde.

Dans *Outils système*, ouvrez l'*Observateur d'événements* et cliquez sur *Applications*. Un événement devrait vous indiquer si l'utilitaire de sauvegarde a bien démarré ; vérifiez la présence éventuelle de messages d'erreurs. Si c'est le cas comme dans la figure 1-23, double-cliquez sur les messages pour lire leur contenu.

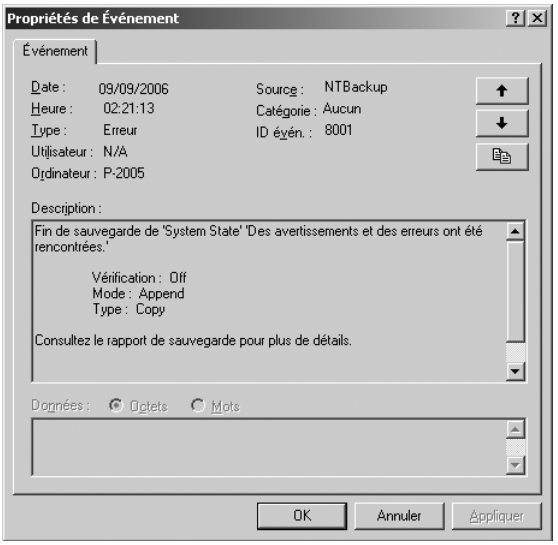


Figure 1–24
Consultez les éventuels messages d'erreurs.

Le message de la figure 1-24 n'est pas très explicite, mais il vous alerte. Il faut donc que vous consultiez le journal que l'application de gestion des sauvegardes crée par défaut (sauf si vous lui indiquez explicitement de ne pas le faire).

AVANCÉ **Paramètres de journalisation de la sauvegarde**

Vous les trouverez en cliquant sur le bouton *Avancé* de la figure 1-18.

À partir de l'utilitaire de sauvegarde, choisissez *Rapport* dans le menu *Outils*. Vous obtenez une liste des journaux de sauvegarde, comme l'illustre la figure 1-25.

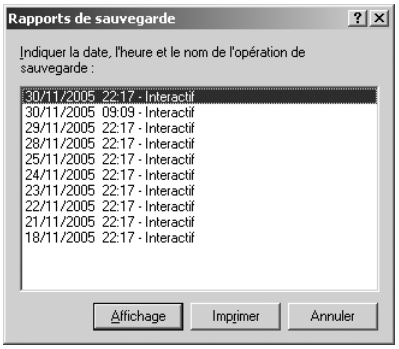


Figure 1–25
Consultez le rapport de sauvegarde.

Cliquez sur le dernier rapport de sauvegarde, examinez son contenu et prenez les mesures nécessaires pour corriger les éventuels problèmes.

Restaurer des données

Les sauvegardes ne servent pas à grand-chose si on ne sait pas les utiliser pour restaurer les données. L'expérience montre que la restauration des données sauvegardées n'est pas toujours une opération simple, d'autant que, sous l'influence du stress, le cerveau a une malencontreuse tendance à cesser de fonctionner normalement. Afin de vous préparer à faire face aux situations extrêmes, nous vous suggérons de vous entraîner à restaurer des données sauvegardées alors qu'aucune urgence ne vous oblige à le faire.

OUTILS Utilitaires de sauvegarde

Les outils livrés avec Windows fonctionnent très bien. Toutefois, si vous souhaitez tester d'autres produits, voici quelques utilitaires de sauvegarde réputés :

- Norton Ghost
- Backup 2004 Pro
- Casper XP
- True Image Server

Restaurer un document de bureautique

C'est extrêmement simple. Partons du principe que l'enregistrement automatique était activé.

Après « plantage », redémarrez votre machine ainsi que le logiciel qui était en cours d'utilisation (Word par exemple). Celui-ci vous affiche automatiquement les fichiers de restauration des documents qui étaient en cours d'édition au moment où le problème est survenu. Si vous avez réglé la période d'enregistrement des informations de récupération automatique à 5 minutes, vous retrouverez votre document dans l'état où il était 5 minutes au maximum avant l'accident. Votre mémoire fera le reste.

Restaurer un document supprimé par inadvertance

Lorsque vous supprimez un fichier, celui-ci est envoyé dans la corbeille, mais n'est pas physiquement détruit. Ouvrez la corbeille, cliquez droit sur le fichier, puis cliquez sur *Restaurer* ; il est replacé automatiquement à son emplacement d'origine.

Attention, les éléments dont la taille est supérieure à la capacité de stockage de la corbeille sont directement effacés. De même, les éléments supprimés à partir d'un lecteur réseau ou d'un média amovible (clé USB par exemple) ne sont pas envoyés dans la corbeille. Vous ne pourrez donc pas les restaurer.

Restaurer la messagerie

Restaurer la messagerie n'est pas une opération particulièrement difficile, mais il est utile que vous vous familiarisiez avec cette procédure : vous apprendrez à gérer les problèmes auxquels vous serez inévitablement confronté lors de la « vraie » restauration.

Si vous pouvez accéder à une machine de tests, vierge de votre client de messagerie préféré, procédez à l'installation complète de celui-ci. Muni des CD-Rom originaux ou de l'exécutable que vous avez téléchargé sur

ALTERNATIVE OPEN SOURCE **Thunderbird**

Remplacez manuellement le contenu du dossier de profil par celui du dossier sauvegardé, par défaut :
`c:\Documents and Settings\`*`nom_utilisateur`*`\Application Data\Thunderbird\Profiles\`*`XXXXXXXX`*`.default`

Internet, lancez la procédure d'installation et suivez les instructions. Vous ne devriez rencontrer aucune difficulté.

Recréez ensuite votre compte. Avec Outlook Express, dans le menu *Outils*, choisissez *Compte*, puis cliquez sur *Ajouter*, et enfin sur *Courrier* (figure 1-26). Suivez les différentes étapes du processus. Il suffit de renseigner tous les champs avec vos paramètres personnels (c'est précisément ici que vous vous féliciterez d'avoir bien soigneusement noté tous les paramètres cités à la figure 1-6).

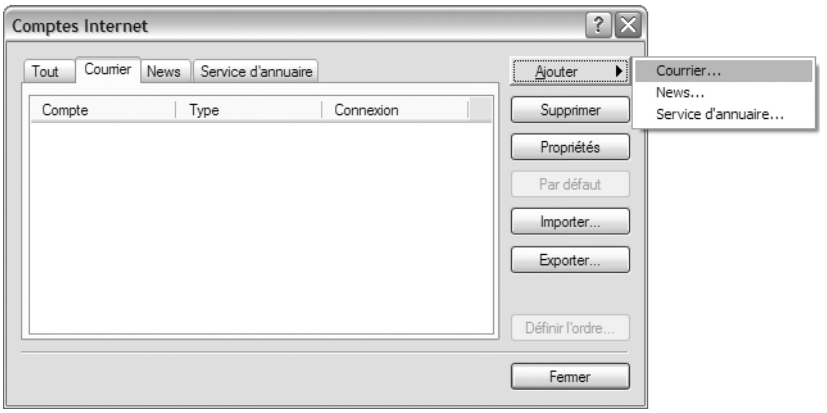


Figure 1–26
Recréez votre compte de messagerie.

À compter de ce moment, votre messagerie est à nouveau opérationnelle et il ne vous reste plus qu'à importer vos messages sauvegardés. Dans le menu *Fichier*, choisissez *Importer*, puis cliquez sur *Messages* (figure 1-27).

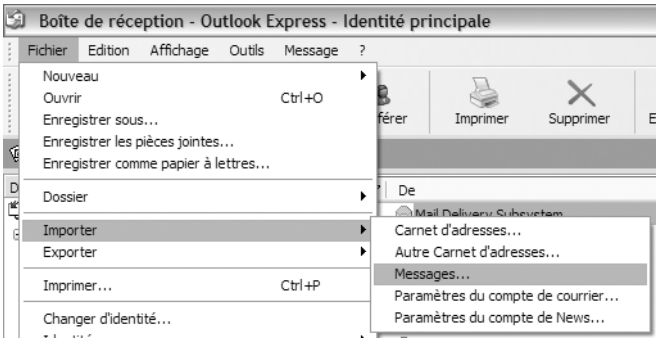


Figure 1–27
Importez vos messages.

Vous pouvez également importer des boîtes d'autres clients (Netscape, Outlook, Exchange, Eudora…). Sélectionnez le programme de messagerie à partir duquel vous souhaitez importer des messages, spécifiez l'emplacement du fichier sauvegardé, puis suivez les instructions. Votre messagerie a été complètement restaurée.

Avec Outlook, c'est encore plus simple. Recréez votre compte, puis fermez Outlook ; un nouveau fichier `Outlook.pst` pratiquement vide est apparu dans l'arborescence. Remplacez-le manuellement par celui que vous avez sauvegardé (qui contient tous vos messages, vos contacts, etc.). Ouvrez à nouveau Outlook ; vous constaterez que votre messagerie est complètement restaurée.

Restaurer les données avec l'utilitaire de sauvegarde

Ouvrez l'utilitaire de gestion des sauvegardes en mode *Assistant* et choisissez *Restaurer*. Affichez le contenu du catalogue des éléments à restaurer (partie gauche de l'écran, figure 1-28) et sélectionnez les fichiers qui vous intéressent (les fichiers ou répertoires sélectionnés sont marqués d'une coche bleue).

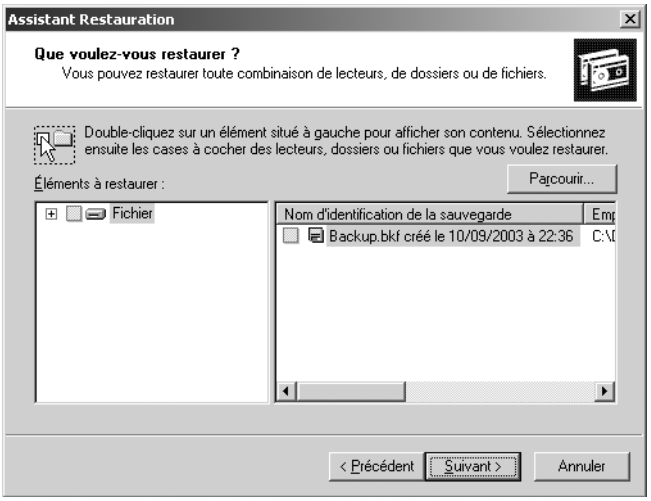


Figure 1–28
Sélectionnez les éléments à restaurer.

Choisissez ensuite, parmi les options de restauration disponibles, celles que vous souhaitez mettre en œuvre :

- emplacement des fichiers restaurés (emplacement d'origine ou autre emplacement) ;
- paramètres avancés : paramètres de sécurité, points de montage, points de jonction (figure 1-29).

Cliquez ensuite sur le bouton *Terminer* dans la dernière page de l'assistant pour lancer la restauration.

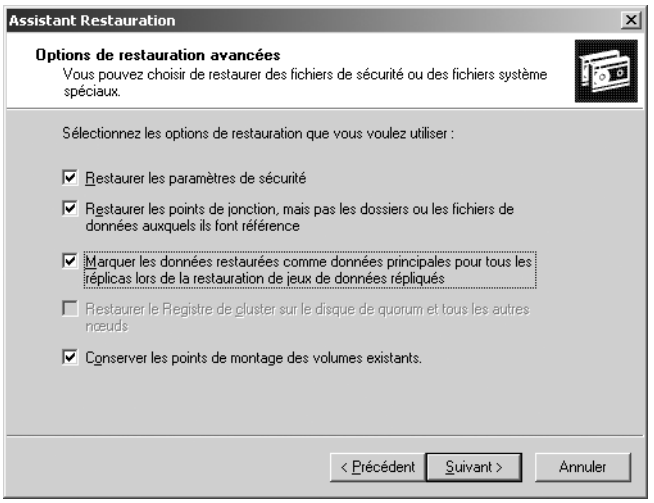


Figure 1–29
Sélectionnez les paramètres de restauration.

Quand le système ne démarre plus…

Avez-vous déjà pensé à cette éventualité ? Vous avez été contaminé par un virus, vous avez installé une nouvelle application ou vous avez éteint votre poste un peu brutalement. Subitement, le système refuse de redémarrer. L'écran est noir, ou bleu selon les cas, et agrémenté d'un message incompréhensible que vous avez peine à déchiffrer (en supposant que vous ayez le temps de le lire). Après avoir fébrilement tenté d'effectuer deux ou trois redémarrages, vous réalisez soudain que vous venez de perdre une quantité impressionnante de fichiers précieux.

C'est exactement dans ces moments difficiles que l'on regrette amèrement de ne pas avoir effectué des sauvegardes, « Ah ! si j'avais su ! ». Nous ne le répéterons jamais assez : sauvegardez vos données, cela vous évitera bien des catastrophes !

Que faire alors ? Avant de céder à la panique, sachez qu'il reste des opérations de la dernière chance. À moins d'une panne sévère d'un composant matériel essentiel, comme le disque dur, il est souvent possible de récupérer tout ou partie du système et de sauver les meubles in extremis.

Identifier la panne

Avant tout, prenez soin de cerner l'origine de la panne. Si l'ordinateur ne démarre plus, cela ne signifie pas nécessairement que les données sont atteintes.

Assurez-vous notamment que :

- Votre matériel est branché (oui, c'est un peu trivial mais… vérifiez tout de même).
- Votre câble d'alimentation n'est pas défectueux (essayez un autre câble).
- Le problème ne vient pas de l'alimentation de l'ordinateur. Si tel est le cas, l'ordinateur ne fait rien du tout, pas même du bruit. Envisagez alors de faire remplacer l'alimentation.

D'autres cas peuvent se présenter :

- Si l'ordinateur ne démarre que son ventilateur, il a probablement un souci avec sa carte mère. Ce point est embêtant car il touche le cœur du système. Toutefois, si tout se passe bien, on vous change la carte mère, on ne touche pas au disque et vous récupérez vos données intactes.
- Si l'ordinateur enclenche le processus de démarrage mais n'affiche rien sur le moniteur (vous l'entendez, mais ne voyez rien), il a sans doute un problème avec la carte vidéo. Il faut alors changer cette carte, mais vos données ne sont toujours pas affectées.

Si, lorsqu'il commence à charger le système, l'ordinateur affiche un écran bleu, cela vous met dans des états fébriles. Un peu de patience, tout n'est pas perdu : puisqu'il a commencé à charger le système, cela veut dire que l'ordinateur reconnaît encore le disque dur. Il vous est alors possible d'intervenir pour réparer l'installation et récupérer vos données. Il s'agit la plupart du temps d'un dysfonctionnement de la mémoire, de la présence de mauvais pilotes de périphériques, d'un virus, ou de l'instabilité d'un système d'exploitation endommagé. Suivez alors la démarche présentée succinctement ci-après.

Enfin, si l'ordinateur ne reconnaît plus le disque, il se peut que celui-ci soit physiquement endommagé. Dans ce cas, vous avez réellement lieu de vous inquiéter. Sachez toutefois qu'il existe des moyens de récupérer des données sur un disque endommagé, mais vous devrez faire appel à une société spécialisée.

Se préparer à une panne du processus de démarrage

Bien entendu, vous le savez déjà, la première mesure à prendre est préventive : sauvegardez régulièrement vos données. Dans ce cas, quoi qu'il arrive à votre poste, vous pourrez toujours restaurer complètement vos données et vos applications, après un éventuel remplacement de la

machine, ou un reformatage en règle du disque dur. C'est fastidieux, certes, éventuellement coûteux s'il faut remplacer la machine, mais au moins, vous n'aurez perdu aucune information.

Cependant, lorsque l'ordinateur a un problème sérieux au moment du démarrage, il existe des moyens plus simples de retomber sur ses pieds :

- Il peut avoir été touché par un virus. Dans ce cas, il vous faut décontaminer la machine.
- Il se peut qu'une modification malencontreuse de la configuration soit à l'origine du blocage. Vous devez alors réactiver une configuration précédente, ou supprimer les éléments responsables du dysfonctionnement.
- Le système d'exploitation est lui-même endommagé. Réparez-le.

Réparer un système gravement endommagé par un virus

Nous aborderons cette question plus en détail au chapitre 3. Sachez que si votre ordinateur a été infecté au point de ne plus pouvoir redémarrer, vous pouvez tout de même lancer le système à partir du CD-Rom d'installation de l'antivirus ou, à la rigueur, d'un jeu de disquettes d'urgence que vous avez pris soin d'établir au préalable, ou encore en vous servant d'une autre machine.

L'antivirus procède au balayage complet du ou des disques infectés à la recherche de virus potentiels. S'il parvient à identifier et à localiser le ou les virus en question, il tente de nettoyer l'infection, de réparer les objets endommagés du système de fichiers, de la mémoire et des secteurs, et restaure les informations d'amorce et de partition (à condition cependant que le système d'exploitation soit réparable).

Attention toutefois : tous les antivirus ne proposent pas cette fonction salutaire et, s'ils la proposent, la réparation n'est pas assurée (dans les cas extrêmes, on ne peut raisonnablement pas demander à l'antivirus d'effacer d'un coup de baguette magique les dégâts considérables causés par les virus dévastateurs).

À l'issue de cette procédure, essayez de redémarrer votre système normalement.

Réactiver la dernière bonne configuration connue

Si les modifications que vous avez apportées récemment à votre système d'exploitation le rendent inutilisable, démarrez l'ordinateur et faites apparaître le menu des options avancées ; pour cela, appuyez sur la touche *F8* lorsque le système d'exploitation est en cours de chargement (dès le début).

Un menu texte de ce type apparaît :

```
Menu d'options avancées de Windows
Sélectionnez une option :

   Mode sans échec
   Mode sans échec avec prise en charge réseau
   Invite de commande en mode sans échec

   Inscrire les événements de démarrage dans le journal
   Démarrage en mode VGA
   Dernière bonne configuration connue (vos derniers paramètres fonctionnels)
   Mode restauration Active Directory (contrôleurs de domaine Windows)
Mode débogage

Démarrer Windows normalement
Redémarrer

Utilisez les flèches HAUT et BAS pour mettre votre choix en surbrillance
```

Windows maintient dans le Registre plusieurs versions des informations de configuration de la machine locale : *Current*, *Default*, *Failed* et *LastKnownGood* (clé de registre `HKLM\System\Select`). Lorsque vous lancez normalement la machine, le contrôle *Default* est utilisé. Si cette configuration est endommagée, l'option *Dernière bonne configuration connue* oblige Windows à démarrer avec le contrôle *LastKnownGood*.

Cette option est véritablement salutaire car, sans toucher au Registre ni réparer quoi que ce soit, elle vous permet de revenir en arrière et de repartir sur des bases solides. N'hésitez pas à en faire usage !

Le mode sans échec

Si les tentatives de réparation lancées jusqu'à présent ont échoué, si vous soupçonnez que le dysfonctionnement d'un pilote est la cause de votre problème, alors appuyez sur la touche *F8* lorsque le système d'exploitation est en cours de chargement et sélectionnez *Mode sans échec*.

Les diverses formes du mode sans échec (avec prise en charge réseau, sans réseau, invite de commande en mode sans échec) chargent une version minimale du système d'exploitation. Cette dernière ne comprend que les pilotes et les fichiers indispensables. En dépit d'une interface singulièrement moins attrayante (travailler en mode sans échec a toujours eu quelque chose d'un peu inquiétant), ces outils sont pratiques pour prendre la main sur un système endommagé et réaliser des interventions manuelles comme le déchargement d'un pilote, la spécification du mode de démarrage d'un service (par exemple démarrage manuel et non automatique) ou la suppression d'une application susceptible d'être à l'origine du blocage.

AVANCÉ **Options de démarrage de Windows**

Au tout début de l'amorçage du système, appuyez sur la touche *F8*. Un menu s'ouvre qui vous propose les différents modes de démarrage de Windows, grâce auxquels vous pourrez tenter de réparer votre installation.

En mode sans échec, vous avez en outre accès à votre système de fichiers et vous pouvez ainsi effectuer des opérations de sauvegarde.

Lorsque vous avez terminé, fermez la session et tentez le redémarrage normal de la machine.

Réparer une installation endommagée

Si des fichiers importants du système d'exploitation ont été corrompus, votre seule issue est de tenter une réparation, voire une réinstallation complète de Windows.

Insérez votre disque d'installation dans le lecteur approprié et choisissez l'option *Réparer le système*. Suivez les instructions et laissez le processus se dérouler normalement. Windows remplace les fichiers endommagés.

En toute logique, Windows vous remet votre système à neuf, sans toucher à vos données. Toutefois, cette opération est lourde car elle peut nécessiter une reconfiguration de plusieurs services et une réinstallation complète de nombreux éléments, comme les correctifs logiciels ou toutes sortes de mises à jour. Néanmoins, après tant d'efforts et une issue favorable, vous accéderez de nouveau à votre système de fichiers comme avant, voire mieux qu'avant. C'est appréciable !

Récapitulatif : les dix commandements à l'usage de l'utilisateur

La négligence est votre principal ennemi. À une époque où les attaques informatiques deviennent de plus en plus sophistiquées, c'est paradoxalement votre propre négligence qui est responsable de la plupart de vos désagréments, bien avant les actes perpétrés par les pirates ou les virus. L'outil informatique repose sur un gigantesque amoncellement de techniques complexes qui le rendent parfois très peu fiable. Conjuguer votre éventuelle négligence avec cet outil somme toute fragile ne peut qu'aboutir à la catastrophe.

Soyons honnêtes : les pertes de temps ou d'information pourraient pour la plupart être facilement évitées. Pour remédier à cet état de fait, prenez dès aujourd'hui une bonne résolution : respectez simplement un code de

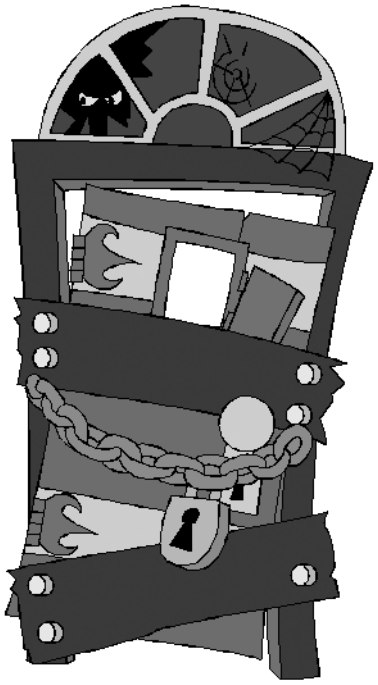
bonne conduite, et essayez de suivre les « dix commandements à l'usage de l'utilisateur d'informatique »[1] exposés ci-après. Vous constaterez bien vite une amélioration notoire dans la qualité de vos relations avec votre outil informatique.

Les dix commandements à l'usage de l'utilisateur

1. TOUTE INFORMATION VITALE TU DUPLIQUERAS
   Toute information vitale doit exister au minimum à la fois sur votre poste, sur un support de sauvegarde, sur un serveur si vous êtes en réseau, et accessoirement sur une clé USB.
2. TOUTE INFORMATION VITALE TU SAURAS RESTAURER
   Il faut être sûr de savoir restaurer toute information sauvegardée.
3. AUCUN PROCESSUS INFORMATIQUE TU NE VIOLENTERAS
   - Sauf extrême nécessité, n'interrompez jamais un processus en cours d'exécution.
   - Quittez proprement une application, laissez-lui le temps de refermer ses fichiers ouverts.
   - N'éteignez jamais brutalement votre poste.
   - N'agissez jamais dans la précipitation. Mieux vaut perdre deux minutes que deux semaines de travail.
4. L'ESPACE SYSTEME TU RESPECTERAS
   - Windows gère l'espace utilisateur dans `%USERPROFILE%` (`C:\Documents and Settings\nom_utilisateur\`) et le système dans `%SystemRoot%` (`C:\Windows`). Ne touchez jamais à ces arborescences et à leur contenu (à l'exception bien sûr des espaces dévolus aux utilisateurs, comme `Mes documents`, `Mes images` ou `Ma musique`).
   - N'intervenez jamais sauvagement sur des fichiers gérés par le système ou par une application.
5. LE MÉNAGE TU FERAS
   - Plus les fichiers grossissent, plus les applications qui les gèrent risquent de rencontrer des problèmes. Veillez à ce que tous les fichiers manipulés conservent une taille raisonnable.
   - Plus les applications sont nombreuses, plus les chances de « plantage » augmentent. Désinstallez les applications inutilisées.
   - Archivez les dossiers non utilisés. Archivez la messagerie.
6. DE NÉGLIGENCE TU NE TE RENDRAS PAS COUPABLE
   - Ne traitez jamais par le mépris un message d'erreur, surtout si c'est un message système. Un tel message est souvent le symptôme d'une infiltration (presque) réussie.
   - Affectez un nom raisonnable à chaque fichier. Proscrivez les noms de plus de 30 caractères.
   - Ne travaillez jamais sur une clé USB.
   - Notez sur un papier et rangez bien soigneusement dans un endroit sûr les éléments secrets sans lesquels vous ne pourrez accéder à votre machine.
7. DES CODES TÉLÉCHARGÉS TU TE MÉFIERAS
   - De nombreux codes exécutables ou applications sur Internet n'ont qu'une vocation : infiltrer le poste de l'utilisateur à travers le pare-feu, prendre son contrôle à distance et semer la pagaille sur le réseau.
   - N'utilisez jamais de logiciels ou de fichiers piratés.
8. AVANT D'EFFACER DES DONNÉES VITALES TU RÉFLÉCHIRAS
   Soyez sûr de votre fait avant d'effacer quoi que ce soit. Vérifiez que toutes (TOUTES) les données importantes ont bien été sauvegardées ou archivées, et que les sauvegardes sont exploitables.
9. TOUT PROCESSUS IMPORTANT TU VÉRIFIERAS
   - N'oubliez jamais qu'un service, une application ou un système d'exploitation est truffé d'erreurs de programmation. En conséquence, n'accordez pas une confiance aveugle à cet outil.
   - Gardez toujours le contrôle sur les opérations effectuées. Vérifiez après coup les travaux réalisés par un processus automatique.
   - Assurez-vous du bon déroulement d'une opération touchant à une donnée vitale : vérifiez qu'une sauvegarde s'est bien passée, qu'un transfert de fichiers à travers un réseau s'est déroulé intégralement, etc.
10. DE LUCIDITÉ TU FERAS PREUVE EN TOUTE CIRCONSTANCE
    - L'informatique est un outil très puissant pour accomplir des tâches simples. Ne lui demandez d'effectuer que les tâches pour lesquelles elle a été conçue. Ne « bidouillez » jamais.
    - Effectuez les tâches quotidiennes calmement. Proscrivez la précipitation.

1. Cette charte n'a rien d'officiel. Elle n'engage que l'auteur de ces lignes et repose sur son expérience personnelle.

chapitre 2



Configurer son système de façon sécurisée

Le système d'exploitation est le premier rempart contre l'envahisseur. Il est donc capital de savoir le configurer pour limiter les accès à votre poste, cacher vos fichiers et votre activité, ou encore partager des données. Dans ce chapitre, vous apprendrez également comment chiffrer vos fichiers les plus sensibles.

SOMMAIRE

- Formater en NTFS
- Sécuriser le Registre
- Protéger l'accès à la machine
- Partager des informations en réseau
- Vider les historiques
- Chiffrer des fichiers ou des répertoires

MOTS-CLÉS

- NTFS, FAT, FAT32
- clé de Registre
- mot de passe
- écran de veille
- dossier partagé
- historique
- fichier « invisible »
- chiffrement
- clé publique/clé privée

Certains informaticiens pensent que la sécurité est un monde étrange et un peu à part, que les ingénieurs en sécurité sont des empêcheurs de tourner en rond et qu'il faut les éviter à tout prix. Ils estiment qu'une fois le système conçu, on peut à la rigueur aller voir l'expert en sécurité informatique, pour se donner bonne conscience, pour que celui-ci entérine des choix déjà faits ou, qu'éventuellement, d'un coup de baguette magique, il ajoute quelque part, dans un endroit qui ne gêne pas trop de préférence, le composant de sécurité miracle qui fera disparaître tous les problèmes. Ils se trompent lourdement !

Tout au long de cet ouvrage, nous verrons que les points d'attaque des systèmes informatiques sont nombreux : failles dans les systèmes d'exploitation, faiblesses des protocoles de communication, bogues dans les applications, codes mobiles, erreurs et négligences de l'utilisateur… Toute fonction, toute application, tout service informatique recèle un nombre considérable de vulnérabilités, leviers potentiels que l'attaquant astucieux saura actionner en temps utile pour s'engouffrer au cœur du système.

Au chapitre précédent nous avons parlé des mesures préventives incontournables destinées à vous aider à refaire surface le jour où se produit la catastrophe annoncée.

Nous abordons à présent les premières mesures défensives grâce auxquelles vous allez commencer à gêner les prétendants à votre système de fichiers : il s'agit de renforcer votre poste à l'aide des fonctions de sécurité présentes dans votre système d'exploitation.

Certes, les mécanismes de sécurité offerts par les systèmes d'exploitation ne sont pas toujours réputés comme étant d'une résistance à toute épreuve. Certains même pêchent par de graves lacunes d'implémentation. Cependant, il est tout de même dommage de négliger ces fonctions, offrant ainsi un boulevard au premier venu, ou lui ouvrant l'accès à votre espace de travail, sans même qu'il ait besoin de casser quelques barrières pour y parvenir. En dépit des faiblesses flagrantes de certains mécanismes, une configuration bien sécurisée donnera du fil à retordre au pirate. Pensée dans la perspective plus large des solutions complémentaires présentées dans les chapitres suivants, votre configuration sécurisée constituera déjà la première couche de votre édifice sécuritaire.

À RETENIR Sécuriser un système

Le problème de la sécurisation d'une machine ou d'un système se pose à plusieurs niveaux. C'est pourquoi une sécurité bien pensée n'est pas autre chose qu'un empilement de couches de protection qui, agissant de concert, parviendront à ralentir l'attaque, voire, peut-être, à l'empêcher.

Configurer le système d'exploitation

Windows, un système sécurisé ?

À l'origine, les systèmes de Microsoft étaient faiblement sécurisés et les utilisateurs étaient nombreux à s'en plaindre. C'est pourquoi, il y a quelques années, la firme de Redmond décida de s'attaquer très activement à ce problème et il faut reconnaître que les choses ont bien changé. Si les premières tentatives de sécurisation ont suscité le scepticisme, voire les sarcasmes des mauvaises langues, les services de sécurité désormais présents au cœur des serveurs de dernière génération écornent sérieusement la position de certains éditeurs spécialisés en sécurité, qui monnayent parfois leurs services au prix de la haute couture.

Certes, la fiabilité des mécanismes de sécurité de Windows reste toujours une question délicate, mais, confiée à un administrateur chevronné, une configuration bien sécurisée offre un premier bouclier protecteur.

- **En entreprise**, une architecture client/serveur fondée sur Windows Server 2003 d'un côté et Windows XP Pro de l'autre, offre une richesse fonctionnelle insoupçonnée : contrôle étroit des utilisateurs (l'expérience montre qu'une partie de la menace vient de l'intérieur), diverses protections contre les attaques extérieures, suivi détaillé de l'activité, centralisation de l'administration dotée de fonctions élaborées pour la définition et le déploiement de stratégies de sécurité.
- **Pour les particuliers**, le fait de posséder un système d'exploitation récent constitue, en soi, une mesure de sécurité. Même si XP édition familiale est loin d'offrir toutes les fonctions de Windows XP Pro, il dispose d'un pare-feu intégré. Il est également doté d'un « Centre de Sécurité », véritable interface d'administration centralisée à partir de laquelle vous accédez directement aux options de configuration du pare-feu, de l'antivirus et des paramètres de sécurité de votre interface Internet. Elle vous permet également de régler les mécanismes de mises à jour automatiques. Tous ces éléments constituent les premiers maillons d'une chaîne de protection visant à prévenir une exploitation malveillante des vulnérabilités du système d'exploitation. Pour accéder à cette interface, cliquez sur *Démarrer>Panneau de configuration*, puis sur *Centre de sécurité* (figure 2-1).

Encore une fois, ces services sont d'une robustesse relative, dans la mesure où des professionnels de la sécurité auront de bonnes chances de les contourner. Cependant, bien configurés, ils constitueront un premier rempart contre des pirates peu expérimentés et compléteront efficacement les solutions de sécurité que nous découvrirons au cours des prochains chapitres.

RENVOI **Pare-feu**

Le pare-feu de Windows est rudimentaire, comparé à d'autres produits spécialisés. Ce sujet sera traité au chapitre 5.

RENVOI **Sécurité de l'interface Internet**

Ce sujet sera traité en détail au chapitre 7.

RENVOI **Antivirus**

Ce sujet sera traité en détail au chapitre 3.

RENVOI **Et Vista ?**

Les évolutions promises par la future version de Windows pour améliorer la sécurité seront discutées au chapitre 10, lorsque toutes les technologies présentées dans cet ouvrage vous seront devenues familières.

Figure 2–1
Interface du Centre de Sécurité

Étapes essentielles d'une configuration sécurisée

Dans ce chapitre, nous nous focaliserons sur la configuration sécurisée d'un poste de travail individuel. Nous délaissons volontairement la problématique des stratégies de sécurité propre à la configuration des serveurs et des parcs informatiques en entreprise, qui relève davantage des tâches d'un administrateur système.

Le renforcement de la sécurité d'un poste de travail repose sur quelques points très simples :

- le formatage des disques en NTFS (si ce n'est pas déjà fait) ;
- la sécurisation du Registre ;
- la gestion des utilisateurs : droits d'accès, protection des comptes à l'aide d'un mot de passe robuste, applications accessibles ;
- la gestion et la sécurisation des partages ;
- le chiffrement éventuel des fichiers sensibles.

Configuration de base : formater les disques en NTFS

Votre système d'exploitation organise et stocke vos fichiers sur le disque selon un ordre bien déterminé, afin de pouvoir les retrouver et y accéder

le plus rapidement possible. La structure selon laquelle les fichiers sont organisés sur le disque est ce que l'on appelle le format.

Les versions récentes de Windows, bien que compatibles avec les anciens systèmes FAT et FAT32, savent tirer parti d'un format beaucoup plus élaboré : NTFS (New Technology File System). Outre les traditionnelles fonctionnalités offertes par ses ancêtres, NTFS prend en charge des fichiers et des partitions volumineux (nettement supérieurs à 2 To), peut restaurer la cohérence d'un système de fichiers en cas de défaillance (par exemple dû à une zone défectueuse sur le disque), permet d'associer des droits d'accès aux fichiers et aux dossiers, offre des fonctions de chiffrement, de gestion des quotas de disque et de compression, et dispose des fonctionnalités nécessaires pour héberger ActiveDirectory (l'annuaire LDAP façon Microsoft).

Vous le constatez vous-même, si l'on est un tant soit peu concerné par les problèmes de sécurité, le système NTFS est absolument inévitable.

Convertir une partition en NTFS

Si vous êtes doté d'un ordinateur récent, vous n'avez probablement pas à vous soucier de ce problème : les volumes des ordinateurs sont désormais formatés en NTFS directement en usine. Si vous n'avez pas cette chance, vous pouvez convertir votre partition FAT ou FAT32 en partition NTFS, si votre système d'exploitation le permet (autrement dit, si vous disposez de Windows 2000 au minimum). Dans ce cas, n'hésitez pas à effectuer une conversion NTFS, cette opération est très simple.

Pour convertir une partition FAT ou FAT32 en NTFS, vous devez d'abord accéder à la ligne de commande DOS. Cliquez pour cela sur *Démarrer*, puis sur *Exécuter* ; entrez `cmd` ou `command` dans le champ *Ouvrir* et appuyez sur *OK* (figure 2-2).

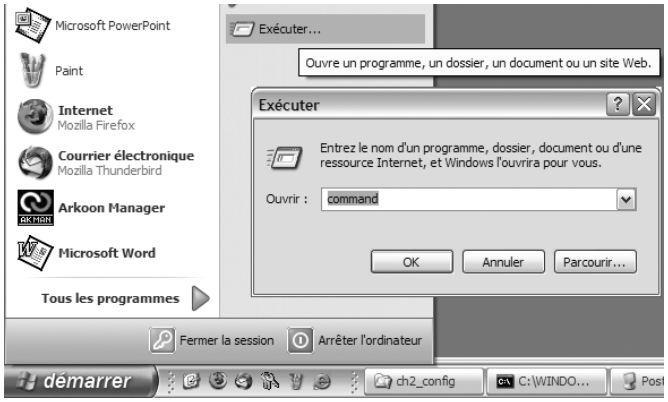


Figure 2–2
Passez d'abord en ligne de commande

HISTOIRE
Anciens formats de fichiers de Windows

Au cours de son histoire, Windows a utilisé trois formats différents, désignés chacun sous un nom un peu barbare : il s'agit des systèmes de fichiers FAT, FAT32 et, aujourd'hui, NTFS. La table d'allocation des fichiers (FAT : File Allocation Table) était à l'origine le système de fichiers employé par MS-DOS, ancêtre de Windows en ligne de commande. Assez rudimentaire, le système FAT gérait assez peu d'informations : principalement l'emplacement des fichiers sur le disque. Toutefois, ce qui est rudimentaire est efficace, et les versions ultérieures de Windows eurent longtemps recours au système FAT, et à sa variante FAT32, qui se distingue principalement par la prise en charge de volumes plus importants (2 To pour FAT32 au lieu de 4 Go pour FAT).
Aujourd'hui, le format NTFS, plus puissant et plus riche en fonctionnalités, a pris le relais.

CONSEIL **Sauvegarder avant tout**

La conversion en NTFS n'endommage pas vos fichiers. Cependant, pensez tout de même à effectuer une sauvegarde complète de vos données avant de lancer cette opération, on ne sait jamais.

L'opération de conversion s'effectue à l'aide de la commande `convert`. Cette dernière s'utilise très simplement. Si vous souhaitez par exemple convertir la partition `D:` en NTFS, il vous suffit de taper la commande :

```
CONVERT D: /FS:NTFS
```

Laissez le processus se dérouler normalement ; dès que celui-ci se termine, votre ancienne partition FAT ou FAT32 est désormais devenue une partition NTFS. Vous avez maintenant la possibilité de faire un usage sans retenue des fonctions de sécurité de Windows.

ATTENTION **Conversion NTFS irréversible**

Sachez que l'opération de conversion en NTFS est irréversible. Pour plus d'informations, n'hésitez pas à vous référer au centre d'aide et de support, accessible directement depuis le menu *Démarrer*.

AVANCÉ **Commande convert**

Vous pouvez visualiser les différents paramètres de cette fonction en lançant la commande `help convert` (figure 2-3).

Figure 2–3 Prenez le temps de comprendre le fonctionnement de la commande convert.

Formater une partition en NTFS

Si vous le souhaitez, au lieu de *convertir* la partition FAT ou FAT32, vous pouvez procéder à son *formatage* en NTFS. C'est ce que conseille Microsoft. Toutefois, cette opération est plus lourde car toutes les données de la partition seront perdues. Vous serez donc obligé de les restaurer à partir de votre copie de sauvegarde.

Insérez le disque d'installation de Windows dans le lecteur de CD-Rom et faites démarrer votre machine sur ce lecteur (appuyez sur la touche *F12* au démarrage et choisissez l'option adéquate). Ensuite, suivez les indications qui s'affichent.

Sécuriser le Registre

Le Registre est un élément essentiel au fonctionnement de Windows : il s'agit d'une base de données hiérarchique au sein de laquelle sont consignées toutes les informations de configuration de votre poste. Votre fond d'écran, vos mots de passe, la configuration du matériel et des applications installés, les réglages internes définis en usine par les développeurs des logiciels, les numéros de licence et de version des logiciels, tout se trouve dans le Registre. Toute opération portant sur la configuration de la machine se solde inéluctablement par une modification du Registre, lequel renferme en outre l'historique des opérations de configuration réalisées au fil du temps.

Risques encourus

Le Registre est donc un élément sensible. Toute manipulation hasardeuse peut nuire gravement au fonctionnement de Windows, et même, parfois, empêcher le démarrage de la machine.

Par conséquent, vous ne souhaitez probablement pas qu'un tiers vienne mettre son nez dans votre Registre. Hélas ! les pirates aguerris maîtrisent parfaitement les techniques d'édition de Registre à distance. Outre le risque de « plantage » complet de Windows, une modification bien pensée du Registre peut entraîner l'ouverture de canaux cachés ou l'installation de chevaux de Troie à votre insu. C'est tout de même gênant !

ATTENTION Une mauvaise manipulation conduit à la réinstallation du système

Nous avons vu au chapitre 1 comment se sortir de situations critiques avec le Registre. Cependant, lorsque des modifications ont entraîné une incohérence sérieuse, les tentatives de récupération ne parviennent pas forcément à reconstruire une situation saine. Dans ce cas, la seule solution consiste à ressortir les CD-Rom d'installation !

Modifier les permissions du Registre

Une mesure pour atténuer ce risque consiste à mieux maîtriser les permissions associées aux objets du Registre. Ouvrez pour cela l'éditeur de Registre (figure 2-4) : dans le menu *Démarrer*, cliquez sur *Exécuter*, puis tapez la commande `regedit`.

Figure 2–4
Accédez aux autorisations associées aux clés de Registre.

Regedit affiche cinq icônes de dossiers. Elles représentent des regroupements logiques d'informations de Registre nommés sous-arbres. Cliquez droit sur n'importe quel dossier et choisissez *Autorisations* (figure 2-5).

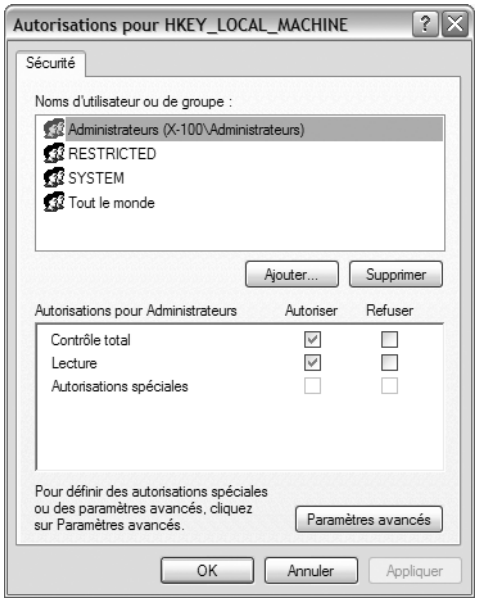


Figure 2–5
Par défaut, l'administrateur dispose d'un accès complet au Registre.

Vous constatez que, par défaut, l'administrateur dispose d'un accès complet au Registre (figure 2-5). A priori, cela semble naturel. Cependant, imaginez un instant que l'administrateur, ce soit vous : c'est en effet très souvent le cas sur les machines individuelles des utilisateurs à domicile ou encore, au sein des petites entreprises. Les processus que vous exécutez sont alors dotés des droits administrateur… C'est ici que les choses se gâtent ! Car, nous le verrons dès le chapitre suivant, une entité extérieure (un pirate, un virus) sachant exploiter une faille présente sur votre ordinateur, peut tout à fait lancer à distance un processus arbitraire sur votre machine. Si elle y parvient, ce processus aura bien entendu les droits administrateur ; et si, de surcroît, il est conçu pour venir modifier votre Registre, vous imaginez la suite...

CONSEIL **Vérifiez les droits du groupe « Tout le monde »**

Tous les utilisateurs disposent de droits d'accès plus ou moins étendus sur le Registre. Prenez soin d'adapter ces autorisations à la politique de sécurité que vous souhaitez effectivement mettre en place. Vérifiez notamment que le groupe *Tout le monde* n'a pas le contrôle total.

FONDAMENTAL **Travaillez avec un compte restreint**

Pour réduire significativement les risques d'intrusion sur votre machine, n'utilisez jamais au quotidien votre poste sous un compte doté des droits administrateur. Définissez plutôt un autre compte utilisateur (voir section suivante) auquel vous attribuerez des droits restreints ; veillez notamment à ce que ce compte ne puisse pas accéder au Registre en modification.

DANGER **Laissez vos programmes modifier les valeurs du Registre**

Attention, Regedit est un outil très puissant permettant de naviguer à l'intérieur du Registre et de modifier les valeurs des clés. À moins d'être absolument sûr de ce que vous faites, ne modifiez *jamais* vous-même une valeur située dans le Registre.

Restreindre l'accès aux applications

Nombreuses sont les raisons de vouloir limiter l'accès aux applications installées sur votre machine. Dans un commerce ou une petite entreprise, enregistrer une vente, établir les bulletins de salaire, documenter un produit, gérer les fonds ou rédiger des courriers sont autant de fonctions utilisant des logiciels distincts et concernant des personnes le plus souvent différentes. Il n'y a généralement aucune raison pour que tous les employés accèdent à tous les logiciels. Le particulier également peut souhaiter restreindre l'accès aux applications : interdire Internet aux enfants (contenus dangereux, téléchargement de fichiers porteurs de virus...), protéger les données de la curiosité et de la maladresse des petits, établir des « profils » d'utilisation de la machine (travail, jeux, gestion domestique...).

Créer un compte restreint

Définir un compte, rien n'est plus simple : avec Windows XP, sélectionnez *Démarrer>Panneau de configuration*, puis cliquez sur *Comptes d'utilisateurs* (figure 2-6).

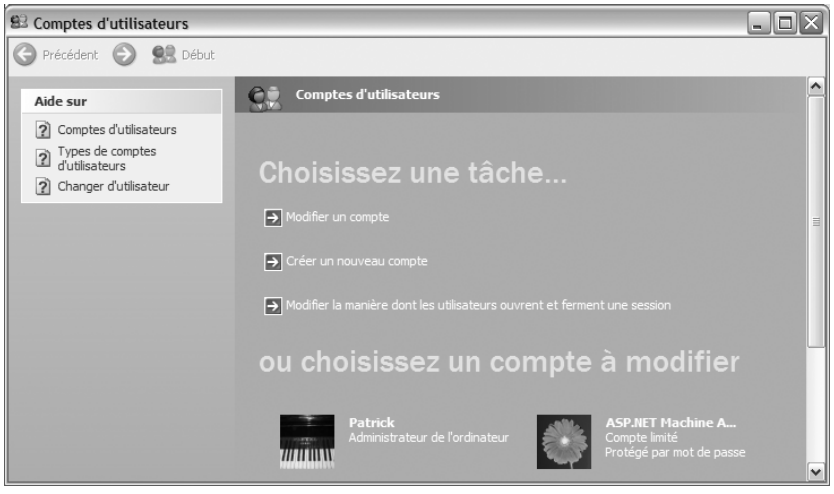


Figure 2–6
Pour un usage quotidien, créez un nouveau compte avec des droits limités.

Cliquez sur le lien *Créer un nouveau compte* et suivez les instructions. Les utilisateurs de XP édition familiale auront le choix entre deux types de comptes : les comptes *Administrateur de l'ordinateur* et les comptes *Limité* (figure 2-7).

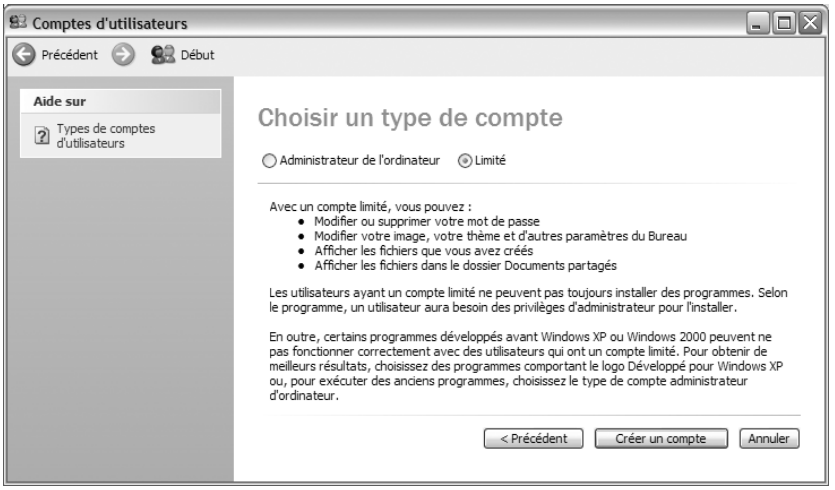


Figure 2–7
Avec un compte limité, vous travaillerez normalement, mais vous ne pourrez pas accéder à certaines fonctions d'administration.

Avec un compte limité, vous pouvez réaliser vos tâches quotidiennes (édition de documents, utilisation d'applications, accès à Internet, etc.). En revanche, il ne permet pas de modifier les paramètres du système ou d'installer des logiciels. Un cheval de Troie aura donc beaucoup plus de mal à s'installer sur votre machine. C'est un élément de sécurité supplémentaire.

Choisir les programmes accessibles par le menu Démarrer

Pour restreindre les accès aux applications, vous souhaitez peut-être regrouper les outils par profil métier, empêcher l'accès à des données sensibles, limiter des accès à des réseaux ou à Internet...

Pour ce faire, vous serez amené à personnaliser le menu *Démarrer* en définissant des applications communes à tous les utilisateurs et d'autres accessibles seulement par certains comptes :

1. Cliquez droit sur le menu *Démarrer* et choisissez l'option *Propriétés*.
2. Cochez l'option *Menu Démarrer classique*, cliquez sur *Personnaliser*, puis *Avancé*.
3. Une fenêtre de l'explorateur s'ouvre sur le dossier *Menu Démarrer* du compte Utilisateur en cours. Vous pouvez le déployer et visualiser le contenu de son sous-dossier *Programmes*.

PRATIQUE **Droits administrateur**

Des droits administrateur sont nécessaires pour réaliser cette opération.

Vous constaterez que si l'arborescence est similaire pour tous les comptes, il n'en est pas forcément de même pour les applications qu'elle contient.

4. Dans le dossier *Menu Démarrer\Programmes* de *All Users*, placez tous les programmes qui doivent être visibles de tous les comptes déclarés sur votre machine (traitement de texte, messagerie électronique...).
5. Dans le dossier *Menu Démarrer\Programmes* d'un compte particulier, placez tous les programmes spécifiques à ce compte.
6. Fermez l'explorateur et cliquez sur *OK*. Choisissez le style de votre menu *Démarrer* et cliquez à nouveau sur *OK*. Toute l'arborescence que vous avez définie est maintenant visible dans le menu *Démarrer*, option *Programmes* (menu *Démarrer* classique) ou *Tous les programmes* (menu *Démarrer XP*). Un compte lambda offre maintenant l'accès à la fois aux logiciels définis pour lui et à ceux autorisés pour tout le monde.
7. Vous pouvez également restreindre les éléments (connexions par exemple) présentés dans le menu *Démarrer XP* : clic droit sur *Démarrer>Propriétés>Menu Démarrer>Personnaliser>Avancé>Éléments du menu Démarrer*.

BON À SAVOIR

Comptes restreints à usage domestique

Le danger vient quelquefois de l'intérieur : vous avez peut-être de grands enfants curieux d'Internet et prompts à télécharger tout et n'importe quoi sans se soucier des conséquences. Pour les protéger et sécuriser votre ordinateur, créez-leur des comptes restreints dépourvus d'accès à Internet.

Protéger l'accès à votre machine

Définir un mot de passe utilisateur

La raison pour laquelle il faut protéger son compte avec un mot de passe peut sembler évidente : on ne souhaite pas forcément que d'autres personnes accèdent à notre espace de travail.

Cependant, si vous êtes le seul utilisateur de votre machine, pourquoi aller s'embêter avec un mot de passe ? Une raison très simple est que le mot de passe ne sert pas uniquement à contrôler l'accès logique à une machine. Tout pirate digne de ce nom est parfaitement capable de lancer un terminal distant sur la machine cible (c'est-à-dire une fenêtre virtuelle à partir de laquelle il travaille comme s'il était physiquement présent sur votre poste !) ou, plus simplement, de se connecter à un partage. Un poste sans mot de passe facilite considérablement l'infiltration à distance et, s'il est relié à un réseau d'ordinateurs, il devient le maillon faible à cause duquel le système informatique tombera (à commencer par les serveurs centraux).

N'offrez pas au pirate les clés de votre système de fichiers sur un plateau. Il faut au moins qu'il se fatigue un peu. Alors, protégez votre compte utilisateur avec un mot de passe !

Pour cela, retournez dans *Démarrer>Panneau de configuration>Comptes d'utilisateurs* (figure 2-6). Cliquez ensuite sur le compte à sécuriser, puis sur le lien *Créer un mot de passe* (figure 2-8).

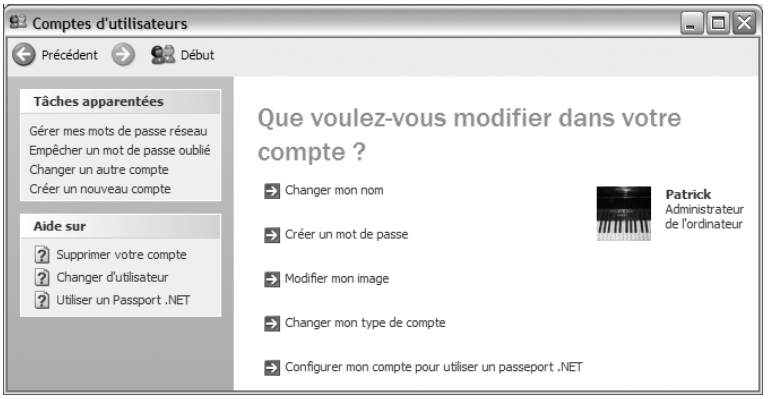


Figure 2–8
Accédez à la gestion des comptes d'utilisateurs pour assigner les mots de passe.

Saisissez un mot de passe robuste (voir plus loin ce qu'est un bon mot de passe). Votre compte est désormais mieux protégé. Vérifiez en outre que tous les autres comptes d'utilisateurs de votre machine soient également munis d'un mot de passe.

Fiabilité des mots de passe Windows

Jusqu'à Windows NT, les mécanismes d'encodage des mots de passe étaient tellement sommaires qu'il était possible à un professionnel de la sécurité de casser un mot de passe à coup sûr.

Attaque dite « du dictionnaire »

Par un moyen ou par un autre (ils sont nombreux !), le pirate subtilise le fichier des mots de passe chiffrés, qui se trouvent stockés sur la machine ou sur le serveur de domaine. Sur son propre réseau, composé de machines performantes dédiées à cette tâche, il déroule ensuite une procédure automatique qui consiste à encoder une liste très complète de mots usuels utilisés en tant que mots de passe.
C'est ce que l'on appelle le « dictionnaire ». Il s'agit en fait d'une suite de noms d'horizons très divers : les noms communs de la langue française et ses dérivés, les prénoms, les noms des personnages les plus obscurs de Star Wars, quelques noms d'oiseaux et autres interjections amicales, les surnoms du chien de la voisine, etc. Lorsqu'il finit par tomber sur une valeur chiffrée qui se trouve à l'intérieur du fichier dérobé, le pirate a gagné.
Avec un peu de chance, les mots de passe d'utilisateurs tombent pour la plupart dans l'heure. N'oublions pas qu'il ne faut pas plus de quelques secondes pour tester 100 000 mots !

DIFFÉRENCE **Hacker ou cracker ?**

Un *hacker* est un spécialiste en informatique qui utilise ses connaissances en sécurité, programmation ou administration de système pour détourner une machine ou un programme de sa fonction initiale. Lorsque ses connaissances sont utilisées à des fins malhonnêtes, il devient un *cracker*, c'est-à-dire un pirate.

Avec les versions plus récentes de Windows, c'est un peu plus difficile. Il est possible de définir des mots de passe plus longs et plus complexes. Pour faire barrage aux utilisateurs un peu trop curieux et à la plupart des pirates, l'utilisateur doit choisir un mot de passe robuste ; sinon, il

s'expose à l'attaque bien connue, dite « du dictionnaire ». Toutefois, les mécanismes d'encodage ne sont pas fiables à cent pour cent et mieux vaut partir du principe que, sans autre mécanisme de protection, un *hacker* professionnel motivé parviendra à entrer dans votre système.

Choisir un mot de passe robuste

Pour que votre mot de passe ait de bonnes chances de résister aux algorithmes classiques de craquage, il doit être composé de :

- lettres majuscules et minuscules, symboles et chiffres, pour vous mettre à l'abri des attaques triviales par dictionnaire ;
- au minimum 8 caractères. En effet, en faisant l'hypothèse que les utilisateurs n'emploieront généralement pas plus de 100 valeurs différentes pour un caractère (26 lettres majuscules, 26 lettres minuscules, 10 chiffres, une quarantaine de symboles), une recherche exhaustive sur 7 caractères représente 100^7 combinaisons possibles. Les algorithmes habilement conçus y parviennent encore. Avec 8 caractères (100^8 combinaisons), cela devient plus compliqué. Et 9 caractères ou plus, c'est encore mieux !

Voici l'exemple d'un mot de passe robuste : 2-Mq*#mES… à condition de ne pas l'écrire sur un post-it ! Et même si cela est moins passionnant que du Marivaux, apprendre par cœur ce genre de texte est très bon pour la mémoire.

CONSEIL Aidez-vous d'une phrase

Une phrase est plus facile à retenir qu'une succession de sigles. Choisissez-en une qui n'ait du sens que pour vous et qui contienne quelques noms propres et des valeurs transformables en chiffres :

- gardez uniquement les initiales, en respectant les majuscules et minuscules ;
- remplacez les lettres « o » par des chiffres « 0 » ou le contraire ;
- remplacez les « et » par des « é » et les « deux » ou « de » par des « 2 » ;
- changez certains caractères particuliers du français par les signes correspondants sur le clavier :« 2 » pour « é », « 7 » pour « è », « 9 » pour « ç », « 0 » pour « à » et « % » pour « ù » ;
- usez d'autres tours de passe-passe pour insérer des caractères tels que « % * $ »…

Ainsi, une phrase comme « Offenbach et Mozart usaient de dièses et de bémols » deviendrait : « 02Mu2#é2b ».

Protéger votre machine lorsque vous vous absentez : écran de veille et mot de passe

Il arrive souvent que l'on soit obligé d'interrompre momentanément un travail et l'on ne souhaite pas forcément perdre le fil en fermant les applications et les documents ouverts. Par ailleurs, il est souhaitable de décourager les indiscrets trop heureux de profiter de cette aubaine pour accéder à votre session, lire vos documents, espionner votre activité, voire commettre des dégats pénalisants dans vos données.

Il existe un moyen très simple pour conserver, pendant les moments d'absence, les documents ouverts sur son poste tout en tenant les curieux à distance : activer le mode veille et protéger la sortie de veille avec un mot de passe.

Affichez pour cela l'onglet *Écran de veille* de la fenêtre *Propriétés de Affichage* :

- cliquez droit sur un espace vide du Bureau et sélectionnez *Propriétés* ;
- ou rendez-vous dans le menu *Démarrer>Panneau de configuration> Affichage*.

ASTUCE Afficher le Bureau

Vous pouvez bien sûr choisir d'« icônifier » une à une les fenêtres de vos applications. Plus simplement, il suffit de cliquer sur l'icône *Bureau* située dans la barre de lancement rapide (figure 2-9).

Figure 2–9 Cliquez sur l'icône Bureau dans la barre de lancement rapide.

Figure 2–10
Protégez la sortie de veille avec un mot de passe.

Il vous suffit de sélectionner un écran dans la liste déroulante *Écrans de veille*, puis de régler le délai correspondant (figure 2-10). Pour forcer la saisie du mot de passe en sortie de veille, cochez la case *À la reprise, afficher l'écran d'accueil* ou *À la reprise, protéger par mot de passe*, selon votre version de Windows, puis sur *OK*.

Faites l'expérience vous-même : laissez votre poste entrer en mode veille ou cliquez sur le bouton *Aperçu*. Appuyez ensuite sur n'importe quelle touche ou bougez la souris : vous voyez apparaître l'écran d'accueil et vous devez alors cliquer sur un nom d'utilisateur (figure 2-11), puis saisir son mot de passe. C'est un peu contraignant, certes, mais si vous n'avez pas entièrement confiance en votre environnement, cette petite protection sera salutaire. N'oubliez pas que la fameuse « attaque du déjeuner » (la « lunch time attack ») est très connue des espions et réputée pour son efficacité !

ASTUCE À la maison aussi, protégez vos données !

Adoptez la mise en veille protégée par mot de passe également sur votre ordinateur familial. De cette façon, votre petit dernier ne pourra pas « saboter » vos feuilles Excel de tenue de compte bancaire et les plus grands ne profiteront pas de votre connexion Internet.

B.A. - BA La mise en veille ne doit être que temporaire

La mise en veille est très pratique, mais elle doit toujours être envisagée de façon temporaire. Ne laissez jamais vos documents ouverts pendant plusieurs jours et subir ainsi le joug de mises en veille et de reprises successives. Sur le long terme, pensez régulièrement à fermer proprement vos documents pour ne pas les altérer.

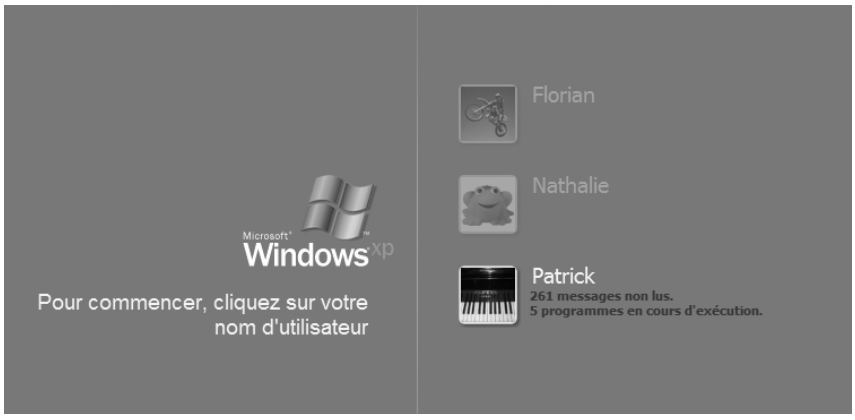


Figure 2–11
À la reprise, vous repassez par l'écran d'accueil et vous êtes obligé de saisir un mot de passe.

BONNE PRATIQUE **Restez vigilant lorsque vous saisissez votre mot de passe.**

Il existe tout de même un effet pervers à la saisie du mot de passe en sortie de veille : vous saisissez votre mot de passe beaucoup plus souvent et vous vous exposez par conséquent plus au risque qu'on vous le vole. Combien de fois avez-vous vu des collègues taper leur mot de passe sous vos yeux ? Même s'il est difficile de mémoriser une séquence complète de caractères saisis au vol, trois ou quatre caractères dans le désordre suffisent pour restreindre considérablement le champ d'une recherche exhaustive et obtenir le mot de passe, à coup sûr et en très peu de temps. En environnement sensible, assurez-vous de ne pas être observé et changez votre mot de passe régulièrement.

Partager des informations sur un réseau

Avec Windows, l'accès à certains dossiers stockés sur un ordinateur peut être ouvert à plusieurs autres ordinateurs reliés en réseau. Ces dossiers particuliers sont appellés des *dossiers partagés* ou, plus communément, des *partages*. Un dossier partagé est reconnaissable à son icône représentant un dossier tendu sur une main (voir figure 2-12).

Le partage est un concept absolument formidable : selon les droits qui lui sont alloués, les utilisateurs peuvent en lire, copier ou modifier les fichiers à partir de leurs machines respectives. Vu de l'utilisateur distant, le partage est perçu exactement comme une arborescence située physiquement sur sa propre machine. Grâce au partage, plusieurs personnes peuvent travailler ensemble sur des répertoires répartis sur diverses machines du réseau, exactement comme si l'ensemble de ces répertoires était physiquement localisé sur la machine de chaque utilisateur. C'est très pratique !

Néanmoins, ce que l'on gagne en convivialité est perdu en sécurité. Un partage est une ouverture légalisée dans votre système de fichiers. C'est pourquoi il faut être vigilant et vous assurer que tous les partages actifs correspondent bien à vos besoins. De plus, il faut maîtriser la sécurité de chaque partage.

Visualiser les partages présents sur votre ordinateur

Dans le menu *Démarrer*, cliquez droit sur *Poste de travail*, puis sélectionnez *Gérer* dans le menu déroulant. Ouvrez les arborescences et *Outils système\Dossiers partagés*, puis cliquez sur *Partages*. (figure 2-13).

À RETENIR **Faut-il protéger les feuilles Excel ou les documents Word avec un mot de passe ?**

À vrai dire, non. Pour être franc, certaines versions de ces logiciels – en particulier les versions françaises – stockent le mot de passe en clair dans le document. Le pirate, muni de l'outil adéquat (il en existe un bon nombre sur Internet), saura le retrouver en quelques nanosecondes.
Si vraiment votre document est sensible, la meilleure solution consiste à le chiffrer. Nous abordons ce sujet plus loin dans ce chapitre.

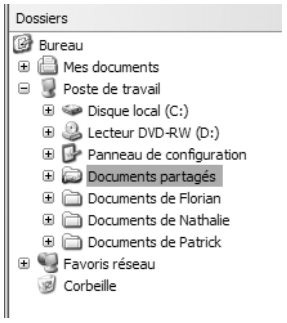


Figure 2–12
Un partage est reconnaissable à son icône.

BONNE PRATIQUE **Vérifiez vos partages**

De temps à autre, consultez cet écran et vérifiez que les partages actifs correspondent bien à des répertoires ou des lecteurs que vous souhaitez effectivement partager (on a vite fait d'oublier un ancien partage dont on n'a plus besoin !).

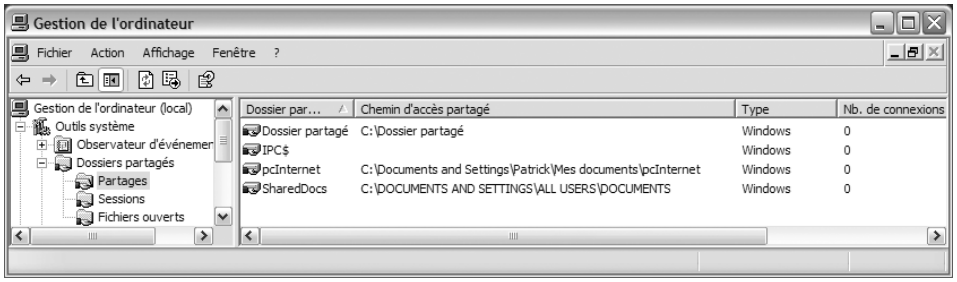


Figure 2–13
Visualisez les dossiers partagés présents sur votre poste.

Régler les autorisations d'un partage

Commencez d'abord par définir un partage. Dans l'Explorateur Windows, cliquez droit sur le dossier que vous désirez rendre disponible sur le réseau, puis sélectionnez l'option *Partage et sécurité* qui apparaît dans le menu contextuel (figure 2-14).

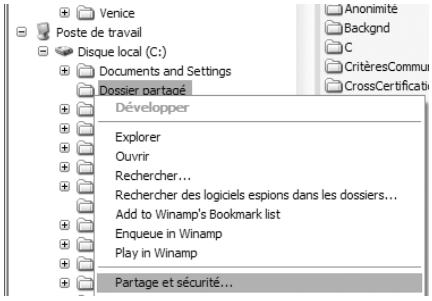


Figure 2–14
Définir un partage

Cochez la case *Partager ce dossier sur le réseau* (figure 2-15). Dans notre exemple, le dossier sera partagé sous le nom `Dossier partagé`.

ATTENTION Noms de fichiers longs

Lorsque vous définissez les noms de partage, sachez que les systèmes d'exploitation antérieurs à Windows 98 ne savent pas gérer les noms dépassant huit caractères. Aussi, si de tels clients sont raccordés à votre réseau, pensez à choisir un nom adéquat (PARTAGE par exemple).

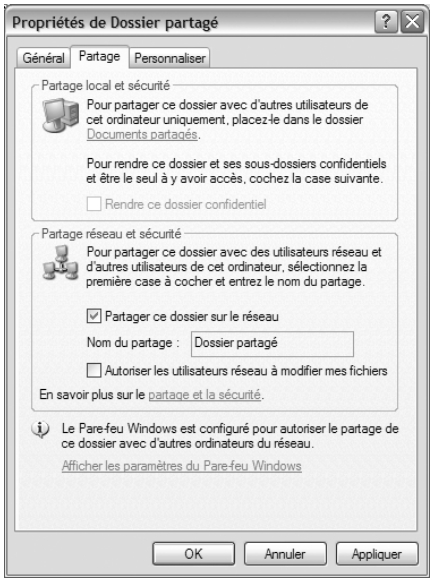


Figure 2–15
Définissez un partage et attribuez-lui un niveau de sécurité ad hoc.

Par défaut, Windows XP édition familiale n'active pas la case à cocher *Autoriser les utilisateurs à modifier mes fichiers*. Dans cette configuration, les utilisateurs du réseau peuvent uniquement lire le contenu de ce dossier.

Si, au contraire, vous souhaitez autoriser les utilisateurs à lire, copier ou modifier les fichiers contenus dans votre dossier partagé, cochez cette case. Cliquez ensuite sur *OK*.

Mettre fin au partage d'un dossier

À partir de l'Explorateur, affichez la page des propriétés du dossier comme vu précédemment, puis, sous l'onglet *Partage* (figure 2-15), désactivez simplement la case à cocher *Partager ce dossier sur le réseau*.

Partages « fantômes »

Voilà un sujet dont les pirates raffolent : les partages masqués ouverts par Windows de son propre chef, sans même vous en informer !

Oui, vous avez bien lu ! Windows met en œuvre une suite de protocoles absolument fantastiques en matière de communication, et qui profitent outrageusement aux pirates lorsqu'ils infiltrent vos machines. Il s'agit de la suite NetBIOS, et plus particulièrement de NBNS (NetBIOS Name Service sur le port UDP 137), NetBIOS Session Service (sur le port TCP 139), ou SMB (Server Message Block sur les ports TCP 139 et 445).

Retenez que des ressources administratives partagées sont présentes sur votre machine (`IPC$`, `C$`, ou `Admin$`, voir figure 2-13) et qu'un pirate peut immédiatement s'y connecter, sans authentification préalable. C'est ce que l'on appelle dans le jargon des connexions nulles.

Il est donc impératif de désactiver les services SMB, au moins sur les cartes raccordées aux réseaux non sûrs (connexion Internet par exemple). Il est possible de bloquer ce protocole au niveau d'un pare-feu, ce que nous examinerons au chapitre 5, mais vous pouvez aussi utiliser les fonctions de Windows pour restreindre l'accès à ces services dangereux.

Il faut pour cela que vous accédiez aux propriétés de votre interface réseau. Dans le menu *Démarrer*, sélectionnez *Connexions* et la connexion à configurer. Dans la fenêtre qui apparaît, cliquez sur le bouton *Propriétés*, puis sur l'onglet *Gestion de réseau*.

Le partage de fichiers et d'imprimantes s'effectue à travers NetBIOS. Veillez donc à ce que la case à cocher correspondante soit désactivée (figure 2-16).

RENVOI **Intrusions basées sur NetBIOS**

Une partie du chapitre 4 sera consacrée aux techniques d'intrusion basées sur NetBIOS. Nous expliquerons notamment comment les pirates procèdent pour investir des machines et des réseaux entiers en se servant des informations collectées grâce à des protocoles aussi bavards. N'hésitez pas à vous reporter à ce chapitre pour de plus amples détails.

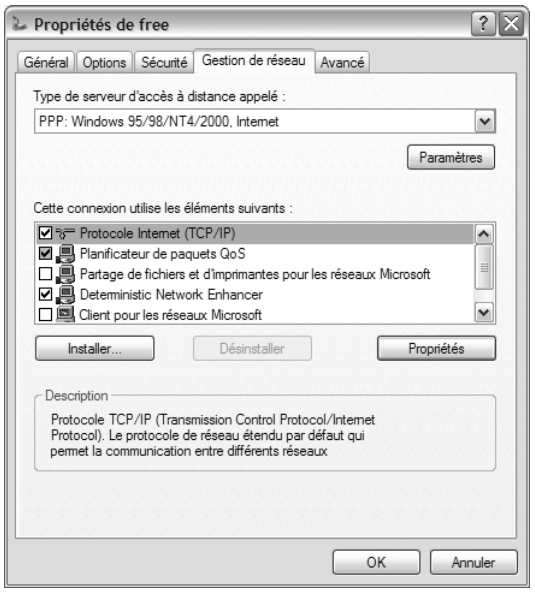


Figure 2–16
Désactivez le partage de fichiers et d'imprimantes.

Ensuite, après avoir sélectionné *Protocole Internet (TCP/IP)*, cliquez sur le bouton *Propriétés*, puis, dans la fenêtre suivante, sur le bouton *Avancé*, et enfin sur l'onglet *WINS* (figure 2-17). Vérifiez bien que NetBIOS avec TCP/IP est bien désactivé pour cette carte réseau. Sinon, cochez la case correspondante.

Figure 2–17
Désactivez les services NetBIOS pour cette interface.

Petites mesures anodines…

À l'heure où préserver sa vie privée est devenu un sujet en vogue, notons que Windows n'est pas toujours d'une discrétion absolue. Le système d'exploitation et certaines applications conservent en mémoire l'historique de vos actions : les documents sur lesquels vous avez travaillé récemment, les sites web visités, les programmes utilisés, etc. C'est très pratique pour l'utilisateur, car, au lieu d'effectuer tous les jours la recherche fastidieuse des mêmes documents sur le disque, il peut les ouvrir très simplement en deux clics de souris à partir du menu *Démarrer*.

Dans l'absolu, tout cela est très bien, sauf si vous travaillez dans un contexte peu amical (un collègue veut votre poste, votre chef veut se débarrasser de vous…) : avec de tels indicateurs, un œil indiscret dispose d'une batterie d'éléments pour espionner votre activité sur votre ordinateur. Si cela vous déplaît, sachez qu'il est très facile de supprimer quelques mouchards et de renvoyer les inopportuns dans leurs pénates.

Vider la liste Mes documents récents

Cliquez par exemple sur le menu *Démarrer* et pointez sur *Mes documents récents* ; vous verrez s'afficher la liste des quinze derniers documents avec lesquels vous avez travaillé. Il suffit de cliquer sur ces liens pour accéder directement aux documents qui correspondent. Avouons-le, cela simplifie considérablement la vie.

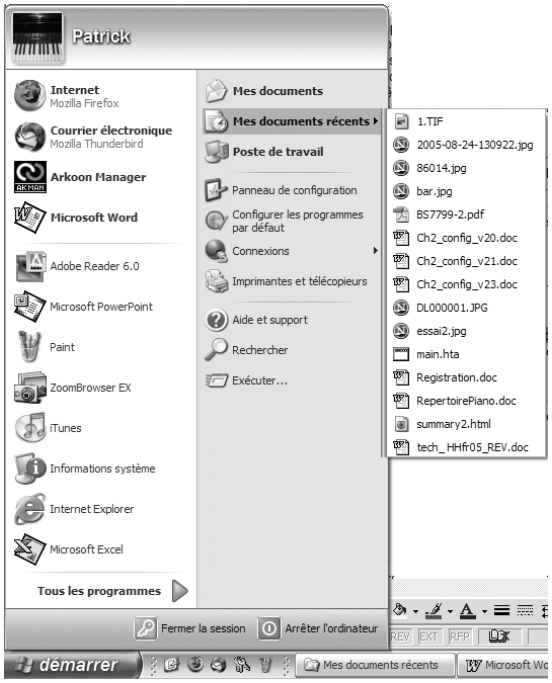


Figure 2–18
La liste des quinze derniers documents ouverts

À RETENIR Le dossier Mes documents récents est un véritable mouchard !

Allez vous promener dans le répertoire `C:\Documents and Settings\`*`nom_utilisateur`*`\Mes documents récents`. Vous constaterez que la modeste liste affichée à la figure 2-18 n'est que la partie émergée de l'iceberg ! Tous les documents que vous avez ouverts depuis des mois apparaissent, avec leur date, et peuvent être immédiatement ouverts en cliquant deux fois sur le raccourci. Vous êtes suivi à la trace !

Le problème est qu'il s'agit aussi d'un beau mouchard ! Si vous recherchez la discrétion, une mesure immédiate et simple consiste à désactiver l'affichage de la liste *Mes documents récents*. Pour cela, cliquez droit à partir du menu *Démarrer* et choisissez *Propriétés*. Choisissez ensuite l'onglet *Menu Démarrer* et cliquez sur le bouton *Personnaliser*. Dans l'onglet *Avancé*, désactivez simplement la case à cocher *Afficher les documents ouverts récemment* et l'élément *Mes documents récents* n'apparaîtra plus dans le menu *Démarrer* (figure 2-19).

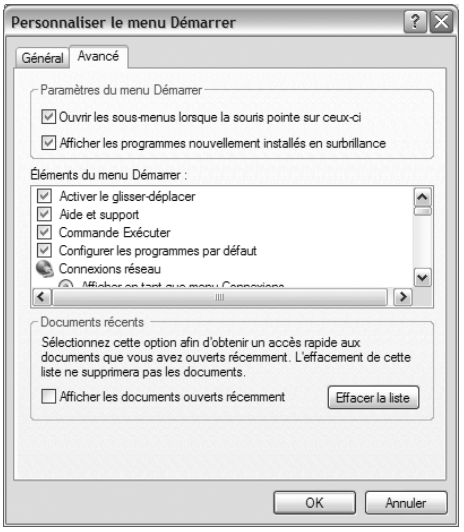


Figure 2–19
Désactivez l'affichage des documents récents.

Bien entendu, cette mesure n'arrêtera que le néophyte, ce qui est peut-être suffisant si votre entourage ne connaît pas bien Windows. Toutefois, la liste complète se trouve toujours dans `C:\Documents and Settings\`*`nom_utilisateur`*`\Mes documents récents`. Pour plus de sûreté, il vous est possible de vider complètement cette liste : il suffit de cliquer sur le bouton *Effacer la liste*, qui apparaît à la figure 2-19.

Évidemment, cette liste se remplira de nouveau à mesure que vous utiliserez votre ordinateur. À terme, le problème reste entier, à moins de la vider régulièrement, ce qui est contraignant.

Si vous vous sentez l'âme vaillante, offrez-vous une expérience audacieuse : configurez directement un paramètre du Registre qui obligerera Windows à nettoyer la liste *Mes documents récents* automatiquement à la fermeture du système. Dans le menu *Démarrer*, sélectionnez *Exécuter*, puis tapez la commande `regedit` qui vous ouvre l'éditeur du Registre. Parcourez l'arborescence et affichez la clé `HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Policies/Explorer`.

RAPPEL Sauvegardez le Registre avant toute manipulation

Attention, toute manipulation du Registre est potentiellement dangereuse. Prenez soin de disposer d'une sauvegarde avant d'envisager toute modification.

Ajoutez une nouvelle clé `ClearRecentDocsOnExit` à laquelle vous donnerez la valeur 1. Cliquez sur *OK*, puis fermez Regedit. La liste *Mes documents récents* cessera désormais de vous trahir.

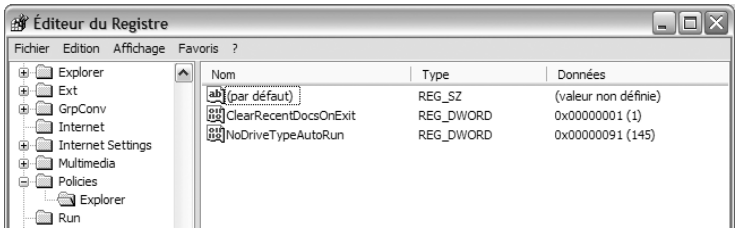


Figure 2–20
Nettoyez automatiquement la liste Mes Documents récents à la fermeture de Windows.

Vider les historiques et paramètres sensibles du navigateur

Votre navigateur est une mine d'informations pour vous, mais aussi pour l'espion ; mine plutôt explosive, si vous n'êtes pas assez vigilant. Avec Firefox par exemple, allez faire un tour dans le menu *Aller à>Historique* et prenez soin de développer l'arborescence à gauche de l'écran (figure 2-21).

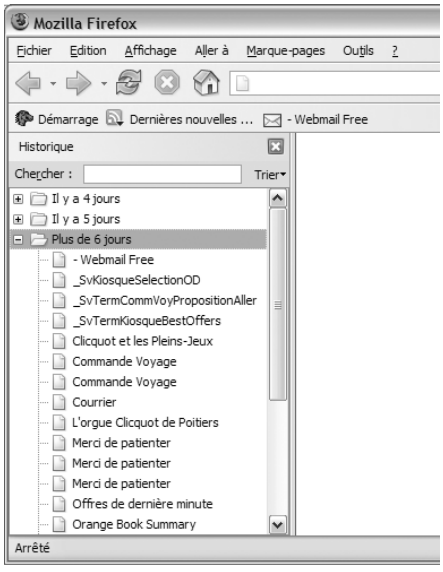


Figure 2–21
Le navigateur conserve l'historique des sites visités.

Tous les sites consultés récemment restent mémorisés au sein du navigateur. Espérons pour vous qu'ils soient fréquentables, sinon cela pourrait se savoir !

Mieux, allez dans *Outils>Options>Vie privée* (figure 2-22). Prenez soin de parcourir chacun des éléments et voyez comme il est facile d'afficher (en

clair, s'il vous plaît !) les mots de passe des sites que vous avez mémorisés. Cliquez vite sur l'option *Modifier le mot de passe principal* pour bloquer l'accès à ces précieux sésames.

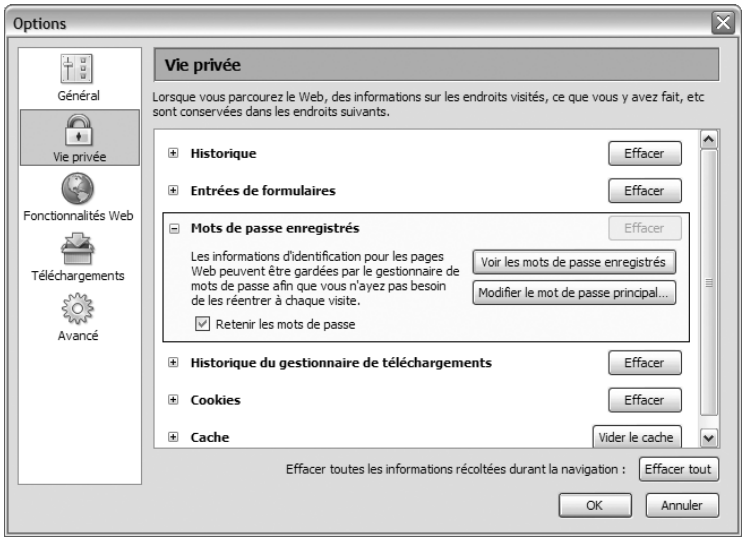


Figure 2–22
Le navigateur conserve en mémoire – en clair ! – les mots de passe des sites sécurisés.

Dans le cas où l'historique des URL visitées n'aurait pas été assez éloquent, offrez-vous le luxe de visualiser les pages stockées dans le cache, dont la taille peut être conséquente (figure 2-23).

Figure 2–23
Videz le cache, voire effacez toutes les informations récoltées durant la navigation.

Tous ces paramètres ont été pensés pour rendre la navigation plus aisée et plus rapide. Néanmoins, si la discrétion est un souci pour vous, n'hésitez pas à faire le ménage. Chaque élément vous propose un bouton *Effacer*, mais le bouton *Effacer tout* vous permet de faire cette opération en une fois (figure 2-24).

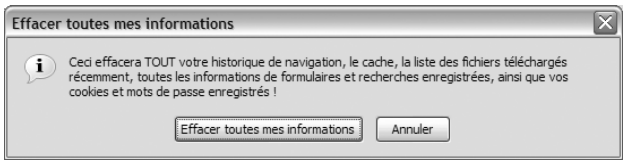


Figure 2–24
Tous les historiques seront effacés.

FIREFOX Effacer ses traces

- *Outils>Effacer mes traces...* ou *Ctrl + Maj + Suppr*
- Pour configurer l'effacement automatique : *Outils>Option>Vie privé*

De la même façon, sous Internet Explorer, rendez-vous dans le menu *Outils>Options Internet>Saisie semi-automatique* et cliquez sur *Effacer les formulaires* et *Effacer les mots de passe*.

Rendre les fichiers « invisibles »

Pas vu, pas pris. Vous disposez d'une petite mesure pour jouer un vilain tour aux fouineurs peu perspicaces : le fichier invisible.

Pour rendre un fichier invisible, il n'est pas nécessairre de sortir votre baguette magique : ouvrez simplement votre Explorateur, cliquez droit sur le fichier en question et choisissez *Propriétés* (figure 2-25).

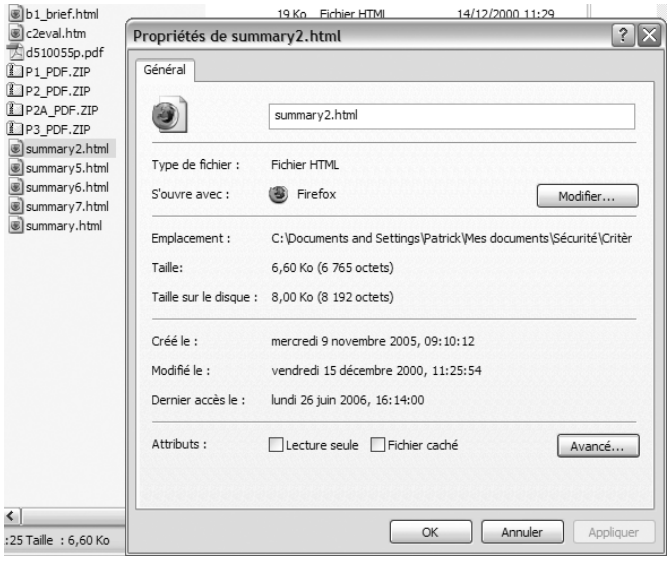


Figure 2–25
Notez l'attribut « Fichier caché »

Vous disposez d'une option *Fichier caché*. Si vous cochez cette case, le fichier n'apparaîtra plus dans l'arborescence et pourra échapper au regard indiscret.

Bien entendu, pour que le subterfuge fonctionne, il faut avoir réglé l'affichage des dossiers afin que Windows se garde bien d'afficher les éléments cachés. Dans l'Explorateur, choisissez le menu *Outils>Option des dossiers*, puis l'onglet *Affichage*. Cliquez sur le bouton radio *Ne pas afficher les fichiers et dossiers cachés* (figure 2-27).

ASTUCE Désactivez la barre d'état

Vous pouvez appliquer l'attribut *Fichier caché* à tout un dossier. Toutefois, si vous envisagez de recourir à ce genre de mesure, pensez à désactiver l'affichage de la barre d'état (dans l'Explorateur, menu *Affichage>Barre d'état*), sinon la protection risque d'être quelque peu illusoire (figure 2-26) !

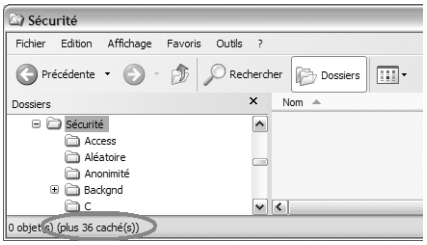


Figure 2–26 Pensez à désactiver l'affichage de la barre d'état !

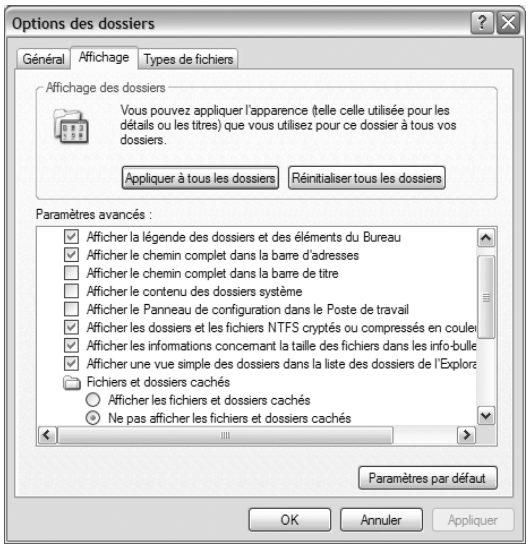


Figure 2–27
Désactivez l'affichage des dossiers cachés.

Le plus : préserver la confidentialité des fichiers par chiffrement

Comme nous venons de le voir, il existe des mesures simples pour restreindre l'accès des utilisateurs à certains fichiers sensibles (contrôle d'accès Windows, fichiers cachés, mots de passe, etc.). Cependant, les dispositifs de protection mis en œuvre sont souvent de très faible niveau et ne résistent pas à un informaticien ou un pirate un peu expérimenté.

La seule façon de préserver sérieusement la confidentialité d'un fichier sensible consiste à recourir à la cryptologie. Il s'agit d'une technique puissante qui ne s'utilise pas n'importe comment : il faut faire usage des services cryptologiques avec beaucoup de prudence et beaucoup de rigueur, sinon la sécurité effective du système risque d'en pâtir douloureusement. Nous analyserons au cours de cette section quelques éléments relatifs à la mise en œuvre de tels services pour sécuriser l'information.

Chiffrer une information

On appelle « chiffrement » le processus de transformation d'un message (le texte clair) visant à le rendre incompréhensible à toute personne non autorisée. Le résultat de cette opération est appelé « texte chiffré », ou « cryptogramme ».

VOCABULAIRE Chiffrer, crypter, coder ?

Vous trouverez parfois les verbes « crypter » et « coder » au lieu de « chiffrer ». Ils ont des sens proches, mais sont souvent contestés. Nous n'utiliserons que les termes « chiffrer », « déchiffrer », « chiffrement », « déchiffrement » et « décryptement » dans cet ouvrage.

HISTOIRE **Diverses formes de clés**

La clé de déchiffrement a pris des formes tout à fait diverses (et poétiques) au cours des âges. Il y eut par exemple la scytale, à l'époque des Lacédémoniens (V^{ème} siècle avant J.C.), un bâton autour duquel on enroulait de façon jointive un bandeau de parchemin. On écrivait ensuite le message secret sur la surface ainsi reconstituée. Une fois déroulé, le bandeau affichait une succession de lettres ou de signes, apparemment sans signification logique. Seul le destinataire, en possession d'une scytale de même diamètre, pouvait accéder au contenu du message.

Certes, un tel procédé est très facilement attaquable, comme tous les mécanismes employés en ces temps anciens, tel le fameux « chiffre de César ». La puissance de calcul phénoménale acquise grâce à l'informatique a considérablement durci ces techniques, mais, en contrepartie, la clé du XXI^{ème} siècle a perdu un peu de son charme ; il ne s'agit plus désormais que d'une banale, ennuyeuse et interminable suite aléatoire de zéros et de uns.

Figure 2–28 Une scytale

HISTOIRE **La cryptologie au cours des âges**

Pour mémoire, la cryptologie est une science presque aussi vieille que le monde. Très tôt, les militaires et les corps diplomatiques eurent recours à ces techniques pour protéger les communications gouvernementales. Citons entre autres :

- la nomenclature de Marie Stuart, sorte de mécanisme par substitution monoalphabétique dont le manque de robustesse entraîna la perte ;
- le chiffre ADFGVX, basé sur les principes de substitution et de transposition alphabétiques, et utilisé au cours la première Guerre Mondiale (figure 2-29) ;
- le chiffre par substitution polyalphabétique de Vigenère, dont l'une des plus brillantes réalisations fut la machine Enigma, conçue par les Allemands à la veille de la seconde Guerre Mondiale.

Les journalistes se sont aussi beaucoup servi de la cryptologie. Et les amoureux, quant à eux, se sont toujours refusés à négliger une technique aussi précieuse, dont les mystérieuses transformations jetaient un voile pudique sur des communications compromettantes et évitaient de bien fâcheuses situations. Le *Kàma-sùtra*, texte fondé sur des manuscrits du IV^{ème} siècle avant J.-C., recommandait notamment aux femmes l'utilisation du *mlecchita-vikalpà*, l'art de l'écriture secrète, afin de dissimuler leurs liaisons ! Néanmoins, des scandales croustillants, témoignages des frasques de nos Rois, nous rappellent à quel point l'exercice de la cryptologie est un art difficile !

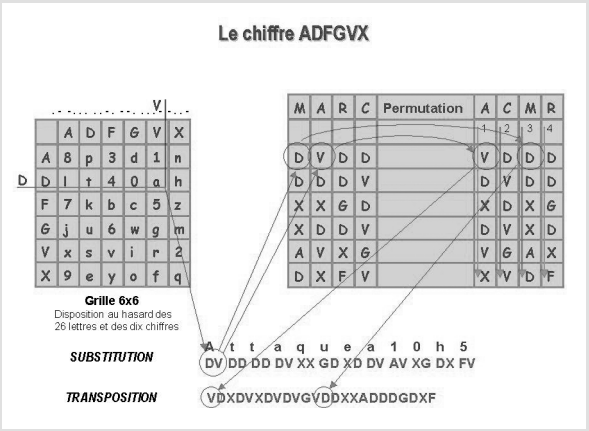


Figure 2–29 Un exemple de chiffre ancien : le chiffre ADFGVX

Bien entendu, un tel processus est réversible, sinon il ne présenterait pas grand intérêt. Cependant, pour reconstruire le texte clair à partir du texte chiffré, il faut faire appel à un élément secret (une clé), que possède seule la personne autorisée à lire cette information.

On appelle « déchiffrement » le processus consistant à retrouver le texte clair à partir du texte chiffré et de la clé. Le processus qui consiste à casser un chiffre afin de reconstruire le texte clair sans connaître la clé, s'appelle le « décryptement ».

Les cryptologues ont coutume de penser qu'il existe deux types de cryptologie : celle qui protège de sa petite sœur, et celle qui protège des principaux gouvernements. L'Histoire le montre : la cryptologie a tou-

RENVOI
Fiabilité des solutions de chiffrement

Nous reviendrons plus en détail sur ce sujet, lorsque nous aborderons la sécurisation de la messagerie et le problème des transactions électroniques sur Internet (chapitres 8 et 9).

jours été considérée comme une arme de guerre, une science exclusivement destinée aux militaires, aux diplomates et aux services de renseignements, afin de préserver le secret des communications gouvernementales et garder le pouvoir sur l'information. Bien comprendre la cryptologie commence par le fait d'admettre que ce principe reste toujours vrai. Cela vous donne-t-il une vague idée de la fiabilité des solutions de chiffrement présentes dans vos machines ?

Chiffrer des fichiers sur son ordinateur

Vous l'avez compris : si vous cherchez à dissimuler des informations importantes aux services de police ou aux agences de renseignements, vous en serez pour vos frais. Apprenez plutôt le navajo, inventez un langage de toutes pièces (complexe, de préférence), ou payez très cher un expert de génie qui vous développera un chiffre robuste sur mesure (ce qui est parfaitement interdit par la loi française, mais, que voulez-vous, la réglementation en matière de cryptologie sur Internet ne gêne que les honnêtes gens…).

Pourquoi chiffrer des documents ? La réponse à cette question est hautement subjective et dépend du contexte dans lequel vous évoluez.

Si vous n'avez rien à cacher, chiffrer des fichiers, voire des partitions, vous soumet au risque de perdre la clé (oubli du mot de passe, sauvegarde égarée, support défaillant...), ce qui confèrerait à vos fichiers le niveau de sécurité absolu... et définitif ! Ces données que vous voulez protéger courent le risque d'être définitivement perdues.

Toutefois, il arrive que la protection de données confidentielles sur un poste de travail soit une réelle nécessité. L'exemple flagrant est celui de l'homme d'affaires en déplacement : sorti du cocon protecteur de l'entreprise, un poste nomade devient excessivement vulnérable ; nous verrons dans les prochains chapitres comment il devient la cible privilégiée du piratage par Wi-Fi ou Bluetooth, lorsqu'il ne disparaît pas purement et simplement dans la chambre d'hôtel, à la suite de la visite discrète et impromptue du concurrent…

Pour les entreprises qui ne souhaitent pas forcément consacrer un budget conséquent à la sécurité, il y a tout à fait moyen d'assurer un très bon niveau de protection sans dépenser des sommes folles. Tout d'abord, il faut partir du principe que le poste nomade ne doit pas héberger de données confidentielles « long terme », comme des éléments de comptabilité, des rapports d'audit effectués sur les clients ou toute autre donnée stratégique dont on n'a pas un besoin immédiat. Toutes ces données doivent être conservées en clair sur des postes fixes reliés au réseau sécurisé de l'entreprise, séparé éventuellement du réseau d'accès à Internet. Si des

données confidentielles doivent néanmoins être présentes sur le poste nomade, par exemple dans le cadre de la préparation à une réunion, il existe des solutions de chiffrement « à la hussarde » qui, sous réserve d'une utilisation rigoureuse, offrent une réelle protection contre les risques de divulgation.

Attention cependant ! Si une protection élevée avec des outils gratuits est tout à fait envisageable, il faut prendre en charge de façon rigoureuse la gestion de vos secrets et de vos fichiers sensibles. Il faut notamment respecter quelques règles de bon sens :

- Si des données confidentielles doivent être stockées de façon chiffrée sur l'ordinateur, cela ne peut être que temporaire. Dès le retour à l'entreprise, il faut rebasculer ces données sur les postes protégés et les supprimer du poste nomade.
- Conserver en lieu sûr (dans les locaux de l'entreprise par exemple) une copie de toute clé de déchiffrement.
- Conserver en lieu sûr (dans les locaux de l'entreprise) une copie en clair de tout fichier chiffré stocké sur l'ordinateur portable.
- Ne jamais stocker la clé de déchiffrement sur l'ordinateur, même si elle est protégée par un mot de passe.
- En déplacement, stocker une copie des éléments sensibles – clé de déchiffrement, fichiers – sur un média amovible que l'on emporte constamment avec soi (clé USB par exemple).
- En déplacement, chiffrer tout fichier sensible stocké sur l'ordinateur. Mieux vaut conserver une copie chiffrée de ces données sur l'ordinateur pour prévenir une perte éventuelle du média amovible. En cas de vol ou d'intrusion réussie sur la machine, ces données resteront inaccessibles pour l'adversaire.
- En déplacement, désactiver toute interface entre le poste nomade et un réseau extérieur (surtout le réseau Wi-Fi !), dès que l'on travaille sur les fichiers sensibles déchiffrés.

Cette manière de procéder est assez contraignante, surtout si vous perdez votre clé USB ; mais si vous la suivez, vos adversaires ne pourront pas vous voler d'information confidentielle.

Toutefois, cette approche est viable uniquement dans le cadre de déplacements ponctuels. Si au contraire votre machine nomade est votre poste principal de travail, et si elle héberge des données stratégiques dont la divulgation est préjudiciable, une solution de chiffrement fiable et entièrement automatisée doit être sérieusement envisagée. Les entreprises sensibilisées à ce problème investissent généralement dans des PC portables équipés d'un dispositif de chiffrement à la volée, mais pas n'importe lequel. Il s'agit le plus souvent de produits édités par des sociétés haute-

ment spécialisées en sécurité, et qui interviennent dans le secteur des banques ou de la Défense (c'est le cas par exemple de Thalès et de son produit MiniCita). Avec ce type de solution, les utilisateurs n'ont absolument pas à se soucier de la manière dont les fichiers sont protégés, et la protection est forte. En revanche, il faut prévoir un investissement plus conséquent car, outre les coûts engendrés par l'acquisition du produit, il faut confier la configuration de sécurité des postes, la gestion des certificats ainsi que la personnalisation des « tokens » accompagnant souvent ce genre de produits à un responsable de sécurité.

Si vous ne souhaitez pas aller jusqu'à déployer une solution coûteuse, la suite du chapitre vous donnera quelques points de repère pour chiffrer vous-même vos fichiers sensibles.

Chiffrer un fichier ou un volume sous Windows 2000/XP avec EFS (Encrypted File System)

SYSTÈME EFS, une fonctionnalité récente

EFS (Encrypted File System) n'est disponible qu'avec les versions 2000 et XP Pro de Windows.

Vous devez tout d'abord disposer de Windows 2000 ou XP Pro (l'édition familiale de Windows XP n'offre pas cette option de chiffrement). Ensuite, la partition hébergeant les fichiers chiffrés doit être au format NTFS.

Une fois ces conditions réunies, le reste est on ne peut plus simple. Pour gérer des fichiers chiffrés, le plus pratique pour l'utilisateur consiste à créer un dossier spécial, dans lequel seront stockés tous les fichiers sensibles :

1 Dans l'Explorateur, cliquez droit sur ce dossier, sélectionnez *Propriétés*, puis *Avancé* (figure 2-30).

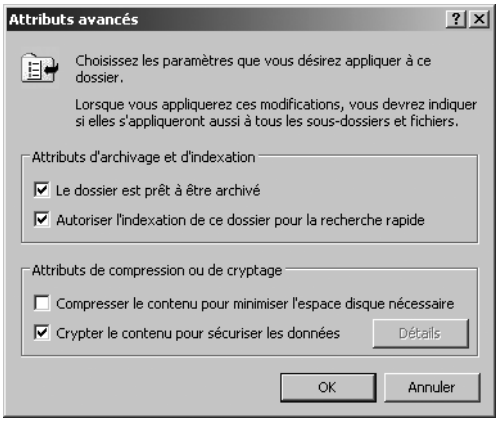


Figure 2–30
Chiffrer un dossier avec EFS

2 Cochez la case *Crypter le contenu pour sécuriser les données*, cliquez sur *OK*, puis sur le bouton *Appliquer*.

3 L'écran suivant vous propose soit d'appliquer le chiffrement aux fichiers situés directement sous la racine du répertoire sélectionné, soit d'étendre le chiffrement à toute l'arborescence de ce répertoire (figure 2-31). Choisissez l'option qui vous convient, cliquez sur *OK*, et c'est tout.

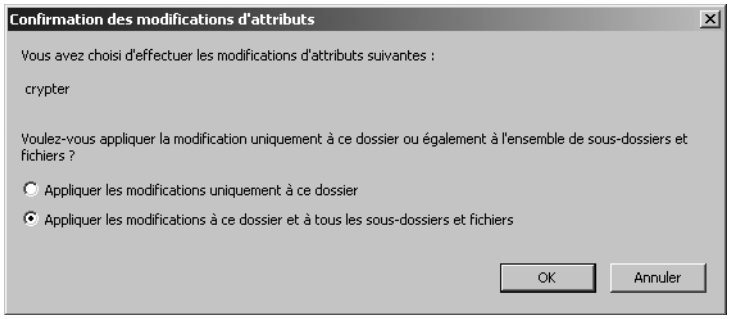


Figure 2–31
Appliquer le chiffrement à la racine ou à toute l'arborescence

Les fichiers contenus dans ce dossier et tout fichier qui y est nouvellement créé sont maintenant automatiquement chiffrés. Ils sont désormais lisibles uniquement sous votre session d'utilisateur ; un autre utilisateur de la même machine ne pourra plus accéder à leur contenu sous sa propre session. S'il tentait malgré tout de le faire, il recevrait un message d'erreur similaire à celui de la figure 2-32.

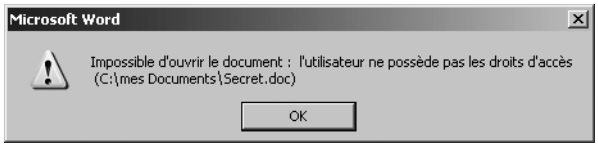


Figure 2–32
Un document chiffré par vos soins est inaccessible à partir de la session d'un autre utilisateur.

> **À RETENIR Le chiffrement/déchiffrement est automatique**
>
> L'option de chiffrement d'un dossier est considérée par Windows comme un attribut attaché au dossier dans son ensemble. En conséquence :
> - Un fichier clair est automatiquement chiffré par Windows lorsque vous le déplacez vers un répertoire chiffré.
> - Un fichier chiffré est automatiquement déchiffré par Windows lorsque vous le déplacez vers un répertoire non chiffré ou vers un volume formaté en FAT ou FAT32 (une clé USB par exemple).

L'option de chiffrement des dossiers est donc très simple d'utilisation, mais il faut être extrêmement vigilant quant à l'emplacement de stockage des fichiers sensibles : si vous placez l'un de ces fichiers dans un mauvais répertoire, il résidera en clair sur votre poste alors que vous le pensiez protégé.

PRUDENCE L'utilisation de EFS

Windows offre des mécanismes de recouvrement des données chiffrées en cas de perte de la clé (par l'intermédiaire notamment de l'agent de récupération). Cependant, il existe des cas (voir plus loin) où les clés ne pourront pas être restaurées. N'oubliez pas que la perte définitive de la clé entraîne celle de vos données.

Ce mode de fonctionnement vous garantit une grande souplesse d'utilisation car vous pouvez jongler en permanence avec les documents chiffrés sans vous en apercevoir, sans même vous préoccuper de lancer vous-même les fastidieuses opérations de chiffrement/déchiffrement. Par exemple, en marquant l'arborescence `Mes documents` comme un dossier chiffré, tous vos documents stockés dans cet espace seront systématiquement chiffrés.

Sachez par ailleurs qu'il vous est possible de chiffrer un seul fichier. La procédure est tout à fait similaire (clic droit sur le fichier, *Propriétés*, etc.). Simplement, quand vous appuyez sur le bouton *Appliquer*, une fenêtre apparaît pour savoir si vous souhaitez également chiffrer le dossier parent (figure 2-33). Choisissez l'option qui vous convient et cliquez sur *OK*. Le fichier est maintenant chiffré.

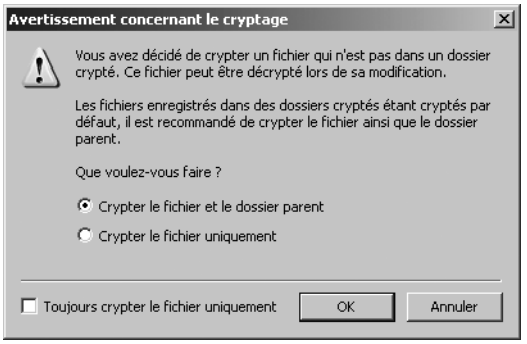


Figure 2–33
Chiffrer un fichier unique ou l'ensemble des fichiers du dossier

Limites des solutions natives de chiffrement fournies par Windows

Avant d'aborder cette question, il est vivement conseillé de lire l'annexe portant sur les bases de la cryptologie à clés publiques et sur les certificats. Des informations complémentaires seront également proposées au chapitre 8 (le chiffrement de la messagerie électronique et ses limites).

En deux mots, sachez que les mécanismes de chiffrement fournis en natif par Windows sont très peu robustes :

- Tout d'abord, pour chiffrer ou déchiffrer un fichier ou un répertoire, vous n'avez à fournir aucun secret (mot de passe, certificat personnel protégé ou autre). Toutes ces opérations se font automatiquement et ont recours à des secrets (certificats, clés de chiffrement des fichiers) engendrés et entièrement gérés par la machine. Ces éléments sont exclusivement dépendants de la session utilisateur ; le niveau de protection vis-à-vis d'un autre utilisateur dépendra donc de la capacité de ce dernier à accéder physiquement à votre machine, et de la robustesse de votre mot de passe.

- Ensuite, le mécanisme de chiffrement est basé sur un algorithme utilisant des clés de 40 bits. Casser une telle clé est une tâche tout à fait routinière pour un professionnel de la sécurité. Aussi, ne comptez pas sur EFS pour vous protéger de vos concurrents. Tout au plus vous mettra-t-il à l'abri de l'indiscrétion de vos collègues.
- De plus, si d'aventure vous deviez procéder à une réinstallation de Windows, sachez que les éléments secrets permettant de déchiffrer vos répertoires chiffrés ne seraient pas restaurés. Vos fichiers chiffrés resteraient alors illisibles.

Bonne pratique **Ne vous fiez pas à EFS pour vos documents sensibles.**

Soyez prudent si vous devez utiliser EFS. Chiffrer toute une arborescence de fichiers est dangereux, d'autant que, face à des professionnels, la protection réelle semble quelque peu illusoire.

Alternatives possibles pour un chiffrement plus robuste

Si vous souhaitez protéger de façon plus efficace vos données et vos courriers électroniques, une solution intéressante consiste à utiliser GnuPG.

GnuPG (GNU Privacy Guard) est un logiciel libre destiné à sécuriser de façon fiable les communications et le stockage des données électroniques. Avec PGP (Pretty Good Privacy), son « père spirituel » en quelque sorte, GnuPG constitue l'une des références les plus marquantes de ces dernières années en matière de cryptologie sur Internet.

GnuPG v1.x est compatible avec PGP v6/7/8.x (commercialisé par Network Associates) et fournit l'ensemble des services de sécurité offerts initialement par PGP :

- chiffrement des données ;
- création de signatures électroniques ;
- infrastructure de gestion de clés.

Renvoi
Sécurisation du courrier électronique

Rendez-vous au chapitre 8 pour une vision détaillée de la sécurisation du courrier électronique.

Histoire **PGP, OpenPGP et GnuPG**

Selon Phil Zimmerman, le concepteur mythique de PGP, il s'agissait de concevoir un logiciel de sécurité suffisamment fiable pour préserver les droits de l'homme, les principes politiques de liberté d'expression et de protection de la vie privée ; en d'autres termes, un logiciel capable de protéger de l'œil inquisiteur des gouvernements. L'existence d'algorithmes cryptologiquement forts et l'augmentation de la capacité de traitement des ordinateurs individuels rendaient désormais cet objectif accessible ; du moins à la portée d'un développeur suffisamment brillant et motivé pour s'atteler à la tâche. C'est ce que fit Zimmerman. Dès sa première version au début des années 1990, PGP offrait une implémentation rigoureuse et très complète des meilleurs algorithmes cryptologiques actuels, et que l'on recense toujours parmi les plus robustes du marché. L'objectif de PGP était largement atteint : il devenait possible, avec un simple logiciel installé sur un poste de travail, de chiffrer de l'information avec un niveau de protection inégalé.

PGP et son concepteur ont traversé depuis des périodes plus ou moins difficiles, tant pour des raisons commerciales que – on pouvait s'en douter – vis-à-vis du gouvernement des États-Unis qui, comme tous les gouvernements d'ailleurs, considère la cryptologie forte comme une arme de guerre. En dépit des interdictions à l'exportation imposées par les lois américaines, le raz-de-marée des internautes a été le plus fort, et le gouvernement américain n'a pu qu'entériner la diffusion légale de PGP partout dans le monde.

Pour s'affranchir des problèmes de droits et d'intérêts commerciaux de certains acteurs économiques, PGP a été soumis en 2001 à l'IETF (Internet Engineering Task Force), qui l'a accepté en tant que standard sous le nom de OpenPGP (RFC 2440). Tout éditeur devenait libre d'implémenter le standard OpenPGP.

Pour faciliter l'accès à OpenPGP, un projet GNU a procédé à l'implémentation de la RFC 2440, donnant ainsi naissance à GnuPG, logiciel libre que vous pouvez désormais télécharger gratuitement. Il a été officiellement autorisé en France par la DCSSI (Direction Centrale de la Sécurité des Systèmes Informatiques), et peut être utilisé pour un usage privé ou commercial.

Si vous voulez en connaître plus sur PGP et GnuPG, reportez-vous à l'ouvrage :

📖 *PGP & GPG : Assurer la confidentialité de ses e-mails et fichiers*, M. Lucas, Éditions Eyrolles, 2006.

L'un des point forts de GnuPG réside dans le fait que son code source est entièrement disponible. Si l'évaluation de la robustesse de l'implémentation d'un cryptosystème est une affaire de spécialistes de haut niveau, le code de GnuPG est continuellement revu par les plus éminents cryptologues au monde. Ceux-ci s'accordent sur le soin méticuleux apporté à l'implémentation des mécanismes cryptologiques ou de génération de nombres aléatoires, et sur l'absence de portes dérobées susceptibles d'affaiblir la sécurité ; ceci est un gage évident de fiabilité.

GnuPG demeure donc un produit de haute stature pour sécuriser le stockage des données et les communications sur Internet. Toutefois, il convient de ne pas oublier qu'en dépit du soin méticuleux apporté à la réalisation des services de sécurité, GnuPG demeure une implémentation logicielle de services cryptologiques, tributaire de l'environnement dans lequel il se trouve, c'est-à-dire un ordinateur standard relié, le plus souvent, à Internet. Par rapport à un équipement matériel dédié et complètement fermé, comme en utilisent les militaires, la sécurité atteinte grâce à GnuPG est inévitablement amoindrie par les erreurs de l'utilisateur (par exemple, le défaut de protection des clés privées) et les faiblesses intrinsèques de l'ordinateur (par exemple, les clés secrètes sont physiquement stockées sur l'ordinateur et finissent tôt ou tard par se retrouver en clair dans la mémoire vive). La réalisation d'attaques de GnuPG nécessite des compétences que tout le monde n'a pas, mais elles demeurent possibles. Sachez donc que si des intérêts stratégiques ou commerciaux importants sont en jeu, GnuPG peut se révéler insuffisant pour garantir la confidentialité de certaines données. Cela dépend notamment de la manière de s'en servir.

Mettre en œuvre et utiliser GnuPG pour chiffrer fichiers et répertoires

Téléchargez gratuitement la version officielle de GnuPG pour Win32, ainsi que toute la documentation associée, depuis le site http://www.gnupg.org/.

Téléchargez ensuite une interface graphique, afin de rendre plus conviviale l'utilisation de GnuPG, qui est en ligne de commande. Vous avez le choix entre plusieurs interfaces :

- GPG Shell : http://www.jumaros.de/rsoft/gpgshell.html ;
- Windows Privacy Tools (WinPT) : http://winpt.sourceforge.net/fr/download.php ;
- GPGee : http://gpgee.excelcia.org/ (une simple extension sous Explorer).

Procédez à l'installation de GnuPG : double-cliquez sur l'exécutable et suivez les instructions. La procédure est très simple.

LOGICIEL Langue utilisée par GnuPG

La procédure d'installation est en anglais (ou en allemand), mais le produit est bien en français.

Installez ensuite l'interface graphique que vous avez choisie. Nous retiendrons WinPT pour nos exemples. Décompressez le fichier `winpt-xxx-exe.zip` que vous avez téléchargé et lancez l'exécutable (figure 2-34).

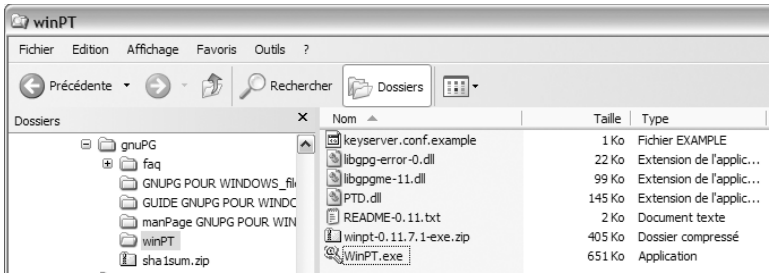


Figure 2–34
Lancez l'utilitaire WinPT.

Lorsque vous lancez WinPT pour la première fois (figure 2-35), le logiciel vous propose immédiatement de vous attribuer une paire de clés publique/privée. Optez pour cette opération si vous ne disposez pas encore de clés.

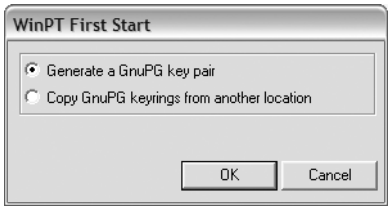


Figure 2–35
Faites-vous attribuer une paire de clés.

WinPT vous demande ensuite d'entrer vos nom et adresse électronique qui seront associés à la clé (figure 2-36).

Figure 2–36
Entrez vos nom et adresse électronique.

CONSEIL

Soignez les éléments vous identifiant

Lorsque vous voudrez faire signer (c'est-à-dire authentifier) votre clé publique par d'autres utilisateurs, ces derniers chercheront à comparer le nom associé à la clé à celui mentionné sur vos papiers d'identité. S'ils diffèrent, vous vous exposez à ce qu'ils refusent de signer votre clé, vous maintenant ainsi à l'écart du réseau de confiance.

Saisissez un mot de passe associé à la clé (figure 2-37). Attention, ce mot de passe sera utilisé pour chiffrer le fichier contenant vos clés privées. Veillez donc à ce qu'il soit complexe (minimum 8 caractères, lettres, chiffres, caractères spéciaux, majuscules, minuscules) et facilement mémorisable.

Figure 2–37
Saisissez votre mot de passe.

Laissez le logiciel s'exécuter. Au bout de quelques secondes, il devrait vous avoir créé ces précieuses clés. WinPT vous propose d'effectuer immédiatement une sauvegarde de votre nouveau trousseau de clés (figure 2-38). Bien entendu, acceptez, sinon vous ne le ferez jamais et vous vous trouverez pénalisé en cas de perte. De préférence, choisissez de stocker la sauvegarde de votre trousseau sur un support amovible que vous placerez dans un endroit sûr.

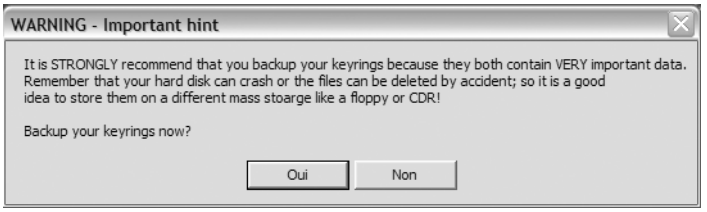


Figure 2–38
Sauvegardez tout de suite votre trousseau de clés.

Félicitations, vous disposez maintenant d'une paire clé publique/clé privée, et pouvez désormais accéder aux services de GnuPG. Bienvenue dans le monde des internautes astucieux !

Si vous êtes observateur, vous remarquez qu'une nouvelle icône, celle de WinPT, vient d'apparaître dans la barre des tâches (figure 2-39). Cliquez droit sur cette icône (figure 2-40).

Figure 2–39 L'icône de WinPT est dans la barre des tâches.

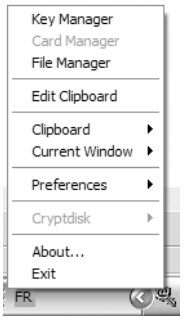


Figure 2–40 WinPT est accessible d'un clic droit sur l'icône.

RÉFÉRENCE Apprendre à utiliser GnuPG

Nous ne détaillerons pas le fonctionnement de tous les services proposés, car ce n'est pas l'objet de cet ouvrage. Si vous souhaitez apprendre à utiliser les riches possibilités offertes par GnuPG, mieux vaut vous reporter vers la documentation de GnuPG et consacrer un peu de temps (et même un temps certain) à comprendre les finesses de ce logiciel. Vous trouverez également de précieuses informations sur l'usage de GnuPG dans l'ouvrage cité plus haut : *PGP & GPG : Assurer la confidentialité de ses e-mails et fichiers*, de M. Lucas.

Choisissez simplement *File Manager*. Si vous souhaitez chiffrer des documents ou des répertoires, sélectionnez-les dans l'Explorateur Windows et faites-les glisser à l'intérieur du *File Manager* (figure 2-41).

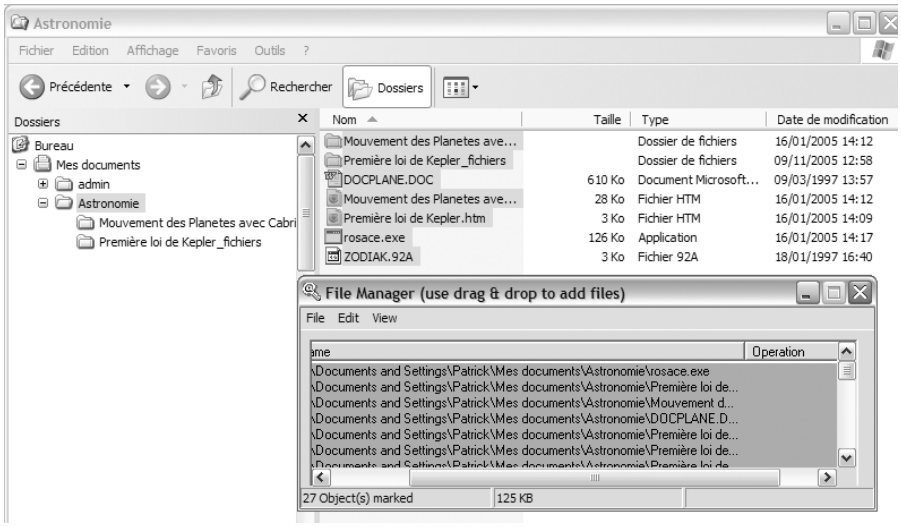


Figure 2–41
Faites glisser vos documents à chiffrer à l'intérieur du File Manager.

Marquez ensuite les documents à chiffrer dans le *File Manager* (en les sélectionnant d'un clic de souris), puis cliquez sur *File*, puis sur *Encrypt* (figure 2-42).

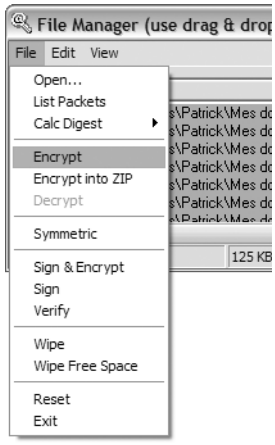


Figure 2–42
Chiffrez les documents sélectionnés.

La fenêtre suivante vous affiche la liste des clés publiques disponibles dans votre trousseau. Choisissez celle avec laquelle vous souhaitez chiffrer les fichiers. Attention : seul le détenteur de la clé privée associée pourra déchiffrer ! Cliquez sur *OK*. Et voilà, le tour est joué (figure 2-43).

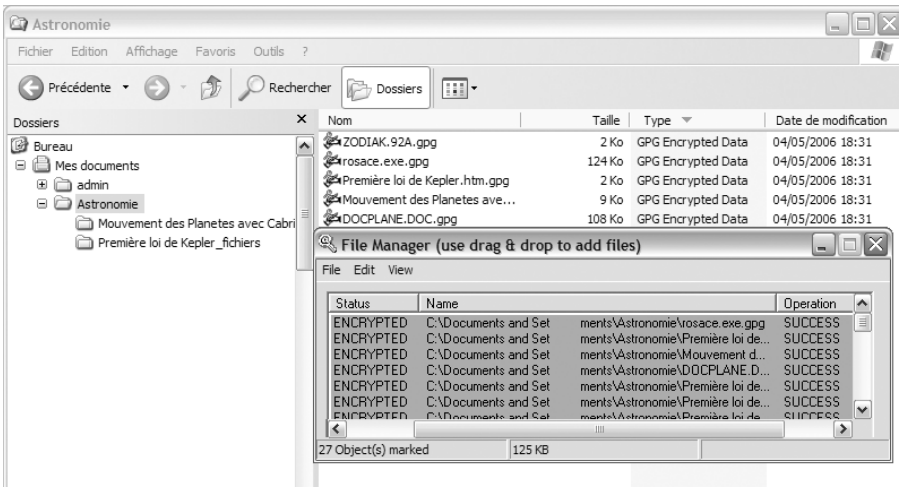


Figure 2–43
Vos fichiers sont maintenant chiffrés à l'aide de GnuPG.

Voilà comment on protège facilement et efficacement des données sensibles. Les portables se volent tellement facilement dans les chambres d'hôtel ! Il est vraiment dommage de ne pas avoir recours plus souvent à ce genre d'outils. Car, s'il ne dispose pas de votre clé privée, soyez assuré que le concurrent pourra toujours essayer de percer le secret de la proposition technique et commerciale en cours (pensez juste à garder sur vous le fichier des clés secrètes !).

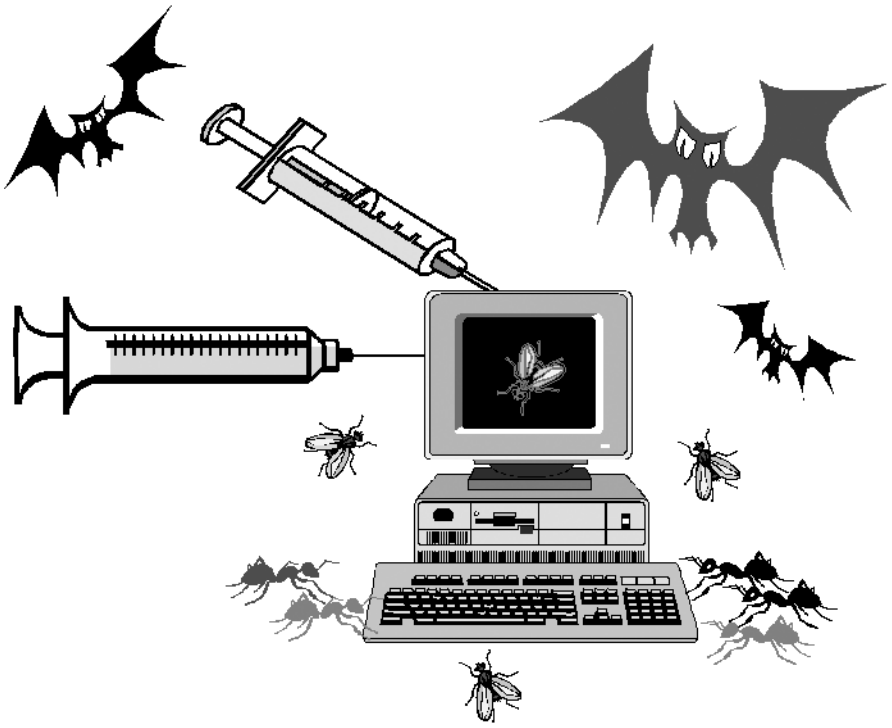
Récapitulatif

Ce chapitre vous a présenté les nombreux moyens à votre disposition pour sécuriser le système d'exploitation :

- formater les disques en NTFS ;
- verrouiller le Registre, limiter l'accès aux applications et à la machine par la création de comptes à droits restreints protégés par des mots de passe robustes ;
- protéger et surveiller les répertoires partagés ;
- effacer les historiques qui tracent votre activité ;
- chiffrer fichiers et répertoires confidentiels ; nous avons montré les limites des solutions natives (EFS) et expliqué comment appliquer un chiffrement fort à l'aide de GnuPG.

Néanmoins, tout cela ne constitue qu'une première étape dans la sécurisation de votre ordinateur. La suite vous montrera à quel point il est important de prêter également la plus fine attention aux protocoles de communication et aux applications sensibles que sont le navigateur Internet et la messagerie.

chapitre 3



Se protéger contre les virus et autres codes malveillants

Virus, vers, chevaux de Troie, logiciels espions... Vous avez hélas tous constaté un jour les effets désastreux de ces codes malveillants. Apprenez à protéger votre installation contre les virus, mais aussi à la soigner en cas d'attaque.

SOMMAIRE

- Virus et logiciels espions
- Choisir et installer un antivirus
- Se débarrasser d'un virus
- Se débarrasser d'un logiciel espion

MOTS-CLÉS

- virus
- ver
- cheval de Troie
- logiciel espion (spyware)
- antivirus

À la question « Avez vous pensé à la sécurité de votre système informatique ? », les entreprises et les particuliers répondent fréquemment « Oui, nous avons un antivirus ».

Cette réponse est symptomatique du niveau de conscience actuel en matière de sécurité : elle est évidemment incomplète (la lecture des chapitres suivants vous en convaincra sûrement), mais elle montre aussi clairement à quel point la protection virale est un souci partagé par tous.

Il ne faut pas prendre à la légère la menace liée aux virus et aux codes malveillants de la même famille, comme les vers, les chevaux de Troie ou les logiciels espions. Les virus sont des petites bêtes vraiment redoutables : il est déjà arrivé qu'une attaque virale mette complètement à plat le système central de contrôle d'une centrale nucléaire ! Suite à l'infection par un virus, vous pouvez très bien perdre une grande partie de vos données, si ce n'est l'usage complet de votre ordinateur. Ensuite, lorsque vous tentez de rétablir le fonctionnement normal de votre machine, vous pouvez y consacrer un temps considérable, allant même jusqu'à réinstaller le système d'exploitation, les applications, et restaurer les données – non contaminées ! – que vous aviez sauvegardées auparavant.

Il faut donc absolument éviter l'attaque virale, et vous devez apprendre à vous prémunir efficacement contre ce danger. Le problème, c'est que la mise en place d'une protection efficace contre les virus n'est pas simple. Il ne suffit pas d'installer un jour un antivirus et de ne plus y penser. Si après cela, vous utilisez abondamment les ressources d'Internet, il faut savoir que votre antivirus ne sera pas capable d'assurer une protection systématique de votre ordinateur. Une protection efficace contre les virus résulte d'un faisceau de mesures qui se complètent mutuellement, et dont vous deviendrez inévitablement l'un des acteurs.

Bien entendu, le premier réflexe consiste à acquérir et à installer sur son ordinateur un logiciel antivirus performant. Seulement voilà : quel produit choisir ? Il existe en effet une profusion d'outils, gratuits ou payants, et démêler l'écheveau des avantages et des inconvénients de chacun n'est pas chose facile. Ensuite (et vous l'avez probablement déjà expérimenté), même les excellents antivirus ne bloqueront pas les virus encore inconnus, susceptibles de surgir d'Internet un jour ou l'autre. Ces derniers peuvent contaminer des millions d'internautes en quelques heures. Il faut donc apprendre les gestes qui sauvent et maîtriser les procédures de décontamination. Cependant il y a bien sûr, et surtout, les comportements dangereux à éviter absolument, comme un clic distrait sur une pièce jointe infectée. Enfin, vous avez à votre disposition toute une panoplie de mesures complémentaires susceptibles de réduire significativement les risques de contamination, comme la mise à jour constante de vos logiciels (application des correctifs) ou la mise en œuvre d'un pare-feu.

Nous aborderons ici tous ces sujets, à l'exception du pare-feu qui sera traité en détail au chapitre 5. Nous expliquerons d'abord succinctement comment les virus procèdent pour contaminer et endommager votre système. Puis, nous exposerons un panorama des principaux logiciels antivirus afin de vous guider dans le choix de l'outil le mieux adapté à vos besoins. Ensuite, nous présenterons les procédures de gestion de l'antivirus, comme la mise à jour du moteur d'analyse ou du fichier des définitions de virus. Nous détaillerons également les procédures à suivre en cas de contamination.

Connaître son ennemi

Qu'est-ce qu'un virus ?

En médecine, un virus est défini comme un micro-organisme qui infecte un organisme hôte. Le virus se multiplie en détournant à son profit le métabolisme de son hôte : il s'introduit dans une cellule dont il utilise les matériaux pour la synthèse de ses propres constituants, détruit son hôte et va infecter d'autres cellules. Il se transmet et sa propagation peut être fulgurante.

Le virus informatique est très semblable à son homologue biologique : c'est un micro-programme qui s'introduit sur votre ordinateur à votre insu, possède la capacité de créer des répliques de lui-même, se transmet entre amis, entre collègues, ou à travers le carnet d'adresses, se propage parfois à une vitesse folle, et réalise accessoirement sur votre machine des opérations dont les conséquences sont parfois désastreuses.

Principaux types de virus

Aujourd'hui encore, le terme de virus est très répandu. Ce phénomène est davantage dû à une habitude langagière qu'à la réalité. En effet, les premiers codes malveillants se transmettaient selon le modèle des virus biologiques, mais maintenant, on a affaire à plusieurs types, tout aussi dévastateurs que leurs ancêtres, sinon plus. Habituellement, on classe les codes malveillants selon leur méthode de propagation.

Virus

Un virus est un code qui s'introduit dans un hôte afin de s'y reproduire, de détruire des données et de se propager à nouveau. Il ne s'exécute pas de manière autonome et n'est activé qu'avec l'exécution d'un programme hôte infecté.

Un virus ne doit sa survie qu'à l'infection massive des programmes ou des fichiers de votre ordinateur ; pour se répandre, il mise sur l'espoir qu'un programme infecté sera transmis d'une façon ou d'une autre vers une autre machine.

Initialement, les virus avaient essentiellement la vocation d'attaquer la machine infectée. Il en existe plusieurs familles :

- Les **virus de secteur d'amorce** déplacent le secteur d'amorce original du PC vers une autre portion du disque et se chargent en mémoire avant le système d'exploitation. Ils interceptent donc les appels système ou les commandes du BIOS et peuvent lancer des attaques de grande envergure.
- Les **virus d'applications** infectent les fichiers exécutables (fichiers `.exe`, `.com`, `.dll`, etc.).
- Les **virus de macros** infectent les documents contenant des macros (développées par exemple en langage Visual Basic for Applications avec la suite Office de Microsoft).

Vers

La RFC 1 135 en donne une excellente définition : « *Un ver (worm) est un programme capable de s'exécuter de manière autonome et d'utiliser les ressources de son hôte à ses propres fins. Il peut se transmettre intégralement à d'autres machines* ». Contrairement au virus, le ver ne cherche pas à se répliquer au sein de votre machine ; sa survie dépend de l'infection massive des ordinateurs de la planète, en un minimum de temps. Il utilise pour cela votre carnet d'adresses. Une fois installé sur votre ordinateur, il peut procéder à des opérations de destruction, tout comme les virus, mais peut aussi mettre en œuvre une stratégie d'attaque plus sournoise et à plus ou moins long terme, pas forcément dirigée contre votre ordinateur. Il peut s'agir par exemple de préparer votre machine à une attaque en déni de service distribué (DDoS), conjointement à des millions d'autres ordinateurs.

RENVOI **Attaque en déni de service distribué (DDoS)**

Les différents types d'attaques cités dans cet ouvrage sont définis à l'annexe B.

Chevaux de Troie ou troyens

Un cheval de Troie (*Trojan*) est un programme en apparence inoffensif ou anodin, mais dont le code recèle des fonctions cachées qui le sont beaucoup moins. C'est le plus souvent des utilitaires, des logiciels gratuits ou des jeux. Au départ, un cheval de Troie ne s'exécute pas sans une action explicite de l'utilisateur ; il utilise donc diverses manœuvres pour se déguiser et inciter celui-ci à l'exécuter. Lorsque le troyen est exécuté, il met tout en œuvre pour s'installer sur la machine et rester résident. Un cheval de Troie n'a pas vocation à se répliquer.

Autres formes de malveillances

Il existe d'autres formes de malveillances :

- En premier lieu, il y a les **logiciels espions** (*spyware*), sortes de troyens actifs collectant et divulguant à l'extérieur toutes sortes d'informations personnelles et sensibles hébergées sur l'ordinateur.
- On peut ensuite citer le spam, ou **pourriel**, messages non sollicités et indésirables, conçus à l'origine à des fins marketing mais dont l'effet conduit progressivement à handicaper les utilisateurs et asphyxier la messagerie électronique.

Pour contrer ces nuisances plus récentes, le seul recours était, il y a quelque temps, de faire appel à des logiciels spéciaux, antispam ou antispyware. Cependant, les éditeurs d'antivirus étendent actuellement les fonctionnalités de leurs produits pour couvrir ces nouvelles formes de pollution.

Quelle que soit la catégorie à laquelle ils appartiennent, les programmes malveillants utilisent les mêmes moyens et ont tous un but commun : infecter l'ordinateur et se servir de celui-ci pour entraver ou porter préjudice. C'est la raison pour laquelle ils sont combattus de la même façon. Dans ce chapitre, virus, vers, chevaux de Troie et logiciels espions seront donc souvent désignés sous le terme générique de « virus ».

MALIN **Protection contre le spam**

Notez que certains clients de messagerie, notamment Thunderbird, offrent aujourd'hui de très bonnes mesures de protection contre les spams (voir chapitre 8).

Agissements des virus

Les codes malveillants ne craignent pas l'oxymore, et on appelle « **charge utile** » d'un virus les opérations, souvent destructrices, qu'il exécute sur votre machine. Les virus sont capables de réaliser les pires desseins imaginés par l'*Homo informaticus* endurci. Cette section dresse un bref aperçu de quelques vilains tours qu'ils vous jouent.

CULTURE **Qui crée les virus ?**

Toutes les attaques « connues » sont en définitive le fruit de travaux d'internautes acharnés, d'étudiants ou de chercheurs, d'informaticiens passionnés, qui partagent leurs connaissances à travers les nombreux forums disponibles sur Internet, voire de pirates exploités ou manipulés à des fins moins avouables.
Néanmoins, cela n'est probablement rien comparé à ce que savent faire actuellement certains gouvernements, dont la recherche militaire s'intéresse semble-t-il beaucoup aux attaques informatiques, et aux virus en particulier.

S'installer discrètement sur votre ordinateur

La caractéristique première d'un ver ou d'un cheval de Troie est de savoir s'immiscer dans le dossier système de votre ordinateur et se dissimuler derrière un nom apparemment parfaitement inoffensif. Le ver Mydoom, par exemple, se cache derrière le processus `taskmon.exe`, peu sujet à éveiller vos soupçons au cas où vous auriez la malencontreuse idée d'afficher la liste des processus actifs (et encore il est bien brave, car pour rien au monde un virus digne de ce nom ne laisserait apparaître la moindre trace susceptible de trahir sa présence !).

Une fois dans la place, le virus modifie à son avantage la configuration de votre ordinateur afin de se lancer systématiquement à chaque redémarrage ou de s'y propager (il faut bien assurer sa longévité !), et de s'octroyer des droits élevés.

Pervertir votre système

Le fonctionnement de votre ordinateur s'appuie sur des milliers d'exécutables, de fichiers `.dll`, de scripts, etc. Imaginez un instant que le virus remplace l'un d'entre eux par un fichier à lui, du même nom, mais n'effectuant plus tout à fait les mêmes tâches. D'un simple regard, vous serez incapable de débusquer la moindre anomalie, mais votre ordinateur ne fonctionnera plus comme avant.

C'est exactement ce que font les virus : ils sont capables de modifier les principales commandes du système, voire les fonctions essentielles du noyau. Ils peuvent ainsi intercepter les appels système (par exemple la demande de visualisation des processus en cours) et ne laisser voir que ce qu'ils veulent bien montrer (par exemple la liste de tous les processus actifs, exceptés les leurs). Si vous scrutez l'état de votre ordinateur en vous servant des fonctions corrompues, il se peut que vous ne trouviez jamais la trace de ces vilains programmes.

Accessoirement, le virus désactive l'antivirus. Le ver Sober.Q modifie notamment le fichier `luall.exe`, pierre angulaire de la fonction Live-Update sur laquelle repose le système de mise à jour de Norton Antivirus.

Ouvrir toutes grandes les portes de votre PC

Une fois confortablement installé et après avoir assuré son emprise sur votre ordinateur, le virus peut préparer l'offensive. Il ne faut pas oublier, comme nous le verrons au prochain chapitre, que votre PC est une ville protégée par un mur d'enceinte qui ne comporte pas moins de 65 535 portes tournées vers l'extérieur ! Par exemple, lorsque vous dialoguez sur Internet en HTTP, la porte numéro 80 est ouverte pour laisser passer le flux échangé avec le serveur web.

À la mise sous tension, toutes les portes sont fermées et votre ordinateur ne peut rien échanger avec l'extérieur. Cependant, lorsqu'une application (ou un service) de communication démarre, par exemple la messagerie ou le navigateur Internet, elle ouvre les portes qui lui sont associées.

Les vers, les chevaux de Troie, et surtout les logiciels espions procèdent de la même façon : discrètement, sans vous avertir, ils ouvrent des portes que les applications ont peu de chances d'utiliser, comme les portes numéro 2 339 à 2 342. C'est ce que l'on appelle des canaux cachés ou des portes dérobées. Dès lors qu'une porte – ou plus exactement un port, dans la terminologie des réseaux IP – est ouverte, votre ordinateur capte toute l'information qui y arrive et la redirige automatiquement vers le virus. Ce dernier n'a plus qu'à traiter les données qu'il reçoit et exécuter sur votre poste les actions qui lui sont demandées. C'est par ce biais qu'un inconnu (le pirate) a la possibilité d'échanger tout ce qu'il veut avec votre

ordinateur et de prendre le contrôle de celui-ci à distance, à travers le pare-feu (nous verrons comment au chapitre 5). Par exemple, le virus peut très bien renvoyer à cet inconnu un interpréteur de commandes ; il suffit que celui-ci tape une commande dans cet interpréteur sur son poste distant pour qu'elle s'exécute directement sur le vôtre. Le pirate peut ainsi rapatrier le fichier des mots de passe ou tous les fichiers sensibles auxquels il souhaite avoir accès, créer des utilisateurs avec des droits administrateur, et installer à votre insu d'autres logiciels malveillants.

Lancer des attaques de grande envergure

À ce stade, le code malveillant possède un pouvoir de nuisance insoupçonné. S'il le souhaite, il peut se connecter à votre insu à n'importe quel site distant afin de télécharger, avec la bénédiction de votre pare-feu, toutes sortes de programmes espions ou malveillants, actifs ou dormants, qui lui permettront de lancer des attaques sophistiquées, ou de mener des offensives en règle sur commande (pollution ou destruction pure et simple des données de la machine, fuite d'informations sensibles, attaques en déni de service distribué vers des sites distants, etc.).

Accessoirement, le virus pourra prendre toutes les mesures nécessaires pour vous bombarder de messages intempestifs et de pourriels (spam).

Vous remarquerez que ces actions sont souvent furtives. Si le virus est conçu intelligemment, vous pouvez très bien vivre des années avec un ordinateur sous contrôle total d'une entité extérieure, sans que vous vous aperceviez de quoi que ce soit. Bien entendu, tout cela reste valable avec n'importe quel ordinateur, qu'il soit situé à votre domicile ou à votre bureau.

Agissements des logiciels espions

Les logiciels espions, ou « spyware », représentent l'une des menaces les plus inquiétantes à l'heure actuelle. Ils s'immiscent furtivement dans vos ordinateurs lorsque vous installez des logiciels peu fiables (clients peer-to-peer, logiciels gratuits ou obtenus par le biais de source non sûre, etc.) ; ces programmes redoutables seraient aujourd'hui installés sur les deux tiers des PC à travers le monde. Touchant sans distinction les particuliers et les entreprises, les logiciels espions doivent leur expansion fulgurante à l'inconscience quasi générale de tout un chacun à l'égard de ce type de menace.

Avec l'apparition des vers et des chevaux de Troie, nous avons observé une mutation et une sophistication progressive de la menace virale : les codes malveillants ne s'installent plus sur votre machine dans le seul but de polluer ou détruire vos données, mais aussi pour procéder à des attaques plus sournoises comme la prise de contrôle de l'ordinateur à dis-

Client peer-to-peer (P2P)

Logiciel d'échange de fichiers directement d'utilisateur à utilisateur à travers Internet. Les logiciels P2P les plus connus sont Kazaa et Emule.

Précaution Logiciels gratuits

Attention, « gratuit » ne signifie pas nécessairement « dangereux ». De nombreuses applications issues des grands projets Open Source sont gratuites, mais sont néanmoins tout aussi fiables que les logiciels du commerce.
Avant de télécharger un logiciel gratuit, vérifiez toujours soigneusement le sérieux de son émetteur (certificats, réputation…).

tance, la subtilisation des données, ou l'utilisation des ressources de l'ordinateur dans des campagnes d'attaque par déni de service distribué (DDoS). Les logiciels espions s'inscrivent dans cette logique, mais vont plus loin : bénéficiant des innombrables techniques d'infiltration éprouvées par leurs prédécesseurs, ils s'immiscent silencieusement dans vos ordinateurs, vous observent ou analysent vos comportements et vos habitudes. Ils envoient ensuite des rapports détaillés sur vos faits et gestes à des inconnus.

Le logiciel espion est un domaine d'activité très en vogue actuellement, au point d'ailleurs que le concept semble vouloir se décliner de façon inépuisable. On compte aujourd'hui plusieurs catégories différentes de logiciels plus ou moins malveillants, que l'on classe parmi les logiciels espions. Pour ne citer que les principaux :

- les **adware** (contraction de *advertising* et *software*), conçus à des fins de marketing sur le Web, qui vous abreuvent de bannières publicitaires ;
- les **enregistreurs de frappe clavier** ou *keyloggers* ;
- les **cookies traceurs** ;
- les **numéroteurs**, qui modifient le numéro d'accès à votre fournisseur ou bien vous connectent à votre insu à des services téléphoniques à tarification élevée ;
- les **spybots**, qui recueillent par exemple vos adresses IP, e-mail et transmettent le tout vers des inconnus.

Au delà de la violation des lois censées préserver la vie privée (qui n'ont d'autre perspective sur Internet que d'être bafouées, au vu et au su de tous), qui peut garantir que les techniques utilisées par les logiciels espions ne seront jamais exploitées illégalement à des fins de surveillance, par un concurrent, par les grandes oreilles d'un gouvernement, ou par un escroc désirant intenter quelque action plus trouble à votre encontre ? Car ces petits programmes savent mettre des techniques incroyables et des trésors d'habileté au service de l'espionnage ; leurs capacités de nuisance sont absolument ahurissantes. Sans être détectés, ils peuvent tout à fait :

- **surveiller et mémoriser** toutes les actions réalisées sur votre ordinateur (sites web visités, applications utilisées, fichiers lus, créés ou modifiés, avec un horodatage précis de vos actions) ;
- **enregistrer** les courriers que vous échangez par messagerie électronique ;
- **effectuer** périodiquement **des copies** de votre écran ;
- parcourir votre ordinateur et en **dresser une configuration** précise (logiciels utilisés, numéros de version, numéros de licence de

Historique

Des fins initialement commerciales

À l'origine, les logiciels espions ont été pour la plupart développés à des fins « bassement » commerciales. Renseignés sur les sites que vous visitez, les produits qui vous intéressent, qui vous êtes, où vous vous situez, les applications que vous utilisez, etc., les fins limiers du marketing savaient désormais vous bombarder de bannières publicitaires en rapport avec vos besoins. Vos informations personnelles finissaient ainsi par entrer dans des bases de données revendues aux spammeurs, aux annonceurs ou aux spécialistes du marketing sur le Web. L'enjeu financier est important pour ces différents acteurs ; il profite d'ailleurs à certains fournisseurs de logiciels gratuits, pour lesquels le logiciel espion est devenu un moyen de rémunération.

logiciels) ; attention donc à la fraude si vous n'avez pas payé vos licences logicielles !

- **polluer votre activité** en vous abreuvant de bannières publicitaires intempestives ;
- **collecter toutes les données sensibles** stockées sur la machine (fichiers personnels ou professionnels, identifiants, cookies, clés de chiffrement de vos fichiers, etc.) ;
- enregistrer toutes vos frappes clavier et **intercepter ainsi des informations précieuses** comme vos mots de passe et vos coordonnées bancaires ;
- **envoyer toutes ces informations** vers un ou plusieurs destinataires inconnus sans que vous vous aperceviez de quoi que ce soit.

Cette menace est d'autant plus préoccupante que les éditeurs d'antivirus ne disposent pas encore d'une offre étoffée en la matière. Certains ont commencé à combler cette lacune, mais sont encore loin d'offrir une protection satisfaisante.

Prenons l'exemple de la figure 3-1 ; l'ordinateur ciblé a été investi par ce que l'on appelle un « keylogger », c'est-à-dire un mouchard capable de mémoriser toutes les informations que vous entrez dans l'ordinateur à partir de votre clavier. Ce mouchard ne se borne pas à capturer vos secrets ; en esclave fidèle et bien discipliné, il renvoie périodiquement des rapports détaillés vers son maître, situé quelque part sur Internet, qui a ainsi le loisir d'entrer au cœur de votre vie privée, en toute tranquillité.

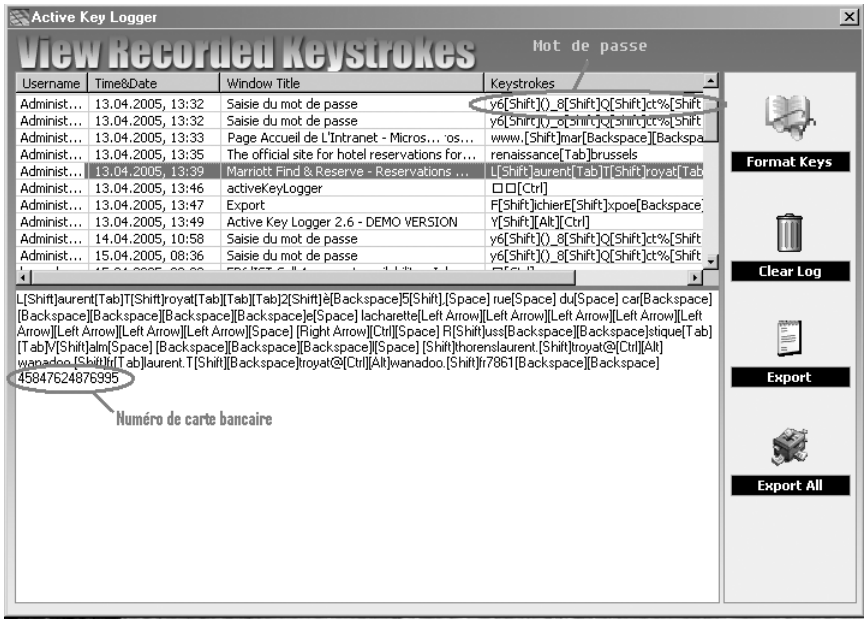


Figure 3–1
Comment l'attaque d'un « keylogger » peut conduire à des divulgations fâcheuses.

La capture d'écran n'est manifestement pas des plus conviviales, mais quelques instants d'attention dévoilent des informations capitales sur l'utilisateur : son nom est Laurent Troyat et son mot de passse, pourtant robuste, est `y6()_8Qct%T` – dommage ! d'autant plus qu'il s'agit d'un mot de passe Administrateur ! Son adresse électronique est laurent.troyat@wanadoo.fr, il vient d'effectuer une réservation d'hôtel et, surtout, vous disposez de son numéro de carte bancaire : 4584 7624 8769 95 !

Autre exemple, vous êtes chef de service et préparez les augmentations de salaire de vos collaborateurs. Malheureusement, l'un d'entre eux, un peu trop curieux, a réussi à installer et à configurer à distance sur votre machine, un vilain petit spyware qui lui envoie, toutes les dix minutes, une belle copie de votre écran. La figure 3-2 montre ce que le collaborateur indélicat réussit à visualiser.

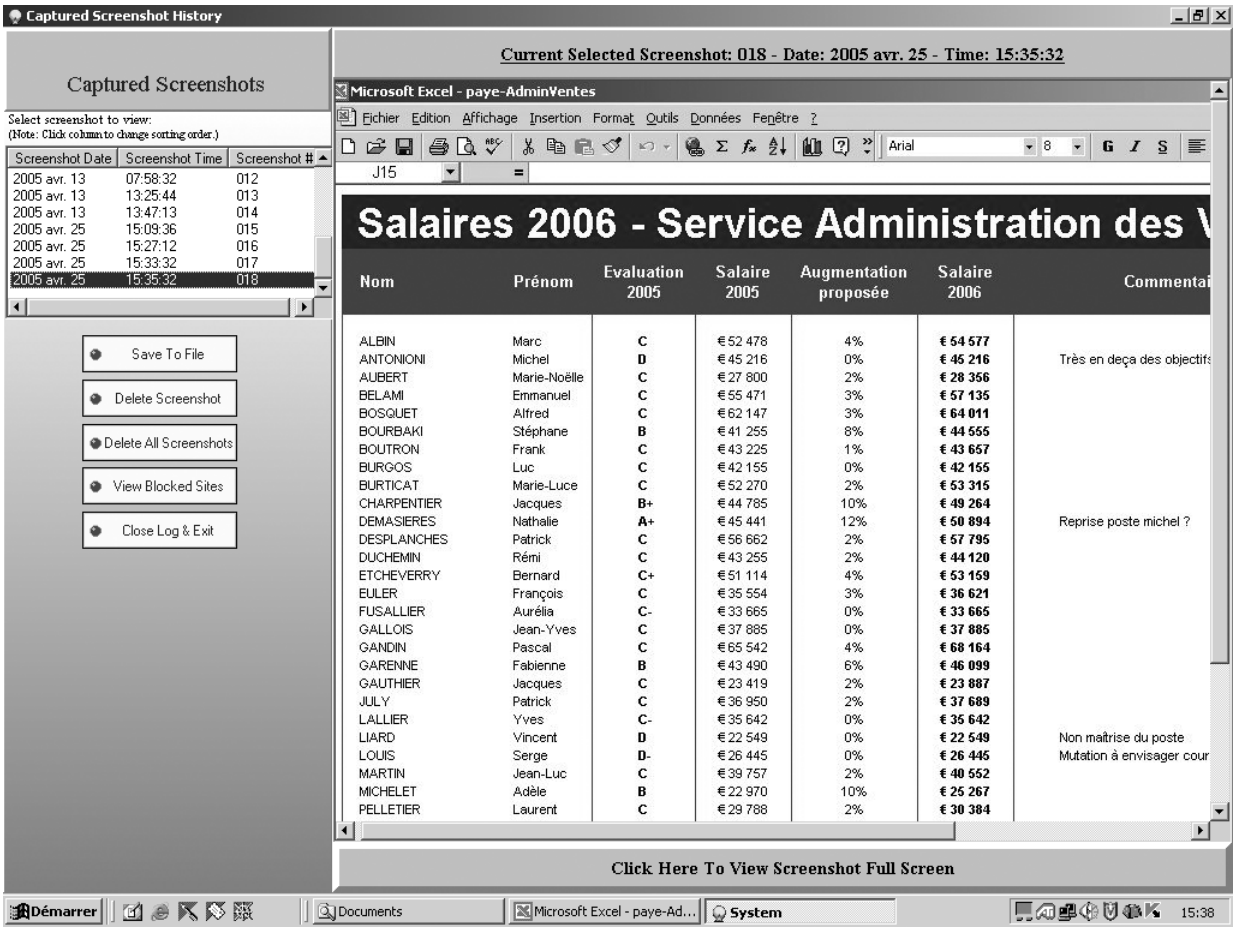


Figure 3–2 Exemple de visualisation d'une copie d'écran à distance

Si, au lieu de préparer les augmentations de vos collaborateurs, vous visualisez simplement, à votre domicile, le contenu de votre compte en banque, celui-ci restera probablement protégé de tous les regards indiscrets, sauf de celui du pirate.

Ces deux figures vous montrent concrètement comment, à l'aide du programme adéquat, il est facile de collecter des données sur un ordinateur distant. Dans ces cas précis, les logiciels n'ont pas été conçus dans le but de nuire (la mémorisation des noms, adresses électroniques et mots de passe est utile par exemple pour éviter à l'utilisateur la saisie récurrente de ces informations lors de ces différentes visites). Toutefois, tous les logiciels espions ne sont pas forcément aussi inoffensifs.

Si vous avez un doute, il est inutile de scruter la liste des messages que vous avez envoyés, de visualiser les processus en cours d'exécution, d'inspecter le menu *Démarrer* ou le panneau de configuration, avec le vague espoir de débusquer une trace de la présence ou de l'activité d'un logiciel espion. Celui-ci sait se camoufler à la perfection et vous ne verrez absolument rien.

Infection de la machine

Clic sur une pièce jointe infectée

Citons tout d'abord le cas le plus fréquent : vous recevez un message électronique infecté vous incitant à cliquer sur la pièce jointe, ce que vous faites... Patatra ! vous vous apercevez, mais trop tard, que celle-ci était en réalité un fichier exécutable malveillant. En cliquant sur cette pièce jointe, vous libérez le virus, vous provoquez l'exécution de sa charge utile, vous êtes en quelque sorte l'acteur de la contamination de votre propre machine.

Le virus Anna Kournikova en est un exemple frappant : un message électronique annonçait une belle photo de la joueuse de tennis en pièce jointe (`Subject :`*Hi : Check This !*). Heureusement, la charge utile du ver n'était pas destructrice, mais sa propagation fulgurante a clairement montré que l'exploitation du carnet d'adresses était un concept efficace… et que Anna Kournikova était appréciée d'un large public.

CONSEIL Pièces jointes

N'ouvrez JAMAIS la pièce jointe d'un message électronique qui vous parvient, à moins d'être absolument sûr de ce qu'elle contient. Gardez à l'esprit qu'un virus peut très facilement usurper l'identité d'une personne en qui vous avez confiance.

Exploitation d'une faille logicielle

Le clic malheureux sur la pièce jointe infectée n'est pas le seul moyen de contaminer un PC, loin de là ! Il est effrayant de constater à quel point les techniques permettant aux virus d'arriver à leurs fins sont nombreuses.

TECHNOLOGIE Les logiciels fonctionnent malgré leurs bogues

Contrairement aux apparences, les applications informatiques, comme les navigateurs, les gestionnaires de bases de données, les clients de messagerie, les protocoles de communication, bref, les logiciels en général, ont tous un point commun : ils sont truffés d'erreurs de programmation. Cela vous surprendra peut-être, car, en dépit de dysfonctionnements mineurs que vous avez bien dû constater, les logiciels fonctionnent en général correctement et délivrent le service que l'utilisateur en attend.

Cependant, beaucoup d'erreurs subsistent bel et bien dans les produits commercialisés. Pour la plupart, ces erreurs résiduelles ne sont pas gênantes si vous utilisez les produits dans des conditions normales. Et, même lorsque vous les poussez dans leurs derniers retranchements, l'omniprésence de bogues cachés n'empêche pas les applications de mener de belles carrières, sans incident notoire.

Types MIME

MIME (Multipurpose Internet Mail Extension) est un standard destiné à étendre les possibilités du courrier électronique par l'adjonction de divers types de fichiers (images, sons, textes...).
Exemples : `image/gif`, `text/html`.

Lorsqu'un pirate a décelé une faille dans un programme, il peut très bien conduire le logiciel dans une situation inattendue pour le mettre hors service. C'est là que l'on entre dans le monde du virus ou de l'infiltration des systèmes. Tout l'art du concepteur d'un code malveillant consiste à **contrôler** cette situation inattendue pour détourner l'exécution de l'ordinateur vers un module exécutable maîtrisé par le pirate (ce que l'on désigne généralement par « code arbitraire »).

Prenons un exemple concret : il y a quelques années, un pirate avait identifié une vulnérabilité d'Internet Explorer : IE ne gérait pas correctement certains types MIME particuliers. En envoyant à un destinataire un message HTML dont l'en-tête MIME avait été modifié d'une certaine façon, le pirate forçait Internet Explorer à exécuter automatiquement la pièce jointe sur l'ordinateur du destinataire, à la simple lecture du courrier électronique. La pièce jointe étant un virus, le destinataire ne pouvait rien faire pour éviter la contamination de son poste. Le nom de ce virus reste tristement célèbre dans les annales : Nimda. Entre autres méfaits, Nimda activait l'utilisateur *Invité* et l'assignait au groupe *Administrateurs*, créait un partage au niveau du répertoire racine doté de tous les droits d'accès, et désactivait certains contrôles et outils de filtrage. Vous imaginez la suite…

Image piégée

Un autre exemple non moins redoutable est apparu récemment. Vous savez certainement que les images numériques sont mémorisées dans les appareils photographiques le plus souvent au format standard JPEG. Ce dernier est très répandu et est d'ailleurs pris en compte par tous les logiciels de traitement d'images et par les navigateurs. Un pirate avait décelé une faille dans un composant logiciel de Microsoft en charge de la gestion de ces images : en modifiant d'une façon judicieuse le fichier JPEG, donc en créant une image « piégée » à ce format, il arrivait à provoquer un dysfonctionnement dans le logiciel et à détourner l'exécution vers un programme à lui, qu'il avait évidemment conçu dans le but d'infiltrer votre ordinateur. Il suffisait au pirate d'envoyer par messagerie cette image piégée, ou de la déposer sur un site web fréquenté ; le simple fait de la visualiser déclenchait l'exécution du programme malveillant et l'infection de votre ordinateur.

Macro infectée

Tout le monde a entendu parler des virus de macros, ces petits programmes écrits en langage de programmation spécifique, interprété par une application hôte (VBA – Visual Basic for Applications – en est un exemple). Le virus Melissa reposait sur l'infection de la macro

`Document_Open` qui s'exécute automatiquement à l'ouverture de tout fichier Word. En infectant le modèle de documents `normal.dot`, il s'assurait que tout nouveau document Word créé sur le poste infecté serait à son tour contaminé. Il se multipliait donc en conséquence. Toujours par le biais du langage Visual Basic, il dérobait la liste des cinquante premières adresses électroniques du carnet de l'utilisateur et s'expédiait lui-même vers ces adresses.

Les techniques pour infiltrer de l'extérieur votre « organisme hôte » sont donc nombreuses, souvent très inattendues, et d'une efficacité ahurissante. L'exemple de l'image JPEG piégée montre de façon éclatante qu'un simple échange de données peut conduire à la prise de contrôle d'un ordinateur à distance. Cela donne à réfléchir, notamment au niveau des entreprises !

Propagation des virus

La messagerie électronique constitue actuellement l'un des principaux vecteurs de propagation des virus. Le célèbre ver I Love You est l'exemple typique du code malveillant transmis en pièce jointe.

Un virus peut aussi proliférer de façon tout à fait classique, suite à l'introduction dans votre ordinateur d'un support amovible contaminé, ou au simple rapatriement d'un fichier infecté à partir d'Internet. La figure 3-3 vous montre explicitement que si l'antivirus n'était pas intervenu, le fichier `eicar.com`, téléchargé à partir d'un serveur web, aurait infecté la machine.

Figure 3–3
Exemple de rapatriement d'un fichier contaminé à partir d'Internet

La propagation des chevaux de Troie ou des logiciels espions est en revanche moins facile à cerner : elle fait appel à des procédures en apparence anodines, et s'appuient de surcroît sur des techniques très diversi-

Fichier eicar.com

Le fichier `eicar.com` est un fichier de tests pour antivirus, développé par l'EICAR (European Institute for Computer Anti-Virus Research).

- www.eicar.org

fiées. Restez donc vigilant car, souvent, votre PC est contaminé à cause d'une action de votre part ! Ces logiciels investissent votre ordinateur :

- lorsque vous accédez à des sites de partage de fichiers, comme Kazaa ;
- lorsque vous chargez une page web contenant des applets Java, des codes Javascript ou des contrôles ActiveX malveillants (voir à ce sujet le chapitre 7) ;
- lorsque vous consultez des sites web drainant un grand nombre de visiteurs, sujets à héberger potentiellement des codes exploitant les failles du système d'exploitation, des services actifs (LSASS, IIS, messagerie électronique) ou des navigateurs ;
- suite à l'infection par un ver qui active le téléchargement et l'installation de logiciels tiers sans votre consentement ;
- lorsque vous téléchargez et installez des utilitaires, des jeux ou des logiciels non fiables (clients peer-to-peer, logiciels gratuits, *shareware*). En effet, il est très facile avec les outils de *packaging* actuels, comme Wise, de cacher toutes sortes de chevaux de Troie et de logiciels espions dans un paquetage d'installation.

Cette liste vous est donnée à titre informatif pour vous sensibiliser à ce type de menace. Sachez bien toutefois qu'elle n'est pas exhaustive.

Logiciel shareware

Un logiciel shareware peut être installé et essayé gratuitement, généralement pour un temps défini ou un nombre limité d'utilisations. Si vous souhaitez garder ce logiciel, vous devrez vous acquitter d'une contribution financière, habituellement modeste.

Périodicité d'apparition de nouveaux virus

Les éditeurs de logiciels antivirus déclarent détecter en moyenne entre 1 000 et 1 500 nouveaux virus, vers, chevaux de Troie, ou logiciels espion par mois ! Cela montre clairement que le fait de posséder un antivirus ne sert à rien si vous ne le mettez pas constamment à jour.

BONNE PRATIQUE Mise à jour de l'antivirus

Veillez à compléter au fur et à mesure la liste des nuisances reconnues et traitées par votre antivirus en installant scrupuleusement toutes les mises à jour proposées par l'éditeur.

Auteurs des virus

Il nous est souvent arrivé de croiser Dupont, avec « t », le sourcil droit froncé et l'air entendu, susurrant discrètement sur le ton de la confidence : « À qui profite le crime, hmm ? ». Il est vrai que les éditeurs d'antivirus occupent un marché promis à de belles perspectives, tant les vocations en matière de piratage semblent inépuisables…

Cependant, les persifleurs auront de quoi être déçus : avec un tel vivier de pirates chez les informaticiens, personne n'a besoin d'entretenir l'incendie ! Nombreux sont, dans le monde, ceux qui écrivent des virus, et les raisons qui les motivent sont très diverses. On recense par exemple :

- Des étudiants en informatique – L'art de créer des virus fait officiellement partie de leur cursus scolaire. Ils conçoivent ces petites bêtes dans des laboratoires à des fins exclusivement pédagogiques, mais il

arrive que certains soient tentés de tester le comportement de leur bébé dans le monde réel.

- Des informaticiens obscurs en quête de notoriété – Ils sont désireux de réussir un coup fumant comme celui d'infester la planète en un temps record.
- Des passionnés d'informatique – Eux considèrent l'écriture de virus comme un exercice intellectuel ou un sport aquatique.
- Des chercheurs – Ils veulent par exemple tester en grandeur réelle la faisabilité d'une technique d'infiltration ou l'efficacité d'un moyen de propagation.
- Des bidouilleurs de codes – Ceux-là prennent du plaisir à modifier le code d'un virus connu afin de se donner l'illusion qu'ils ont réussi un exploit. C'est notamment par ce biais que l'on voit apparaître plusieurs mutations successives d'un même virus, notées généralement « nom_du_virus.B », « nom_du_virus.C », etc.
- Des redresseurs de torts – Ils veulent pointer du doigt l'existence de vulnérabilités gênantes, et attirer ainsi l'attention des utilisateurs sur la nécessité de maintenir les logiciels à jour (exemple : le virus Sasser).
- Des gamins débrouillards qui aiment les farces de potaches.
- Des militants – C'était par exemple le cas des concepteurs de MyDoom, qui avaient un contentieux avec la société Santa Cruz Operations. Le ver MyDoom était censé lancer un gigantesque bombardement du site web de SCO, à travers les millions d'ordinateurs qu'il avait infectés.
- Des individus ou des groupements d'individus animés d'intentions plutôt mauvaises, comme la vengeance ou l'escroquerie.

Cette liste a pour but de donner un aperçu, elle ne prétend pas à l'exhaustivité.

Toutefois, l'existence de virus n'a pas que des conséquences néfastes. D'abord, on pourrait affirmer sur le ton de la provocation que les virus ont donné lieu à une industrie florissante, assurant aujourd'hui quelques milliers d'emplois. Ensuite, les virus ont progressivement obligé les éditeurs à mettre au point des procédures rapides et efficaces pour colmater les failles et, de ce fait, réduire significativement les risques d'attaques. En ce sens, les virus contribuent globalement à rendre les logiciels plus fiables. Enfin, on peut imaginer que les publications successives de correctifs donnent du fil à retordre à certains gouvernements. Sans ce handicap, ils auraient le champ libre pour exploiter, à des fins peu sympathiques, toutes les failles possibles des systèmes. Les entreprises impliquées dans les secteurs stratégiques (administration, économie, défense) ne doivent pas oublier que certains gouvernements travaillent

activement à la mise au point d'attaques pour contrôler ou, en cas de conflit, mettre hors service à distance les systèmes informatiques de l'adversaire.

Comprendre le fonctionnement d'un logiciel antivirus

Les antivirus ont pour objectif de protéger les postes de travail contre les virus, les vers et les chevaux de Troie. Après un léger retard à la décision, certains éditeurs étendent leurs fonctionnalités à la lutte contre les logiciels espions et les messages non sollicités ; ils proposent soit une extension des fonctions natives de leur produit de base, soit un enrichissement de leur gamme de produits avec la mise à disposition d'outils additionnels de type antispyware ou antispam. Toutefois, chez la plupart des éditeurs, la prise en compte de ce nouveau type de menace est récente et l'offre n'est pas encore mûre. Pour une protection efficace contre les logiciels espions, il convient d'avoir recours à des utilitaires spécifiques, dits « tueurs de spywares », dont les principaux seront présentés à la fin de ce chapitre.

Bien entendu, la protection qu'offrent un antivirus et un tueur de spywares est nécessaire, mais elle n'est pas suffisante. Les antivirus ne vous protégeront pas contre les tentatives d'intrusion perpétrées par un pirate, pendant que vous êtes connecté à Internet. Pour cela, vous devrez mettre en œuvre d'autres mesures de protection, comme l'installation et la configuration d'un pare-feu. Ce point sera abordé dans les prochains chapitres.

RENVOI Et Vista ?

Vista intègrera des outils de protection contre les codes malveillants, mais de quelle qualité ? Voir la discussion à ce sujet au chapitre 10.

Fichier de définitions de virus

Il faut le savoir : le virus, cette bête si redoutable, n'est pas toujours particulièrement habile. Le virus agit parfois comme un commando exhibant ses banderoles aux couleurs vives, ou soufflant à pleins poumons dans des cuivres au moment de l'assaut. Prenons le cas d'un virus élaboré : Bagle.BJ. C'est un troyen « téléchargeur » capable de désactiver les principaux antivirus et pare-feux installés sur la machine. Il sait rapatrier et exécuter le corps de sa charge utile à partir d'une liste de sites web distants, puis ouvrir une porte dérobée permettant la prise de contrôle à distance et se propager par courrier électronique en utilisant votre carnet d'adresses et son propre moteur SMTP. Belle performance ! Cependant, Bagle.BJ est lui-même très vulnérable. Grâce à un faisceau d'indices qui le caractérisent, il est facilement identifiable. Il emploie par exemple

toujours les mêmes sujets et corps de message, sa taille est constante (17 ou 19 Ko) et les différents noms et types de sa pièce jointe sont eux aussi parfaitement identifiés. Pour un programme informatique, c'est un jeu d'enfant d'analyser vos messages entrants et, à la lumière de ces indices (en supposant qu'il les connaisse) d'identifier rapidement un message dont les caractéristiques trahirait la présence potentielle de Bagle.BJ.

Dès l'apparition d'un nouveau virus, les éditeurs se mobilisent : ils décortiquent minutieusement son code, cherchent à comprendre précisément son fonctionnement, son mode de propagation et les risques potentiels qu'il fait courir aux ordinateurs. Ils vont aussi tenter de dégager un faisceau d'indices caractéristiques de ce virus : ce que l'on appelle communément la **signature** du virus.

Signature d'un virus

C'est un ensemble d'indices caractéristiques d'un virus. Lorsque tous ces indices sont détectés dans un fichier ou un message, il est très probable que ce dernier soit infecté.

L'ensemble des signatures de tous les virus connus jusqu'à ce jour est ce l'on appelle la base de signatures ou **fichier des définitions de virus**. Les programmes antivirus se basent en partie sur ce fichier pour mener à bien leur analyse. Pour que les derniers virus puissent être reconnus, il va de soi que le fichier des définitions de virus doit être scrupuleusement maintenu à jour sur votre machine.

Détection des menaces

Il existe à l'heure actuelle plusieurs techniques pour détecter la présence potentielle d'un virus. Tous les grands antivirus font appel à l'ensemble de ces techniques, bien qu'ils ne leur accordent pas nécessairement la même importance.

Détection par reconnaissance de la signature d'un virus

Il s'agit de la méthode la plus répandue : tous les grands logiciels antivirus, ou presque, y ont recours. Le moteur d'analyse recherche sur le disque dur toute chaîne de caractères, séquence ou caractéristique identifiée comme appartenant à un virus. Bien entendu, l'identification ne peut avoir lieu que si la signature est présente dans le fichier des définitions de virus. Cette méthode est très efficace, mais elle a des limites : si le fichier des définitions n'est pas à jour ou si le virus est encore inconnu, le programme antivirus ne vous sera d'aucune utilité.

COMPRENDRE Fichier des définitions de virus

Ce fichier regroupe toutes les signatures connues et sert de base aux antivirus. Il est complété au fur et à mesure que de nouveaux virus sont découverts et doit donc être constamment mis à jour sur votre machine.

Détection par vérification de l'intégrité des fichiers

Cette technique n'identifie pas nécessairement le virus, mais détecte une éventuelle compromission de votre poste. Nous avons vu précédemment qu'un virus pouvait modifier les exécutables, voire les commandes du système. L'un des symptômes de la contamination peut être la modification de la taille d'un exécutable. Le programme antivirus calcule donc un

Fonction de hachage

Les fonctions de hachage servent beaucoup en cryptologie ou lorsqu'il s'agit de contrôler des données. Elles associent un entier particulier à une chaîne de caractères, de telle façon qu'il soit extrêmement peu probable de trouver une autre chaîne produisant le même entier.
Pour plus de détails sur ces fonctions, reportez-vous à l'annexe A.

condensé des fichiers qu'il juge importants (sur le modèle des codes de hachage cryptologiques de type MD5 ou SHA-1) et compare régulièrement les valeurs recalculées aux valeurs originales. En cas de modification, votre système est probablement contaminé et il vous appartient de prendre les mesures qui s'imposent.

Surveillance du comportement des processus de l'ordinateur

Un processus du programme antivirus reste actif en arrière-plan et observe en temps réel le comportement des autres processus. Il ne cherche pas à identifier les virus, mais plutôt à tracer les activités suspectes qui pourraient traduire la présence éventuelle d'un code malveillant. Il va donc rechercher les tentatives d'ouverture en lecture/écriture de fichiers exécutables, les tentatives d'écriture sur les secteurs d'amorce ou les accès en écriture dans certaines zones du registre. En effet, l'une des actions de prédilection des vers, des chevaux de Troie ou des logiciels espions consiste à entrer certaines clés de registre dans des endroits stratégiques, de manière à ce que Windows les lancent automatiquement au démarrage de la machine.

Méthode heuristique

La méthode heuristique est une technique puissante permettant la détection des virus inconnus. Mise en œuvre dans la plupart des grands antivirus, elle complète avantageusement les deux méthodes précédentes, ainsi que les techniques basées sur l'analyse des signatures. La méthode heuristique consiste à localiser tous les codes potentiellement exécutables sur votre ordinateur. Elle analyse leur structure et leur logique de programmation, dans le but d'identifier les symptômes pouvant trahir la présence d'un virus. Par exemple, un code contenant une fonction d'envoi massif vers toutes les adresses du carnet est potentiellement suspect. De même, les routines d'ouverture de ports inhabituels, ou la présence de certaines routines cryptologiques dans un code (utilisées notamment par les virus polymorphes pour masquer leur signature) sont des éléments caractéristiques de codes malveillants pouvant conduire à la détection d'un virus inconnu.

Les grands antivirus ont globalement recours à toutes ces méthodes. Ils les utilisent judicieusement en fonction du type de tâche à réaliser (balayage complet du disque dur, analyse d'un simple fichier, protection en temps réel, analyse de la messagerie, etc.) en tâchant de ne pas perturber les performances de la machine. Les logiciels antivirus permettent généralement de paramétrer l'usage de ces méthodes.

Fonctionnalités importantes d'un logiciel antivirus

Il faut parfois se méfier des messages marketing des éditeurs, qui mettent en avant des fonctions d'intérêt mineur et passent sous silence d'autres souvent plus utiles. Sachez qu'un antivirus doit, au minimum, répondre aux exigences listées dans le tableau 3-1.

Tableau 3–1 Liste des fonctions indispensables d'un antivirus

Fonction	Description
Réponse aux urgences	En cas d'infection grave (l'ordinateur ne démarre plus !) : - possibilité de redémarrer l'ordinateur à partir du CD-Rom d'installation ou d'un jeu de disquettes d'urgence ; - balayage du ou des disque(s) infecté(s) et recherche des virus ; - nettoyage de l'infection, réparation des objets du système de fichiers, de la mémoire et des secteurs, restauration des informations d'amorce et de partition (à condition toutefois que le système d'exploitation soit réparable) ; - possibilité de créer des jeux de disquettes d'urgence.
Analyse et protection en temps réel	Pendant l'utilisation au quotidien, surveillance continue de l'ordinateur : - analyse des fichiers lors de leur création, modification ou accès ; - analyse des fichiers entrants et sortants lorsque la connexion Internet est active ; - recherche de virus à chaque utilisation d'un logiciel, ou lors de l'insertion d'un support amovible ; - analyse comportementale et/ou heuristique pour suppléer l'absence éventuelle d'une signature de virus ; - recherche permanente de codes malveillants sur la machine.
Analyse sur demande	Analyse planifiée ou sur requête explicite de l'utilisateur : - analyse d'un fichier, d'un répertoire ou d'un disque dur complet (tous les fichiers doivent être passés au crible) ; - détection et nettoyage des virus contenus dans des fichiers compressés (ZIP, GZIP, RAR, TAR, etc.).
Réparation	Capacités réelles de l'antivirus à réparer l'ordinateur après l'infection : - réparation des objets du système de fichiers, de la mémoire et des secteurs ; - suppression ou mise en quarantaine des fichiers infectés, nettoyage du registre ; - mise à disposition d'outils de nettoyage récents par l'éditeur (via par exemple une page web de type *Security Response*) ; - redémarrage ou non de l'ordinateur en mode sans échec.
Mises à jour de l'antivirus	Téléchargement et installation automatiques des mises à jour par l'antivirus : - actualisation automatique des fichiers de définitions de virus et des composants du moteur d'analyse ; - publication quotidienne, voire plusieurs fois par jour, des nouvelles définitions de virus ; - publication rapide des mises à jour et des outils de nettoyage en cas d'alerte virale.

Les antivirus fournissent aussi d'autres fonctionnalités pratiques. Elles présenteront toujours un caractère stratégique moins important que les fonctions listées au tableau 3-1. Toutefois, elles peuvent renforcer le niveau de protection général de l'antivirus, et en faciliter l'utilisation.

Tableau 3–2 Liste des fonctions optionnelles d'un antivirus

Fonction	Description
Analyse de la messagerie	Analyse des messages entrants et/ou sortants (logiciel de courrier électronique et messagerie instantanée) : - analyse continue des pièces jointes ; - détection des virus et des vers envoyés par d'autres utilisateurs ; - blocage des courriers sortants infectés afin d'empêcher la transmission et la propagation des vers ; - filtrage du courrier électronique non sollicité (analyse antispam). Soyez tout de même vigilant : les antivirus ne prennent pas forcément en charge tous les clients de messagerie. Si vous utilisez des messageries basées sur les protocoles POP3 et SMTP (Outlook, Thunderbird, Eudora, Netscape Messenger, etc.) vous n'aurez probablement pas de problème. En revanche, vérifiez que l'antivirus prend bien en charge, si vous les utilisez : - les clients de messagerie tels que IMAP, AOL ou Lotus Notes ; - les messageries instantanées telles que Hotmail, Yahoo! ; - les messages sécurisés avec le protocole SSL.
Blocage de scripts	Analyse des scripts JavaScript dynamiques et contrôles ActiveX téléchargés depuis Internet.
Mise en quarantaine	Isolement des objets suspects afin de tenter une réparation manuelle.
Affichage du rapport d'analyse	Affichage de l'historique d'activité de l'antivirus (menaces, alertes, activité système, incidents rencontrés lors de l'analyse, etc.).
Mise à jour à partir d'un réseau interne	Mise en place d'un serveur capable de mettre à jour l'antivirus à partir d'un réseau interne (ce besoin concerne plutôt les entreprises dotées d'un réseau protégé par un pare-feu).
Restriction d'accès aux fonctions d'administration	Protection de l'accès aux fonctions de configuration et de gestion de l'antivirus (mot de passe par exemple).

BON À SAVOIR **Antispam et blocage de scripts**

Certaines fonctionnalités, comme l'antispam ou le blocage de scripts, seront prises en charge par d'autres éléments de votre architecture (client de messagerie, navigateur web, etc.). Nous aborderons ces sujets ultérieurement dans cet ouvrage.

Si l'antivirus ne prend pas en charge votre client de messagerie, cela ne veut pas dire que vous n'êtes pas protégé contre la réception d'un ver par courrier : un message reçu, en tant que fichier nouvellement créé sur votre poste, sera analysé de toute façon par l'antivirus.

Principaux antivirus du marché

Il existe aujourd'hui de nombreux antivirus ; tous n'offrent pas le même niveau de protection et certains se révèlent plus efficaces que d'autres. Le tableau 3-3 dresse la liste des logiciels qui présentent actuellement les meilleures performances du marché.

Cette liste n'est pas exhaustive. Il existe d'autres produits tels que Avast ! antivirus (Alwil Software), le logiciel gratuit AVG Antivirus (Grisoft), Command Antivirus (Authentium), GFI Mail Security (GFI software), Norman (Norman) ou ViGuard (Tegam International), qui se base exclusivement sur la détection des comportements malveillants.

Tableau 3–3 Liste des principaux antivirus du marché

Logiciel Antivirus	Suite logicielle	Éditeur	Site web
F-Secure Antivirus	F-Secure Internet Security	F-Secure	http://f-secure.fr/france
Kaspersky Antivirus Personal	Personal Security Suite	Kaspersky Lab	http://www.kaspersky.com/fr
BitDefender Standard Edition	BitDefender Professional Edition	SOFTWIN	http://fr.bitdefender.com
VirusScan	Internet securitysuite	McAfee	http://fr.mcafee.com
Panda Antivirus	Platinium Internet Security	Panda Software	http://www.pandasoftware.com/fr
PC-cillin Internet Security	PC-cillin Internet Security	Trend Micro	http://fr.trendmicro-europe.com
Norton Antivirus	Norton Internet Security	Symantec	http://www.symantec.fr
Antivir PersonalEdition Classic		AntiVir PersonalProducts GmbH	http://www.antivir.de
Sophos antivirus	Sophos Small Buisiness Suite	Sophos	http://www.sophos.fr
F-Prot Antivirus		FRISK Software International	http://www.f-prot.fr

Vous noterez que, pour la plupart, les grands éditeurs ne se contentent pas du seul produit antivirus. Ils commercialisent une suite logicielle intégrant dans un même produit un antivirus, un pare-feu personnel, un tueur de logiciels espions (antispyware), un bloqueur de pourriels (antispam) et d'autres programmes comme le contrôle parental ou des outils dédiés à la protection de la vie privée.

FONCTIONNALITÉ **Antivirus en ligne**

Notez que la plupart de ces éditeurs offrent gratuitement le scan anti-virus en ligne. Si vous n'avez pas encore acquis de logiciel antivirus et si votre poste est contaminé, connectez-vous sur le site d'un éditeur et laissez-vous guider par les instructions.

Choisir un antivirus

Pour beaucoup d'entre vous, cette question est un véritable casse-tête. Il faut bien se l'avouer, si on ne consacre pas du temps à étudier et à comparer les produits, le choix éclairé d'un antivirus n'est pas évident.

Pour rester simple, en choisissant l'un des logiciels du tableau 3-3, vous aurez peu de risques de vous tromper et bénéficierez globalement d'une bonne protection. Cependant, il existe entre ces produits des différences notables, que nous nous efforçons de mettre en évidence ci-après.

Une remarque toutefois : de façon générale, il faut rester prudent vis-à-vis des suites logicielles ; si elle garantissent un confort d'utilisation évident, tous les produits d'un même éditeur ne sont pas forcément de même niveau. Le pare-feu commercialisé avec un excellent antivirus peut très bien se révéler plus faible qu'on ne l'imaginait. Il est souvent plus intéressant d'avoir recours à l'excellent antivirus d'un éditeur, et au très bon pare-feu d'un autre éditeur tout en utilisant l'efficace tueur de logiciels espions d'un troisième éditeur. Attention toutefois aux problèmes de conflits entre produits : si vous optez pour cette approche, prenez soin de valider la viabilité technique de votre architecture en testant les versions d'évaluation proposées sur les sites web des éditeurs.

PRÉCISION

Nos critères de jugement des antivirus

L'expérience prouve que l'évaluation d'un produit antivirus n'est pas une science exacte. Il existe visiblement plusieurs manières de comparer les produits entre eux, et les classements finaux obtenus dans les revues spécialisées varient au gré des critères – objectifs et subjectifs – retenus, et de leur pondération. Le but de ce livre n'est pas de faire la promotion commerciale de tel ou tel produit, mais de vous guider dans votre choix, afin qu'il réponde parfaitement à votre besoin. Pour cette raison, nous laissons volontairement de côté des critères secondaires ou annexes, comme l'espace disque occupé, la facilité d'installation ou le prix du logiciel, que nous vous laisserons découvrir sur les sites des éditeurs, et en fonction desquels il vous appartiendra de prendre votre décision.

PARTICULIERS **Fréquence des mises à jour**

Par ailleurs, au risque de faire hurler certains administrateurs systèmes, nous ne pensons pas que la fréquence des mises à jour soit un critère susceptible d'influencer significativement votre décision. Entendons-nous bien : nous parlons ici au nom des particuliers. Si vous avez en charge la sécurité des postes d'une petite entreprise, la fréquence des mises à jour est évidemment un critère à prendre en compte. En cas d'alerte virale, tous les grands éditeurs publient généralement leur mise à jour dans un laps de temps compris entre 3 et 10 heures, parfois plus mais cela dépasse rarement les 20 heures. Si vous êtes un particulier, en cas d'alerte sérieuse, un moyen simple d'éviter la contamination consiste à laisser passer l'orage et à attendre que la mise à jour soit disponible avant de vous risquer à nouveau sur Internet.

Les trois critères que nous jugeons importants pour choisir un antivirus sont les suivants :

- Efficacité – Le principal critère est son efficacité, c'est-à-dire sa capacité à détecter et à bloquer les codes malveillants avant qu'ils infectent votre machine. L'antivirus parfait serait capable de détecter 100 % des attaques, connues ou inconnues ; malheureusement cet antivirus n'existe pas, bien que certains, comme nous allons le voir, s'en approchent de plus en plus.
- Fonctions indispensables – Le taux de couverture des fonctions indispensables répertoriées au tableau 3-1 doit être le plus grand possible.
- Capacité de nettoyage – Enfin le troisième critère (et non le moindre) est la capacité à nettoyer la machine après l'infection. Il faut que vous sachiez qu'en dépit des plaquettes commerciales, beaucoup d'outils, y compris les grands, pêchent réellement lorsqu'il s'agit de nettoyer une machine infectée. Malheureusement, nous disposons de peu d'éléments relatifs à ce dernier critère. Il convient toutefois de ne pas incriminer déraisonnablement un antivirus qui ne parviendrait pas à réparer correctement une machine ; n'oublions pas que les virus sont destructeurs et que les dommages causés par certains codes malveillants sont difficilement réparables.

F-Secure Antivirus

Il est indiscutablement l'un des meilleurs antivirus du marché, sinon le meilleur, en raison de l'excellence de son moteur d'analyse et de la compétence de ses techniciens, parmi les meilleurs au monde. F-Secure Antivirus détecte près de 100 % des virus connus et surclasserait même ses concurrents BitDefender, McAfee VirusScan et surtout Kaspersky, qui jouit d'une excellente réputation auprès des professionnels du domaine.

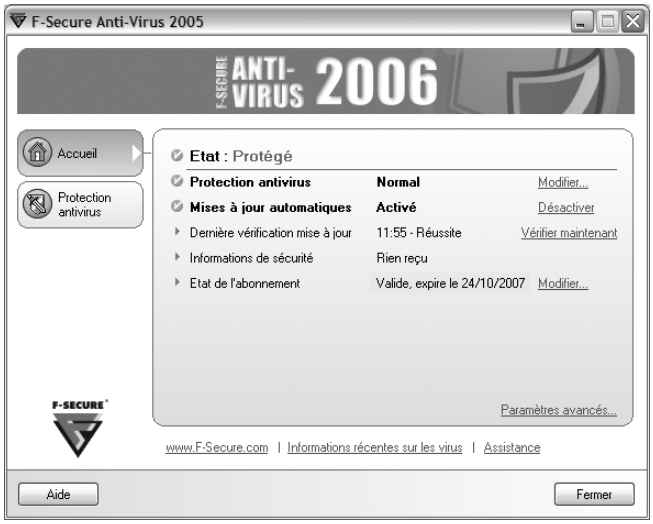


Figure 3–4
Fenêtre d'accueil de F-Secure Antivirus

La simplicité de l'interface de F-Secure Antivirus s'apparente à celle de Panda Antivirus, et son élégance en fait un produit très agréable à utiliser.

Selon certains experts, F-Secure Antivirus serait gourmand en ressources et s'avèrerait par conséquent plutôt indiqué pour des PC puissants. Toutefois, nous l'avons testé sur des machines récentes d'entrée et de moyenne gamme, mais n'avons pas décelé de ralentissement significatif susceptible de gêner le travail, y compris lorsque l'analyse en temps réel était activée. Ce produit est visiblement bien conçu ; il se fait complètement oublier. Il détecte automatiquement la connexion à Internet et engage lui-même les procédures de mise à jour. Si vous fermez cette connexion avant la fin des téléchargements, F-Secure reprendra le processus lors de la prochaine connexion, là où il s'était interrompu.

Figure 3–5
Fenêtre d'accueil de F-Secure Anti-Spyware

Les mises à jour sont assez fréquentes ; elles ont lieu généralement sous 6 heures. F-Secure Antivirus fonctionne en outre avec un tueur de logiciels espions, F-Secure Anti-Spyware, dont l'interface ressemble à s'y méprendre à celle du logiciel Ad-Aware présenté plus loin.

F-Secure Antivirus est un excellent produit offrant un panel de fonctions très complet et un bon niveau d'efficacité.

Kaspersky Anti-Virus

TROU DE MÉMOIRE **Analyse heuristique**

La méthode heuristique est expliquée page 86

Considéré comme l'un des plus efficaces du marché, Kaspersky Anti-Virus détecte aussi près de 100 % des virus connus. Il dispose d'une analyse heuristique dépistant les activités ou les comportements suspects, et bloque en conséquence des virus inconnus (pas tous cependant). Les mises à jour sont rapides : Kaspersky Lab met un nouveau fichier de définition de virus à disposition toutes les quatre heures environ.

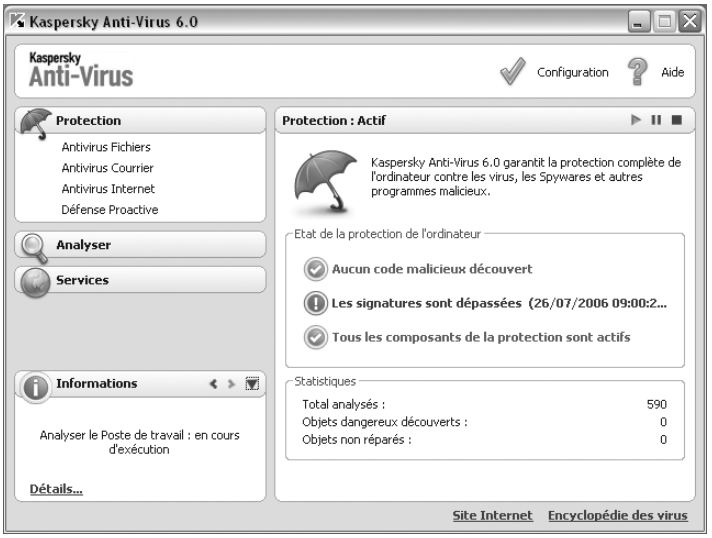


Figure 3–6
Fenêtre d'accueil de Kaspersky Antivirus Personal Pro

Kaspersky dispose de multiples paramétrages offrant aux utilisateurs avertis de riches possibilités de configuration. Vous pouvez définir des politiques de protection en descendant jusqu'à un niveau extrêmement fin. Notez chez Kaspersky un très intéressant volet fonctionnel intitulé *Défense Proactive* (figure 3-7). Ce module regroupe les mécanismes de protection contre les menaces récentes, dont la signature ne figure pas encore dans la base. Cet élément offre notamment :

- une fonction de détection des activités dangereuses des applications (introduction de valeurs suspectes dans le Registre, tentatives d'implantation de rootkits, activités suspectes du système) ;

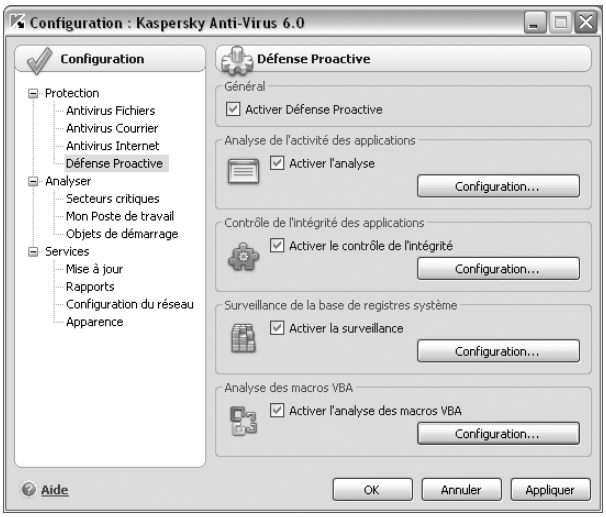


Figure 3–7 Exemple des possibilités de configuration de Kaspersky Anti-Virus Personal Pro

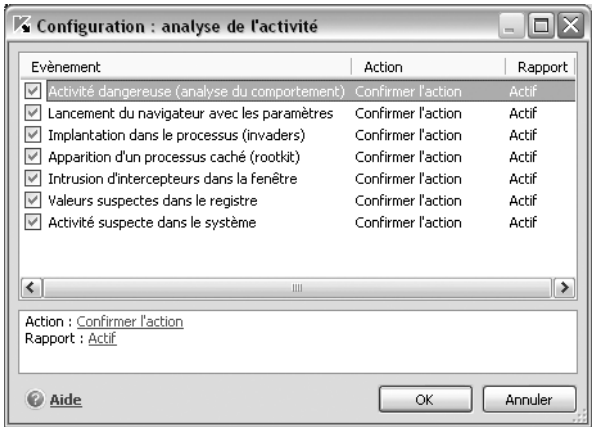


Figure 3–8 Surveillance de l'activité du système

- un contrôle d'intégrité des applications (pour assurer notamment que les processus et applications clés du système ne soient pas pervertis par un processus malveillant) ;
- un système de surveillance en temps réel de la base de registres, et l'étonnant module d'analyse des macros VBA, déjà présent dans les versions précédentes (macros contenues à l'intérieur des documents MS-Office), permettant d'effectuer un contrôle extrêmement fin des actions réalisées par ces macros.

Kaspersky Antivirus offre en outre un module d'analyse de trafic de la messagerie (il prend notamment en charge les protocoles POP3, SMTP, IMAP et NNTP), d'Internet (HTTP), et intègre un programme de détection des programmes espions et des logiciels publicitaires. Bien entendu, toutes les fonctions primordiales d'un antivirus sont présentes : analyse des fichiers et des courriers électroniques, quarantaine, mise à jour automatique, protection en temps réel, analyse complète de l'ordinateur ou analyse des fichiers, dossiers ou lecteurs de votre choix, rapports détaillés, etc. Fidèle à sa réputation, Kaspersky Antivirus offre une ligne de protection de haute volée.

BitDefender

BitDefender fait lui aussi partie des antivirus de tout premier plan : sa capacité de détection avoisine les 100 % en ce qui concerne les virus connus et affiche de très bons résultats pour la détection des virus inconnus.

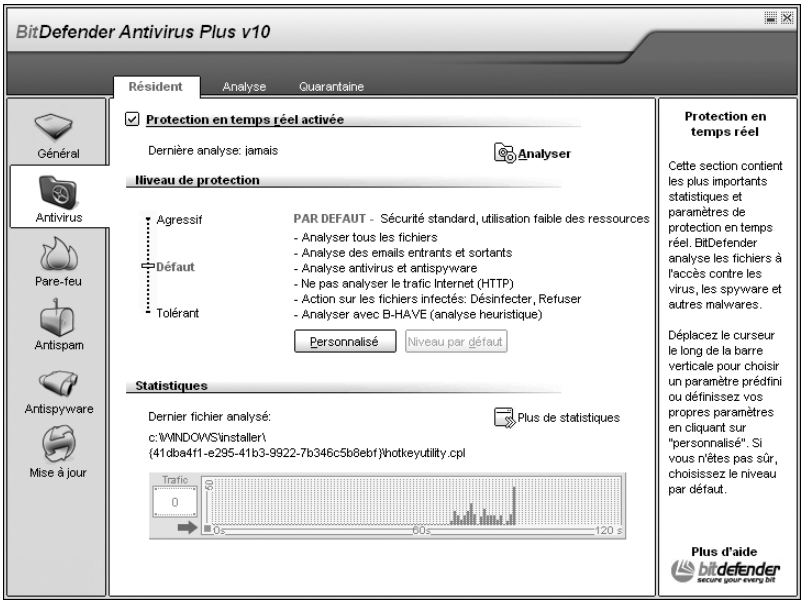


Figure 3–9
Fenêtre d'accueil de
BitDefender Antivirus Plus V10

Figure 3–10 BitDefender détecte, entre autres, les tentatives de modification du registre.

Contrairement à la plupart de ses concurrents, BitDefender sait balayer les volumes en réseau. Il présente l'avantage de prendre en charge plusieurs messageries instantanées, comme ICQ, Yahoo! Messenger, NetMeeting ou MSN Messenger, ainsi que les échanges peer-to-peer (Kazaa, Emule) et offre une protection pour de nombreux clients de messagerie, comme MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat.

Il protège votre ordinateur en temps réel et vous alerte dès qu'un programme tente de modifier le registre, comme le montre la figure 3-10.

Par ailleurs, BitDefender semble ne pas trop accaparer de ressources système, car l'utilisateur peut continuer à travailler pendant l'analyse complète de son PC, sans gêne significative. En outre, le résident qui assure la protection en temps réel de l'ordinateur se fait complètement oublier.

L'interface utilisateur est agréable. BitDefender Standard Edition est globalement un très bon produit pour les particuliers. On peut regretter en revanche qu'il ne permette pas de créer un jeu de disques de secours.

McAfee VirusScan

Le logiciel VirusScan de McAfee fait lui aussi partie du gratin des produits dotés d'un très haut niveau de fiabilité. Son taux de détection des virus connus est proche de 100 % et il montre un certain talent à découvrir les virus inconnus. D'une efficacité très légèrement inférieure à celle de F-Secure Anti-Virus, VirusScan est comparable à Kaspersky, BitDefender ou Panda Antivirus.

McAfee VirusScan est en outre performant pour assurer la protection antivirale au niveau d'une entreprise et dispose de fonctions de configuration et de contrôle très étoffées. Cependant, on peut déplorer un net ralentissement de la machine pendant les phases de balayage complet, qui s'avère réellement gênant sur des ordinateurs anciens.

Panda Antivirus

L'efficacité du produit Panda Antivirus est elle aussi très élevée, puisqu'elle talonne de près celles de Kasperky, BitDefender, VirusScan ou F-Secure et surpasse généralement celle de ses autres concurrents. Sa vitesse d'analyse est absolument impressionnante. En outre, le logiciel télécharge et installe lui-même, sans vous déranger, les mises à jour des définitions de virus et du moteur d'analyse. On peut toutefois noter que les fonctions de protection en temps réel induisent un léger ralentissement de l'ordinateur, ainsi qu'une certaine latence au moment du démarrage, qui, à la longue, s'avère agaçante.

Néanmoins, Titanium Antivirus dispose d'une interface utilisateur d'une simplicité déconcertante, à la fois attrayante et ludique. Les concepteurs du produit ont délibérément choisi de limiter les capacités de configuration du logiciel. En cela, ils se situent aux antipodes de Kaspersky et ont probablement ciblé des utilisateurs peu sensibles aux problèmes de paramétrage. Ce choix est tout à fait respectable, d'autant qu'il ne diminue absolument pas le niveau de protection offert par l'antivirus. Les quelques options disponibles, à savoir l'analyse heuristique, la détection des logiciels espions, des outils de piratage ou des numéroteurs, ainsi que la mise à jour automatique, sont presque toutes activées par défaut. Sans intervention de l'utilisateur, le logiciel délivre donc son niveau de protection maximale.

Parallèlement à cela, Panda Antivirus intègre un programme antispyware (figure 3-11) pouvant se révéler particulièrement utile dans certaines circonstances !

Le produit Panda Antivirus est un très bon antivirus pouvant tout à fait convenir aux utilisateurs peu familiers de l'outil informatique.

Figure 3–11 Protection antispyware de Titanium Antivirus

PC-cillin Internet Security

PC-cillin Internet Security est une suite logicielle incluant l'antivirus, le pare-feu, l'anti-programmes espions et un logiciel de filtrage antispam. Ce logiciel propose également des outils additionnels comme l'anti-phishing, un système de contrôle parental et une détection d'intrusion Wi-Fi. L'antivirus n'est pas commercialisé séparément.

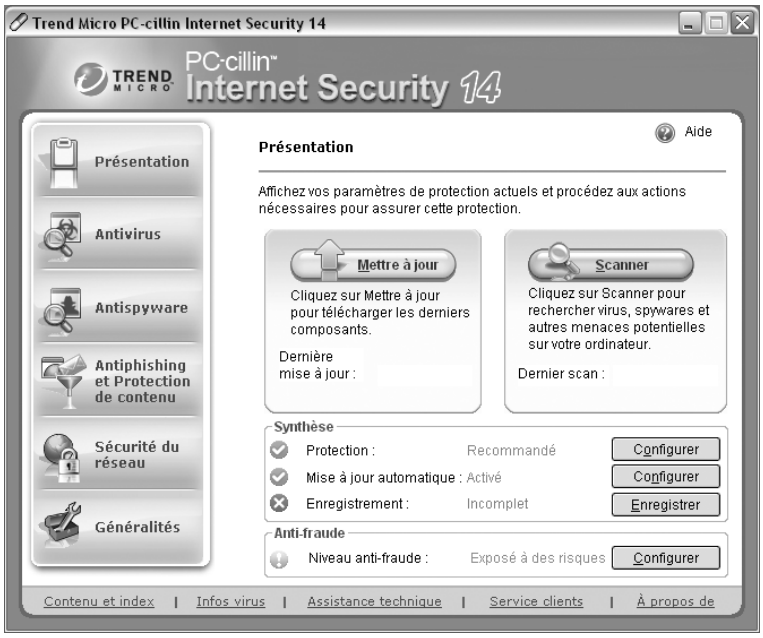


Figure 3–12
Fenêtre d'accueil de PC-cillin

Il s'agit globalement d'un produit très complet. Il est clair que la possibilité d'accéder directement aux différents logiciels à travers une interface unique apporte un certain confort à l'utilisateur, mais sur ce point PC-cillin n'offre rien de plus que les éditeurs qui commercialisent une suite logicielle.

En terme de fiabilité, l'antivirus de PC-cillin Internet Security affiche de bons résultats, bien que, de temps en temps, il manifeste quelques faiblesses, surtout vis-à-vis des chevaux de Troie et des logiciels espions. En revanche, son filtre antispam est excellent. Nous avons noté que, sur une machine récente d'entrée de gamme, la fonction de protection en temps réel n'affectait pas l'utilisateur dans ses tâches quotidiennes, y compris après avoir activé tous les paramètres. De plus, la fonction de balayage complet du système n'affecte pas la poursuite du travail.

Son interface est simple et offre de nombreuses fonctions de configuration (figure 3-12). En outre, PC-cillin dispose d'une fonction intéressante : il vous permet d'effectuer des tests de sécurité sur votre poste, et vous affiche une alerte s'il détecte des vulnérabilités inquiétantes (figure 3-13).

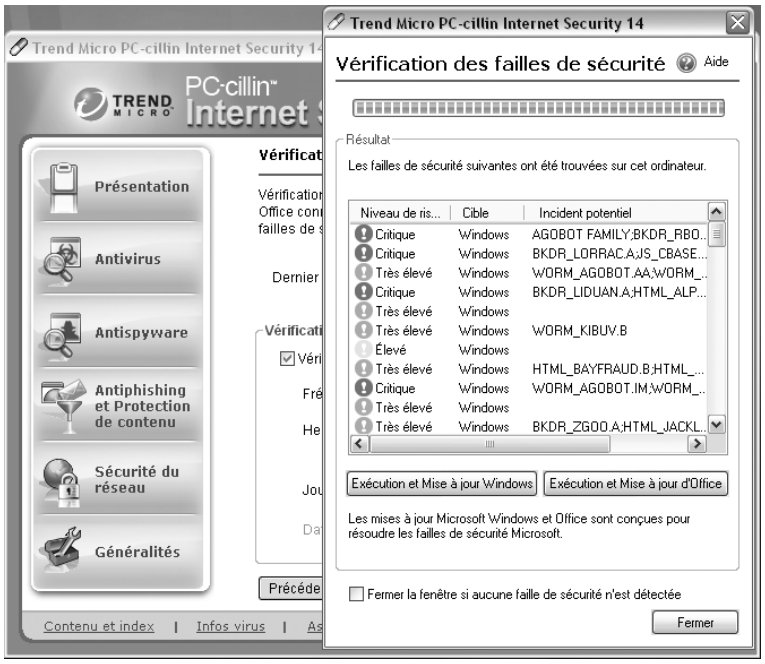


Figure 3–13
Test de sécurité avec PC-cillin

Norton Antivirus

Norton Antivirus fait lui aussi partie des produits les plus répandus du marché. Il affiche globalement de bons résultats bien que, de temps en temps, il ne parvienne pas à repérer un virus ou un cheval de Troie. De plus, de nombreux utilisateurs se plaignent du manque de réactivité de Symantec, en matière de publication et de mises à jour.

Cependant, Norton Antivirus offre de riches fonctionnalités. Avant même d'avoir installé le logiciel, vous pouvez lancer un balayage du disque dur à partir du CD-Rom d'installation ou de disquettes de secours, et procéder ainsi à la réparation d'urgence – ou à la mise en quarantaine – des fichiers infectés. Cette fonctionnalité s'avère réellement salutaire en cas de contamination.

L'interface de Norton Antivirus est élaborée, claire et très bien faite. Un seul coup d'œil sur la fenêtre principale vous renseigne sur l'état du système et vous disposez, à partir de cet écran, d'un accès direct et rapide à toutes les fonctions de l'antivirus. Vous configurez les paramètres de celui-ci à travers le bouton *Options* et vous activez manuellement la procédure de mise à jour d'un simple clic sur *LiveUpdate*.

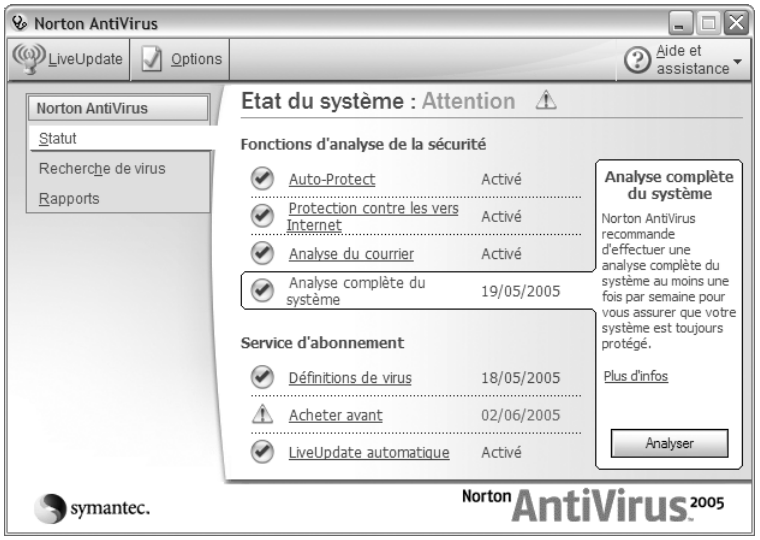


Figure 3–14
Fenêtre d'accueil de Norton Antivirus

En outre, Norton Antivirus vous offre une protection contre les logiciels publicitaires, les logiciels espions, les scripts malveillants, les numéroteurs ou les outils de piratage (figure 3-15). Lorsqu'une menace est identifiée, vous avez la possibilité de réparer, supprimer ou mettre en quarantaine le fichier incriminé.

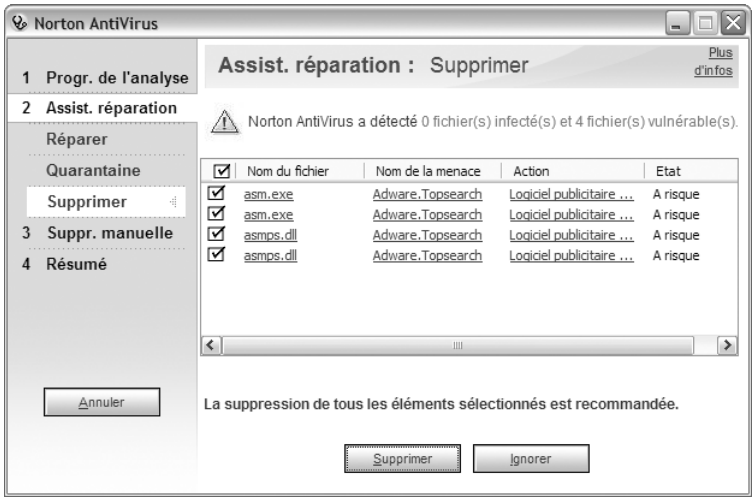


Figure 3–15
Identification de logiciels publicitaires ou de logiciels espions avec Norton Antivirus

En revanche, quelques points négatifs sont tout de même à déplorer. Norton Antivirus est gourmand en ressources et nous avons noté un ralentissement de l'ordinateur, surtout pendant la phase d'analyse complète, y compris sur une machine récente. Le système d'actualisation est manifestement moins souple qu'avec d'autres produits et nous avons

parfois été obligés de lancer plusieurs fois la fonction LiveUpdate afin de réussir à télécharger complètement une mise à jour.

Globalement, Norton Antivirus est un produit sérieux, mais qui nécessite quelques améliorations. Une détection plus complète des virus serait la bienvenue, ainsi qu'une diminution très nette de la consommation des ressources de l'ordinateur. En outre, Symantec devrait s'attacher à le rendre plus transparent, notamment en ce qui concerne les mises à jour.

AntiVir Personal Edition Classic

Bien que se situant en moyenne légèrement en retrait des meilleurs antivirus payants, Antivir Personal Edition Classic affiche tout de même un bon niveau d'efficacité en matière de détection, et s'offre parfois le luxe de détecter des codes malveillants que certains de ses concurrents laissent passer ! Ceci est particulièrement remarquable sachant que cet antivirus est gratuit pour une utilisation personnelle.

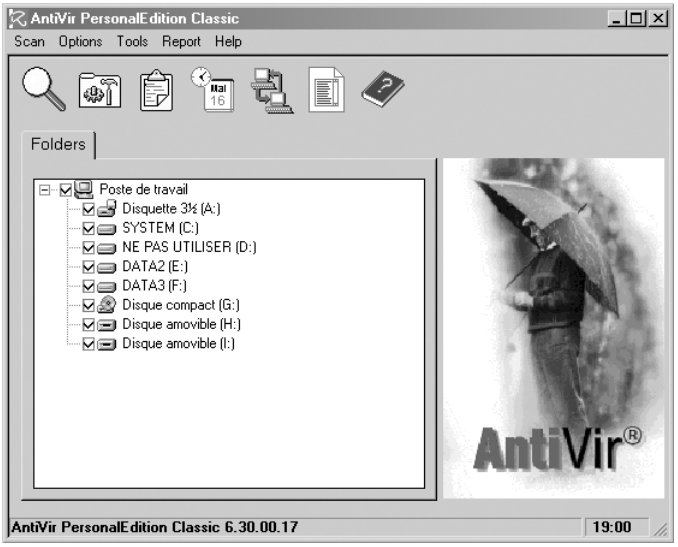


Figure 3–16
Fenêtre d'accueil d'AntiVir

Son interface est en anglais, elle n'est pas particulièrement attractive et s'avère relativement confuse. Cependant, AntiVir dispose d'un paramètre de configuration très précieux : si vous réglez *Priority* (à partir de l'écran principal, cliquez sur *Options*, puis sur *Configuration*) sur *medium* ou sur *low*, AntiVir s'alloue un faible quota de ressources ; vous pourrez ainsi continuer à travailler sur votre poste sans noter de dégradation significative des performances, y compris pendant une analyse complète, même si votre PC est ancien.

AntiVir offre les fonctions de base des antivirus : un module de protection automatique fonctionnant en tâche de fond (AntiVir Guard), la mise à jour automatique sur Internet, l'analyse heuristique des macros et des fichiers Windows, la planification de tâches, comme l'analyse complète du poste. Il est incontestablement le meilleur antivirus gratuit disponible à l'heure actuelle. Si vous disposez d'un budget limité, AntiVir est une très bonne solution pour protéger votre poste.

Sophos antivirus

Bien que les produits Sophos soient plutôt orientés vers les entreprises (PME et grandes entreprises), il convient de mentionner l'excellence d'un logiciel qui peut tout à fait répondre à votre besoin, si vous souhaitez équiper votre petite entreprise.

Les produits Sophos pour les PME (Sophos Small Business Suite, Sophos Antivirus Small Business Edition) détectent un pourcentage très élevé de virus et ont été conçus pour protéger les réseaux d'ordinateurs fonctionnant sous Windows et MacIntosh, ainsi que les serveurs de messagerie et les serveurs de réseau. Ils disposent d'outils permettant le déploiement centralisé du logiciel.

En outre, les moteurs de détection antivirus et antispam de Sophos sont également utilisés par différents constructeurs d'équipements de sécurité pour renforcer le niveau de protection délivré par leur produit. C'est le cas par exemple des pare-feux Arkoon (voir chapitre 5), au sein desquels un contrôle antivirus est systématiquement appliqué par rapport à tous les protocoles jugés à risque sur Internet (HTTP, SMTP, FTP, etc.). Ce type de solution est très intéressant pour les entreprises (y compris les petites entreprises de moins de dix postes). Ainsi, elles peuvent éventuellement mettre en œuvre une double protection antivirale pour atteindre un haut niveau de sécurité. La deuxième protection est obtenue avec un produit antivirus d'un autre éditeur sur les serveurs et sur les postes.

BON REFLEXE **Prévenir vaut mieux que guérir**

Les éditeurs réagissent souvent avec diligence lorsqu'une nouvelle menace apparaît. Toutefois, ils gèrent leurs priorités et il leur arrive de publier tardivement l'outil de désinfection et la mise à jour, même en cas d'alerte sérieuse. Pendant ce laps de temps, vous serez vulnérable : évitez les connexions et clics potentiellement dangereux.
En dépit des plaquettes commerciales flatteuses, les antivirus, y compris les grands, ne sauront pas forcément nettoyer correctement votre machine après l'infection. Si vous tenez à vos données, mettez tout en œuvre pour éviter la contamination.

PRÉCISION Choisir son antivirus

Tous ces avis vous sont donnés à titre indicatif et n'engagent que l'auteur de ces lignes. Sachez qu'à l'heure actuelle, il n'existe pas d'avis consensuel ou de recommandation d'experts en matière de choix d'antivirus. N'oubliez pas que, même si certains produits s'en approchent, aucun logiciel antivirus ne sait reconnaître 100 % des attaques. C'est la raison pour laquelle les entreprises optent généralement pour le choix de deux – voire trois ! – antivirus d'éditeurs différents, en espérant que l'attaque ignorée par l'un sera contrée par le ou les autres. Par ailleurs, hormis le logiciel AntiVir, les antivirus gratuits offrent un taux de détection moins bon (certains sont même perçus comme de vraies passoires).

Installer un nouveau logiciel antivirus

Si votre machine est déjà dotée d'un produit antivirus, vous n'aurez probablement pas d'autre choix que de le désinstaller. Cliquez pour cela sur *Démarrer*, *Panneau de configuration*, puis sur *Ajouter ou supprimer des programmes*. Cliquez ensuite sur le programme antivirus à désinstaller et sur *Supprimer* (figure 3-17).

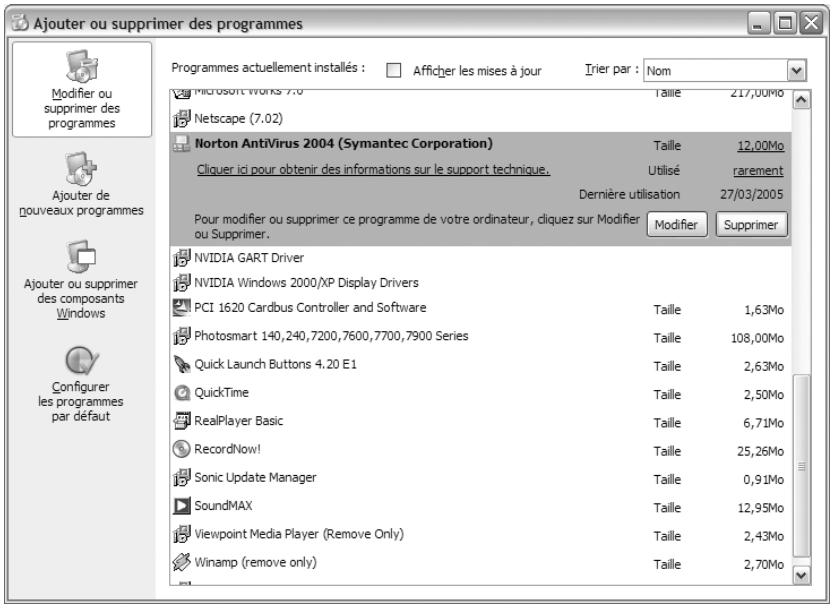


Figure 3–17
Désinstaller l'ancien antivirus

Pour installer votre nouvel antivirus, insérez le CD-Rom d'installation dans votre lecteur, ou bien cliquez deux fois sur le module exécutable que vous avez téléchargé sur Internet. Suivez ensuite les instructions, le logiciel s'installe tout seul.

PRÉCISION Désinstaller un antivirus

La figure 3-17 montre à titre d'exemple comment procéder pour supprimer un antivirus. N'y voyez pas de message caché, Norton Antivirus est un bon produit.

Dans la plupart des cas, il vous faudra redémarrer votre poste à la fin de l'installation. Cette opération effectuée, votre nouvel antivirus fonctionne et protège déjà vos fichiers et vos accès Internet, grâce à la protection automatique généralement activée par défaut. La petite icône qui apparaît dans la barre des tâches du système (figure 3-18) vous indique clairement la présence de l'antivirus en tâche de fond.

Figure 3–18
Le petit panda indique que l'antivirus fonctionne en tâche de fond et protège votre ordinateur en temps réel.

Mise à jour et première analyse

La première chose à faire après l'installation est de vous assurer que votre antivirus est bien à jour. En effet, le moteur d'analyse a peut-être évolué par rapport à la version gravée sur le CR-Rom ou celle que vous avez téléchargée depuis Internet ; par ailleurs, il est certain que plusieurs centaines ou plusieurs milliers de nouveaux virus sont apparus depuis le jour de la publication de cette version. Il faut donc télécharger le nouveau fichier de définitions de virus. Il se peut d'ailleurs que votre antivirus détecte lui-même son niveau d'obsolescence et vous incite spontanément à effectuer cette mise à jour (figure 3-19).

Pour effectuer la mise à jour, vous n'avez qu'à cliquer sur le lien *Mettre à jour l'antivirus*, situé en bas de cet écran. Vous pouvez aussi réaliser l'opération en faisant apparaître la fenêtre principale de l'antivirus ; pour cela, cliquez droit sur son icône dans la barre des tâches et sélectionnez *Ouvrir Panda Antivirus*. Vous constatez d'ailleurs sur la figure 3-20 qu'il s'est écoulé un laps de temps considérable (à l'échelle « virusienne », cela s'entend), entre la date de la version du produit que vous venez d'installer et la date effective de l'installation (vous pouvez visualiser cette date à la figure 3-19).

Avec Panda Antivirus, il vous suffit donc de cliquer à l'intérieur de la section gauche de l'écran sur l'option *Mise à jour* pour accéder aux fonctions d'actualisation de l'antivirus (figure 3-21). Cliquez sur *Mettre à jour Panda AV 2007 maintenant !* et votre logiciel téléchargera les modules récents du programme ainsi que les nouvelles définitions de virus. Si la mise à jour automatique est activée par défaut (ce qui est le cas avec la plupart des antivirus), celle-ci se fera automatiquement.

Notez au passage que votre connexion à Internet doit être active pour effectuer cette opération.

MÉTHODE Antivirus exemple

Dans les exemples présentés, nous illustrerons notre propos en faisant essentiellement appel à l'interface du logiciel Panda Antivirus. N'y voyez pas de message commercial particulier. Ce produit est simplement doté d'une interface très pédagogique, qui contient à peu près toutes les grandes familles de paramètres et de fonctions rencontrées avec la plupart des antivirus ; elle est intuitive et simple, ce qui vous aidera à vous familiariser avec les problèmes de gestion de l'antivirus.

Figure 3–19 Niveau de protection réel de l'ordinateur lorsque l'antivirus n'est pas à jour

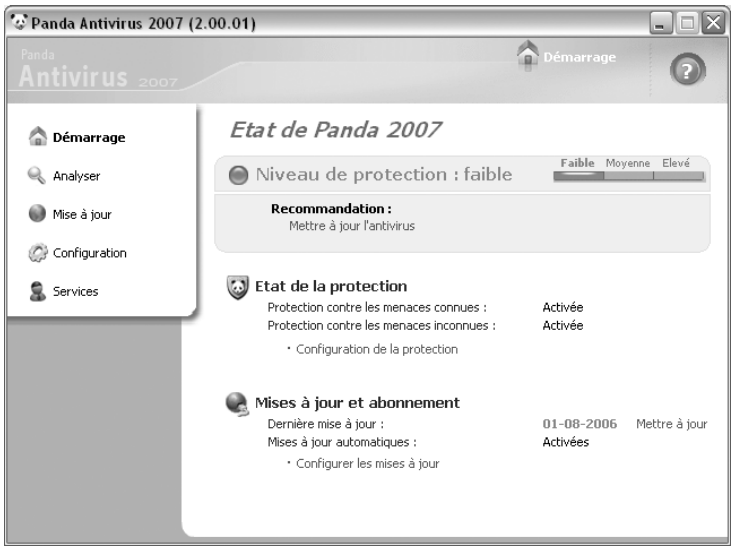


Figure 3–20
Fenêtre principale de Panda Antivirus

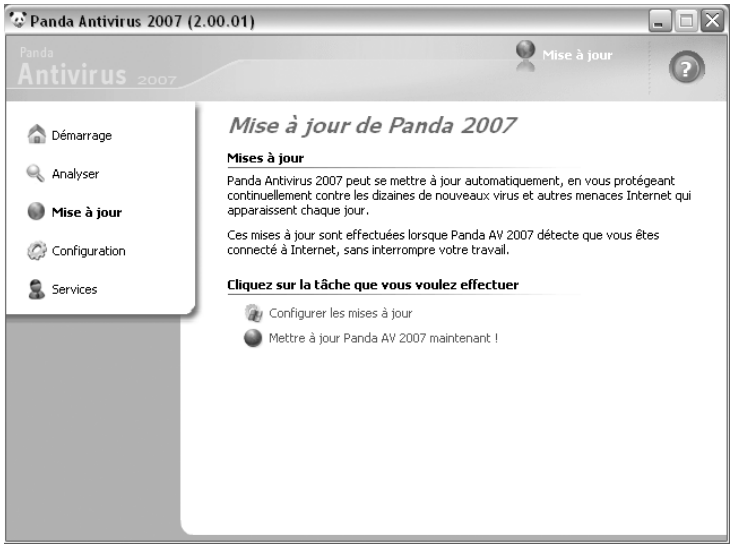


Figure 3–21
Lancement de la mise à jour de l'antivirus

Dès que l'antivirus est à jour, vous verrez s'afficher un message similaire à celui de la figure 3-22. Il est recommandé de lancer une analyse complète de votre système afin d'éradiquer la présence éventuelle de virus.

Avec Panda Antivirus, sélectionnez l'option *Analyser*, puis cliquez sur *Analyser tout mon ordinateur* (figure 3-23).

Figure 3–22 Lorsque l'antivirus est à jour, le niveau de protection est élevé.

Figure 3–23
Analyse complète de l'ordinateur

Vous pouvez analyser tout l'ordinateur, ou bien de limiter l'examen aux disques durs, au courrier électronique ou à d'autres éléments, tels que la mémoire, certains répertoires ou des fichiers individuels. Ces nombreuses possibilités se révéleront particulièrement utiles lorsque, notamment, vous voudrez être sûr d'un fichier ou d'un lecteur amovible transmis par un collègue ou un ami. Dans le cas présent, même si ce processus peut monopoliser les ressources de l'ordinateur pendant quelques minutes, optez pour une analyse complète de l'ordinateur. Vous surveillerez le déroulement du processus à travers l'écran présenté figure 3-24.

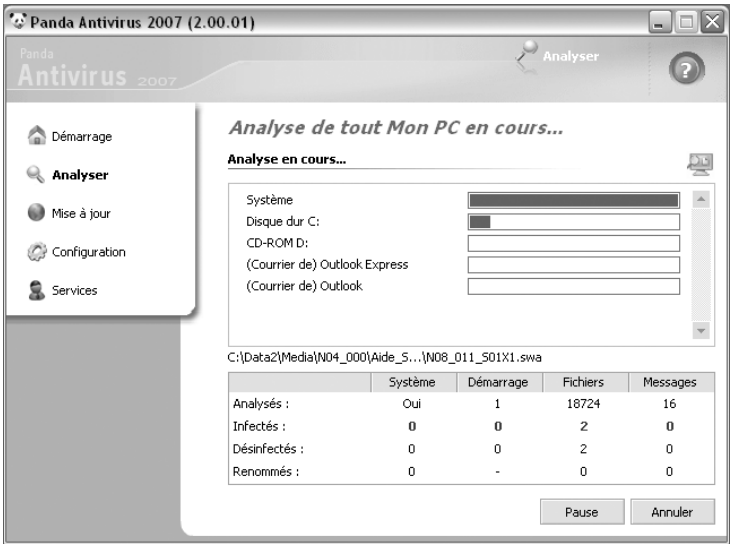


Figure 3–24
Déroulement du processus d'analyse complète de l'ordinateur

Si tout se passe bien, l'antivirus vous affichera un message réconfortant, comme « Aucun virus trouvé ! ». Sinon, il vous indiquera la présence éventuelle de virus et les actions qu'il a entreprises pour supprimer la menace (figure 3-25).

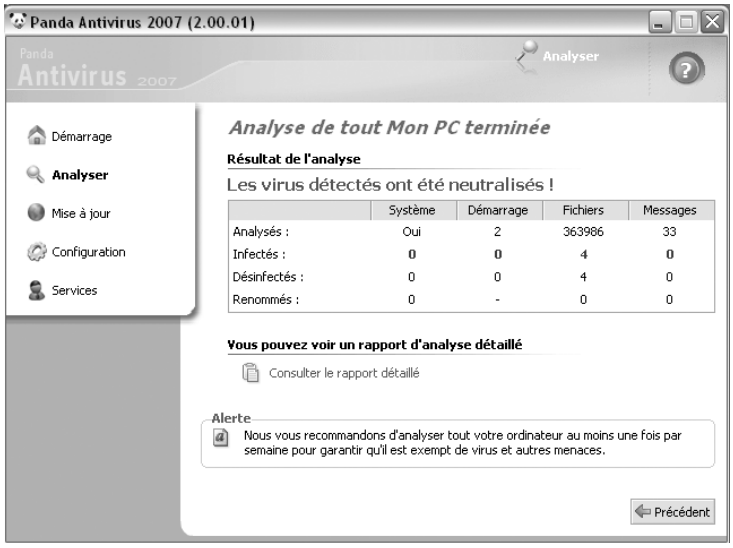


Figure 3–25
Résultat de l'analyse

Tous les antivirus vous fournissent des informations détaillées à propos des analyses effectuées et des problèmes rencontrés. Avec Panda Antivirus, cliquez sur le lien *Consulter le rapport détaillé* pour accéder à ces informations. Le rapport d'analyse détaillé (figure 3-26) vous indique notamment les fichiers incriminés et leur emplacement. Vous avez ainsi la possibilité de les supprimer manuellement, si l'antivirus ne s'en est pas chargé.

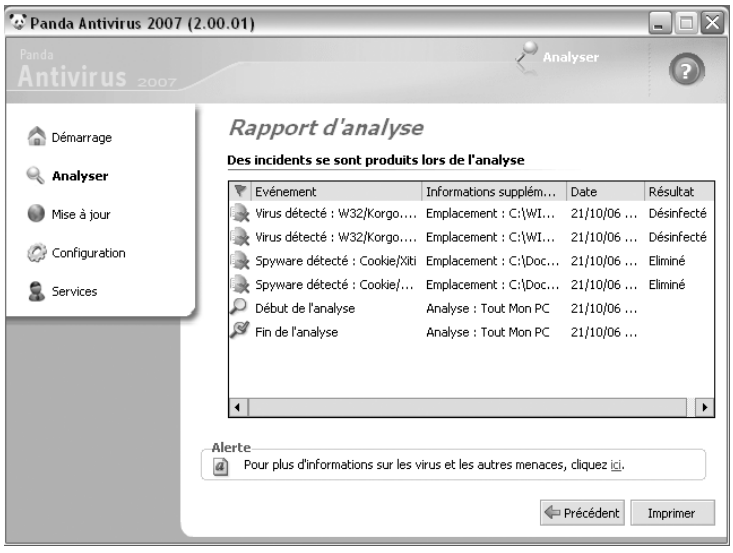


Figure 3–26
Rapport d'analyse détaillé

CHOIX En cas de détection d'un virus

Certains antivirus vous offrent plusieurs options en cas de détection de virus : la réparation automatique, la mise en quarantaine en cas d'échec, le renommage ou la suppression (figure 3-27). La suppression est une mesure efficace, mais si, par malheur, l'antivirus ne parvient pas à réparer votre fichier infecté, vous le perdez. Le renommage ou la mise en quarantaine peut être un bon palliatif.

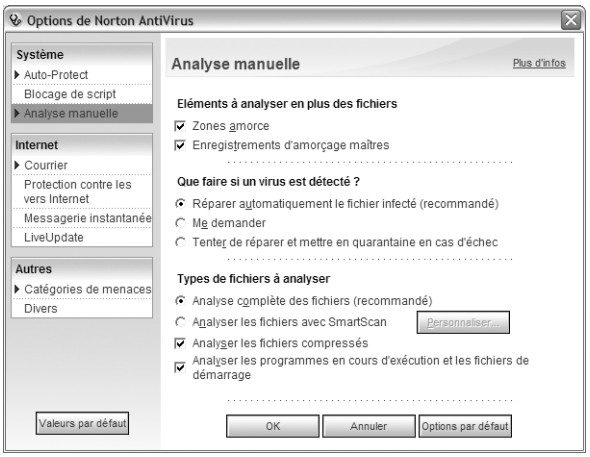


Figure 3–27 Principales options de l'antivirus

Vous pouvez maintenant considérer que votre ordinateur ne contient aucun des codes malveillants détectables par votre antivirus. Si vous ouvrez à nouveau la fenêtre principale, vous visualiserez la situation actuelle et constaterez que le niveau de votre protection est élevé (figure 3-28).

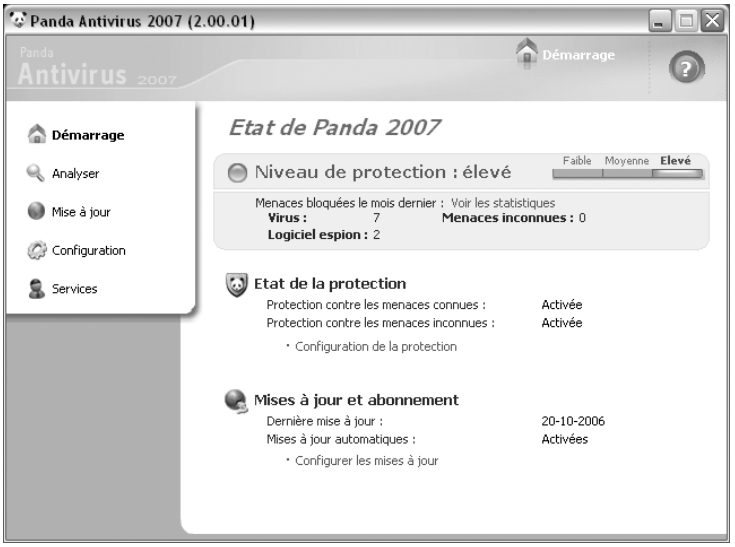


Figure 3–28
Fenêtre principale reflétant les actions réalisées pour élever le niveau de protection de l'ordinateur

Vous n'avez plus qu'à vous assurer que la protection automatique est activée (ce qui devrait être le cas par défaut sur tous les antivirus). Dans Panda Antivirus, il vous suffit de sélectionner *Configurer la protection automatique* à partir du menu *Configuration*, puis de cliquer sur *Fichiers à analyser* dans la section *Options avancées*.

Configurer le logiciel antivirus

Vous avez déjà tous constaté qu'un antivirus pouvait dégrader sensiblement les performances d'un ordinateur. Plus les contrôles sont profonds, plus le niveau de protection est élevé, mais plus votre ordinateur risque de « ramer » si l'antivirus s'alloue beaucoup de ressources. Il faut donc configurer votre outil afin de trouver le meilleur ratio entre les performances de l'ordinateur et le niveau de protection assuré. Ce ratio dépendra évidemment des caractéristiques de votre machine.

Avec Panda Antivirus, les options de configuration sont simples et souvent suffisantes. En cliquant sur *Configuration* dans la fenêtre principale, vous accédez à tous les paramètres (figure 3-29).

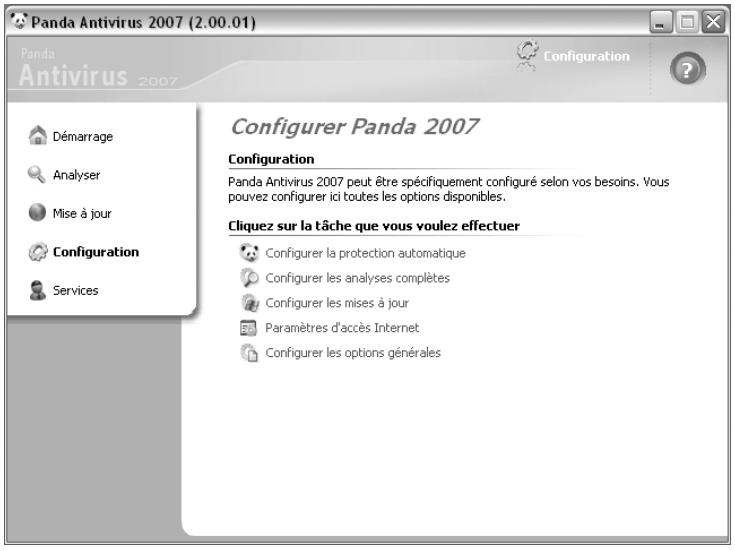


Figure 3–29
Accès aux paramètres de configuration de Titanium Anrivirus

Le tableau 3-4 donne un aperçu des options que vous pouvez choisir d'activer ou non. Si certains antivirus s'attachent à proposer une liste de paramètres plus détaillée, la philosophie est globalement la même. La protection est maximale lorsque tous ces paramètres sont activés et si votre machine est récente, dotée d'un microprocesseur cadencé à une vitesse élevée, vous ne devriez pas être gêné de façon significative.

CONSEIL Configuration de l'antivirus

Il n'existe pas de règle générale en matière de configuration. Testez le comportement de votre ordinateur afin de trouver le meilleur compromis entre le niveau de protection et les performances. Si vous avez un peu de temps, testez éventuellement plusieurs antivirus et étudiez le comportement de votre machine par rapport à chaque produit (les éditeurs proposent généralement une version d'évaluation complète, valable pendant quinze ou trente jours). Notez simplement qu'il ne faudrait jamais désactiver la protection automatique en temps réel. Si, pour une raison ou une autre, vous êtes amené à interrompre momentanément ce processus, n'oubliez pas de le réactiver dans les plus brefs délais.

Tableau 3–4 Paramètres de configuration types d'un logiciel antivirus (basé sur les paramètres de Titanium Antivirus)

Paramètres	Commentaires
Protection automatique	
Protection antivirus	Cette option devrait toujours être activée.
Types de fichiers à analyser	
Fichiers désignés par leur extension	Spécifier les extensions de fichiers à analyser (une liste par défaut est toujours proposée par les antivirus)
Fichiers Office	Activer
Fichiers compressés	Cette option consomme des ressources. Si votre antivirus ralentit significativement votre machine, vous pouvez la désactiver. N'oubliez pas en revanche de procéder à des analyses complètes régulièrement.
Détection des logiciels espions	Très utile, mais avoir recours à un outil dédié est fortement recommandé.
Détection des numéroteurs	Activer
Protection de la messagerie instantanée	Selon utilisation
Blocage des pièces jointes potentiellement dangereuses (fichiers exécutables, etc.)	Activer
Détection des outils de piratage	Activer
Détection des canulars	Activer
Blocage des scripts	Activer
Protection contre les menaces inconnues	
Détection des menaces inconnues	Ces options sont importantes et renforcent votre niveau de protection. Cependant, elles peuvent être consommatrices de ressources.
Analyse du comportement	Activer
Analyse heuristique	Activer
Affichage des alertes	Activer
Protection pare-feu (bloque les tentatives d'intrusion lorsque vous naviguez sur Internet)	Si vous disposez d'un pare-feu séparé, ces options peuvent éventuellement être désactivées.
Protection de l'accès à Internet	
Analyses complètes	Activer toutes les options.
Types de menaces à chercher	Activer
Virus	Activer
Numéroteurs	Activer
Logiciels espions	Activer
Canulars	Activer
Outils de piratage	Activer
Analyse heuristique	Activer

Tableau 3–4 Paramètres de configuration types d'un logiciel antivirus (basé sur les paramètres de Titanium Antivirus) (suite)

Paramètres		Commentaires
Mises à jour automatiques		Toujours activer cette option
Options générales		
	Analyse des lecteurs de disquette avant la fermeture	Pas indispensable
	Diagnostic périodique (toutes les 15 minutes et au démarrage de l'ordinateur)	Cette option peut nettement ralentir l'ordinateur et la procédure de démarrage.

Optimiser au quotidien la protection de votre ordinateur

En toute logique, vous n'avez presque plus rien à faire. Toutes les options nécessaires à la lutte contre les codes malveillants sont activées par défaut au sein de la plupart des antivirus et la protection de votre ordinateur est maximale.

Par exemple, si vous n'avez pas désactivé la mise à jour automatique, les antivirus détectent votre connexion Internet, se connectent à leurs centres respectifs de mise à jour et actualisent les fichiers des signatures et le moteur d'analyse sur votre ordinateur, de façon tout à fait transparente (tant que votre abonnement est toujours valide). Vous verrez donc apparaître fréquemment des fenêtres similaires à celles des figures 3-30 et 3-31.

La figure 3-30 vous montre par exemple que l'antivirus sait désormais détecter 47 nouveaux virus… qui n'existaient pas encore la veille ! D'où l'intérêt de maintenir ces fichiers à jour...

Figure 3–30 Votre antivirus vous signale qu'il vient de remettre à jour son fichier des signatures de virus.

Si votre moteur d'analyse est lui-même remis à jour (figure 3-31), vous en serez probablement informé et serez peut-être obligé de redémarrer votre ordinateur. C'est tout ce que vous aurez à faire.

Toutes ces opérations de mise en route effectuées, votre antivirus ne devrait pas, au quotidien, vous embêter plus que cela. Il se peut que vous ayez à intervenir ponctuellement pour résoudre quelques problèmes mineurs, lorsque vous faites appel à des services non compatibles avec l'antivirus (lors de la manipulation de courriers électroniques chiffrés, par exemple), ou lorsque l'antivirus déclenche un trop grand nombre de fausses alertes. Vous pouvez être amené à désactiver temporairement certaines fonctions, mais cela ne devrait pas aller plus loin.

Figure 3–31 Votre moteur d'analyse vient d'être remis à jour.

Cependant, une action doit **impérativement** être lancée régulièrement : l'analyse complète de votre système.

FONCTIONNALITÉ **Mises à jour manuelles**

Avec certains antivirus, il faudra peut-être activer vous-même les mises à jour. Il suffit par exemple de cliquer sur le bouton *LiveUpdate* situé en haut à gauche de l'écran principal de Norton Antivirus pour ouvrir l'assistant de téléchargement des mises à jour. Celui-ci recherche les nouveaux composants sur le site de Symantec, vous propose de sélectionner la liste de ceux que vous souhaitez installer, télécharge et installe ces composants (figure 3-32).

Figure 3–32 Mise à jour de Norton AntiVirus

Procéder à une analyse complète du système

Lorsque la protection automatique est activée, l'antivirus recherche en temps réel la présence éventuelle de virus dans les logiciels que vous manipulez, sur les supports amovibles que vous insérez dans les lecteurs, au sein des fichiers que vous utilisez ou lorsque vous accédez à Internet.

Afin de limiter la dégradation éventuelle des performances de l'ordinateur, la protection automatique n'analyse pas systématiquement tous les fichiers. Seuls ceux dont l'extension est spécifiée dans les paramètres de configuration de l'antivirus subissent une analyse (il convient généralement d'inclure dans cette analyse tous les types de fichiers susceptibles de contenir des codes malveillants, tels que les fichiers HTML, les contrôles ActiveX, les fichiers contenant des macros, les messages électroniques, les images JPEG, etc.). Vous pouvez d'ailleurs modifier vous-même très simplement la liste par défaut des types de fichiers à analyser avec la protection automatique. Dans Panda Titanium, il suffit de sélectionner *Configurer la protection automatique* à partir de la fenêtre principale, de cliquer sur *Protection antivirus* puis sur *Fichiers à analyser* dans la section *Options avancées*. Vous visualisez ainsi l'écran de la figure 3-33.

Étant donné que la protection automatique ne couvre pas tous les fichiers de l'ordinateur, il est recommandé de lancer une analyse complète de votre système une fois par semaine, afin de détecter les éventuels

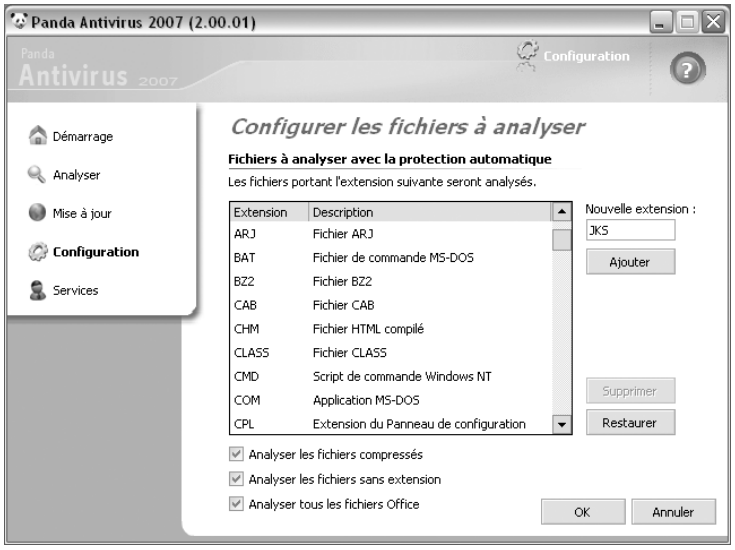


Figure 3–33
Visualisation et modification de la liste des types de fichiers analysés avec la protection automatique

virus qui seraient parvenus à passer entre les mailles du filet. L'analyse complète passe au crible **tous** les fichiers de la machine, à l'exception peut-être des fichiers que vous avez explicitement identifiés dans les exclusions. Dans la fenêtre principale de Titanium Antivirus, cliquez sur *Analyse complète* et procédez comme indiqué à la figure 3-22.

FONCTIONNALITÉ **Planification de l'analyse complète**

Certains antivirus proposent une planification automatique. C'est le cas par exemple de F-Secure Anti-Virus : la figure 3-34 montre combien il est facile de programmer automatiquement l'analyse complète de votre poste, en cochant quelques cases.

Figure 3–34 Planification de l'analyse complète hebdomadaire du système

Éradiquer un virus

Code malveillant reconnu par l'antivirus

Si vous avez mis en œuvre toutes les mesures de prévention décrites au cours des sections précédentes, les vilains petits codes malveillants qui ne manqueront pas de se présenter sournoisement aux portes de votre ordinateur trouveront à qui parler.

Par exemple, la figure 3-35 montre que le produit Norton Antivirus a détecté la présence du virus Netsky.P dans un courrier électronique. Netsky.P est un ver assez virulent qui exploite une vulnérabilité bien connue d'Internet Explorer, aujourd'hui corrigée, qui permettait à l'époque d'exécuter automatiquement la pièce jointe à la simple lecture du corps du message.

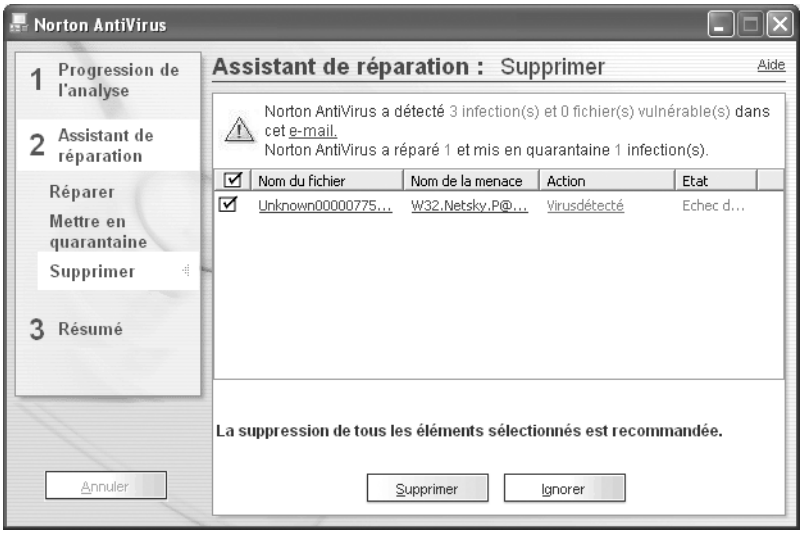


Figure 3–35
Cas de détection d'un virus

Comme vous pouvez le constater, le ver Netsky.P a essayé d'infiltrer l'ordinateur à travers l'envoi d'un message électronique, mais n'a pas pu aller très loin. Quand une telle situation se présente, le logiciel antivirus intervient immédiatement : il bloque le virus, l'empêche de se propager, et s'empresse de le détruire ou de le mettre en quarantaine.

Vous n'avez qu'à vous laisser guider par les instructions et votre machine ne sera pas infectée. Si l'antivirus ne parvient pas à supprimer le fichier contaminé, empressez-vous de le faire vous-même. N'oubliez pas de vider la corbeille.

Nettoyer une machine contaminée

COMPRENDRE La machine est contaminée en dépit de l'antivirus

Votre antivirus n'est pas parfait, et vous commencez à comprendre pourquoi une infection est possible en dépit de sa présence sur votre machine. Cela vous paraîtra peut-être déprimant, mais il faut que vous en soyez conscient : même si vous disposez d'un antivirus performant à jour, vous n'êtes pas totalement à l'abri d'une attaque virale et votre machine peut se faire contaminer du jour au lendemain. Pourquoi ?

- Tout d'abord, n'oubliez pas que votre antivirus ne sait probablement pas détecter et supprimer de manière exhaustive tous les codes malveillants existant dans la nature. En dépit de riches bases de connaissances sur les virus et de techniques de détection complémentaires et performantes comme l'analyse heuristique, il est possible que votre logiciel ne parvienne pas à détecter un virus et ne réussisse pas à vous éviter la contamination.
- Ensuite, lorsqu'un nouveau virus apparaît, les éditeurs ne peuvent pas réagir immédiatement : il faut laisser aux ingénieurs le temps de décortiquer le virus (certains, comme les virus polymorphes, utilisent des techniques sophistiquées), de comprendre son moyen de propagation, les actions qu'il entreprend, etc. et de mettre au point le programme qui permettra de l'éradiquer et de réparer les fichiers endommagés. Ces opérations ne sont pas toujours simples à réaliser et il faut tout de même saluer la performance d'un éditeur qui publie une mise à jour en moins de quatre heures !

Les grands virus sont conçus pour se répandre à une vitesse fulgurante ; beaucoup d'ordinateurs, dont le vôtre, risquent l'infection pendant cette période critique. Il faut donc que vous vous prépariez psychologiquement à subir un jour une infection, et que vous sachiez comment agir en pareille situation.

Tout d'abord : pas de panique ! En dépit des apparences alarmistes dans ce type de situation, il se peut que le virus contracté n'ait procédé à aucune opération de destruction irréversible.

Votre machine ne démarre plus

Votre antivirus propose une fonction de démarrage à partir du support d'installation

Insérez votre disque (ou vos disquettes) d'urgence dans le lecteur, redémarrez l'ordinateur à partir du CD-Rom (ou du lecteur de disquettes), suivez les instructions affichées à l'écran, en consultant au besoin votre manuel utilisateur, et laissez le programme antivirus rechercher, supprimer le virus et, le cas échéant, réparer les fichiers infectés. Selon votre antivirus et la nature du code malveillant, cette simple opération

PRUDENCE Disquettes d'urgence

Les antivirus renommés offrent pour la plupart la possibilité de créer vous-même un jeu de disquettes d'urgence. Ces dernières contiennent une version du moteur d'analyse et les fichiers de définition de virus nécessaires. Comme toujours en cas de contamination grave, il est rare de disposer de disquettes d'urgence, leur fastidieuse réalisation étant toujours remise à plus tard, voire oubliée (la fameuse négligence du premier chapitre !). Dans ce cas, il est urgent de prendre votre temps : trouvez un moyen de vous fabriquer ces disquettes (sur une autre machine, demandez à un ami, etc.), même si cela doit vous prendre deux jours. Au bout du compte, vous serez gagnant.

résoudra peut-être votre problème. Retirez le CD-Rom ou les disquettes du lecteur et relancez l'ordinateur normalement. N'oubliez pas de remettre votre antivirus à jour et, pour plus de sûreté, effectuez un balayage complet du disque.

Votre antivirus ne propose pas de fonction de démarrage à partir du support d'installation

Si votre machine ne démarre plus et si votre antivirus n'offre pas de fonction de démarrage à partir du CD-Rom d'installation ou d'un jeu de disquettes d'urgence, il vous reste maintenant du temps pour mesurer à quel point cette fonction vous aurait été utile ! Avant de vous avouer vaincu, si vous disposez d'un accès à Internet à partir d'une machine saine, allez sur le site d'un autre éditeur qui propose cette fonction, téléchargez une version de démonstration et fabriquez-vous un jeu de disquettes d'urgence. À défaut, faites le tour de vos connaissances ou contactez les administrateurs système de votre entreprise, et essayez de voir si quelqu'un peut vous fabriquer ce précieux jeu de disquettes.

Votre machine démarre encore

Mettez à jour votre antivirus

Si l'ordinateur fonctionne encore, tout n'est pas perdu. Pensez d'abord à sauvegarder vos données, si cela n'a pas déjà été fait (attention, vous sauvegarderez peut-être aussi le virus). Il se peut que vous ayez été infecté par un code que votre antivirus est capable de reconnaître, mais dont la signature ne figure pas dans votre fichier des définitions de virus. Mettez donc votre antivirus à jour et lancez une analyse complète de votre système.

PRUDENCE Ne pas contaminer les sauvegardes

Prenez bien garde de ne pas polluer des données qui auraient été sauvegardées avant l'infection en les écrasant par des fichiers contaminés. Choisissez donc un support dédié pour votre sauvegarde d'urgence.

C'est un nouveau virus

S'il s'agit d'un nouveau virus, votre antivirus ne le reconnaît peut-être pas encore. Prenez votre mal en patience, éteignez sagement votre poste et attendez que l'éditeur publie la mise à jour correspondante. Actualisez votre fichier de définitions et lancez un balayage complet de votre système.

Votre antivirus ne sait pas éradiquer le virus

Si l'éditeur de l'antivirus que vous utilisez tarde à publier sa mise à jour, ou si le virus responsable de l'infection n'est pas reconnu, ou encore si votre antivirus le détecte mais s'avère incapable de le supprimer, vous avez la ressource de faire appel à un autre fournisseur : les éditeurs d'antivirus mettent à disposition gratuitement des utilitaires de nettoyage spécifiques à un virus donné (vous devez dans ce cas avoir une idée précise du virus présent sur votre poste). Vous pouvez tenter de désinfecter votre ordinateur avec l'un d'eux. Connectez-vous au site de l'un des éditeurs (voir à ce

sujet l'exemple de la figure 3-36), téléchargez cet utilitaire et lancez la procédure de désinfection sur votre machine. S'il s'avère que le virus en question n'est effectivement pas reconnu par votre antivirus, n'hésitez pas à envoyer à votre éditeur un fichier infecté pour qu'il l'étudie.

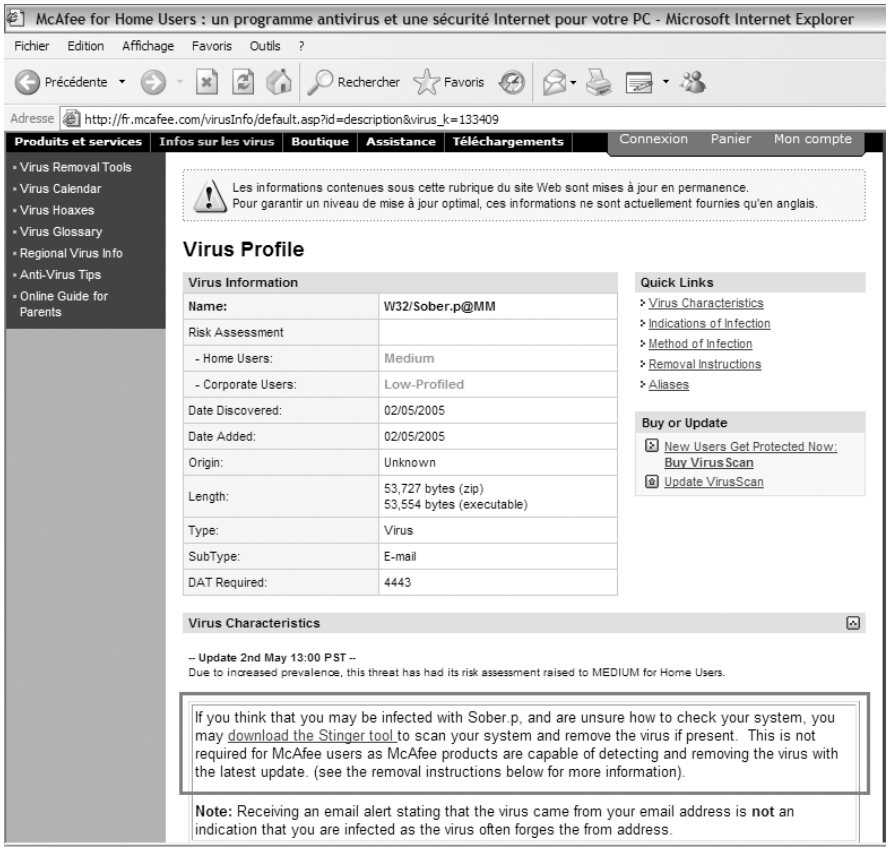


Figure 3–36
Les éditeurs mettent gratuitement à disposition des utilitaires permettant de désinfecter une machine contaminée par un virus particulier.

Vous n'avez pas d'antivirus

Si vous n'avez pas de programme antivirus installé sur votre ordinateur, dites-vous d'abord que ce n'est pas bien du tout. Toutefois, les éditeurs offrent à peu près tous une aide d'appoint que vous apprécierez grandement en cas d'infection : vous pouvez utiliser gratuitement leur antivirus en ligne, accessible directement à partir de leur site web. Comme vous le constatez avec l'exemple de Network Associates à la figure 3-37, cette opération est simple : il vous suffit de cliquer sur le lien *Freescan* pour procéder à l'analyse et, éventuellement, éliminer votre virus (l'antivirus présent sur le Web est remis à jour en permanence).

CONSEIL Tirez les leçons d'une infection

Si la perspective de perdre vos données vous a effrayé au cours de cette expérience, réfléchissez à une sécurité moins précaire à l'avenir…
De façon générale, n'hésitez pas à utiliser les nombreux services d'urgence offerts par les éditeurs sur leur site. Ils vous permettront, dans certains cas, de vous sortir d'un mauvais pas.

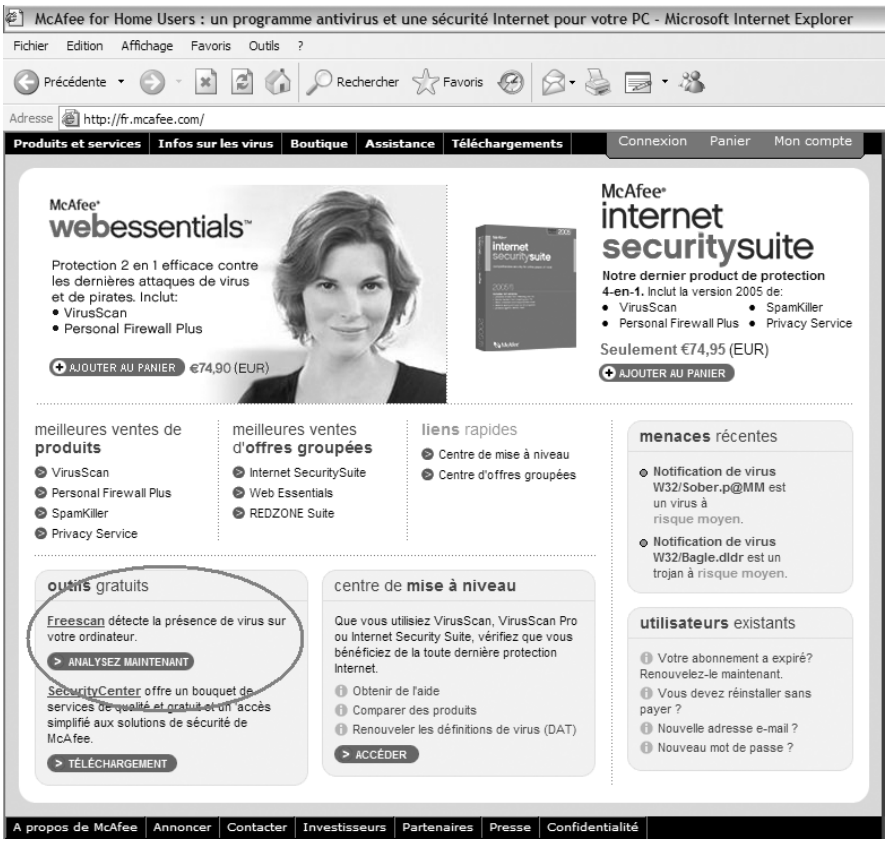


Figure 3–37
Désinfectez votre machine à l'aide d'outils d'appoint mis à disposition par les éditeurs d'antivirus.

Si toutefois, après ces opérations, vous sentez que le système n'est pas correctement réparé (vous ne réussissez plus à accéder à certains programmes, vous notez des instabilités ou un fonctionnement erratique, le clavier imprime des caractères bizarres, le système ralentit fortement, etc.), sauvegardez vos données et envisagez sérieusement de formater votre disque dur, ainsi que de réinstaller votre système d'exploitation.

Créer un jeu de disquettes d'urgence

Vous l'avez compris, disposer d'un jeu de disquettes d'urgence peut vous sauver.

Cela est généralement très facile à réaliser : avec Panda Antivirus, sélectionnez *Services* à partir de la fenêtre principale. Vous faites ainsi apparaître la fenêtre de la figure 3-38. Cliquez ensuite sur *Disquettes de secours* et suivez les instructions de l'assistant.

Entreposez bien soigneusement ces disquettes dans un lieu sûr.

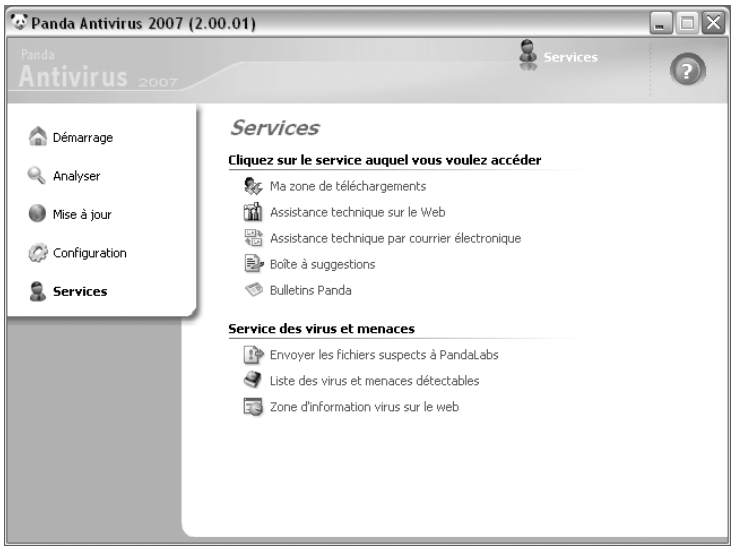


Figure 3–38
Créez un jeu de disquettes d'urgence.

Mesures complémentaires à prévoir pour éviter l'infection par un virus

Une protection complète contre les virus n'implique pas seulement la mise en place d'un antivirus, mais résulte d'un faisceau de mesures dont l'antivirus est, évidemment, la pierre angulaire. Il convient généralement de prévoir les mesures additionnelles minimales suivantes :

- La mise en œuvre d'un **mur pare-feu** – Votre pare-feu restreindra les moyens de communication entre votre ordinateur et le monde extérieur et contrôlera les flux que vous autorisez. En cela, le pare-feu diminue significativement l'occurrence des d'attaques. Cet aspect sera abordé au chapitre 5.
- La **mise à jour** impérative et régulière de Windows et des principales applications – Beaucoup de virus n'existent que par la présence de failles au sein des logiciels. Si vous utilisez une version à jour de ces logiciels, incluant donc tous les correctifs destinés à colmater les vulnérabilités connues, le virus n'aura aucune prise sur votre poste (en d'autres termes, évitez de rester dans la situation de la figure 3-13).

BONNE PRATIQUE Évitez les logiciels trop souvent victimes d'attaques

Certaines attaques virales tiennent à la simple vulnérabilité, non encore corrigée, d'un navigateur. Si vous entendez parler d'un virus foudroyant de ce type, affectant par exemple Internet Explorer, et non encore contré par les éditeurs, n'hésitez pas à avoir recours à Firefox, Netscape ou Opéra.

- http://www.mozilla-europe.com
- http://www.netscape.fr
- http://www.opera.com

Peut-on se passer d'un antivirus ?

Après ce que vous venez de lire, cette question paraît incongrue. Cependant, beaucoup d'entre vous se la posent et se demandent si, au bout du compte, la nécessité de l'antivirus n'est pas le fruit d'une psychose ambiante.

Si vous faites un usage intensif d'Internet, nous espérons vous avoir convaincu que la réponse était clairement non.

Cependant, il y a parmi vous des personnes qui n'envisagent pas l'utilisation d'Internet autrement que de façon parcimonieuse. Si cela peut vous éclairer, sachez que l'auteur de ces lignes dispose d'une machine sur laquelle aucun antivirus n'est installé (Ah !… la bonne blague !) ; elle sert uniquement pour accéder, épisodiquement, à un compte de messagerie via un modem et, en plus de deux ans d'utilisation, elle n'a jamais été contaminée. Bien entendu, il a fallu prendre des précautions ; la machine n'est jamais connectée plus que nécessaire à Internet et tous les messages suspects sont systématiquement détruits avant même de les ouvrir. De plus, cette machine n'a jamais contenu de données importantes et réinstaller le système en cas d'urgence n'aurait pas posé de problème.

Ainsi donc, une machine très peu connectée à Internet ou qui ne contient pas de données vitales, doublée d'un comportement méfiant vis-à-vis des messages douteux, n'a effectivement pas forcément besoin d'un antivirus.

Expulser les logiciels espions

Les éditeurs d'antivirus commencent à s'intéresser sérieusement aux logiciels espions. Cependant, pour lutter contre ces mouchards, les solutions les plus efficaces consistent actuellement à faire appel à des logiciels spécialisés, dits « tueurs de spywares ».

L'un des plus réputés est Spybot – Search & Destroy de PepiMK Software. Très facile à utiliser, il vous suffit de cliquer sur le bouton *Vérifier tout* dans la fenêtre principale pour qu'il vous dresse une liste des codes douteux présents sur votre poste, ainsi que de leur niveau de gravité.

Spybot – Search & Destroy balaye toutes les zones stratégiques qu'affectionnent les logiciels espions, telles que le registre, les zones de stockage des programmes téléchargés et les sous-répertoires hébergeant les codes exécutables. Vis-à-vis de chaque menace identifiée, vous avez la possibilité de visualiser des informations explicatives. Pour illustrer cela, vous pouvez observer à la figure 3-40 un exemple de vulnérabilité d'Internet Explorer.

Où le trouver ? Spybot - Search & Destroy

C'est un logiciel proposé en shareware que vous pouvez télécharger gratuitement sur le site :

- http://www.safer-networking.org/fr/index.html.

Figure 3–39
Fenêtre d'accueil de Spybot - Search & Destroy

Toutes les menaces identifiées sont présélectionnées. Vous pouvez modifier cette présélection et il vous suffit d'appuyer sur le bouton *Corriger les problèmes* pour renvoyer les codes malveillants sélectionnés définitivement en enfer. Assurez-vous toutefois que la modification ne viendra pas perturber le fonctionnement de votre ordinateur.

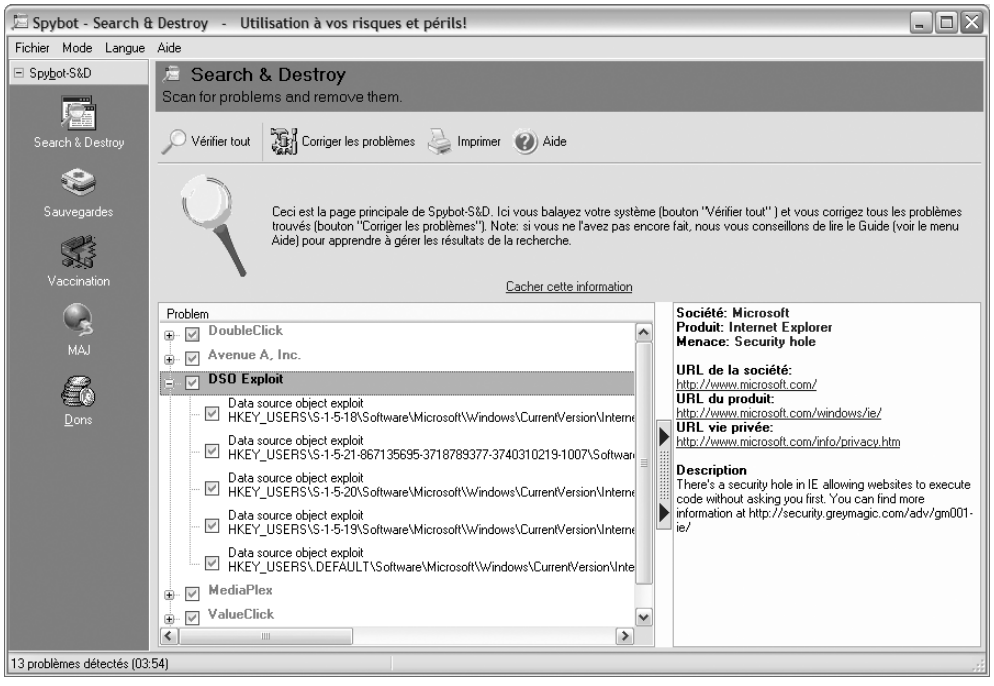


Figure 3–40
Exemple de menace identifiée par Spybot – Search & Destroy

Spybot – Search & Destroy dispose en outre d'un agent résident qui vous offre une « immunité permanente », surveillant vos échanges en tâche de fond et bloquant ainsi l'installation des logiciels espions qu'il reconnaît.

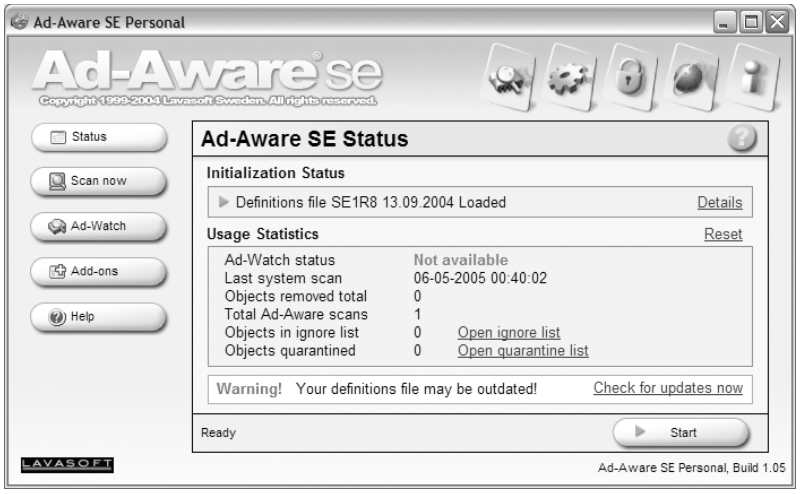
Comme avec les antivirus, il faut penser à le remettre périodiquement à jour (il vous suffit d'appuyer sur le bouton *MAJ* pour enclencher la procédure). Si vous êtes satisfait avec Spybot – Search & Destroy, vous pouvez envoyer une donation de votre choix au concepteur de ce logiciel, qui fait un travail remarquable.

Un autre tueur de spywares réputé est Ad-Aware, conçu par la société suédoise Lavasoft. Il est proposé en téléchargement gratuit pour un usage non commercial. D'une utilisation aussi simple que Spybot – Search & Destroy, Ad-aware scrute la mémoire, le registre, les lecteurs amovibles ou les dossiers, à la recherche de tous les types de logiciels espions, codes traceurs, parasites, adwares, chevaux de Troie, etc.

Il suffit de sélectionner le type de vérification que vous voulez effectuer (lecteurs, dossiers, processus en cours, système complet) et de cliquer sur *Scan now* dans la fenêtre principale pour lancer l'analyse.

▸ www.lavasoft.de

Figure 3–41
Fenêtre d'accueil de Ad-aware



Ad-aware offre en outre de riches fonctions de configuration et permet l'installation de modules externes (plug-ins).

LOGICIELS Autres antispywares

Il existe bien d'autres tueurs de logiciels espions. Parmi les plus efficaces, on peut citer par exemple celui inclus dans la suite logicielle Panda Platinium Internet Security, AntiSpyware (Microsoft), CounterSpy (Sunbelt software), SpywareBlaster (Javacool Software).

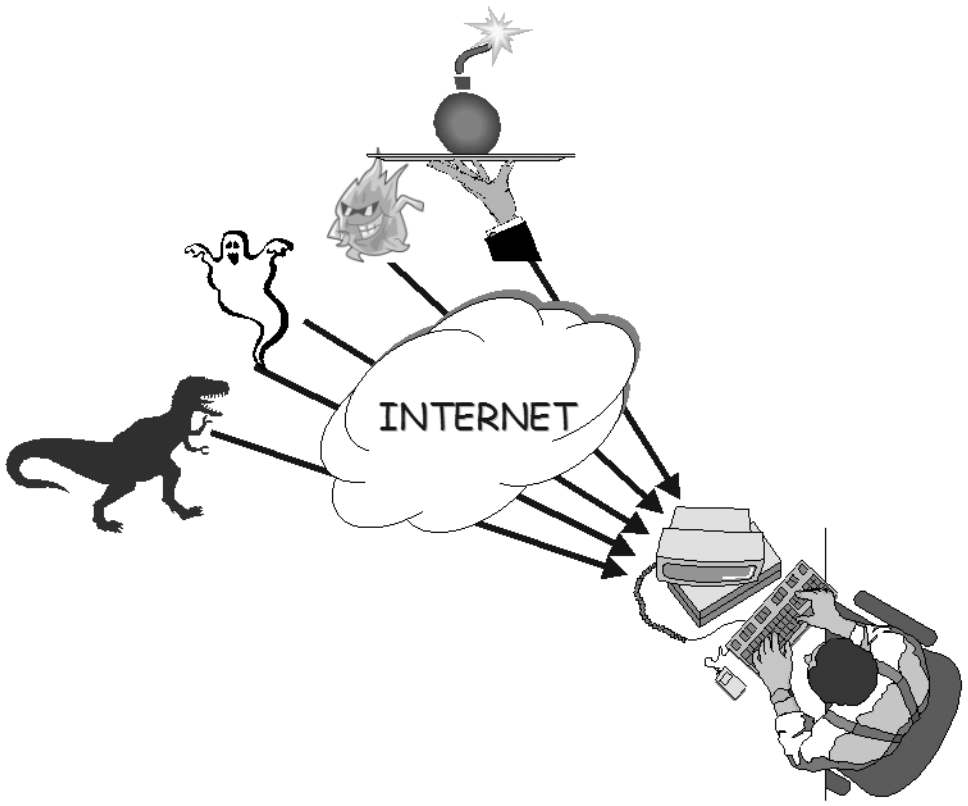
Récapitulatif

- Effectuez des sauvegardes et conservez plusieurs copies de vos fichiers effectuées à des dates différentes.
- Maintenez systématiquement votre système d'exploitation et vos principaux logiciels à jour.
- Mettez en œuvre un pare-feu et configurez-le correctement.
- Installez un bon antivirus sur votre machine et maintenez-le à jour.
- Activez la fonction de mise à jour automatique.
- Activez la protection automatique.
- Assurez-vous de pouvoir démarrer votre PC à partir d'un disque d'urgence ou de disquettes de secours.
- Ne téléchargez pas de programmes d'origine douteuse.
- N'exécutez pas un programme inconnu sans l'avoir analysé avec un antivirus.
- N'ouvrez jamais une pièce jointe sauf, exceptionnellement, si vous êtes sûr de son contenu.
- Préparez-vous à faire face à l'infection de l'ordinateur et aux situations d'urgence.

EN UN MOT **Avenir des antivirus**

N'oublions pas cette réflexion d'un internaute interceptée sur un forum : « *Tant que les gens cliqueront sur tout et n'importe quoi, les antivirus ont de l'avenir !* ».

chapitre 4



Les réseaux, autoroutes de l'intrusion

Il faut constater avec regrets que l'objet essentiel des réseaux n'est pas d'acheminer des flux honnêtes. Il est très difficile d'aborder le délicat problème de la protection des ordinateurs sans une bonne perception de l'état d'esprit du pirate et de ses pratiques d'intrusion.

SOMMAIRE

- Risques induits par les protocoles de transmission
- Attaques perpétrées via les protocoles réseau
- Attaques perpétrées via les protocoles applicatifs
- Risques liés aux applications Internet
- WI-FI

MOTS-CLÉS

- IP
- TCP, UDP, ICMP
- Telnet, FTP, TFTP, SNMP
- NetBIOS
- HTTP
- WI-FI

Votre PC est une formidable machine à communiquer. On pourrait le comparer à une grande ville reliée au monde extérieur par l'intermédiaire de 65 000 routes partant dans toutes les directions ! Chaque route quitte la ville par une porte pouvant être ouverte à la circulation dans les deux sens. Poursuivons notre métaphore : chaque route impose à celui qui l'emprunte l'utilisation d'une langue ou d'un dialecte particulier, que seuls quelques spécialistes de la ville, en charge de la communication, sont capables de comprendre. Quelle aubaine pour les trafiquants polyglottes ! Sous couvert d'une crédibilité accordée d'office (par le seul fait qu'ils sachent communiquer dans ces langages hermétiques), ils se glissent incognito dans l'immense flot des échanges, exploitent à leur profit cette incroyable diversité des moyens de communication, et font librement circuler, au nez et à la barbe des douaniers qui ne comprennent rien à ce qu'ils racontent, toutes sortes de marchandises – y compris les plus douteuses. Ils s'installent et dissimulent leur quartier général au cœur de cette ville immense, spolient subrepticement ses richesses, acquièrent le pouvoir et prennent petit à petit son contrôle.

Votre PC ressemble vraiment beaucoup à cette ville. C'est une machine capable de dialoguer avec le monde entier à travers plus de 65 000 ports d'entrée/sortie. Chaque port est associé à un protocole de communication spécifique capable d'établir, en un clin d'œil, un lien direct d'égal à égal avec n'importe quel ordinateur situé sur Internet. Avec un tel dispositif, comment les tricheurs pourraient-ils résister et ne pas détourner à leur profit des protocoles qui ne demandent qu'à communiquer, infiltrer votre machine et s'installer au cœur de votre système ?

Contrairement aux informaticiens, les entreprises en bâtiment spécialisées dans la construction des banques le savent très bien : il ne suffit pas de construire des murs épais ou de concevoir des systèmes d'alarme sophistiqués, encore faut-il prévoir les stratagèmes des tricheurs, qui sauront par exemple exploiter élégamment la cartographie des égouts ou la situation des toilettes du bâtiment d'à côté. Il ne faut jamais oublier que nos vrais adversaires, ceux qui conçoivent les redoutables outils d'intrusion prêts à l'emploi, sont de grands professionnels de l'informatique et des réseaux. Ils connaissent à fond les détails de l'implémentation (et les faiblesses) des souches de protocoles IP de chaque constructeur. Ils maîtrisent les systèmes d'exploitation – y compris les fonctions système non documentées. Ils désossent les applications sous toutes leurs coutures, ils étudient les spécifications, analysent les codes sources ou désassemblent les exécutables, et finissent tôt ou tard par découvrir la faille fatale, celle dont l'exploitation mène à la reddition pure et simple de la machine distante. Ils échangent entre eux le fruit de leurs précieuses découvertes, capitalisent sur cette connaissance en produisant avec brio et efficacité des outils passés maîtres dans l'art de tri-

cher, de tromper, d'abuser, de contourner, d'infiltrer et de tenir en échec bien des lignes de défense. À l'heure actuelle, le monde de l'intrusion dispose d'une force de frappe mettant en jeu des techniques d'une incroyable complexité, dont les informaticiens professionnels, pour la plupart, ignorent jusqu'à l'existence.

C'est la raison pour laquelle une protection efficace contre les intrusions – et la manière dont il faut configurer les pare-feux – découle de concepts difficiles à appréhender pour l'utilisateur non informaticien. Nous présenterons de façon simple quelques méthodes utilisées pour détourner les protocoles les plus ciblés, afin de mettre en lumière la manière dont agissent les pirates, et de vous enseigner les principaux réflexes à acquérir pour vous défendre. Cette présentation a en outre l'objectif de vous préparer au sujet des pare-feux, traité au chapitre suivant.

Messagerie, forums ou navigation sur Internet : les risques induits par les protocoles de transmission

Rôle majeur des protocoles « IP » dans les communications sur Internet

Sans entrer dans les détails techniques, vous avez certainement entendu parler des réseaux dits « IP », et vous savez que toutes les communications sur Internet les utilisent. Pour configurer son pare-feu en vue de se protéger efficacement contre les attaques venues d'Internet, il est indispensable de comprendre succinctement ce que sont les réseaux IP et comment ils fonctionnent.

Adressage IP

Il est important que vous disposiez de connaissances minimales en adressage IP : vous ne pourrez vous en passer au cours de ce chapitre et lorsque vous vous attaquerez à la configuration de votre pare-feu.

La notion d'adresse IP est absolument fondamentale ; elle est considérée comme l'adresse postale, le numéro de téléphone ou le numéro de fax dans le monde des ordinateurs. En IPv4, une adresse IP n'est ni plus ni moins qu'un simple nombre de 32 bits. Voici par exemple l'adresse IP d'un ordinateur :

```
11001000010001011110000001010001
```

Hmm !… Vous en conviendrez, ce nombre est plutôt difficile à retenir. Afin de rendre son utilisation plus commode, il a été convenu de longue date de représenter une adresse IP sous la forme « w.x.y.z », où w, x, y et z sont des valeurs décimales comprises entre 0 et 255. Pour convertir l'adresse précédente en notation décimale à points, on la divise d'abord en groupes de 8 bits, qu'on convertit en leur équivalent décimal :

- Notation binaire : 11001000 01000101 11100000 01010001
- Notation décimale : 200 69 224 81

L'adresse IP de l'ordinateur désigné ci-dessus est donc notée « 200.69.224.81 ». Ceci est effectivement beaucoup plus exploitable que « 11001000010001011110000001010001 ».

En fait, une adresse IP regroupe deux informations essentielles : le numéro du réseau et le numéro de la machine à l'intérieur de ce réseau. On distingue trois cas :

- Le nombre de gauche est compris entre 0 et 126 : c'est un réseau de classe A. Le réseau est identifié par le premier nombre et la machine par les trois suivants. Il existe donc seulement 127 réseaux de classe A dans le monde, mais ils sont gigantesques puisqu'ils peuvent contenir environ 16 millions d'ordinateurs (2^{24}) chacun.
- Le nombre de gauche est compris entre 128 et 191 : c'est un réseau de classe B. Le réseau est identifié par les deux premiers nombres et la machine par les deux suivants. Il existe 16 384 réseaux de classe B, comptant chacun jusqu'à 65 636 hôtes (2^{16}).
- Le nombre de gauche est compris entre 192 et 223 : c'est un réseau de classe C. Le réseau est identifié par les trois premiers nombres et la machine par le dernier. Il peut y avoir 2 097 152 réseaux de classe C pouvant héberger un maximum de 254 hôtes (2^8), l'adresse 255 étant réservée pour la diffusion.

À RETENIR **Adresse commençant par 127**

127 est une adresse réservée pour le « bouclage », c'est-à-dire pour qu'une machine puisse se référencer elle-même.

Transmission d'informations avec le protocole IP

IP (Internet Protocol) est en quelque sorte aux ordinateurs ce que le fax, DHL ou UPS est à chacun d'entre nous : un service express qui permet d'envoyer et de recevoir de l'information (un lettre, un colis, une transaction commerciale) vers et en provenance de n'importe quel ordinateur dans le monde.

Très schématiquement, lorsque vous désirez envoyer une information vers un ordinateur situé quelque part sur la planète (un message électronique, un morceau de musique, une photo, un ordre d'achat, etc.), votre application se contente de placer cette information à l'intérieur d'un colis et d'écrire en gros sur ce colis l'adresse de votre correspondant. Cela se passe exactement comme avec les services postaux, sauf que, dans le

monde virtuel, l'adresse est matérialisée par l'adresse IP du correspondant, par exemple 172.27.5.202 (pour simplifier, partons du principe que l'adresse IP d'un destinataire est unique au monde).

Ce colis est ensuite déposé dans une boîte aux lettres située à l'intérieur de votre ordinateur ; disons qu'il s'agit par exemple de la case *courrier-départ*.

À ce stade, voici comment on pourrait représenter (très schématiquement, cela s'entend) la suite des événements : un coursier rapide, dont l'une des tâches consiste à inspecter en permanence le contenu de votre case *courrier-départ*, attrape votre colis au moment même où vous le déposez dans la boîte aux lettres. Tel un joueur de rugby, il le lance, à une vitesse à peine imaginable, vers son coéquipier le plus proche sur la route des buts. Les buts, ici, matérialisent votre correspondant, mais à la différence du rugby, il peut y en avoir dans toutes les directions et à des distances très rapprochées ou très éloignées. En outre, nous ne parlerons pas encore de l'existence d'une équipe adverse, qui pourrait à la rigueur symboliser la présence de pirates ; nous verrons cela plus tard. Autre point qu'il convient de noter : malgré la rapidité extrême avec laquelle le coursier vient de faire partir votre colis, considérez qu'il a eu le temps au préalable de déterminer, parmi ses coéquipiers les plus proches, lequel était situé sur la route des buts à atteindre. Lorsque le coéquipier suivant dans la chaîne se saisit de votre colis, le coursier considère que son travail est terminé : peu lui importe comment la transmission se poursuivra, il part du principe qu'il a bien fait son travail et retourne surveiller le contenu des boîtes aux lettres.

La suite est à peu près analogue au cheminement du ballon ovale sur le terrain (à condition bien sûr que l'équipe ne soit pas constamment dérangée par ses adversaires) : votre colis passe à la vitesse de l'éclair de joueur en joueur jusqu'à atteindre son but final, c'est-à-dire la case *courrier-arrivée* de votre correspondant. Tel le coursier que nous évoquions, chaque joueur se préoccupe d'envoyer votre colis vers le joueur situé immédiatement après lui dans la chaîne qui vous relie à votre correspondant, et s'en désintéresse tout à fait dès qu'il l'a transmis.

Réseau IP

Chaque joueur tient en quelque sorte le rôle de centre de tri ; cette fonctionnalité, sur un réseau de communication tel qu'Internet, est assurée par un équipement appelé « routeur ». Internet est en effet constitué par un maillage extrêmement complexe de routeurs, dont la tâche essentielle consiste à « router », à acheminer vos données à travers le réseau, en se servant de la simple information que vous leur avez fournie : l'adresse IP de votre correspondant. Notez au passage que ces routeurs (certes, avec l'aide des applications) effectuent ce travail avec un certain talent, puisqu'il est rare qu'une information se perde en cours de route.

Entre le moment où le coursier vient se saisir de votre colis sur votre ordinateur et celui où le joueur en bout de chaîne le dépose sur l'ordinateur de votre correspondant, votre message aura peut-être beaucoup voyagé. Toutefois, peu importe l'itinéraire suivi ; que votre paquet emprunte le réseau Transpac, les faisceaux de lignes posées sur le fond de l'Atlantique, le réseau satellitaire, le réseau téléphonique via modem ou des artères haut débit, ce qui importe c'est que le réseau public connaisse votre adresse IP et celle de votre correspondant. L'acheminement d'un message fait appel à des mécanismes complexes de transmission, mais dont il est inutile de connaître les subtilités, puisque les routeurs s'en chargent pour nous avec une maîtrise exceptionnelle.

Voici donc, de façon simplifiée, en quoi consiste le réseau IP : tel un tissu organique observé au fort grossissement du microscope, il s'agit d'un gigantesque maillage déployé autour de la planète, constitué de câbles et de liaisons radio interconnectés, et desservant une infinité de branches dont vous êtes l'une des extrémités. Ce maillage s'accompagne d'un service universel installé absolument partout dans le monde, sur chaque appareil contenant un microprocesseur : le service IP, capable de traiter, d'envoyer ou de recevoir n'importe quel message doté d'une adresse IP. Vous pouvez dialoguer avec n'importe quelle autre extrémité dès que vous connaissez son adresse IP.

Protocole TCP

Le service (ou la couche) IP est donc le service de base qui sert à acheminer « quelque chose » vers n'importe quel ordinateur dans le monde. Dotés d'un moyen d'une telle puissance, les concepteurs d'IP furent tentés d'aller au delà, de définir, en s'appuyant sur cette infrastructure de communication, des protocoles capables de rendre des services bien plus élaborés que la simple transmission de l'information.

Citons par exemple le plus connu : le fameux protocole TCP, de TCP/IP. TCP (Transport Control Protocol) est, par certains côtés, comparable au service de transmission en recommandé. En effet, le schéma que nous venons de décrire souffre d'une lacune évidente : IP offre les mécanismes de transmission d'un message d'un ordinateur à un autre via des routeurs, mais rien dans ce protocole ne garantit que le message soit arrivé à bon port. Si un paquet IP se perd quelque part sur le réseau, ou s'il est endommagé au cours de son transfert, l'expéditeur n'en sera pas informé. IP n'offre pas de service fiable.

C'est là qu'intervient TCP : lorsque votre ordinateur désire envoyer un message, il peut très bien faire appel à ce protocole au lieu de se servir directement de IP. Avant d'émettre votre message, TCP contacte au préalable votre correspondant (en fait, le TCP de votre correspondant) afin de se

mettre d'accord avec lui sur le fait que vous allez échanger de l'information. Si les deux TCP sont d'accord pour communiquer, ils négocient ensemble les meilleurs paramètres possibles pour optimiser la transmission de cet échange ; votre TCP ouvre en quelque sorte avec celui de votre correspondant un chemin virtuel temporaire qui relie les deux ordinateurs comme s'ils disposaient d'une ligne dédiée pour faciliter les futurs échanges.

Bien sûr, TCP se sert de IP au cours de cette phase préalable d'établissement de session : dans ce cas précis, IP est utilisé par TCP non pas pour échanger de l'information utilisateur, mais pour acheminer des paramètres « d'administration ». Une fois que les deux extrémités se sont mises d'accord, les échanges d'information utilisateur peuvent commencer. Toutefois, la grande différence avec IP, c'est que votre TCP entretient un dialogue constant avec le TCP distant, afin de contrôler le bon déroulement des échanges : il s'assure que les messages arrivent bien à destination, dans le bon ordre (car un message peut être découpé en plusieurs paquets IP), et ne subissent pas d'altération durant leur transfert. TCP est chargé de demander à votre ordinateur de réexpédier les éventuels paquets perdus. Grâce à ce protocole, vous êtes sûr que l'information arrive à bon port, et sans erreur.

Couches fonctionnelles : modèle OSI

Comme vous le constatez, TCP se préoccupe de la qualité du transport de l'information de bout en bout ; il utilise pour cela un autre logiciel comme moyen d'acheminement de l'information sur un réseau, un logiciel de « plus bas niveau » : IP. TCP est donc une couche logicielle située « au dessus » de la couche IP. C'est la raison pour laquelle on a coutume de représenter les concepts de télécommunications sous la forme d'un empilement de couches fonctionnelles, appelé modèle de référence OSI. Pour mieux situer les services réseau et comprendre plus facilement la mécanique compliquée des échanges – et des attaques – sur Internet, évoquons quelques instants ce modèle.

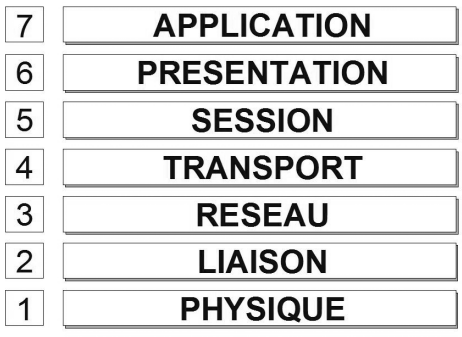


Figure 4–1
Modèle de référence OSI

Le modèle OSI définit une architecture générique censée décrire les principes de fonctionnement d'un système de communication (par exemple, une session entre votre ordinateur et un serveur sur Internet). Même si cette vision a quelque peu vieilli (elle fut proposée bien avant l'adoption généralisée des protocoles de communication utilisés à l'heure actuelle), bon nombre de concepts demeurent toujours valables. En observant la figure 4-1, vous constatez que ce modèle est constitué d'une superposition de sept couches fonctionnelles, chacune jouant un rôle bien précis dans le processus global de communication. Pourquoi adopter spécialement un modèle en « couches » ? Pour décrire ce qui se passe dans la réalité, tout simplement : l'expérience montre qu'une communication est bâtie en fait sur une série de processus disjoints et complémentaires s'appuyant les uns sur les autres. Voyons à quoi correspondent, dans le monde Internet, ces couches mystérieuses du modèle OSI.

Couches 1 (physique) et 2 (liaison)

Nous ne parlerons pas beaucoup des couches 1 et 2, le niveau « physique » et le niveau « liaison ». Elles sont matérialisées physiquement par deux éléments :

- votre carte ethernet ou votre carte modem, grâce à laquelle l'ordinateur peut se raccorder avec le médium physique du réseau ;
- son pilote, logiciel permettant à cette carte d'envoyer et de recevoir des trames sur ce médium physique, en un mot de communiquer avec d'autres cartes raccordées au même réseau.

Lorsque vous achetez votre ordinateur et que celui-ci comporte une carte réseau, vous disposez, sans le savoir, des deux premières couches du modèle OSI.

Couche 3 (réseau)

La couche 3 s'appuie sur la capacité à émettre et à recevoir des trames (couches 1 et 2), pour acheminer des paquets d'information sur le réseau, jusqu'à l'utilisateur final – d'où son nom, couche « réseau ».

Dans le monde Internet, le niveau 3 est universellement couvert par la couche IP. Cette dernière est implantée bien sûr sur votre poste (car lorsque vous achetez un ordinateur muni d'une carte ethernet, il y a de fortes chances pour que celui-ci soit livré avec la pile IP), mais aussi partout sur le réseau, à commencer par les routeurs, les serveurs distants et toute machine censée communiquer sur le réseau. La couche IP est transversale ; c'est en quelque sorte le dénominateur commun, la « plateforme » universelle, le ciment qui lie toutes les machines entre elles sur Internet.

Couche 4 (transport)

Vous saurez de même trouver la place de la couche TCP : elle se situe au dessus de IP, donc au niveau de la couche 4, la couche « transport ». C'est logique : TCP se soucie principalement de la façon dont les informations sont transportées de bout en bout entre l'expéditeur et le destinataire. Beaucoup d'applications se servent de TCP. Par exemple, les messageries SMTP utilisent les services présumés fiables de TCP (elles sont associées par exemple au port TCP 25). Un autre protocole bien connu d'Internet utilise TCP : le protocole HTTP. Il est associé généralement au port TCP 80.

Couche 7 (application)

Tout comme TCP se sert de IP, il existe d'autres protocoles de plus haut niveau qui, au lieu de s'appuyer directement sur la couche IP, préfèrent utiliser les services fiables de TCP pour communiquer. Autrement dit, il existe des protocoles situés « au dessus » de TCP dans l'empilement des couches. Nous sommes au cœur du modèle OSI : prenez l'exemple du navigateur Internet que vous connaissez bien. Vous êtes habitué à le manier pour accéder, entre autres, à des pages HTML sur un serveur web ; pour vous, ce navigateur est perçu comme une application, au même titre que la messagerie, le traitement de texte ou le simulateur de vol. Toutefois, pour rendre le service que vous attendez, ce navigateur doit dialoguer avec le serveur web distant, ce qui s'effectue dans un langage particulier. Il s'agit là encore d'un protocole de communication, à ceci près que celui-ci manipule des concepts de niveau applicatif : des URL, des images, des scripts, etc. C'est donc un protocole « applicatif », de niveau 7 dans le modèle OSI. Bien sûr, vous l'avez deviné, nous sommes en train de parler de HTTP (ou de HTTPS lorsque les échanges ont lieu dans un mode sécurisé).

Modèle simplifié TCP/IP

Si l'on considère l'empilement des différentes couches protocolaires intervenant dans le cadre du Web, nous avons au sommet l'application matérialisée sur votre poste de travail par le navigateur. Ce dernier s'appuie sur le protocole de niveau 7 HTTP (ou HTTPS), lequel s'appuie sur TCP, lui-même adossé à IP qui, à son tour, utilise les ressources de la carte réseau (couches 1 et 2). Voici donc exposée de manière simplifiée, la pile complète des protocoles mis en œuvre lorsque vous surfez sur Internet.

Avec les autres applications, c'est exactement la même chose. Par exemple, votre client de messagerie – qui est une application – se sert des protocoles de niveau 7 SMTP, POP3 ou IMAP4 pour communiquer ;

AVANCÉ Modèle OSI et modèle TCP/IP

Dans le monde IP, les concepts définis initialement par l'OSI au niveau des couches 5 (Session) et 6 (Présentation) sont généralement implémentés au sein des protocoles de niveau 7 (voir figure 4-2), voire au niveau des applications.

ceux-ci s'appuient sur TCP, lequel utilise IP, etc... Si l'on représentait l'empilement de ces différentes couches protocolaires, le schéma obtenu donnerait une vision particulière du modèle de référence OSI appliquée au monde Internet (figure 4-2).

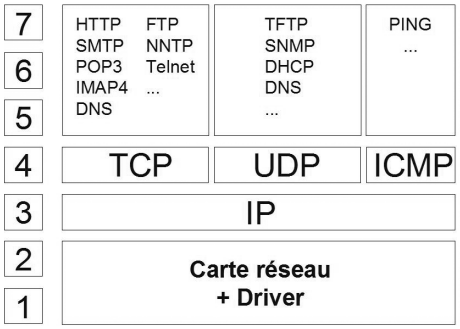


Figure 4–2
Modèle de référence OSI appliqué au monde IP

Il est important de conserver ce schéma en tête car cela vous aidera à comprendre la philosophie des attaques sur Internet, la diversité des mesures à prendre pour se protéger efficacement, ou les différences qui existent entre les pare-feux.

Protocoles UDP et ICMP

Avant de clore cette longue introduction, n'oublions pas d'évoquer les protocoles UDP et ICMP : IP, TCP, UDP et ICMP sont des protocoles fondamentaux d'Internet que nous aborderons sans cesse dans la suite de ce chapitre et au chapitre suivant.

Comme nous l'avons vu, TCP rend des services fort utiles sur le plan de la fiabilité des communications. Toutefois, il ne présente pas toujours que des avantages car, il ne faut pas l'oublier, la gestion d'une session a un coût en terme de performances : passer par TCP ralentit indiscutablement les échanges. C'est la raison pour laquelle, lorsque les contraintes de performances sont élevées, ce qui est souvent le cas pour les fonctions système ou proches du système, les développeurs optent pour une approche plus souple : au lieu de confier la gestion de la transmission à TCP, l'application ou le service se charge elle-même (ou lui-même) des paquets perdus, endommagés ou reçus dans le désordre et utilise un accès beaucoup plus direct à IP. Le service définit ainsi généralement une procédure de gestion beaucoup plus allégée – donc plus rapide – que les procédures luxueuses de TCP. Cet accès direct s'appelle UDP.

UDP (User Datagram Protocol) fournit une grande partie des services intéressants de TCP, comme le fait d'associer un numéro de port à un pro-

gramme. Toutefois, UDP n'est pas un service fiable, il n'est pas orienté connexion et ne garantit pas l'intégrité des données de bout en bout, ce qui oblige le protocole qui l'utilise à combler lui-même cette lacune. En revanche, UDP est idéal pour transmettre ou recevoir des datagrammes (c'est comme cela que l'on nomme les paquets IP avec UDP), spontanément, sans formule de politesse exaspérante susceptible de ralentir les échanges. De nombreux services réseau utilisent UDP, comme le protocole DHCP (attribution dynamique des adresses IP aux postes du réseau) ou SNMP (gestion de réseau). Notez que le protocole DNS utilise à la fois TCP et UDP (DNS est associé aux ports TCP 53 et UDP 53).

ICMP (Internet Control Message Protocol) est quant à lui entièrement dédié à la gestion des problèmes qui surviennent sur un réseau : c'est grâce à lui que les machines ou les passerelles peuvent rendre compte des anomalies de fonctionnement. Par exemple, pour vérifier si une machine distante connectée au réseau est bien « visible » de votre poste, un moyen simple consiste à effectuer un `ping` de cette machine à travers le réseau, c'est-à-dire à lancer la commande :

```
ping adresse_IP_machine_distance
```

`ping` fait ni plus ni moins appel au protocole ICMP et se contente tout simplement d'envoyer une trame ICMP `ECHO` à cette machine (en quelque sorte un « coucou es-tu là ? »), en attendant en retour une trame de type ICMP `REPLY` (« Oui, je suis là »). Si vous recevez effectivement cette trame ICMP `REPLY`, cela veut dire que les deux machines vont pouvoir communiquer.

Si d'aventure vous tentiez d'envoyer une requête vers une adresse qui n'existe pas, il y a de fortes chances pour que le réseau vous retourne un message ICMP de type `DESTINATION UNREACHABLE`, vous informant ainsi de la raison pour laquelle votre requête est restée sans réponse ; cette simple information peut en effet vous faire gagner un temps considérable.

Pour éviter les congestions du réseau, chaque paquet IP contient dans son en-tête une information « durée de vie », ou `TTL` en anglais (Time To Live). Initialisé à une valeur donnée (128 la plupart du temps), ce champ est décrémenté chaque fois qu'il passe au travers d'un nœud du réseau. Si ce paquet n'a pas atteint sa destination finale avant que son `TTL` soit égal à zéro, il est impitoyablement détruit par le nœud qui le voit transiter. Toutefois, dans sa grande bienveillance, le routeur vous informe de son sinistre forfait. Là encore, ICMP est mobilisé et le routeur vous envoie un message ICMP `TIME EXCEEDED`, qui contient toutes les références au paquet détruit ; vous pouvez ainsi prendre les mesures adéquates (pas vous bien sûr, mais le service émetteur), comme réémettre ce paquet.

ICMP renferme bien d'autres messages de contrôle, qu'il serait fastidieux de décrire dans cet ouvrage. Il s'agit d'un protocole essentiellement orienté administration, et votre intérêt pour ses activités, en tant qu'utilisateur, est somme toute assez limité. Toutefois, nous allons le voir un peu plus loin (et c'est pourquoi nous abordons ce sujet), ICMP est un protocole royal pour un pirate. Ayez quelques instants l'âme d'un tricheur et voyez comment tirer parti de tous ces protocoles de communication.

Comment l'attaquant perçoit-il un protocole de communication ?

Rentrons maintenant dans le vif du sujet. Pour un attaquant, sachez qu'un protocole de communication n'est rien d'autre qu'un moyen puissant grâce auquel il est possible de faire avaler à votre ordinateur les mensonges les plus énormes ; il suffit juste de lui parler poliment.

Si vous saisissez les implications de ce propos surprenant, vous comprendrez la philosophie des attaques informatiques et saurez mettre en œuvre les vraies mesures de protection.

À travers les quelques exemples suivants, nous allons voir comment leurrer les protocoles de communication.

Attaques perpétrées via les protocoles réseau

Derrière leur apparente innocence, les protocoles IP sont de redoutables vecteurs d'intrusion

Il y a au moins deux raisons à cela. La première tient au fait que TCP/IP et les protocoles qui lui sont associés ont été conçus vers la fin des années 1970. Ils étaient à l'origine destinés au département américain de la Défense (le DARPA) et visaient à permettre aux grands systèmes centraux de la Défense de communiquer entre eux. À l'époque, personne ne parlait d'Internet public. Bien que cette suite de protocoles ait été définie pour servir un domaine hautement stratégique, les concepteurs ont jugé – à juste titre d'ailleurs – qu'il n'était pas nécessaire de prévoir de mécanismes de sécurité particuliers, cette infrastructure évoluant en circuit fermé.

TCP/IP s'est ainsi développé au fil des ans jusqu'à former le groupe de protocoles robustes et efficaces (en terme de communication, cela

s'entend) que nous connaissons aujourd'hui. Bien entendu, il n'intégrait toujours pas les mécanismes de sécurité qui n'auraient pas manqué de voir le jour s'il avait été pensé pour des réseaux ouverts. Cependant, victime de son incroyable popularité, TCP/IP s'est progressivement répandu dans les entreprises au cours des années 1980, puis s'est retrouvé, en toute logique, propulsé en première ligne lorsqu'il a fallu acheminer le trafic public du monde entier. Voilà comment la communication sur Internet repose sur des protocoles non prévus au départ pour contrer les attaquants.

La deuxième raison est évidemment liée au fait que TCP/IP est présent sur tous les ordinateurs et équipements de communication du monde entier. Les spécifications, ainsi que le code source de nombreuses implémentations des couches protocolaires de TCP/IP, sont publics et accessibles à toute personne qui a suffisamment de courage pour se plonger dans les méandres des mécanismes complexes de son fonctionnement. Bien entendu, les pirates ne s'en privent pas. Ils prennent tout leur temps pour étudier dans ses moindres détails le fonctionnement de chaque service, de chaque fonction, qu'elle soit documentée ou non. Ils s'en donnent à cœur joie, rivalisent de subtilités, trouvent parfois des astuces étonnantes, et mettent au point des mécanismes, « bruyants » ou furtifs, exploitant les faiblesses de ces protocoles, contournant les pare-feux et pénétrant ensuite des infrastructures de millions de sites. Le balayage TCP, succinctement décrit plus loin, en est un exemple, mais il en existe des dizaines d'autres.

TCP, UDP ou ICMP : des protocoles bien utiles aux pirates pour analyser une installation à distance

Exploitation de ICMP

Nous avons vu précédemment à quoi pouvait servir la commande `ping`. Imaginez par exemple qu'un pirate décide de l'exploiter pour sonder automatiquement une plage d'adresses IP qui correspond justement à celle de votre réseau 192.168.0.x. Pour parler concrètement, imaginez qu'il lance à distance les commandes suivantes :

```
ping 192.168.0.1
ping 192.168.0.2
ping 192.168.0.3
ping 192.168.0.4
ping 192.168.0.5
…
ping 192.168.0.253
ping 192.168.0.254
```

En analysant les réponses reçues, l'attaquant saura, en très peu de temps, quels sont les systèmes individuels actifs sur votre réseau. En exploitant simplement les protocoles de communication, il peut déduire une cartographie complète et précise de votre installation ; commencez-vous à percevoir le danger inhérent à ce protocole ?

Vous apprendrez très vite à contrer cette attaque grossière au chapitre suivant, mais peut-être entrevoyez-vous déjà la nécessité de restreindre sérieusement, voire d'interdire le protocole ICMP au niveau du pare-feu.

Ouverture de session TCP

Bien qu'il existe des exceptions (curieusement, le pare-feu de Windows ne permet pas de bloquer les paquets ICMP `ECHO` et `REPLY`), partons du principe que le protocole ICMP est désormais systématiquement bloqué en entrée de site ou sur votre machine unique. Cela désarme-t-il le méchant pirate ? Disons que cela lui complique un peu la vie. Il existe en effet des attaques plus sournoises qui permettent de recueillir toutes sortes d'informations précieuses sur les machines et les services actifs.

Par exemple, détaillons quelques instants le schéma dit de la « poignée de main à trois états », la procédure standard d'ouverture d'une session TCP. Lorsque votre poste client décide d'ouvrir une session avec un serveur Web distant (donc via le protocole HTTP), TCP contacte ledit serveur et entame la petite négociation suivante :

- Votre poste : « Bonjour Monsieur le Serveur, je souhaiterais ouvrir une session avec vous ».
- Le serveur : « Bonjour Monsieur le Client. D'accord pour ouvrir cette session, je suis prêt ».
- Votre poste : « Merci Monsieur le Serveur, bien reçu, nous pouvons commencer ».

À compter de ce moment, la session est ouverte, sans autres fioritures. Notez au passage comme cette procédure est simple ! De façon générale, les protocoles IP sont bâtis sur des mécanismes simples et de bon sens (peut-être est-ce là le secret de leur succès ?).

Balayage de ports

Nous avons écrit plus haut que les communications ne pouvaient avoir lieu que si le port était ouvert. Dans le cas de notre serveur Web, les communications transiteront par le protocole HTTP, le protocole du Web. Traditionnellement, tout le monde considère que le port 80 d'un serveur Web est ouvert (port associé au protocole HTTP). Dans le cas de notre poignée de main, tous les échanges se font donc sur ce port (son numéro est un champ des en-têtes TCP et UDP). Si, au lieu d'utiliser le

port 80, votre poste avait engagé une poignée de main avec ce même serveur, mais cette fois sur le port 7 561 (très rarement ouvert), il est fort probable que celui-ci ne lui eût jamais répondu.

À ce stade, vous devinez peut-être comment un attaquant peut tirer parti de ce mécanisme. Alors, avez-vous l'âme d'un tricheur ?…

Peut-être pas encore suffisamment. Alors imaginez ceci : supposez que, connaissant l'adresse IP d'une de vos machines (192.168.0.12), l'attaquant initie avec celle-ci une poignée de main, en utilisant le port numéro 1. Si ce port est fermé, l'attaquant ne recevra aucune réponse. Supposez maintenant qu'il réitère cette tentative sur le port numéro 2, et ainsi de suite jusqu'au port numéro 65 535. Il y a de fortes chances pour que cet attaquant reçoive très peu de réponses positives, puisque tous vos ports sont fermés… Tous ? sauf ceux délibérément ouverts par vos applications pour communiquer sur Internet. Supposons que l'attaquant reçoive deux réponses : une sur le port 25, l'autre sur le port 80. 65 535 requêtes, pour 2 réponses… que d'énergie gaspillée ! Certes, mais peu importe, c'est l'ordinateur qui fait le travail, et très rapidement. Au bout du compte, le pirate sait maintenant que la machine située à l'adresse 192.168.0.12 a deux ports ouverts, d'où il peut déduire que cette machine héberge votre serveur de messagerie (traditionnellement associé au port 25) et votre serveur web (port 80). Désormais, il n'a plus qu'à concocter une belle attaque, exploitant de manière éhontée la cohorte de vulnérabilités de SMTP, de HTTP et des logiciels serveurs qui les exploitent.

Cette attaque est tout simplement ce que l'on appelle un balayage de ports. Ne vous y trompez pas, c'est une attaque élémentaire, qui ne nécessite aucune compétence (une multitude d'outils existent). Vous saurez la contrer très rapidement. Malgré tout, les balayages de ports continuent à être utilisés de plus en plus massivement et sont rarement gratuits. Il sont souvent suivis de stratégies d'attaques beaucoup plus précises (des attaques spécifiques dirigées contre les services actifs par exemple).

En examinant le résultat du balayage ci-après, un pirate sait par exemple qu'il pourra tenter d'infiltrer votre machine directement sur les ports ouverts (111, 512, 32772…), ou en exploitant les vulnérabilités des services actifs identifiés, comme Telnet, SMTP ou FTP (oui, ça y est, ils sont identifiés !). Le pirate expérimenté saura même déduire de tout ceci qu'il a affaire à une machine Unix et qu'il s'agit probablement de Solaris.

```
192.168.1.51   echo              7/tcp Echo [95,JBP]
192.168.1.51   discard           9/tcp Discard [94,JBP]
192.168.1.51   sunrpc          111/tcp rpcbind SUN RPC
192.168.1.51   daytime          13/tcp Daytime [93,JBP]
192.168.1.51   chargen          19/tcp ttytst source
```

Comparaison

Important trafic de balayage de ports

Le nombre d'entreprises pénalisées par les trafics de balayage est impressionnant. Retirer le trafic de balayage serait un peu comme rendre la rue de Rivoli fluide le samedi après-midi à l'approche de Noël.

```
192.168.1.51   ftp                21/tcp File Transfer
[Control] [96,JBP]
192.168.1.51   exec              512/tcp remote process
execution;
192.168.1.51   login             513/tcp remote login a la
telnet;
192.168.1.51   cmd               514/tcp shell like exec, but
automatic
192.168.1.51   ssh                22/tcp Secure Shell
192.168.1.51   telnet             23/tcp Telnet [112,JBP]
192.168.1.51   smtp               25/tcp Simple Mail Transfer
[102,JBP]
192.168.1.51   nfs              2049/tcp networked file system
192.168.1.51   lockd            4045/tcp
192.168.1.51   unknown         32772/tcp unassigned
192.168.1.51   unknown         32773/tcp unassigned
192.168.1.51   unknown         32778/tcp unassigned
192.168.1.51   unknown         32799/tcp unassigned
192.168.1.51   unknown         32804/tcp unassigned
```

Évidemment, cela n'est qu'un début, mais détailler les opérations suivantes n'étant pas l'objectif de cet ouvrage, nous nous arrêterons là.

Exploitation du TTL

Avec un autre exemple, examinons comment un tricheur peut découvrir des données capitales sur votre installation. Il fera simplement appel aux riches fonctionnalités des protocoles, sans même chercher à les violenter.

Partons du principe que le pirate engage avec vous un dialogue insolite : il vous envoie un message constitué de plusieurs paquets, mais s'attache à régler la durée de vie du premier paquet (TTL, Time To Live) à 1, celle du deuxième à 2, et ainsi de suite pour les suivants. Rappelez-vous que le TTL d'un paquet est diminué de 1 chaque fois qu'il traverse un routeur. Lorsque le premier paquet traverse le premier routeur situé sur la route qui relie le pirate à votre machine, son TTL passe donc à 0 et le paquet est détruit. Comme les routeurs sont des tueurs polis, celui-ci vous informe et vous renvoie un paquet ICMP `TIME EXPIRED`, dans lequel se trouvent les références du paquet détruit, mais aussi les coordonnées du routeur impitoyable. Le pirate connaît donc l'existence et l'adresse de ce routeur. Lorsque le paquet suivant est détruit (TTL=2), le pirate reçoit un nouvel ICMP ; il a donc connaissance de l'existence et de l'adresse du routeur suivant. Et ainsi de suite jusqu'à votre poste, le pirate parvient à identifier tous les routeurs qui le séparent de votre machine. Il obtient ainsi l'adresse IP du dernier saut avant sa cible… c'est-à-dire, probablement, celle du routeur d'entrée de votre site ou de votre pare-feu, autrement dit le point de raccordement du réseau visé : le dispositif auquel les pirates sont susceptibles de s'intéresser en premier vient de dévoiler sa présence et son adresse IP ! Il faudra malheureusement peu de temps

avant qu'il ne dévoile à l'attaquant ses vulnérabilités et, si sa configuration est faible, il succombera certainement à ses coups de boutoirs. Percevez-vous maintenant l'intérêt de restreindre ICMP ?

Telnet, FTP, TFTP et SNMP, facteurs de risque

Une attaque correspond à une procédure précise. La plupart du temps, elle exploite la fonction boguée d'un logiciel d'une version donnée, tournant sur un système d'exploitation particulier (une attaque dirigée contre Outlook sur Windows Me peut être inopérante contre Outlook sous XP). Pour cela, la connaissance du système d'exploitation, des logiciels que vous utilisez, de leur version, du fabriquant ou de l'éditeur (particulièrement dans le cas des piles IP) représente pour le pirate un élément stratégique majeur sans lequel il ne saura poursuivre son action.

Telnet

Imaginez que vous hébergiez un serveur web sur l'une de vos machines et que le service Telnet soit actif (rappelez vous la sortie de balayage précédente). Qui empêche le pirate, maintenant parfaitement informé de la chose, de lancer la commande `telnet www.votreSiteWeb.com 80` ? Personne. Il lui suffit juste de saisir ensuite n'importe quoi et de presser la touche *Enter* pour recevoir une réponse ressemblant à peu près à ceci :

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Mon, 12 Sept 2005 10:36:26 GMT
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title></head><body>The parameter is
incorrect. </body></html>
```

Bien sûr, la commande a échoué, mais quelle importance ? En l'espace de quelques secondes il connaît le nom et la version du logiciel de votre serveur web. À partir de cet instant, faites confiance au pirate averti ; il possède certainement les outils capables d'exploiter à merveille les vulnérabilités spécifiques de IIS 5.0. Il est déjà en train de mitonner une belle attaque sur mesure et si, par malheur, votre logiciel n'est pas à jour, considérez que vous avez désormais perdu le contrôle de votre serveur !

IMPORTANT **Intérêt du pare-feu applicatif**

Notez au passage que si un grand spécialiste de Telnet avait analysé à la volée le contenu sémantique de l'information transmise par le pirate, il se serait vite aperçu de la supercherie et aurait bloqué son transfert, avant même qu'elle atteigne le serveur web. En conséquence, le pirate n'aurait pas eu accès à cette information capitale « Microsoft IIS/5.0 », en tous cas pas par ce biais-là. Vous vous doutez évidemment que le mystérieux grand spécialiste est le pare-feu. Pourquoi cette remarque ? Simplement pour que vous perceviez mieux l'intérêt des pare-feux applicatifs (nous en débattrons au chapitre suivant) : il ne suffit pas qu'un pare-feu sache seulement autoriser ou bloquer un service (c'est-à-dire autoriser ou bloquer un port), il est très important qu'il sache aussi analyser le contenu sémantique des informations véhiculées à l'intérieur de ce protocole. Un pare-feu qui se respecte doit absolument être capable d'effectuer une analyse dans les couches hautes du modèle OSI (notez par exemple à la figure 4-2 que Telnet est un protocole de niveau 7). Considérez qu'un pare-feu matériel qui se cantonne à un niveau 4 (autorisation/blocage des ports TCP/UDP) est une passoire.

TFTP

TFTP (Trivial File Transfer Protocol) est un autre boulevard assidûment fréquenté par les pirates. Vous n'avez peut-être jamais entendu parler de ce protocole étant donné que peu d'utilisateurs y ont recours. Cependant, pratiquement tous les routeurs – dont peut-être le vôtre – prennent en charge TFTP, employé par les administrateurs pour sauvegarder et restaurer, entre autres, les fichiers de configuration. Malheureusement, dire que TFTP est un protocole mal sécurisé est un euphémisme : ses informations circulent en clair sur le réseau, il n'utilise aucun mécanisme d'authentification et offre parfois un accès direct aux systèmes de fichiers. Après avoir effectué une reconnaissance préliminaire de votre réseau, un pirate peut très bien se connecter à votre installation par TFTP et, avec la simple commande :

```
> get configFichier.cfg
```

accéder à – ou modifier – des informations sensibles comme les noms de communautés SNMP, ainsi que les listes de contrôle d'accès. Muni de ce sésame, le pirate envisage des attaques de plus grande envergure par le truchement de SNMP et des protocoles de routage. Il peut notamment modifier les tables de routage de vos équipements afin d'intercepter vos sessions et de vous amener ainsi à lui fournir des informations précieuses. Ces dernières seront utilisées pour compromettre la sécurité de l'ensemble de votre système ainsi que l'intégrité de vos données.

SNMP

Nous ne parlerons pas beaucoup de SNMP (Simple Network Management Protocol), étant donné qu'il s'agit d'un protocole de gestion utilisé essentiellement dans les grands systèmes pour effectuer la supervision d'équipements et de matériels informatiques. Cependant, SNMP est tellement répandu et si peu sécurisé qu'il représente un vecteur d'intrusion ahurissant ; à ce titre, il mérite d'être mentionné.

Beaucoup d'administrateurs réseau, pourtant très au fait des possibilités offertes par SNMP, ignorent qu'en autorisant, même partiellement, un tel service, ils ouvrent toute grande une porte à travers laquelle les loups auront tôt fait de s'engouffrer ! À l'heure où de plus en plus de protocoles traditionnels (comme Telnet) cèdent la place à des homologues sécurisés (c'est le cas par exemple de SSH), SNMP ne chiffre ni les mots de passe, ni les contenus. Par ailleurs, contrairement à ce que beaucoup d'administrateurs croient, il ne suffit pas de restreindre de manière significative les possibilités d'utilisation de SNMP pour que la configuration soit sécurisée. SNMP reste vulnérable à de nombreuses attaques par débordement de tampon. Pour un pirate, SNMP est un moyen efficace pour accéder au répertoire racine d'une machine avec les droits administrateur : c'est un protocole vraiment dangereux. Les experts en sécurité sont unanimes et préconisent la désactivation pure et simple de ce service dès que cela est possible.

À RETENIR **SNMP n'est pas sécurisé**

De mauvaises langues prétendent que SNMP signifie « Security is Not My Problem ».

CONSEIL **Évitez Telnet, TFTP ou SNMP**

De façon générale, les actions à mener sont simples : il faut interdire totalement les services comme Telnet, TFTP ou SNMP sur votre installation, soit en les désactivant au niveau de vos équipements, soit en les bloquant au niveau de votre pare-feu.

Les protocoles NetBIOS : une pièce maîtresse de Windows très apréciée des pirates

Dans le monde Windows, le service NetBIOS mérite une attention particulière sur le plan de la sécurité.

NetBIOS est un pilier de l'édifice de Microsoft : il s'agit d'une suite de protocoles applicatifs (donc situés au niveau 7 du modèle OSI) accessibles à travers une interface logicielle et des outils intégrés au système d'exploitation. NetBIOS est très puissant et est l'une des chevilles ouvrières de la communication entre ordinateurs sous Windows. Il est omniprésent sur toutes les machines qui fonctionnent avec un système d'exploitation Microsoft. NetBIOS vous concerne tous.

Or, ce service est très mal sécurisé, voire pas du tout. Il réunit donc à lui tout seul les trois éléments d'un cocktail détonnant : large diffusion, puissant, non sécurisé.

Aussi, vous ne serez pas surpris d'apprendre que NetBIOS est très prisé par la communauté des hackers, qui l'utilisent comme cheval de Troie, agent efficace pour la collecte d'informations et l'infiltration rapprochée.

B.A.-BA **NetBIOS**

Ce service a en charge la gestion du partage des ressources en réseau et de tous les problèmes qui s'y rapportent. Par exemple, lorsque vous accédez à une imprimante partagée, c'est grâce à NetBIOS. Lorsque vous établissez une connexion directe à un lecteur réseau (lecteur de type H:\, M:\, Z:\…), c'est encore NetBIOS qui le gère. Lorsque vous obtenez des informations sur les noms, les machines, les domaines et les groupes de travail de votre réseau, c'est encore à NetBIOS que vous le devez.

Prenons un exemple : le service de nommage NBNS (NetBIOS Name Service), fonctionnant sur le port UDP 137, est capable, en deux commandes d'une simplicité désarmante, de dresser la liste des domaines du réseau et des machines rattachées à chaque domaine. Pire, il fournit une liste valide de noms d'utilisateurs pour un domaine donné. Voyons plutôt :

```
H:\>net view /domain
Domain
-------------------------------------------------------
FINANCE
PROJET
DEV_DOMAIN
The command completed successfully.
```

En réitérant la même commande, mais en focalisant cette fois sur le domaine `FINANCE`, cela donne :

```
H:\>net view /domain:FINANCE
Server Name             Remark
-------------------------------------------------------------
\\MSG_PARIS             Serveur messagerie interne
\\DELL_CATHY            Catherine DUPONT
\\SECRETARIAT           Corinne MARTIN
\\SIT                   Stéphane DURAND
The command completed successfully.
```

Imaginez de telles informations entre les mains d'un pirate. À ce stade, il pourrait presque se connecter directement au système avec les droits d'un utilisateur authentifié (combien d'entre vous se reconnaîtront dans le cas de Corinne Martin : login « martin », mot de passe « corinne » ?).

Maintenant, si vous croyez que le pirate va s'arrêter en si bon chemin, c'est que vous ignorez les formidables capacités de NetBIOS. Le service SMB (Server Message Block), autre service NetBIOS fonctionnant sur le port TCP 139 ou 445, permet d'établir le plus simplement du monde et sans authentification aucune, une session SMB avec un partage situé sur n'importe quel ordinateur qui figure dans la liste précédente. Vous direz, à juste titre, que le pirate n'est pas supposé connaître le nom de ces partages. La belle affaire : Windows ouvre par défaut sur toutes les machines des partages masqués, comme `IPC$`, `C$` ou `Admin$`. Vous ne saviez pas que vous aviez des partages ouverts sur votre machine, autres que ceux que vous aviez définis explicitement ? Quel dommage ! car le pirate, lui, le sait. En lançant la simple commande :

```
net use \\DELL_CATHY\IPC$ "" /u:""
```

il se connecte directement à votre ordinateur, sans authentification, il établit ce que l'on appelle dans le jargon une connexion nulle.

Connexion nulle

Qu'est-ce qu'une connexion nulle pour un pirate ? C'est tout simplement un lien privilégié qui relie désormais sa machine à la vôtre. À partir du moment où une connexion nulle existe, votre machine devient subitement intarissable sur des sujets divers, comme celui des paramètres système ou réseau.

Le pirate sera capable de recenser les partages ouverts sur votre machine (les vôtres, les vrais, ceux que vous avez définis), de s'y connecter, de visualiser et d'accéder à votre arborescence de fichiers comme s'il se trouvait physiquement présent sur votre poste ! Si le partage se trouve au niveau de la racine, le pirate accède à tous les fichiers, y compris ceux de login/mots de passe du système, de votre messagerie, de votre site FTP, ou de vos bases de données. Même si ces mots de passe sont stockés chiffrés, partez du principe que le pirate saura les décrypter en très peu de temps, surtout lorsqu'ils figurent dans le dictionnaire !

À RETENIR **Sécuriser NetBIOS**

Une politique laxiste vis-à-vis des accès NetBIOS, et c'est la sécurité de tout le site qui s'écroule. Nous verrons au chapitre suivant qu'il est possible de se protéger de ce genre d'assaut. Globalement, il faut impérativement :

- ne jamais partager de dossier à la légère ;
- rester vigilant par rapport aux autorisations associées aux partages, définir des mots de passe robustes ;
- filtrer soigneusement les protocoles NetBIOS : autoriser à la rigueur sur votre réseau local les ports associés à ses services (ports UDP 137 – NetBIOS Name Service, TCP 139 – NetBIOS Session Service, ou 445 – service SMB directement sur TCP/IP), mais les interdire impérativement sur les réseaux non sûrs.

Attaques perpétrées via les protocoles applicatifs

En quoi HTTP, le protocole du Web est-il dangereux ?

Hormis les réseaux à caractère vraiment sensible (sièges d'entreprises, partis politiques, Défense…) – et encore ! – existe-t-il un pare-feu dans le monde qui interdise le protocole HTTP ? Pratiquement pas. Quelles que soient les politiques de filtrage mises en œuvre par ces produits (même quand elles sont des plus restrictives), ils ont à peu près tous le même point commun : celui de laisser passer HTTP, protocole universel d'Internet. S'il paraît en effet inconcevable de supprimer aux utilisateurs l'accès au Web, un protocole mondialement autorisé, pour un pirate, c'est ce qui s'appelle une aubaine : vaincre HTTP signifie faire main basse sur les réseaux du monde entier. Alors vous imaginez l'énergie déployée depuis des années par les cyber-voyous de tous bords pour y parvenir ! Résultat, HTTP (et, dans une moindre mesure, son petit frère HTTPS) constitue un véritable boulevard pour les intrusions. Examinons quelques exemples.

À RETENIR **Encapsulation de protocole**

Bien entendu, cette technique reste valable avec n'importe quel protocole autorisé sur la plupart des pare-feux, comme DNS, FTP ou SMTP (pour ne citer que ceux-là).

Encapsulation de protocole

Beaucoup pensent que, disposant d'un pare-feu quelque part sur le réseau, le problème de la sécurité est réglé. Alors pour fixer les idées, supposons que vous êtes protégé avec un pare-feu interdisant tout, sauf les connexions sortantes sur le port 80. Que peut bien tenter le pirate ? Une chose est certaine : si une trame HTTP venue de l'extérieur semble répondre à la requête d'un utilisateur situé à l'intérieur de la zone de protection du pare-feu, elle passera. Le pirate jouit donc d'une possibilité incontestable, celle qui consiste à détourner l'usage normal du protocole : en faisant l'hypothèse que votre machine a été préalablement infiltrée, qui pourrait bien empêcher un processus malveillant installé sur votre poste d'initier sans votre consentement une connexion arbitraire avec la machine du pirate ? Le pare-feu peut-être ? Non, puisqu'il autorise justement ce type de flux. Malgré sa présence, votre machine et le pirate peuvent communiquer tout à fait librement, à condition bien sûr d'enfermer les bribes de leur conversation à l'intérieur d'innocentes trames HTTP, autrement dit de se « déguiser » en HTTP. En d'autres termes, le pirate utilise HTTP comme protocole de transport pour acheminer un autre protocole, le sien, dont le contenu n'a probablement pas grand chose à voir avec des pages web. Ce protocole encapsulé peut contenir tout et n'importe quoi, y compris des commandes que seul le code malveillant installé sur votre poste saura interpréter. À partir de là, via un canal de communication établi au travers du pare-feu, avec la bénédiction totale de celui-ci et la complicité involontaire de HTTP, le pirate peut inonder le réseau avec des trames inutiles (attaque par déni de service), collecter et rapatrier vos données confidentielles, détruire des fichiers, installer à distance d'autres codes malveillants, etc. Voici donc un premier risque majeur, l'encapsulation d'un protocole arbitraire à l'intérieur d'un protocole autorisé.

Téléchargement de codes mobiles

Une caractéristique importante du protocole HTTP, nous le verrons plus en détail au chapitre 6, est sa capacité à transmettre les codes mobiles (contrôles ActiveX, scripts, applets Java, etc.), c'est-à-dire à télécharger sur votre poste en même temps que les pages web, de façon transparente et totalement à votre insu, des codes exécutables de toutes sortes, dont des codes malveillants. Qui donc peut bien empêcher ces téléchargements malheureux ? Pour que le pare-feu puisse faire quelque chose, encore faut-il :

- qu'il soit capable d'analyser le contenu des données véhiculées par HTTP (les pare-feux se limitant à une simple analyse de niveau 4, c'est-à-dire effectuant un filtrage basé sur les numéros de ports, sont donc complètement hors course) ;

À RETENIR **Danger de l'encapsulation de protocole**

Vous comprendrez aisément l'effet inattendu – et dévastateur en ce qui concerne la sécurité – produit par l'acceptation généralisée de HTTP et de HTTPS : la tendance actuelle des applications est de se servir de HTTP comme protocole de transport pour véhiculer les protocoles d'applications P2P, comme KaZaA, Emule, Bittorrent ou Overnet. Cela veut dire que HTTP ne sert plus seulement à transporter les objets du Web, il est utilisé par les éditeurs comme support universel pour transporter… des protocoles de plus haut niveau qui se révèlent souvent spécifiques, complexes et sujets à de nombreux changements. Or, ceci pose un problème évident en matière de sécurité, car, à l'heure actuelle, aucun outil de filtrage ne sait analyser de façon fiable le contenu de ces protocoles et il n'est pas sûr que ce genre de produit voie le jour, tant la tâche est ardue. Qui n'a jamais expérimenté l'infection par un virus ou l'installation d'un cheval de Troie par ce canal ? Hélas, à cause de HTTP, l'injection de codes malveillents devient courante, sans que ce protocole ne soit jamais violé.

- qu'il dispose d'une base de référence à jour répertoriant les « bons » codes et les mauvais.

Aujourd'hui, de tels pare-feux n'existent pas et il semble pour le moment illusoire d'espérer voir apparaître des produits efficaces dans un proche avenir.

CONSEIL **Mesures contre les codes mobiles**

Nous incitons fortement le lecteur à consulter le chapitre 6, dans lequel quelques mesures pour remédier à ce problème délicat sont proposées.

Détournement des flux chiffrés

L'utilisation croissante des flux chiffrés, qui transitent par exemple via les protocoles VPN-SSL et HTTPS, constitue paradoxalement une autre source d'infiltration : le trafic étant chiffré de bout en bout entre le poste utilisateur et le serveur distant, le pare-feu ne peut examiner son contenu et n'a d'autre choix que de laisser passer ce flux en bloc (ou de le bloquer complètement mais, dans ce cas, aucun trafic via un protocole sécurisé ne circulera). Si donc ce type de flux est autorisé et faisant l'hypothèse que votre poste a été infiltré, un processus malveillant peut très bien établir un tunnel chiffré avec l'ordinateur d'un pirate distant ; ce canal établi, le pirate pourra faire tout ce qu'il veut, télécharger des codes arbitraires, lancer des commandes à distance, collecter des informations… au nez et à la barbe du pare-feu qui reste aveugle.

Piratage par courrier électronique

Nous avons déjà abordé les problèmes classiques de contamination virale due à la réception de messages contenant une pièce jointe infectée. Ce type d'attaque est bien connu, au point d'ailleurs de faire presque oublier

qu'il existe d'autres moyens d'accès à votre espace informatique par la messagerie – moyens qui se révèlent pourtant d'une efficacité redoutable. Si vous n'êtes protégé par aucun pare-feu, ou si votre pare-feu laisse passer les protocoles usuels de la messagerie (SMTP, POP3, IMAP4), ce qui est fort prévisible, un pirate habile peut tout à fait jouer sur les mécanismes des protocoles de la messagerie, voire des forums de discussion sur Internet, pour transformer un canal de transmission « officiel » en un véritable boulevard d'intrusion.

Avez-vous déjà réfléchi à ce qu'est un client de messagerie ? Disons grossièrement qu'il s'agit d'un enrobage convivial destiné à vous faciliter la saisie des paramètres nécessaires à l'élaboration des messages (enveloppe et contenu), et à traiter ensuite ces messages. Une fois que vous avez entré les éléments caractéristiques du message (destinataire, corps du message), le client de messagerie fait appel à un moteur interne chargé de traduire ces paramètres en un langage particulier, que le serveur de messagerie saura interpréter. Ce langage est ce que l'on appelle SMTP, le protocole universel de la messagerie. Évidemment, exposé comme cela, parler de SMTP peut sembler tout à fait barbare. En réalité, il s'agit d'un langage de haut niveau, simple et de bon sens, à tel point que vous pourriez presque saisir directement, dans une fenêtre MS-DOS, des commandes SMTP vous permettant d'envoyer un message. Par exemple, si vous envoyez à un serveur de messagerie les commandes suivantes :

```
mail from:<addr_source>
rcpt to:<addr_desti>
```

en renseignant les champs d'adresses électroniques source et destination avec de bonnes valeurs, celui-ci enverra le message. Certes, il faut entrer d'autres commandes pour que le message soit complet, mais le principe est celui-là. Bien sûr, il faut aussi ranger les commandes SMTP, ainsi que les paramètres que vous fournissez, dans le bon ordre à l'intérieur de trames IP pour que celles-ci parviennent jusqu'au serveur (empilement de la couche SMTP au dessus de TCP/IP selon le modèle OSI – voir figure 4-2). Et évidemment, il ne faut pas se tromper dans la syntaxe des commandes, car sinon le serveur risque de considérer le message comme invalide. Tout ceci est un peu pénible ; c'est pourquoi nous utilisons tous un client de messagerie, qui a le mérite de nous débarrasser de ces problèmes de syntaxe et de rendre ces opérations automatiques.

Cependant, la tentation du pirate de se passer du client de messagerie est grande, car en élaborant ses messages directement en ligne de commande, il peut agir à sa guise sur chaque paramètre.

Supposez par exemple qu'il entre la séquence suivante :.

```
ehlo
mail from: <utilisateur.usurpé@domaine1>
rcpt to: <victime@domaine2>
data
subject: Panne de serveur e-mail
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
<HTML>
Suite à l'opération de maintenance ayant eu lieu récemment sur
le serveur mail de votre fournisseur d'accès, veuillez vous
connecter au site suivant et ressaisir vos identifiants afin de
valider votre compte :
http://www.asep-maintce.fr/comptesMail/
</HTML>
.
quit
```

Doté d'un outil adéquat, le pirate peut déjà envoyer un message qui semble provenir d'un autre utilisateur à l'adresse victime@domaine2. Jusque là, il n'y a encore rien de bien méchant, sauf si l'utilisateur victime tombe dans le piège, car dans ce cas précis, il s'agit d'un exemple simple de phishing.

Seulement, en enrichissant quelque peu ce squelette, le pirate peut tout à fait lancer des attaques extrêmement préjudiciables. Sachez par exemple qu'en ajoutant ne serait-ce que trois lignes bien choisies entre les deux balises <HTML> et </HTML>, le pirate peut activer l'exécution d'un programme sur votre machine : le code malveillant établissant une connexion HTTP avec le pirate.

Bien entendu, ces techniques datent un peu et sont actuellement fort heureusement déjouées par les programmes antivirus ou par les correctifs des clients de messageries. Cependant, de nouvelles vulnérabilités apparaissent tous les jours et n'oubliez jamais que la messagerie est un vecteur de piratage potentiel.

RENVOI **Phishing**

Les différents types d'attaques cités dans cet ouvrage sont définis à l'annexe B.

Risques liés aux applications sur Internet

Applications sur Internet : des vecteurs potentiels d'intrusion

Nous faisons ici allusion aux applications qui dialoguent sur Internet, qui reposent donc sur la pile des protocoles présentés schématiquement à la figure 4-2 ; nous nous situons donc maintenant en haut du modèle

OSI. Parmi les plus connues, citons notamment les navigateurs web (HTTP, HTTPS), les messageries (SMTP, POP3, IMAP4), les agents de gestion de réseaux ou d'équipements (SNMP), ou les applications poste à poste (P2P), basées sur des protocoles encapsulés (Kazaa, Emule, etc.). Cependant, il y en a bien d'autres.

Pour fixer les idées, prenons l'exemple du Web et de la messagerie électronique et partons du principe, pour continuer à ébranler les idées reçues, que vous êtes protégé avec un pare-feu. Qui plus est, votre pare-feu délivre à vos yeux une politique restrictive : il est configuré de manière à ce que tous les ports soient fermés, à l'exception bien sûr de ceux du Web, car vous hébergez un serveur web, ou de ceux de la messagerie ; les seuls protocoles autorisés à traverser le pare-feu sont donc HTTP (sur le port 80), HTTPS (HTTP sur SSL, sur le port 443), SMTP (sur le port 25) et POP3 (sur le port 110).

Malgré le caractère obsolète de cet exemple (peu de serveurs web sont encore vulnérables à cette attaque très ancienne), voyez comment il est facile à un pirate de récupérer à distance des données confidentielles : les premières versions du serveur web Apache était vulnérables à l'attaque dite PHF. Il n'était pas capable d'analyser, ni de valider correctement les entrées qu'il recevait. Le script PHF acceptait notamment le caractère de nouvelle ligne (`%0a`), interprétait la chaîne qui suivait comme une commande qu'il s'empressait d'exécuter avec les droits associés au processus du serveur web (c'est-à-dire, le plus souvent, les droits administrateur). Pour parler concrètement, lorsque le serveur web recevait la commande suivante :

```
/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

il renvoyait tout bonnement au pirate le fichier contenant la liste des identifiants utilisateurs et des mots de passe chiffrés (pour le pirate averti, retrouver ensuite les mots de passe en clair n'était pas très compliqué).

Vous trouvez peut-être que cet exemple n'est pas assez spectaculaire ? Qu'à cela ne tienne. Imaginez qu'à la place de la commande `/bin/cat /etc/passwd`, le pirate lance à distance un espion installé à l'avance ou, pourquoi pas, la commande `telnet`. Sur une fenêtre de son ordinateur, il récupère ainsi un interpréteur de commandes, grâce auquel il peut lancer sur sa machine, de façon interactive, des commandes qui s'exécute sur la vôtre ! Et le tout, bien sûr, avec la bénédiction de votre pare-feu. À ce niveau là, ce n'est plus une brèche…

Ceci n'est qu'un exemple, certes dépassé (notre but n'est pas de vous apprendre à pirater les systèmes !), mais il en existe des dizaines d'autres qui, eux, sont parfaitement opérationnels.

Rappel **Applications boguées**

N'oubliez jamais que tout logiciel vous apporte sa petite ration de bogues, qui, exploités « à bon escient », offrent aux pirates un moyen d'entrer au cœur de votre système (voir à ce sujet les quelques exemples présentés aux chapitres 3 et 6). Si la découverte d'un bogue et l'écriture du programme qui l'exploite demandent une haute expertise et un réel talent, l'utilisation de l'outil prêt à l'emploi qui en résulte, généralement publié sur Internet, est à la portée de n'importe quel « cyber-plouc ».

Le virus Netsky.P doit notamment sa brillante carrière au bogue d'Internet Explorer, lorsque celui-ci se trouve en présence d'un courrier infecté et dont l'en-tête MIME est incorrect (voir chapitre 3). Si vous utilisiez une version d'IE vulnérable à cette attaque (c'est-à-dire un IE que vous n'aviez pas remis à jour), la simple réception d'un message mal formaté provoquait l'exécution automatique de la pièce jointe, et vous étiez contaminé. Voyez encore comme il est aisé d'abuser un pare-feu effectuant un simple filtrage basé sur le numéro de port (agissant donc aux niveaux 3 et 4 du modèle OSI), alors que l'attaque se situe aux niveaux plus élevés des couches de protocoles. Si votre pare-feu laisse les ports 25 et 110 ouverts (donc autorise les protocoles SMTP et POP3), il n'a aucune raison d'intervenir…

> À RETENIR **Nécessité d'un pare-feu « applicatif »**
>
> Il n'est pas dans notre intention d'évoquer les dizaines et les dizaines de possibilités qui existent aujourd'hui pour entrer au cœur de votre système ; vous trouverez quelques exemples épars un peu partout dans cet ouvrage et plusieurs livres sont entièrement consacrés à ce sujet. Nous espérons au moins qu'à la lumière de ces exemples, vous commencez à comprendre à quel point tout objet communiquant est un ennemi en puissance et, surtout, pourquoi une protection efficace passe obligatoirement par un pare-feu « applicatif », capable d'analyser le contenu véhiculé à l'intérieur d'un protocole. Nous verrons ces points en détail au chapitre 5.

Se protéger des attaques dirigées contre les applications

Une protection efficace contre ce type d'attaque résulte inévitablement d'un faisceau de mesures qui se complètent.

La première consiste évidemment à mettre régulièrement à jour vos logiciels ; si vous installez les correctifs publiés chez les éditeurs, vous augmentez vos chances de colmater les failles connues et diminuez ainsi les risques d'attaque par cette voie.

La deuxième mesure est liée à la manière dont vous faites usage d'Internet. Pour la plupart d'entre vous, l'informatique n'est pas votre métier. Néanmoins, il est vraiment important que vous preniez définitivement conscience des pièges qui se cachent derrière une application. Vous constatez à quel point une application « honnête » est potentiellement exploitée par les pirates, alors, surtout, ne prêtez pas le flanc aux attaques en téléchargeant tout et n'importe quoi, de préférence des applications douteuses. Dites-vous bien que chaque code exécutable est un cheval de Troie en puissance, surtout s'il est gratuit, et encore plus s'il sert à échanger des fichiers piratés !

Ensuite, vous percevez sans doute qu'il y a urgence à installer un pare-feu. Ce problème sera traité au prochain chapitre mais, nous n'insisterons jamais assez, si un pare-feu limite son action à filtrer les protocoles sur la base des numéros de ports… il n'y voit que du feu ! De toutes façons, mettre en place un pare-feu, quel qu'il soit, est utile au moins pour interdire les protocoles, ou pour filtrer les applications dans le cas d'un pare-feu personnel. Cependant, sachez que, en ce qui concerne les protocoles autorisés, sa capacité de filtrage sera tout à fait partielle si c'est un pare-feu de niveau 4. Dans certains cas, en entreprise par exemple, il faut faire appel à un pare-feu applicatif.

Enfin, il faut aussi vous doter d'un bon antivirus pour contrer les attaques qui se situent dans les hautes sphères du modèle OSI.

ANTIVIRUS OU PARE-FEU **Jamais l'un sans l'autre**

Nous ne le répéterons jamais assez : pas de pare-feu sans antivirus, pas d'antivirus sans pare-feu.

Mention spéciale pour le Wi-Fi

Avec le Wi-Fi, nous entrons dans le monde fascinant des réseaux sans fil. Quand nous disons fascinant, nous pensons bien sûr aux utilisateurs qui y trouvent l'intérêt que l'on sait, mais aussi, et surtout, aux pirates. En effet, du point de vue de l'intrusion, les réseaux Wi-Fi offrent une voie royale ! Ces technologies nouvelles sont encore mal maîtrisées en ce qui concerne la sécurité, et sont aujourd'hui perçues par les attaquants comme le moyen le plus efficace pour contourner la sécurité d'un site, généralement affectée aux réseaux filaires.

Qu'est-ce que le Wi-Fi

Le Wi-Fi (*Wireless Fidelity*) est un label de certification désignant des équipements de communication radio et infrarouge qui satisfont à des critères techniques bien spécifiques : notamment une portée comprise entre 10 et 100 mètres, un débit de l'ordre de la dizaine de Mbits/s, voire plus dans le futur, et des exigences d'interopérabilité. Il s'agit donc d'un profil tout à fait adapté à la problématique du réseau local. Munis de la technologie Wi-Fi, les terminaux échangent de l'information et interagissent en réseau, comme s'ils étaient reliés par un câble Ethernet.

Si votre matériel est un terminal natif Wi-Fi (caméra, PDA, etc.), ou si vous équipez votre PC d'une carte réseau 802.11, il vous est possible de joindre un réseau sans fil. Il existe deux manières de se raccorder à un réseau Wi-Fi : via l'établissement d'un accès direct avec les autres terminaux Wi-Fi situés dans la zone accessible par votre carte (mode ad-hoc), ou bien à travers un point d'accès qui assure en général la passerelle vers le réseau Internet (mode infrastructure). Sitôt votre terminal allumé et quel que soit l'endroit où vous vous trouvez, à supposer bien sûr qu'il bénéficie d'une couverture suffisante, vous pouvez, sans formalité préalable, accéder à Internet, lire votre courrier électronique, accéder à distance aux données de votre entreprise ou communiquer avec vos interlocuteurs habituels en utilisant vos applications préférées.

JARGON **IEEE 802.11**

IEEE 802.11 représente la famille de normes qui définit les protocoles du Wi-Fi.

Risques liés au Wi-Fi

N'hésitons pas à rappeler une règle fondamentale en sécurité : plus une technologie devient populaire, plus elle est attaquée. Et comme, de surcroît, la sécurité n'a jamais été la préoccupation majeure des concepteurs du Wi-Fi, tirez-en vous-même les conclusions…

Commençons par le plus facile : il est très simple pour un pirate d'écouter ce que vous envoyez et ce que vous recevez. Comme ces informations sont transmises par voie radio, n'importe quel terminal Wi-Fi situé à la portée du point d'accès peut les capter. Certes, il reste au pirate un petit travail pour décrypter ces données, mais, comme nous allons le voir, ceci n'est pas bien méchant.

CONSEIL **Rien d'important par Wi-Fi**

Attention, avec le Wi-Fi, votre petite sœur saura lire votre courrier galant. Alors évitez ce canal pour envoyer à votre patron la dernière mouture de la proposition commerciale du contrat stratégique à venir.

Ce que nous venons d'évoquer pourrait être qualifié d'attaque passive pour pirate pantouflard. En étant un peu plus actif, on peut faire bien pire. À travers le réseau Wi-Fi, un pirate accède directement à votre poste. Il peut lire votre messagerie, accéder à des données financières, récupérer les fichiers sensibles, les mots de passe, les clés privées servant à déchiffrer ces mêmes fichiers...

Si, par malheur, le poste Wi-Fi est raccordé à un réseau d'entreprise, le pirate peut entrer directement au cœur de ce réseau, visiter les autres ordinateurs, les serveurs. Il accède ainsi à toutes les données commerciales ou financières, aux documents stratégiques, au nez et à la barbe des pare-feux ou de tout autre type de filtres.

À RETENIR **Wi-Fi = Danger**

Les risques liés au Wi-Fi sont majeurs. L'introduction de terminaux Wi-Fi dans un réseau filaire sécurisé est comparable à une ville fortifiée vaincue suite à l'invasion discrète et nocturne de parachutistes.

Localisation des points d'accès

Avec le Wi-Fi, les pirates ont remis au goût du jour une technique désuète utilisée au cours de la seconde guerre mondiale pour pister les opérateurs radio, le concept de *wardriving*. La détection et la prise d'empreinte de réseaux sans fil consiste à arpenter dans un véhicule (à la vitesse normale de la circulation) une zone d'activité, un centre-ville ou un dédale de rues, dans le but de localiser les points d'accès. Munis de dispositifs disponibles dans le commerce, c'est-à-dire un ordinateur portable, une carte réseau sans fil, une antenne et un récepteur GPS, ainsi que de quelques logiciels spécifiques, les pirates établissent tranquillement une cartographie très précise des points d'accès de votre région. Cette détection peut très bien se faire d'une manière tout à fait passive (il suffit d'écouter les trames balises émises par les points d'accès).

Parfois, il n'est même pas nécessaire de se fatiguer à faire ce travail. Des pirates, probablement soucieux d'économiser l'énergie des autres membres de leur confrérie, ont établi de magnifiques cartographies… que l'on trouve très facilement sur Internet !

Bien entendu, ces outils performants de *wardriving* ne se limitent pas à la simple détection des points d'accès. Ils fournissent aussi les précieux identifiants sans lesquel il est impossible de joindre le réseau, le fameux SSID (Service Set IDentifier), les adresses MAC des cartes référencées sur chaque point d'accès (ayez confiance, le pirate saura régler la sienne à une « bonne » valeur), et le mode de chiffrement du trafic.

Intrusion au cœur de votre système

Une fois que le pirate a localisé et identifié les points d'accès du secteur, il se sert de son analyseur de réseau pour classer les données interceptées, par point d'accès, puis par client. Il cherche ensuite à en savoir plus sur le mode de chiffrement (si les données sont chiffrées), notamment si elles sont chiffrées par SSL (c'est-à-dire par vous), ou si elle sont chiffrées par une implémentation de WEP (c'est-à-dire par l'infrastructure du Wi-Fi). Bien entendu, le pirate préfère le WEP, nous allons tout de suite voir pourquoi.

WEP (Wired Equivalent Privacy) est un algorithme cryptologique à clés secrètes destiné à protéger les trames émises sur un réseau sans fil. Les clés sont partagées entre le terminal et le point d'accès au réseau, et si le système ignore cette clé secrète partagée, il ne peut, en théorie du moins, faire partie du réseau. Seulement il y a un hic ! Contrairement à ce que pensent de nombreux utilisateurs, WEP n'a jamais eu la vocation d'offrir une sécurisation fiable du réseau ; WEP a été conçu dans un seul but : protéger le trafic d'un réseau WLAN contre les espions passifs et

involontaires. Les implémentations du WEP vous protègent en quelque sorte de votre petite sœur.

Le pirate n'a donc pas beaucoup de difficultés à casser cette clé. Dans la réalité, il y parvient… en trois secondes (parce que c'est un bon pirate, rassurez-vous ; un mauvais mettrait au moins dix secondes pour y arriver).

Dès lors, l'édifice s'écroule ; avec de bons outils et un peu de métier, tout est permis au pirate, ou presque. Il accède au contenu de votre machine et au réseau auquel elle est raccordée. Franchement, avec le développement des réseaux comme le Wi-Fi, pourquoi se fatiguer à contourner les équipements de sécurité périmétriques, comme les pare-feux ?

Mesures de protection

Après avoir brossé un tel tableau, faut-il abandonner le Wi-Fi ? Avant d'en venir à de telles extrémités, laissons à l'avocat de la défense le soin de présenter de nouvelles perspectives en matière de protection des réseaux sans fil. En effet, le constat alarmiste exposé précédemment reflète plutôt le mode d'utilisation actuel du Wi-Fi, et non la réalité de cette technologie, dotée des avancées récentes en matière de sécurité. Il faut savoir que depuis quelques années, les constructeurs se sont mobilisés pour développer des mécanismes (plus) fiables de sécurité. Malheureusement, si ces mécanismes sont pour la plupart intégrés aux produits Wi-Fi de nouvelle génération, les utilisateurs n'ont pas encore le réflexe de les employer. Essayons donc d'attirer votre attention sur ces points et de dresser une liste de mesures qui rehaussera indiscutablement le niveau de sécurité de votre infrastructure Wi-Fi.

Installez un pare-feu personnel

Si la carte Wi-Fi est installée sur le PC, il faut systématiquement installer un pare-feu personnel sur le poste. En effet, celui-ci réduira les risques d'intrusion par ce canal, et fera barrage à toute application qui tenterait d'établir à votre insu une connexion sortante vers Internet. Ce sujet sera examiné en détail au chapitre 5.

Utilisez WPA, voire WPA2

Comme nous venons de l'évoquer, disposer d'une liaison Wi-Fi non chiffrée est absolument suicidaire et les liaisons protégées avec un chiffre WEP ne valent guère mieux.

À la fin de l'année 2003, la Wi-Fi Alliance a lancé le concept de Wi-Fi sécurisé de nouvelle génération, en s'appuyant notamment sur un nouvel algorithme cryptologique, le WPA (Wi-Fi Protected Access), conçu

cette fois dans le but réel de sécuriser le trafic radio. WPA garantit un niveau de confidentialité plus élevé et l'intégrité du trafic échangé entre le terminal (votre poste) et le point d'accès ; il fournit en outre un service d'authentification forte du terminal, basé sur des mécanismes compatibles avec les protocoles d'authentification RADIUS.

En septembre 2004, une nouvelle évolution de WPA était disponible. WPA2 utilise l'algorithme AES, conçu par les cryptologues belges Vincent Rijmen et Joan Daemen (Rijndael), reconnu aujourd'hui dans le monde entier et massivement utilisé au sein des produits de sécurité actuels.

Ces deux algorithmes ont été spécifiés pour combler les vulnérabilités de WEP. Il est donc fortement recommandé d'abandonner WEP au profit de WPA, voire de WPA2.

Attention, vous ne pouvez utiliser ces algorithmes que si votre carte d'interface Wi-Fi et le point d'accès les acceptent mutuellement. En toute logique, les points d'accès fournis par les opérateurs doivent au moins proposer le WPA. Sachez en outre que la mise à niveau vers le WPA est réalisable sans changer d'équipement si ce dernier est certifié Wi-Fi. La mise à jour WPA2 risque en revanche de nécessiter l'installation d'un nouveau matériel.

Activez la traduction d'adresse (NAT)

Si vous disposez de votre propre routeur Wi-Fi et si celui-ci gère physiquement votre accès au réseau public, activez la traduction d'adresse (voir chapitre 5) : l'adresse privée de votre machine, ou le plan d'adressage interne de votre réseau, restera ainsi invisible du monde extérieur. Les pirates ne pourront donc pas joindre votre machine directement.

Masquez le SSID

Le nom du réseau sans fil (SSID) étant fort utile aux pirates, désactivez l'option de diffusion du SSID si votre équipement le permet. Si vous ne le faites pas, le SSID est émis continuellement sur les ondes à l'intérieur des trames balises, et c'est un jeu d'enfant d'intercepter cette information.

Ayez recours aux tunnels VPN

Si vous utilisez les réseaux Wi-Fi dans votre activité professionnelle, notamment pour accéder à distance aux ressources de votre entreprise ou pour échanger avec vos collègues des documents confidentiels, il est impératif de vous faire établir un tunnel privé de type VPN (*Virtual Private Network*) entre votre poste nomade et un serveur VPN installé dans l'entreprise. Le trafic sera ainsi chiffré de bout en bout entre votre poste et le serveur, qui plus est (si vous choisissez un bon produit – voir

chapitre suivant) avec un chiffre robuste. Ce trafic sera bien entendu surchiffré par le système Wi-Fi sur le tronçon radio.

Désactivez le Wi-Fi lorsque vous vous raccordez au réseau filaire

Pour les professionnels, si l'utilisation du Wi-Fi se justifie lors de vos déplacements, vous ne devriez en toute logique pas vous en servir, sauf cas particuliers, lorsque vous êtes de retour et lorsque votre poste est à nouveau raccordé au réseau filaire de l'entreprise.

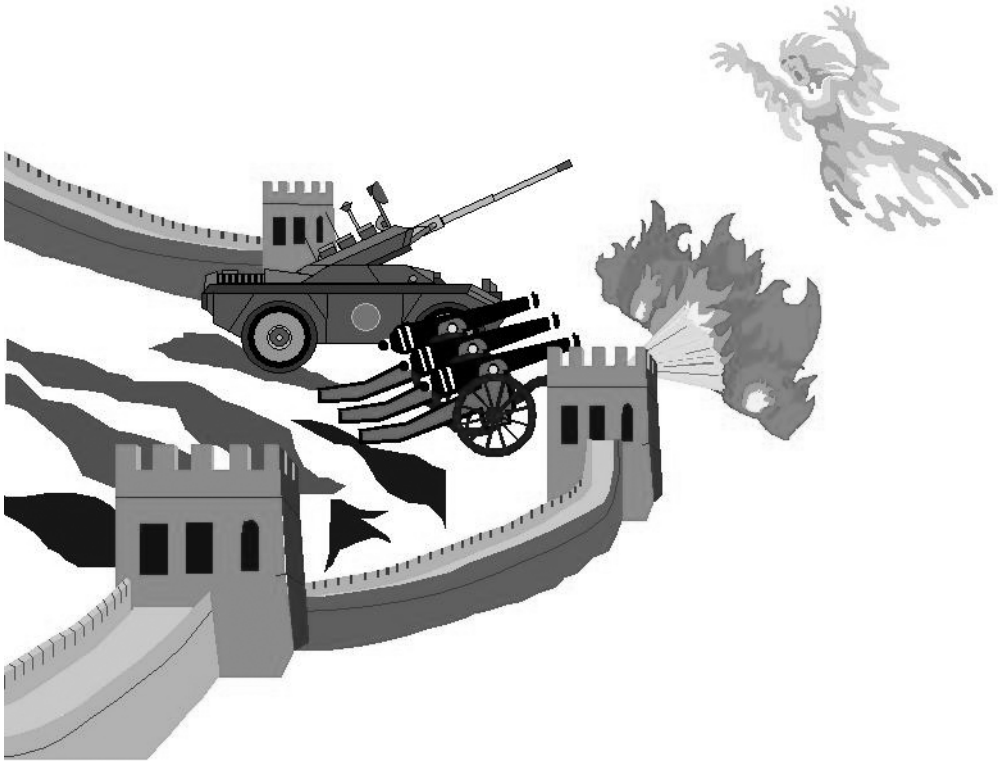
Ne prêtez pas le flan aux attaques. Configurez votre poste de manière à activer manuellement votre liaison Wi-Fi à la demande, et veillez à ce qu'elle soit désactivée dès que vous vous branchez sur le réseau filaire.

Récapitulatif

L'objectif de ce chapitre n'était pas de vous présenter toutes les techniques qui existent à l'heure actuelle pour infiltrer les machines et en prendre possession : plusieurs ouvrages ne suffiraient pas pour décrire ne serait-ce que les attaques les plus connues.

En revanche, nous espérons vous avoir fait prendre conscience qu'à partir du moment où existe le plus petit canal ouvert entre le monde extérieur et votre informatique, un pirate peut s'en servir pour entrer et vous attaquer (en détournant le protocole de communication, en exploitant une vulnérabilité du protocole ou de l'application, en encapsulant un protocole de plus haut niveau, une donnée ou un programme malveillant, ou en utilisant une quantité d'autres astuces). Dès qu'un moyen de communication, quel qu'il soit, est ouvert entre vous et le monde extérieur, vous êtes potentiellement vulnérable. Sachez que, dans l'esprit du pirate chevronné, l'accès à une machine et l'obtention des droits administrateur sur cette machine ou sur un autre équipement (routeur) est une formalité. Le vrai travail commence après… Aujourd'hui, l'enjeu pour les pirates se situe beaucoup plus au niveau des couches hautes du modèle OSI, à savoir les protocoles applicatifs (HTTP, SMTP, DNS, etc.), les protocoles encapsulés à l'intérieur de HTTP (P2P, VoIP, H323, etc.) et les applications, c'est-à-dire une zone où le pare-feu devient de moins en moins pertinent. Contrairement à l'idée reçue, un pare-feu ne constitue pas la panacée : il ne fait que restreindre considérablement les « occurrences » possibles, et nous verrons dans quelle mesure au chapitre suivant, mais le risque subsiste toujours. Une protection efficace résulte d'un faisceau de mesures.

chapitre 5



Installer et configurer son pare-feu personnel

Installer un pare-feu ne suffit pas à protéger un réseau. Toutefois, si vous le configurez avec rigueur, il limitera très fortement les risques d'intrusion et vous protègera d'un grand nombre d'attaques.

SOMMAIRE

- Antivirus et pare-feu
- Types de pare-feux
- Installer et configurer un pare-feu logiciel
- Règles de filtrage
- Installer un pare-feu matériel
- Détecter et prévenir les intrusions

MOTS-CLÉS

- « stateful inspection »
- pare-feu applicatif
- DMZ (DeMilitarized Zone)
- filtrage protocolaire
- traduction d'adresse
- VPN (Virtual Private Network)

La sécurité informatique n'est pas un sujet très distrayant. L'impopularité de ce thème rencontre sans doute toute sa justification dans ce chapitre. En effet, il est difficile d'évoquer les pare-feux sans entrer dans des considérations techniques délicates, que beaucoup d'informaticiens professionnels – hormis peut être les administrateurs de systèmes – rechignent à aborder. Pour la plupart d'entre vous, la sécurité n'est pas une préoccupation majeure et vous n'êtes probablement pas disposé à intégrer des notions d'administration de systèmes informatiques.

Toutefois, il serait vain de croire que l'installation d'un pare-feu suffit à protéger un réseau. Il ne faut jamais oublier que nos adversaires sont d'habiles tricheurs qui repoussent très loin les limites de leur talent. Ils savent exploiter la moindre faiblesse de configuration et contourner les protections. Ils réussissent à s'engouffrer à l'intérieur des canaux que vous autorisez, malgré les restrictions, et à se ménager de multiples points d'accès pour pénétrer au cœur de votre système. Ils n'hésitent pas, s'il le faut, à exploiter les propres failles du pare-feu, voire à le désactiver. Protéger efficacement un PC ou un réseau d'ordinateurs raccordé à Internet nécessite une bonne connaissance de la mentalité des pirates avertis et des techniques qu'ils emploient. Il est également utile d'avoir une bonne compréhension des règles de filtrage et de leurs conséquences, ainsi qu'un suivi attentif de l'activité du réseau, spécialement aux points d'accès avec les réseaux non sûrs. Mettre en œuvre et exploiter un pare-feu est presque une affaire de spécialiste.

Cela dit, même sans être un spécialiste, il suffit d'un peu de rigueur et d'attention pour réduire fortement les risques et décourager les pirates dénués de motivation stratégique (lesquels constituent l'essentiel de la menace à l'encontre des particuliers et des petites entreprises). Si vous n'êtes pas informaticien, il vous faudra un peu de persévérance pour comprendre le jargon et les concepts manipulés par les pare-feux. Cependant, cet ouvrage est là pour vous faciliter la tâche et vous aider à y parvenir.

Notez tout de même que ce chapitre n'a pas la prétention d'être exhaustif (plusieurs ouvrages n'y suffiraient pas). Son principal objectif est de vous familiariser avec les techniques de configuration et de gestion d'un pare-feu, afin de vous rendre autonome lorsque vous serez vous-même confronté à ce problème.

Notions générales sur les pare-feux

Qu'est-ce qu'un pare-feu ?

Certains pensent s'acheter une bonne conscience en installant un pare-feu. Soit, un pare-feu est un élément important de la chaîne de protection d'un système informatique, mais il ne résout pas tout !

Le pare-feu est en quelque sorte le médecin du trafic circulant sur le réseau : sa mission consiste à ausculter attentivement les paquets IP qu'il voit transiter. Il transmet les « bons » paquets issus d'un trafic normal, il bloque les « mauvais » paquets, symptômes d'attaques, et restreint éventuellement le trafic, dans un sens ou dans l'autre, en fonction d'une politique de filtrage que vous pouvez définir.

Comme son nom l'indique, le pare-feu est une cloison destinée à protéger votre installation du feu extérieur. Situé généralement à l'entrée du site, ou en amont entre votre poste de travail et Internet, il constitue la première ligne de défense contre les menaces actives issues de réseaux non sûrs.

Toutefois, un pare-feu ne constitue pas la panacée. Dans le chapitre précédent, nous avons vu que les protocoles de communication étaient empilés les uns sur les autres au-dessus de la couche IP. Or, au sein d'un paquet IP, les données transportées peuvent très bien représenter plusieurs niveaux d'en-têtes protocolaires, renfermant, au bout du compte, quelques données applicatives (par exemple IP – TCP – HTTP – Kazaa – contenus applicatifs plusieurs fois « zippés »). L'efficacité d'un pare-feu dépend donc de sa capacité à « remonter » à travers ces différentes couches de protocoles pour analyser leur contenu. Plus loin, nous verrons par exemple que certains pare-feux se limitent à l'analyse des couches TCP/UDP/IP et ne vont pas au-delà. D'autre part, même si des experts chevronnés en matière d'intrusion de réseaux pensent les pare-feux impénétrables, c'est compter sans les nombreuses erreurs de configuration, chacune ouvrant sur votre système une voie royale aux pirates de toutes sortes. Par ailleurs, à l'image des systèmes d'exploitation ou des applications informatiques, le pare-feu renferme lui aussi des vulnérabilités l'exposant à des attaques potentielles.

Le pare-feu est donc un élément fort qui renverra les assaillants d'où ils viennent. Attention néanmoins : il faut bien le choisir puis le configurer. Il faut également le maintenir, et surveiller régulièrement son activité.

Antivirus et pare-feu

Les deux sont indispensables, car ils ne sont pas conçus pour combattre les mêmes menaces. Au milieu de toute l'information que vous téléchargez, l'antivirus doit déceler la présence du code malveillant et bloquer son parcours ; il agit un peu comme le service des douanes à la recherche du stock de cocaïne dissimulé parmi les marchandises. À l'inverse, le pare-feu est plutôt comparable à une armée postée à l'entrée de votre forteresse, chargée de repousser les attaques incessantes de commandos plus ou moins habiles. Un pare-feu et un antivirus constituent donc des outils complémentaires, et vous avez absolument besoin des deux pour assurer une bonne protection de votre poste.

COMPRENDRE

Différence entre virus et attaque liée aux protocoles de communication

Historiquement, les pirates ont très vite identifié les faiblesses inhérentes aux protocoles des réseaux de transport (tels que IP, UDP, TCP), et se sont engouffrés dans cette brèche en mettant au point ce que l'on appelle aujourd'hui les attaques « réseau ». Par la suite, ces incorrigibles petits malins ont cherché des techniques plus sophistiquées et se sont logiquement tournés vers les protocoles de plus haut niveau, comme HTTP, DNS ou SMTP. Ils ont donc mené des attaques contre les logiciels de communication et, à travers eux, ils sont parvenus à entrer dans votre système. Ce qu'il faut retenir, c'est qu'un pare-feu est programmé pour contrer en temps réel des attaques orientées plutôt « communication ». Ces attaques peuvent être lancées à distance par un pirate, ou encore, par une armée de pirates, pouvant atteindre des milliers d'individus, s'ils sont suffisamment organisés pour mener de front une offensive groupée, comme les attaques par déni de service.
En revanche, les virus sont des codes « préfabriqués » dont l'action se situe au niveau des contenus applicatifs, donc largement au dessus des couches de communication. Ils n'attaquent pas tout de suite. Lorsqu'ils se présentent aux portes de votre système, ils sont encore inoffensifs. Ils n'agissent qu'après avoir infiltré le système hôte et leur action est programmée par avance. En quelque sorte, ils constituent une bombe à retardement.

Il convient de remarquer que les périmètres de protection des pare-feux et des antivirus ont actuellement tendance à se rejoindre, car la menace, à l'origine orientée « réseau » s'étend de plus en plus au modèle applicatif. On peut observer ce phénomène avec, par exemple, l'exploitation des techniques de débordement de tampons, ainsi que celle des faiblesses liées aux contenus. C'est la raison pour laquelle on constate aujourd'hui un net élargissement des fonctions du pare-feu vers la détection de virus, ainsi que l'apparition de fonctions de pare-feu au sein des programmes antivirus. Néanmoins, il n'existe pas à l'heure actuelle de solution globale satisfaisante, car les excellents pare-feux se révèlent encore de faibles antivirus, et les excellents antivirus ne sont pas encore de bons pare-feux.

RENVOI **Débordement de tampons - Exploitation des faiblesses liées aux contenus**

Reportez-vous à l'annexe B pour toutes les définitions des attaques citées dans le texte.

À RETENIR **Utilisation conjointe d'un antivirus et d'un pare-feu**

Aujourd'hui, une bonne protection passe indiscutablement par l'utilisation d'un pare-feu et d'un antivirus séparés et performants.

Cible du pare-feu

Un pare-feu contrôle le trafic TCP/IP circulant sur le réseau, et qui le traverse ; il permet donc de se protéger contre :

- les attaques « réseau » portant sur les faiblesses des protocoles des couches réseau et transport (TCP/UDP/IP) :
  - balayage d'adresses et de ports, ainsi que toutes les techniques de recensement renseignant l'attaquant à distance sur votre installation, pour qu'il en cerne les vulnérabilités ;
  - ouverture intempestive de sessions interactives à distance, ces dernières étant établies avec des processus, malveillants ou non, sur des ports en veille ou, plus directement, par connexion à des ressources partagées ;
  - exploitation de droits accordés à des entités autorisées (par exemple par usurpation d'adresse IP ou par vol de sessions) ;
  - techniques visant à saturer les ressources de la machine (attaque en déni de service) ;
- les attaques dirigées contre les protocoles « applicatifs », comme HTTP, SMPT ou FTP, et qui permettent d'exploiter les vulnérabilités des logiciels de communication (navigateurs Internet, clients de messagerie) et de se rendre maître de votre ordinateur à distance ;
- les attaques liées aux contenus applicatifs, visant à installer sur votre machine des points d'entrée utilisés par la suite par les pirates pour accéder à vos informations :
  - cookies, vers, logiciels espions ou codes mobiles malveillants (scripts, applets Java, contrôles ActiveX, etc.) ;
  - portes dérobées (les programmes qui tentent par exemple d'accéder à Internet à votre insu).

Différents types de pare-feux

Tous les pare-feux ne reposent pas sur les mêmes concepts et n'offrent pas le même niveau de protection. Il est important de bien saisir les différences entre les grandes catégories de pare-feux actuels, étant donné qu'une confusion des genres aboutit parfois, y compris chez les professionnels de l'informatique, à de sérieux trous dans la barrière de protection.

Pare-feux de niveau 4, dits « stateful inspection »

Citons tout d'abord les pare-feux que nous qualifions dans le jargon de *stateful inspection*, ce qui veut dire à peu près « filtrage à états ». Derrière ce terme se cachent le plus souvent des pare-feux qui agissent principalement au niveau des couches 3 et 4 du modèle OSI, c'est-à-dire aux niveaux réseau (IP) et transport (TCP, UDP). Leur action se résume essentiellement à autoriser ou à refuser les demandes de connexions selon une liste de règles préétablies faisant intervenir des adresses IP et des numéros de ports. Le qualificatif « à états » signifie que le pare-feu gère une table des connexions actives, c'est-à-dire qu'il sait déterminer si un paquet entrant sur le réseau interne protégé fait bien partie d'une connexion sortante précédemment autorisée ; ceci permet notamment d'empêcher un pirate sur Internet d'initialiser spontanément une session avec votre poste dans le but de l'infiltrer.

Ces équipements sont très répandus : la plupart des pare-feux personnels et certains pare-feux matériels sont de type *stateful inspection*. Ils délivrent une protection fort utile, car ils déjouent globalement toutes les attaques réseau basées sur les vulnérabilités intrinsèques des couches IP, TCP ou UDP, et qui figurent maintenant parmi les dinosaures que les pirates (débutants ou chevronnés) utilisent tout à fait couramment. Parmi les plus connues, on peut citer notamment des attaques comme le « Ping de la mort », les balayages TCP et UDP, l'usurpation d'adresse IP (IP spoofing), le vol de session (TCP hijacking), etc.

Cependant, dans le cadre d'une petite ou d'une grande entreprise, la protection assurée par les pare-feux de niveau 4 est insuffisante : en effet, ce type de matériel autorise tous les paquets appartenant à une connexion préalablement acceptée, sans chercher à examiner l'information qu'ils contiennent. À cause de cela, ils restent inefficaces contre les attaques exploitant les vulnérabilités des protocoles de couche supérieure (HTTP, DNS, FTP, SMTP) ou d'une application, comme un navigateur Internet. Le cas de l'image JPEG piégée, exposé succinctement au chapitre 3, en est un exemple flagrant : il se peut très bien que vous autorisiez le protocole HTTP au niveau du pare-feu (c'est-à-dire les connexions sortantes sur le port 80). Seuls les paquets HTTP appartenant à une session que vous aurez initialisée avec un serveur distant seront donc acceptés. Seulement, si le pare-feu ne désosse pas suffisamment la trame IP jusqu'à analyser son contenu applicatif (c'est-à-dire la donnée transportée ici par le protocole HTTP), il sera incapable de détecter que l'image JPEG est piégée et le pirate prendra le contrôle de votre ordinateur à distance.

RENVOI « Ping de la mort », IP spoofing, vol de session

Reportez-vous à l'annexe B pour toutes les définitions des attaques citées dans le texte.

AVANCÉ Pare-feu de Windows

Lorsque vous définissez des connexions dans Windows, le système vous propose de les placer derrière son pare-feu (*Propriétés>Paramètres avancés>Protéger mon ordinateur et le réseau en limitant ou interdisant l'accès à cet ordinateur à partir d'Internet*). Ce pare-feu est considéré comme « à mémoire d'états » : seul le trafic de réponse est autorisé en entrée. Tout autre flux entrant est bloqué, sauf autorisation explicite dans l'onglet *Services*.

RENVOI Et Vista ?

Voir le chapitre 10 pour en apprendre davantage sur ce que proposera la nouvelle version de Windows en matière de pare-feu.

Pare-feux applicatifs

Pour que son action soit plus complète, un pare-feu doit offrir une protection applicative. Il doit idéalement :

- analyser le protocole applicatif et vérifier que son utilisation reste conforme aux standards ;
- analyser les éventuels protocoles de plus haut niveau encapsulés à l'intérieur des protocoles applicatifs ;
- analyser les données transportées par ces protocoles, appelées aussi le contenu applicatif ;
- déjouer les attaques avancées de type Cross Site Scripting (XSS), injection SQL, débordement de tampons, violation de répertoires (Directory traversal), etc.

Actuellement, certains pare-feux dits *stateful inspection* tendent à couvrir les niveaux élevés du modèle OSI ; c'est notamment le cas des pare-feux matériels. Ceux qui sont capables de pousser l'analyse jusqu'au niveau 7 sont dits « applicatifs ». Ils représentent actuellement d'excellents choix et devraient systématiquement être adoptés, tout au moins dans les entreprises.

RAPPEL Encapsulation de protocole

Le protocole HTTP, par exemple, sert à véhiculer les protocoles d'échange de poste à poste tels que Kazaa, utilisés parfois comme vecteurs de pénétration de logiciels espions sur votre poste. Pour plus de détails, voir au chapitre 4.

RENVOI CrossSite Scripting, injection SQL, violation de répertoires

Reportez-vous à l'annexe B pour toutes les définitions des attaques citées dans le texte.

Fonctionnement d'un pare-feu

La figure 5-1 montre de façon schématique la manière dont procède un pare-feu lorsqu'il reçoit un paquet. Il décortique la trame IP et vérifie couche par couche si les données de protocole, ou bien les contenus applicatifs, sont bien conformes à la politique de sécurité présente à l'intérieur de ce pare-feu.

Aux niveaux IP (couche 3 du modèle OSI) et TCP/UDP (couche 4), il s'assure par exemple que les adresses IP source et destination, ainsi que les numéros de port source et destination, correspondent bien aux valeurs autorisées par votre politique de filtrage. Si ce n'est pas le cas, le pare-feu bloque la trame.

S'il s'agit d'un pare-feu applicatif, il inspecte le contenu des couches protocolaires supérieures. Il vérifie notamment que les échanges n'enfreignent pas les règles d'utilisation du protocole, que l'usage de ce protocole est normal ; il ausculte la valeur des paramètres (pour prévenir des attaques de type débordement de tampons ou XSS), tente de détecter la présence de virus ou de toute sorte de code malveillant au niveau des contenus.

Si tous ces tests sont passés avec succès, le pare-feu transmet le paquet vers son destinataire.

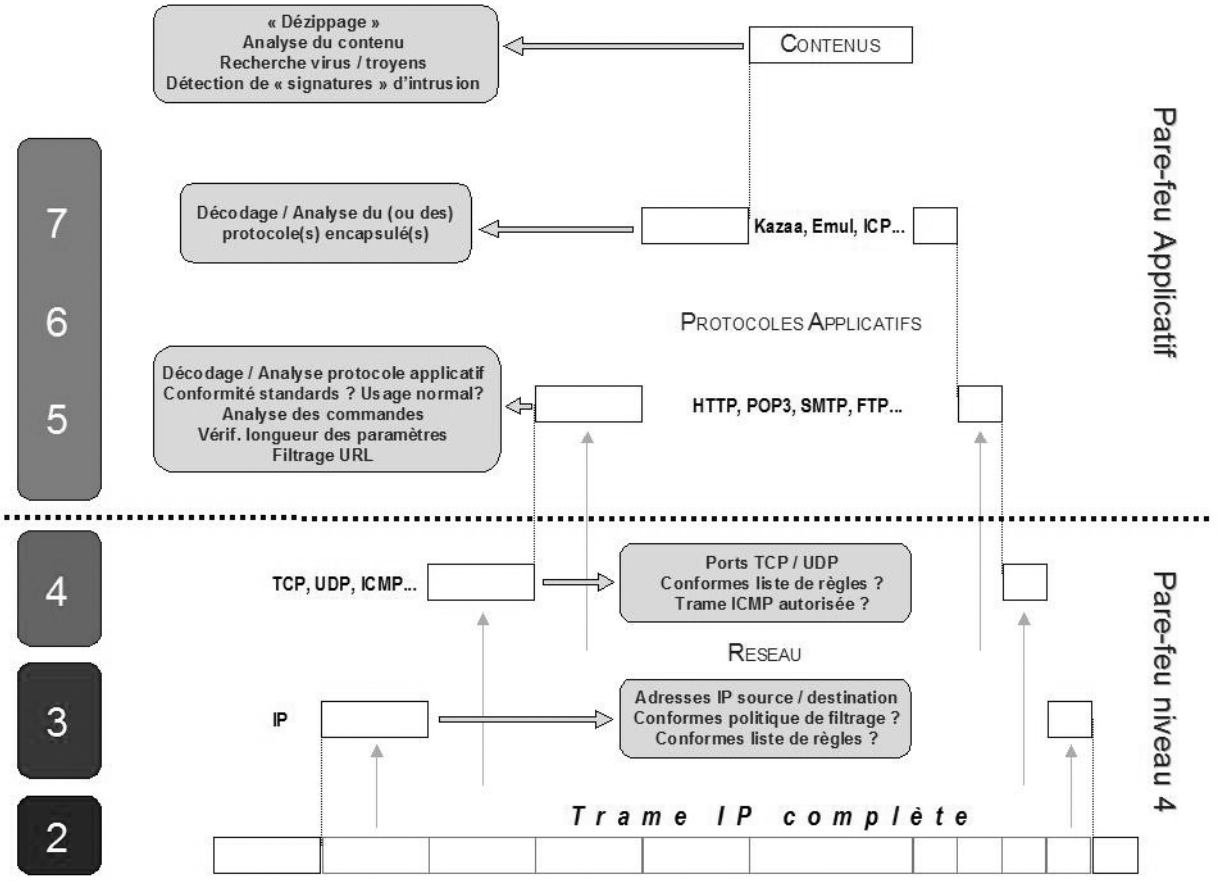


Figure 5–1 Schéma de principe simplifié du moteur de filtrage d'un pare-feu

Bien entendu, l'efficacité d'un pare-feu dépend de la richesse des traitements effectués au niveau de chaque couche. Certains pare-feux matériels savent mener des analyses sophistiquées sur les flux échangés entre les tiers communiquants, au point de reconnaître les « signatures » d'attaques lors des tentatives d'intrusion ; ils se comportent ainsi en véritables sondes de détection d'intrusions. D'autres analysent les contenus des protocoles HTTP (Web), FTP (transferts de fichiers), SMTP et POP3 (messagerie), et sont capables de filtrer les URL (adresses web de la forme http://www.serveur.com) sur la base d'une liste noire d'URL constamment remise à jour, de détecter la présence de pourriels (spam), de virus, de troyens et de logiciels espions. Dotés de filtres antispam et de logiciels antivirus, ils assurent ainsi une protection de haut niveau, couvrant un large spectre des redoutables attaques de niveau applicatif.

Limites des pare-feux

La Palice aurait pu le dire : un pare-feu est inefficace contre les attaques qu'il ne sait pas éviter. Encore une fois, gardez toujours à l'esprit que la présence d'un pare-feu ne garantit pas automatiquement la sécurité.

Si votre pare-feu filtre les protocoles jusqu'au niveau 4, vous serez protégé contre les attaques réseau, exploitant les vulnérabilités des protocoles IP, TCP ou UDP. En revanche, comme l'indique la figure 5-1, vous serez vulnérable à toutes les attaques dirigées contre les protocoles de plus haut niveau qui exploitent les vulnérabilités :

- des protocoles applicatifs, comme HTTP, HTTPS, DNS, SMTP, POP3, IMAP4... ;
- des logiciels de communication (Netscape, Internet Explorer, clients de messagerie) ;
- des protocoles applicatifs encapsulés, comme Kazaa, Gnutella, transportés à l'intérieur d'un protocole applicatif de plus bas niveau, comme HTTP.

Si vous utilisez un pare-feu applicatif, vous serez protégé contre les attaques applicatives les plus courantes parmi les cas précédemment cités, dans la mesure où votre installation dispose des modules d'analyse des protocoles en question. Ces pare-feux savent généralement ausculter les protocoles, voire certains contenus véhiculés par HTTP, SMTP, FTP ou DNS. Toutefois, les applications récentes ont recours à des protocoles de plus en plus complexes, que les pare-feux ne sauront probablement jamais analyser totalement. Si vous êtes un « téléchargeur » invétéré d'applications sur Internet, vous finirez tôt ou tard par installer une application reposant sur un protocole inconnu, ou mal maîtrisé par votre pare-feu, qui aura ainsi de grandes chances de laisser passer les attaques les plus redoutables. Prudence donc avant de télécharger n'importe quoi sur Internet !

Enfin, votre pare-feu ne saura pas vous protéger contre les innombrables attaques exploitant les vulnérabilités d'applications sans cesse renouvelées et publiées sur Internet. Elles donnent d'ailleurs souvent naissance à toutes sortes de virus, vers, chevaux de Troie ou logiciels espions. À ce titre, hormis quelques offres particulières disponibles actuellement sur le marché, aucun pare-feu ne peut aujourd'hui vous immuniser efficacement contre la menace virale.

Choisir un type de pare-feu

Il existe donc deux types de protection : le pare-feu logiciel, installé directement sur le poste de travail de l'utilisateur, et le pare-feu matériel, implanté dans un équipement dédié. Si la finalité de ces deux types reste la même, leurs rayons d'action diffèrent quelque peu :

DMZ (DeMilitarized Zone)

La zone démilitarisée, ou DMZ, est un réseau bénéficiant d'une ouverture plus large que votre réseau privé, et dans lequel vous installez les serveurs accessibles au public : serveur web ou de messagerie.

- Un pare-feu matériel est en général positionné en entrée de site, au niveau du point d'interface entre votre réseau privé et le réseau non sûr (un réseau local en lequel vous n'avez pas confiance, un réseau public comme Internet, etc.). De par sa situation, le pare-feu matériel peut très bien gérer plusieurs réseaux privés et appliquer des politiques de filtrage différentes sur chaque réseau : le cas le plus connu est celui de la DMZ

  Le pare-feu matériel est généralement doté de règles de filtrage puissantes, élaborées et flexibles, capables de résoudre la problématique complexe posée par des réseaux constitués de nombreux postes de travail, de serveurs, ou de sous-réseaux. Il s'intéresse exclusivement au trafic réseau échangé entre votre infrastructure et l'extérieur, et procède généralement à une inspection très approfondie des flux qui le traversent. Un pare-feu matériel renferme souvent des fonctions additionnelles comme des sondes de détection et de prévention d'intrusion (IDPS pour Intrusion Detection and Prevention System), des services de type VPN (Virtual Private Network) permettant l'établissement de liens chiffrés avec des postes nomades via Internet, ou des fonctions sécurisées d'administration et de contrôle à distance.
- Le pare-feu logiciel, quant à lui, met en œuvre des principes différents. Installé sur votre poste, il est conçu pour protéger une seule machine. Par conséquent, il n'hésite pas à faire appel à tous les moyens qui sont à sa disposition pour vous protéger. En premier lieu, il procède, comme son cousin le pare-feu matériel, à l'analyse des flux qui transitent entre votre poste et l'extérieur. Cependant, il se limite le plus souvent aux niveaux « réseau » et « transport » du modèle OSI (couches 3 et 4), ce qui offre déjà une protection utile. En revanche, tirant parti de leur localisation privilégiée, ces pare-feux ne se privent pas de contrôler aussi les agissements des applications situées sur votre poste, notamment celles qui tentent d'accéder à Internet. Cette fonction, qui ne peut être prise en compte par un pare-feu matériel, est ici vraiment salutaire, car elle permet de déjouer les actions malveillantes de programmes espions ou de toutes sortes de portes dérobées, installés furtivement par un pirate qui serait parvenu à infiltrer partiellement votre ordinateur. De plus, les pare-feux logiciels savent aussi détecter et bloquer certains virus ou logiciels espions.

Un pare-feu logiciel fournit donc une protection plus personnalisée qu'un pare-feu matériel, qui a vocation à protéger globalement une infrastructure plus importante. Toutefois, les mécanismes d'un pare-feu matériel sont généralement robustes.

Si votre installation se réduit à un seul poste connecté à Internet, un simple pare-feu logiciel devrait largement subvenir à vos besoins. Si, en revanche, vous disposez d'un réseau d'ordinateurs dédiés à un usage pro-

fessionnel, il est préférable d'avoir recours à un pare-feu matériel en entrée de site. De telles solutions ne sont pas toujours onéreuses : il existe à l'heure actuelle des produits très performants pour sécuriser des réseaux de moins de 25 postes, dont le coût s'élève à moins de 2 000 euros.

Bien entendu, l'utilisation d'un pare-feu matériel en entrée de site n'exclut pas d'installer des pare-feux logiciels sur les postes de travail. La combinaison des deux approches confère généralement un haut niveau de protection à votre installation.

Pare-feux logiciels disponibles gratuitement ou dans le commerce

Il existe actuellement plusieurs pare-feux logiciels sur le marché. Certains sont gratuits, comme Kerio et ZoneAlarm, d'autres sont payants. Ainsi que nous l'avons indiqué au chapitre 3, certains produits sont apparus sur le marché par le biais des grands éditeurs d'antivirus (ces produits sont disponibles sous forme de « suites logicielles »). D'autres en revanche, ont été clairement conçus à l'origine comme pare-feux.

Le tableau suivant identifie les pare-feux logiciels les plus utilisés. Cette liste vous est fournie à titre d'information pour vous donner des points de repère, mais elle n'est évidemment pas exhaustive.

Tableau 5–1 Liste des principaux pare-feux logiciels

Pare-feu	Suite logicielle	Éditeur	Payant/gratuit	Site web
BlackICE PC Protection	Non	Internet Security Systems	Payant	http://blackice.iss.net
F-Secure Internet Security	Oui	F-Secure	Payant	http://f-secure.fr/france
Internet securitysuite	Oui	McAfee	Payant	http://fr.mcafee.com
Kerio Personal Firewall	Non	Kerio	Gratuit pour un usage domestique, mais certaines fonctionnalités disparaissent après 30 jours	www.sunbelt-software.com/Kerio.cfm
Look n'Stop	Non	soft4Ever	Payant	www.looknstop.com/Fr/index2.htm
Norton Internet Security	Oui	Symantec	Payant	www.symantec.fr
Outpost Free	Non	Agnitum	Gratuit pour un usage domestique	www.agnitum.com/products/outpostfree/index.php
PC-cillin Internet Security	Oui	Trend Micro	Payant	http://fr.trendmicro-europe.com
Personal Security Suite	Oui	Kaspersky Lab	Payant	www.kaspersky.com/fr
Platinium Internet Security	Oui	Panda Software	Payant	www.pandasoftware.com/fr
ZoneAlarm Pro ZoneAlarm (version gratuite)	Non	Zone Labs	ZoneAlarm est gratuit pour un usage domestique	http://fr.zonelabs.com

Choisir un pare-feu logiciel

Le tableau précédent dresse une liste assez complète des produits disponibles à l'heure actuelle. Vous trouverez bien sûr d'autres solutions sur Internet, mais la liste proposée contient déjà quelques très bons produits.

Si vous disposez de l'antivirus d'un des éditeurs cités dans le tableau précédent, utiliser la suite logicielle correspondante présente des avantages incontestables : la simplicité, un coût optimisé et une intégration réduisant les risques d'incompatibilité entre les produits. Cependant, il faut rester prudent avec les suites logicielles, essentiellement bâties sur la notoriété du logiciel antivirus : le pare-feu n'est pas toujours à la hauteur de ce que l'on pourrait attendre.

Certains pare-feux personnels jouissent de toute évidence d'une excellente réputation. C'est le cas notamment de ZoneAlarm, dont la version Pro s'adresse plus particulièrement aux administrateurs de petits réseaux locaux. D'autres sont également bien cotés comme F-Secure, Look n'Stop, Outpost Free, ou Kerio Personal Firewall.

BONNE IDÉE

Tester avec un pare-feu logiciel gratuit

Une façon simple d'aborder le problème de la sécurité applicative consiste à installer et expérimenter, dans un premier temps, un pare-feu gratuit. Parmi les produits proposés dans le tableau 5-1, vous trouverez certainement votre bonheur.

Sécurité assurée par les fournisseurs d'accès

Étant donnée la position stratégique et peu enviable qu'ils occupent dans la chaîne du piratage, les hébergeurs et les fournisseurs d'accès à Internet (FAI) sont devenus, par la force des choses, des champions respectés de la lutte contre les chapeaux noirs. Afin de préserver l'intégrité et la disponibilité de vos données, de limiter les risques de contamination en cas d'attaque virale, ou d'assurer la disponibilité des serveurs malgré les attaques intempestives par déni de service, certains déploient des solutions complexes, diversifiées et performantes pour vous garantir un niveau de sécurité satisfaisant.

Les pare-feux (ou les fonctions de filtrage équivalentes) d'un fournisseur d'accès rompu au problème de la sécurité mettent donc en œuvre des politiques suffisamment fines pour bloquer la majorité des attaques, sachant qu'elles sont nombreuses et, parfois, sophistiquées. Il faut donc partir du principe que – hormis les problèmes de confidentialité – les ressources hébergées dans les locaux du fournisseur d'accès (par exemple votre serveur web, votre serveur de messagerie et toutes vos données publiquement accessibles) sont bien protégées des pirates.

Les FAI vont même jusqu'à vous proposer l'externalisation pure et simple de votre sécurité, à travers des services de pare-feux virtuels destinés à éliminer les trafics malveillants qui vous sont destinés, ainsi que des services d'antivirus.

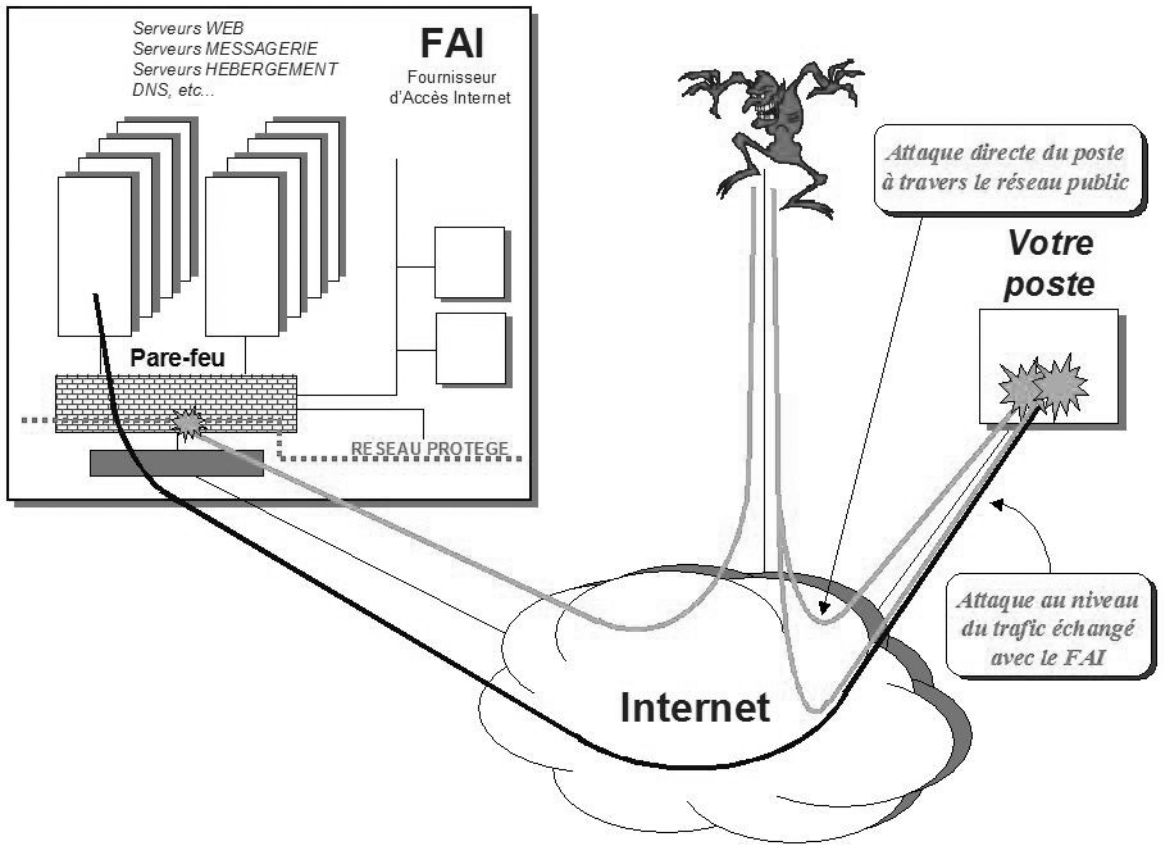


Figure 5–2 Attaques possibles en dépit de la protection offerte par les FAI

Cette approche est indéniablement intéressante, car une lutte efficace contre la menace informatique passe inévitablement par un faisceau de mesures, et toute forme de traitement en amont constitue un atout fort.

Toutefois, il ne faut pas oublier, comme le montre la figure 5-2, qu'entre votre fournisseur d'accès et vous se trouve un réseau public dont cet opérateur n'a pas plus la maîtrise que vous. Il se peut très bien qu'un pirate réussisse à s'immiscer dans vos communications, attaque votre poste, écoute ou altère le trafic échangé avec votre correspondant.

La protection offerte par votre fournisseur est donc une bonne chose. En complément toutefois, vous devez aussi prévoir de traiter sérieusement ce problème au niveau de votre installation, afin de bénéficier d'une sécurité optimale.

Configurer son pare-feu personnel

Installer un pare-feu logiciel

Installer un pare-feu logiciel sur votre ordinateur est une opération très simple : il suffit d'insérer dans votre lecteur le CD-Rom du produit que vous vous êtes procuré chez votre revendeur, ou de double-cliquer sur l'exécutable du logiciel que vous avez téléchargé sur Internet. L'assistant d'installation vous guide, mais vous n'avez pratiquement plus à intervenir.

PRÉCISION Pare-feu exemple

Cette partie du chapitre fait largement appel à l'interface utilisateur du produit ZoneAlarm Pro. Notre intention n'est pas de promouvoir ce produit ni de vous en présenter un manuel utilisateur ; d'autres pare-feux logiciels répondent aussi très bien à la problématique de la protection du poste, et la documentation de l'éditeur est bien plus complète. À travers les fonctions de ZoneAlarm Pro, l'objectif est de vous expliquer les principaux concepts mis en œuvre dans les pare-feux, afin que vous puissiez ensuite les appliquer vous-même sur votre produit.

Figure 5–3
Installation du pare-feu ZoneAlarm Pro

Si votre poste est déjà équipé d'un pare-feu actif, ce qui est le cas par défaut sur Windows XP, le mieux est de le désactiver avant de débuter l'installation, vous éviterez ainsi tout problème d'incompatibilité.

À la fin de la procédure d'installation, vous devrez probablement redémarrer votre ordinateur. Cette dernière opération effectuée, votre pare-feu fonctionne et protège déjà votre ordinateur, grâce notamment au paramétrage par défaut que l'éditeur a sélectionné pour vous.

Définir la politique de filtrage des flux d'information

Les meilleurs pare-feux logiciels offrent de riches possibilités de paramétrage et permettent ainsi de définir des politiques de filtrage relativement sophistiquées.

Avant d'entrer dans le vif du sujet, ayez à l'esprit que la tendance naturelle d'un pare-feu consiste à interdire tous les échanges : selon le principe simple que n'auraient pas désavoué les Shadocks, pour éviter l'intrusion via un système de communication, il suffit juste d'interdire les communications. C'est simple, efficace, un peu frustrant si vous souhaitez vous servir d'Internet, mais, au moins, vous êtes bien protégé.

Pour filtrer l'information, les pare-feux commencent donc par bloquer automatiquement tous les ports qui pourraient être inutilement ouverts sur votre ordinateur. Cela empêche donc toute possibilité de communiquer sur ces ports, et, par la même occasion, cela coupe l'herbe sous le pied du pirate désireux de se servir d'un port libre pour vous attaquer.

Tous les ports sont donc fermés, sauf, bien sûr, quelques uns. Vous ne laissez ouverts que les ports utiles aux communications que vous autorisez, explicitement ou implicitement.

BONNE PRATIQUE Ports ouverts implicitement

Attention aux autorisations accordées implicitement au niveau du pare-feu. Prenez le temps de vérifier périodiquement la configuration de celui-ci.

Il y a en général trois manières de définir ces exceptions dans un pare-feu :

- Configuration explicite du pare-feu – Vous précisez ainsi que telle ou telle application, par exemple votre client de messagerie instantanée, ou bien l'exécutable qui procède à la mise à jour de votre antivirus, a l'autorisation de se connecter à Internet. Sous cette condition, le pare-feu laissera l'application ouvrir le port qui lui est associé au moment où elle initiera elle-même une session avec le serveur distant ; le reste du temps, le pare-feu maintiendra ce port fermé. C'est ce que l'on appelle le filtrage d'applications.
- Modification par vous-même, si elles existent, des quelques règles génériques de filtrage prédéfinies dans le pare-feu – Ces règles affectent par exemple des protocoles de gestion, comme DNS, ICMP ou DHCP, ou d'autres protocoles fréquemment utilisés. En agissant sur elles, vous autorisez le pare-feu à accepter les connexions sortantes ou entrantes sur les ports associés aux protocoles concernés.
- Création de vos propres règles, que certains pare-feux désignent parfois sous le nom de règles « expertes » – Elles s'avèrent nécessaires pour répondre à des besoins spécifiques à votre installation (pour autoriser par exemple des flux d'administration uniquement sur certaines machines).

L'ensemble de ces règles constitue la politique de filtrage mise en œuvre à l'intérieur du pare-feu. Il faut être très rigoureux par rapport au contenu de ces règles, car elles pèsent fortement sur le niveau de sécurité atteint par votre installation. Si vous « ouvrez » exagérément les possibilités de communication au sein de votre pare-feu, vous serez fatalement moins protégé.

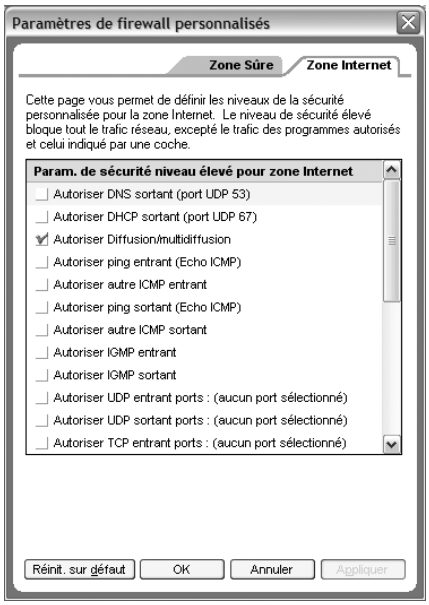


Figure 5–4 Règles de filtrage prédéfinies pour le niveau *Élevé* de ZoneAlarm Pro

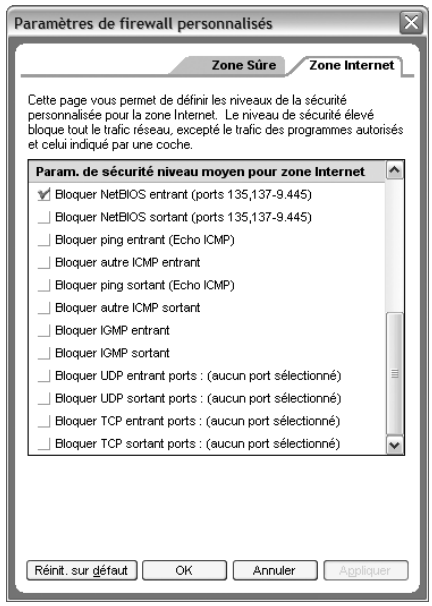


Figure 5–5 Règles de filtrage prédéfinies pour le niveau *Moyen* de ZoneAlarm Pro

Principales règles de filtrage protocolaire proposées par les pare-feux logiciels

Immédiatement après avoir installé votre pare-feu, vous bénéficiez généralement de l'ensemble des règles – restrictives – que l'éditeur a prédéfinies pour vous en usine, ce qui confère déjà à votre poste un bon niveau de protection. Cependant, vous serez assurément obligé d'affiner ce paramétrage, afin d'accroître ou de restreindre le filtrage. Vous adaptez ainsi vos autorisations de communiquer aux spécificités de votre installation et à vos besoins. Il faut pour cela se familiariser avec les principales règles de filtrage des protocoles.

Raisonnons sur un cas concret. Pour vous simplifier la vie, le pare-feu ZoneAlarm Pro a défini les concepts de zone Internet et de zone sûre (à ne pas confondre avec les zones Internet Explorer). La zone sûre regroupe tous les réseaux en lesquels vous avez confiance, par exemple votre réseau local ou votre réseau privé d'entreprise ; la zone Internet, comme son nom le suggère, concerne tout ce qui provient d'un réseau non sûr, en particulier le réseau Internet (à vous d'affecter aux zones adéquates les réseaux avec lesquels vous communiquez). Le pare-feu définit en outre une zone dite « bloquée », à l'intérieur de laquelle vous spécifiez les ordinateurs ou les réseaux avec lesquels vous souhaitez interdire toute communication. Étant donné que la configuration et le fonctionnement de cette dernière zone sont faciles à comprendre, nous nous focaliserons plutôt sur les deux premières.

Le principe consistant à tout interdire sauf ce que l'on autorise est bien sûr valable dans le cas de ZoneAlarm Pro. Avec un niveau de sécurité *Élevé*, tous les protocoles – donc tous les ports – sont bloqués, à l'exception :

- des ports explicitement autorisés lorsque vous cochez les cases affectées aux règles prédéfinies listées à la figure 5-4 ;
- des ports associés aux programmes qui disposent d'une autorisation pour chaque zone (le pare-feu doit être configuré de manière à ce que ce soit vous qui accordiez cette autorisation, dans tous les cas) ;
- des ports désignés explicitement à partir des règles expertes que vous définirez plus tard.

Avec un niveau de sécurité *Moyen*, notez que tous les protocoles – donc tous les ports – sont bloqués, à l'exception :

- des ports autorisés par défaut, listés à la figure 5-5, sauf si vous les bloquez vous-même en cochant les cases correspondantes (attention donc à cette ouverture !) ;
- des ports associés aux programmes qui disposent d'une autorisation pour chaque zone ;
- des ports désignés explicitement à partir des règles expertes que vous définirez plus tard.

COMPRENDRE Rôle des principaux protocoles

Afin de vous aider à préciser quels sont les protocoles que vous devez autoriser et ceux qu'il faut bloquer, nous allons brièvement rappeler le rôle qu'ils jouent dans votre installation.

- **DNS (Domain Name Service, port UDP 53)** – Votre ordinateur aura besoin de lancer des requêtes DNS vers un serveur de noms, pour trouver par exemple l'adresse IP d'un serveur désigné par son nom, comme smtp.free.fr ou download.windowsupdate.com. Ce dialogue peut avoir lieu sur votre réseau local, si votre ordinateur s'adresse à un serveur DNS local, et si ce serveur dispose réellement de cette information, ou sur Internet, par exemple avec le serveur DNS de votre fournisseur d'accès. Il faut généralement que vous puissiez accéder au(x) serveur(s) DNS (primaire et secondaire) de votre fournisseur d'accès. Pour cela, vous avez la possibilité de cocher la case *Autoriser DNS sortant* (voir figure 5-4), ou de définir une règle experte (voir plus loin), autorisant le port UDP 53 sortant uniquement avec les deux serveurs de votre FAI, identifiés explicitement par leur adresse IP. Cette règle est plus restrictive que la première.
- **DHCP (Dynamic Host Configuration Protocol)** – Si l'adresse IP de votre ordinateur n'est pas fixe, elle lui est attribuée dynamiquement par un serveur dit « DHCP » au moment de la mise sous tension ou au moment de la connexion avec Internet. Si le serveur DHCP est situé au delà du pare-feu, il faut autoriser ce protocole sinon votre ordinateur ne pourra recevoir son adresse IP. Si le serveur DHCP se trouve en amont du pare-feu, ou si l'adresse IP de votre poste est fixe, il n'y a aucune raison d'autoriser ce protocole.
- **ICMP (Internet Control Message Protocol)** – C'est le puissant – et dangereux – protocole de gestion des réseaux IP (voir chapitre 4). Il peut être utile à votre opérateur ou à votre administrateur système pour effectuer des opérations de contrôle sur le fonctionnement du réseau, mais il n'est pas absolument indispensable au fonctionnement de votre ordinateur. La question du filtrage ICMP sera traitée plus loin.
- **NetBIOS** – Comme nous l'avons vu au chapitre 4, NetBIOS est utilisé lorsque, à travers le réseau, vous établissez des connexions directes à des ressources partagées (un partage situé sur un serveur raccordé au réseau local, l'accès à une imprimante, etc.). Malheureusement, ce protocole recèle de grandes faiblesses : il permet à un pirate d'établir, entre autres, une connexion sans authentification avec un partage masqué de votre machine (comme IPC$) et de recueillir des informations précieuses, comme la liste des utilisateurs, les caractéristiques de votre domaine, etc. L'établissement d'une session NetBIOS et l'utilisation des services sous-jacents (comme SMB – Server Message Block) représentent pour les pirates un moyen formidable – et simple de surcroît – de s'introduire au cœur de votre système. Vous pouvez donc autoriser les ports associés au protocole NetBIOS (ports UDP 137 NetBIOS Name Service, TCP 139 NetBIOS Session Service, ou 445 service SMB directement sur TCP/IP) sur votre réseau local, mais vous devez impérativement les interdire lors de toute communication avec des réseaux non sûrs.
- **IGMP (Internet Group Management Protocol)** – Internet définit le concept de groupe de diffusion, un service qui permet la création momentanée de groupes restreints de machines à travers les réseaux IP. À la manière des groupes fermés d'abonnés, l'objectif principal des groupes de diffusion est d'offrir un espace privilégié de communication entre ses membres, afin par exemple de faciliter les interactions ou les travaux en coopération. Le rôle du protocole IGMP est de gérer les communications au sein des groupes de diffusion. Il est chargé notamment de l'affectation des adresses IP *multicast* qui acheminent les émissions multipoints vers l'ensemble des participants, et de la gestion dynamique des groupes, ce qui permet aux utilisateurs de joindre ou de quitter à tout moment le groupe de diffusion. Si vous n'avez pas particulièrement besoin de ce service, il est recommandé de le bloquer au niveau du pare-feu.
- **TCP (Transport Control Protocol)** et **UDP (User Datagram Protocol)** – Ces règles vous permettent de définir des politiques de filtrage précises par rapport aux protocoles les plus répandus.

En règle générale, il est chaudement recommandé d'affecter un niveau de sécurité *Élevé* à la zone Internet et de rester prudent si vous ouvrez d'autres ports sur cette zone. Selon votre environnement, vous pourrez affecter le niveau de sécurité *Moyen* à la zone sûre, car, en principe, vous la maîtrisez, mais surtout n'hésitez jamais à bloquer les protocoles dont vous ne vous servez pas. Avec ZoneAlarm Pro, vous accédez à ces réglages à partir de l'onglet *Firewall*, comme cela est visualisé à la figure 5-6 (onglet *Pare-feu* dans la version gratuite).

Notez au passage (figure 5-6) qu'un pare-feu peut rendre votre machine « invisible » aux autres ordinateurs. Les pare-feux sont en effet programmés pour ignorer certaines séquences de trames IP, caractéristiques d'une tentative de recensement ou d'intrusion sur votre machine. Certains vont même jusqu'à renvoyer des informations factices et incohé-

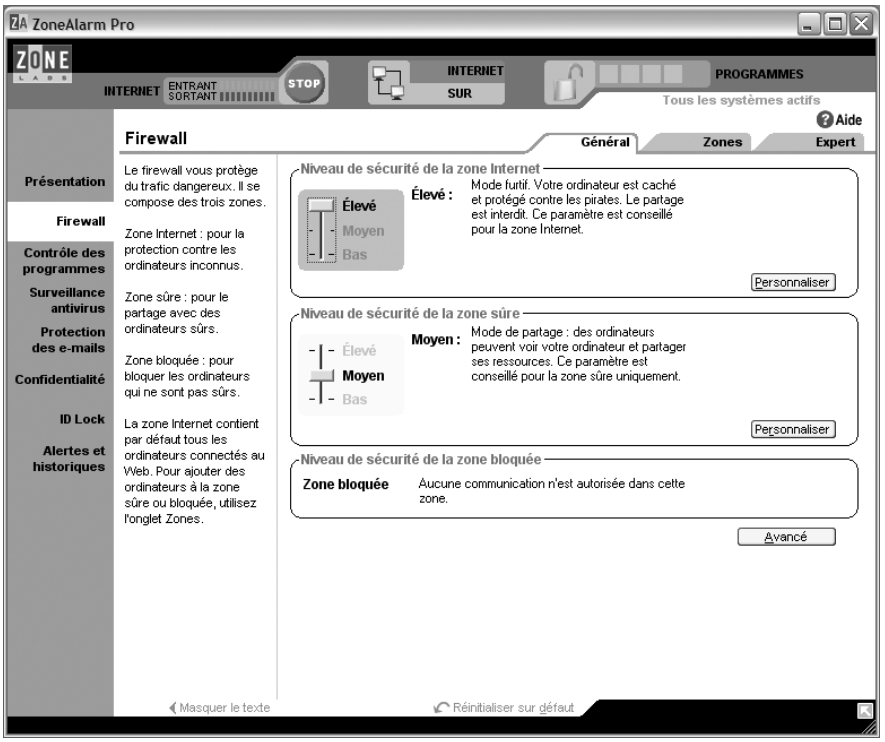


Figure 5–6
Fenêtre de contrôle du trafic entrant et sortant

rentes, afin de déconcerter l'attaquant averti, pour lequel un silence trop pesant est le signe de la présence d'un poste maladroitement protégé. Quels farceurs ces pare-feux ! Cette fonction est réellement salutaire et vous évitera à coup sûr de nombreuses attaques.

Filtrage du trafic ICMP

Nous avons établi au chapitre précédent que de nombreuses techniques de sondage et d'intrusion avaient recours au protocole ICMP. Si vous laissez les trames ICMP franchir la frontière de votre installation, vous ouvrez potentiellement la porte à plusieurs attaques dangereuses.

Dans le cadre d'un environnement peu sûr, comme celui d'Internet, il est impératif de limiter au maximum le trafic ICMP. Si vous êtes un particulier, optez pour un blocage systématique du protocole ICMP au niveau de votre pare-feu. C'est notamment grâce à des restrictions de ce genre que vous deviendrez invisible de l'extérieur.

En principe, le même raisonnement s'applique si vous êtes dans une entreprise. Cependant, pour des questions d'administration de réseau, vous serez peut-être contraint de laisser passer certains types de trafic ICMP. Il vous appartient de déterminer les trames ICMP qu'il convient

FONCTIONNALITÉ
Définition de règles personnelles

La possibilité de définir ses propres règles de filtrage est une fonction indispensable à tout pare-feu digne de ce nom.

d'autoriser (cette identification sort du cadre de cet ouvrage) et, surtout, d'en limiter la portée, c'est-à-dire le nombre de postes autorisés à recevoir et à émettre ces trames. Une approche minimaliste consiste, par exemple, à autoriser uniquement les paquets ICMP ECHO, REPLY, HOST UNREACHABLE et TIME EXCEEDED dans la zone DMZ du réseau, et à restreindre ce trafic aux adresses IP de votre fournisseur d'accès.

Dans le cadre d'un environnement plus sûr, un réseau local par exemple, vous pouvez adopter une politique moins restrictive. Cependant, n'oubliez pas que la menace vient souvent de l'intérieur. Si vous n'avez pas particulièrement besoin d'ICMP, n'hésitez pas à bloquer complètement ce protocole.

Politique de filtrage des protocoles du Web et de la messagerie

Sur certains pare-feux, la politique de filtrage des protocoles HTTP, HTTPS pour le Web, SMTP, POP3, IMAP4 pour la messagerie, est implicite lorsque vous attribuez les autorisations des applications qui les utilisent.

Par exemple, si Netscape dispose de l'autorisation d'accès à Internet, votre pare-feu autorisera les protocoles HTTP et HTTPS en sortie. De même, si vous utilisez Outlook Express, Exchange ou d'autres clients de messagerie, votre pare-feu autorisera les protocoles SMTP et POP3.

Si votre pare-feu ne contrôle pas automatiquement les ouvertures de ports en fonction des autorisations accordées à vos programmes, vous serez obligé d'établir vous-même les règles de filtrage par rapport à ces protocoles. Pour utiliser les services de navigation sur le Web et les services de messagerie, vous devez donc spécifier à votre pare-feu d'ouvrir en sortie les ports TCP 80 (HTTP), 443 (HTTPS), 25 (SMTP) et 110 (POP3).

ATTENTION Évitez d'autoriser les connexions entrantes

Vous ne devez autoriser les connexions entrantes qu'avec beaucoup de prudence. Même si cela semble évident, on peut se faire piéger facilement. Le cas se présente notamment lorsque vous recevez une alerte pointant du doigt un programme qui tente d'agir en tant que serveur (figure 5-7) : si vous acceptez, le port associé à ce programme passera en veille, en attente d'une connexion entrante. Ce choix est dangereux, car les pirates peuvent ainsi ouvrir une connexion sur votre poste en se faisant passer pour une entité autorisée, entrer dans votre machine à l'aide d'une porte dérobée, ou exploiter les bogues éventuels du programme, ce qui conduit bien souvent à la prise de contrôle de votre ordinateur à distance. Les chevaux de Troie sont un cas typique de programmes agissant en tant que serveurs sur votre machine.

JARGON Autoriser un port en sortie

Lorsque vous autorisez un port en sortie, cela veut dire que l'ordinateur a le droit d'initialiser la connexion, et que les informations circuleront ensuite dans les deux sens, sans être filtrées par le pare-feu (sauf, bien sûr, s'il s'agit d'un pare-feu applicatif et que l'analyse des protocoles de plus haut niveau révèle une anomalie). Cela signifie notamment qu'une entité extérieure ne peut avoir l'initiative de la connexion sur ce port. Ceci est une protection importante.

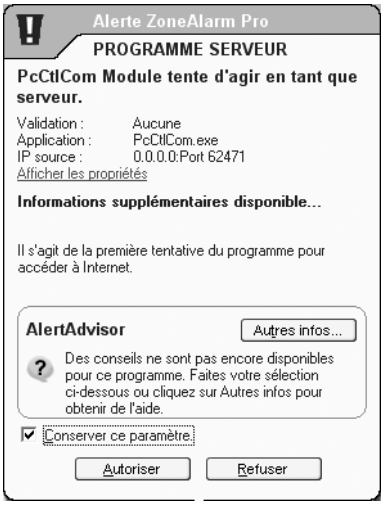


Figure 5–7 Attention à ne pas autoriser les programmes serveur à la légère

B.A.-BA

Règles comportementales de bon sens

Éviter la catastrophe découle inévitablement d'un faisceau de mesures appropriées, parmi lesquelles figurent l'utilisation d'un bon pare-feu et d'un bon antivirus à jour, le paramétrage optimal de vos navigateurs, l'utilisation de logiciels tueurs de spywares, et quelques règles comportementales de bon sens.

Sans vouloir faire de morale, sachez que fréquenter assidûment les sites pornographiques, de pédophilie ou d'échange massif de logiciels et de fichiers piratés, est proprement suicidaire en ce qui concerne la sécurité !

En règle générale, vous ne devez jamais oublier qu'autoriser des services tels que HTTP au niveau d'un pare-feu équivaut parfois à l'ouverture d'une belle autoroute pour pirates initiés aux techniques sophistiquées : il existe des dizaines d'attaques véhiculées à l'intérieur d'un contenu HTTP, capables de mettre votre système à genoux. A fortiori, toutes ces attaques ne sont pas forcément détectées par tous les pare-feux ou antivirus.

Il existe bien entendu des parades pour limiter ce problème. Les entreprises ont toujours le loisir de faire appel à la technologie de « proxy » (relais), présente plus particulièrement au sein des pare-feux matériels. Une session web ou messagerie avec un serveur distant est scindée en deux communications distinctes : l'une entre le client et le proxy, l'autre entre le proxy et le serveur. Ce type d'architecture complique sérieusement les techniques mises en œuvre pour réussir une attaque. En ce qui concerne les pare-feux logiciels, le problème est plus délicat car, d'une part, ils sont plus vulnérables à cette menace que les pare-feux matériels, surtout les pare-feux applicatifs, et, d'autre part, ils sont situés directement sur votre poste : si le pirate réussit à tromper le pare-feu, il se retrouve sur votre système.

Politique de filtrage des ports TCP et UDP

La tentation est grande d'ouvrir des ports supplémentaires. Vous installez des jeux en réseau, des clients qui vous donnent accès à travers Internet à toutes sortes de contenus passionnants, les logiciels de gestion et de contrôle à distance, comme Citrix ICA, Windows Terminal Server, Timbuktu ou pcAnywhere, etc. Attention, n'oubliez jamais qu'un port ouvert offre à l'attaquant un excellent moyen de contrôler votre ordinateur.

CONSEIL **N'ouvrez pas de ports supplémentaires**

Gardez à l'esprit qu'en autorisant un port vous ouvrez un nouveau canal, qu'un pirate utilisera tôt ou tard pour transmettre, à travers votre pare-feu, un flux qui trompera le protocole correspondant et qui lui permettra d'attaquer votre système. Il est fortement recommandé de ne spécifier aucun port supplémentaire à ce niveau.

Si vous y tenez absolument, vous avez la possibilité d'autoriser d'autres connexions, entrantes ou sortantes, sur des ports TCP ou UDP bloqués par défaut par votre pare-feu. La figure 5-8 vous montre comment procéder dans le cas de ZoneAlarm Pro.

La figure 5-8 illustre la meilleure politique de filtrage de ports TCP et UDP sur Internet (aucun port supplémentaire n'est autorisé). Bien sûr, la réalité peut être différente, mais sachez que tout écart par rapport à cette ligne directrice diminue votre niveau de protection.

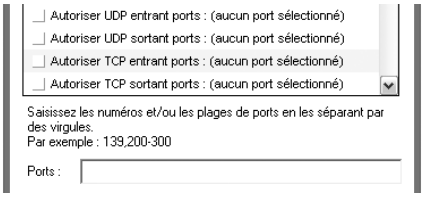


Figure 5–8 Politique de filtrage des ports TCP et UDP

Filtrer les applications avec un pare-feu

Les pare-feux logiciels savent contrôler les accès des applications et programmes situés sur votre poste.

Avec un pare-feu comme ZoneAlarm, vous n'avez pas grand-chose à faire pour définir la politique de filtrage de ces applications : elle s'échafaude par apprentissage, le pare-feu vous demandant votre avis à chaque fois qu'il détecte une tentative de connexion vers un réseau de la zone Internet ou de la zone sûre. La figure 5-9 vous montre l'exemple d'une application désireuse de se connecter à Internet. Vous constatez de visu que la décision d'autoriser ou non telle ou telle application n'est pas toujours difficile à prendre.

Concrètement, vous interviendrez fréquemment après avoir installé votre pare-feu, mais à mesure que vous accorderez vos autorisations ou imposerez vos refus, la matrice de contrôle des programmes se construira peu à peu et votre pare-feu deviendra de plus en plus autonome.

Si vous cliquez sur *Contrôle des programmes* avec ZoneAlarm Pro, vous pouvez visualiser la matrice des droits alloués à chaque programme, pour chaque zone (figure 5-10). Vous décidez ainsi des autorisations dont ils disposent (*autoriser*, *bloquer*, *demander*), par rapport aux droits d'accéder à la zone Internet, d'accéder à la zone sûre, au fait d'agir en tant que serveur, ou à la capacité d'envoyer du courrier électronique.

Figure 5–9 Le filtrage des applications avec ZoneAlarm se fait par apprentissage.

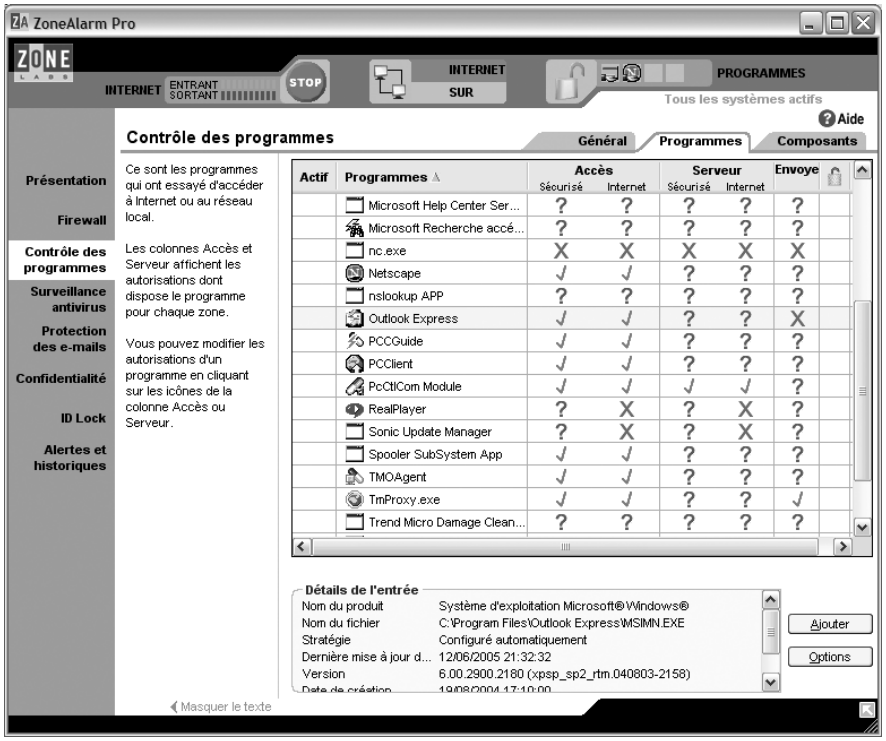


Figure 5–10
Filtrage des programmes

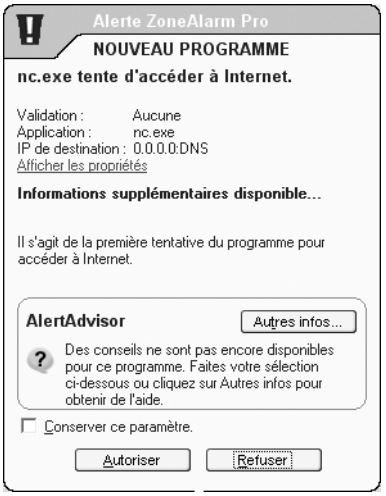


Figure 5–11 Un programme tente d'accéder à Internet à votre insu.

Vous avez bien entendu la possibilité de modifier manuellement ce paramétrage. Cette fonction est particulièrement importante car elle permet de déjouer l'action de nombreux programmes malveillants qui, comptant sur une mauvaise configuration du pare-feu, initient des opérations d'intrusion à partir de votre poste.

Jetons un rapide coup d'œil à la figure 5-11. Un tel message n'est pas très explicite, car tout le monde n'est pas censé connaître le programme `nc.exe`. Cependant, si vous effectuez une recherche rapide sur Internet, vous vous rendrez vite compte que le programme `netcat` n'est autre que l'un des plus beaux couteaux suisses de l'intrusion de réseaux jamais écrits en la matière. Le message de la figure 5-11 signifie que votre poste a déjà été sérieusement infiltré, que `netcat` tente d'ouvrir un ou plusieurs ports afin de permettre au pirate distant d'entrer au cœur de votre système, et que le coup de grâce final n'est plus très loin.

Voici donc, en flagrant délit, un cheval de Troie qui tente d'accéder à Internet, et qui montre à quel point le contrôle des programmes sur votre machine est une fonction importante. Cette dernière constitue d'ailleurs une excellente parade contre les chevaux de Troie et les logiciels espions, comme Bagle.BJ (voir chapitre 3), qui établissent leur quartier général au sein de votre système et lancent ensuite les opérations offensives à partir de celui-ci. Cet exemple illustre au passage de quelle manière les pare-feux et les programmes antivirus sont complémentaires.

Dans le cas présent, il faut évidemment cliquer sur *Refuser* après avoir coché la case *Conserver ce paramètre*, et vous dépêcher de supprimer ce petit exécutable aux bras longs.

Certains pare-feux vous permettent en outre d'effectuer un réglage plus fin des paramètres de chaque programme. Avec ZoneAlarm Pro, si vous cliquez sur le bouton *Options* (en bas à droite de la fenêtre visualisée à la figure 5-10), vous aurez la possibilité de spécifier des permissions supplémentaires par rapport à ce programme (voir figure 5-12), notamment décider s'il peut ou non utiliser d'autres programmes pour accéder à Internet.

Par ailleurs, notez que vous avez la possibilité de définir des règles spécifiques supplémentaires, dites règles « expertes », pour chaque programme. Nous aborderons cet aspect un peu plus loin.

Prenez garde toutefois à ne pas vous laisser abuser par votre pare-feu : dans un souci de convivialité, cet outil complexe prend parfois des décisions à votre place. Illustrons notre propos à l'aide de la configuration du pare-feu PC-cillin présentée à la figure 5-13. En parcourant la liste des exceptions, vous constatez que le pare-feu autorise les connexions entrantes sur l'application Windows Messenger. À la lecture de ce qui précède, cette

CONSEIL Utilisation de programmes tiers pour accéder à Internet

Vous pouvez décider si un programme (Netscape sur la figure 5-12) a ou non le droit d'utiliser d'autres programmes pour accéder à Internet. À l'exception de ceux que vous connaissez et en lesquels vous avez confiance, mieux vaut ne pas cocher cette option ; cela vous évitera les désagréments causés par le programme inconnu qui accède à Internet à l'aide de programmes de confiance.

Figure 5–12
Options de sécurité supplémentaires attribuées à chaque programme

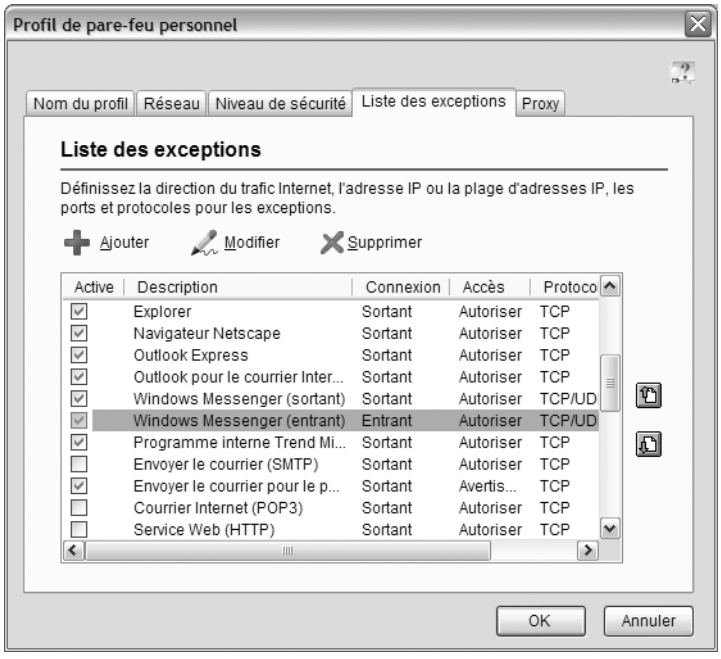


Figure 5–13
Exemple d'une configuration potentiellement dangereuse

simple indication « entrante » devrait maintenant systématiquement vous alerter. Windows Messenger est une messagerie instantanée qui permet de

ATTENTION **Usurpations d'identité sur MSN**

Sachez que toutes les communications MSN passent en clair, sont très facilement interceptables, et que les usurpations d'identité ne sont pas rares... De plus, MSN est un vecteur d'infiltration très prisé par les pirates désireux de transformer votre PC en « PC Zombie » (PC passé sous la domination d'un pirate ou d'une organisation criminelle, utilisé à votre insu dans les grandes attaques par déni de service). Pour plus de confidentialité, la messagerie instantanée de Skype offre des services de chiffrement (attention toutefois, le code de Skype est lui-même fortement obscurci et personne n'a encore réussi à analyser son contenu. Donc à ne pas utiliser pour échanger des informations sensibles).

faire des choses merveilleuses en matière de communication : vous échangez des données textuelles, audio ou vidéo avec d'autres personnes, vous établissez des conversations vocales avec vos correspondants, vous pouvez même les laisser accéder à vos programmes à distance !

Si vous cliquez sur le bouton *Modifier*, vous découvrez l'étendue de cette brèche (figure 5-14).

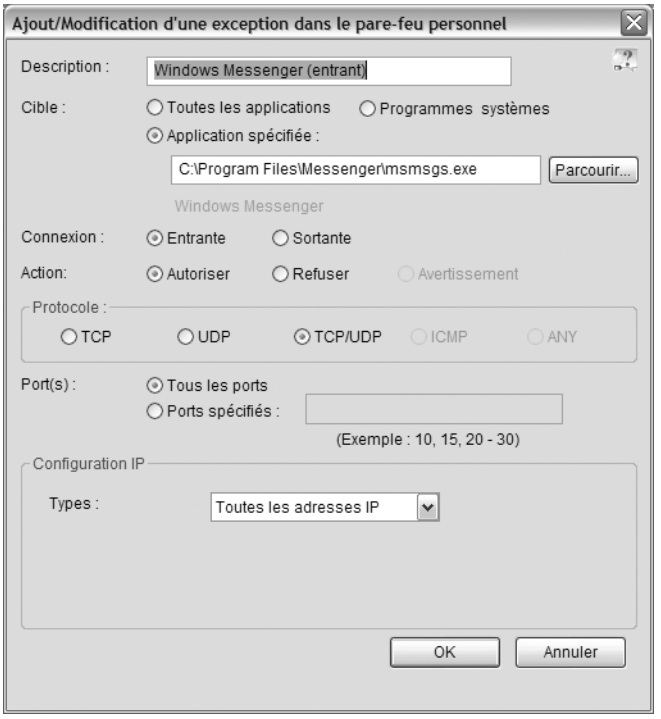


Figure 5–14
Filtrage des programmes

Dans la configuration actuelle du pare-feu, vous autorisez n'importe qui sur Internet (toutes les adresses IP) à ouvrir sur votre poste une session Windows Messenger (ou une session qui ressemble à une session Windows Messenger, mais qui n'en est pas une), sans restriction particulière quant au numéro de port. Fichtre ! Si vous n'utilisez pas Windows Messenger, mieux vaut interdire cette exception.

BONNE PRATIQUE **Vérifiez la configuration de votre pare-feu**

Certaines erreurs conduisent à d'énormes trous de sécurité. De façon générale, prenez périodiquement le temps d'inspecter la configuration de votre pare-feu et de vérifier si la politique de filtrage en vigueur est bien en accord avec ce que vous attendez.

Traduction d'adresses

La notion de traduction d'adresses est un tour de passe-passe inventé à l'origine pour résoudre le problème de la pénurie d'adresses IP, mais dont les conséquences inattendues nous rendent de fiers services en terme de protection.

En effet, le nombre d'adresses IP disponibles est très important (2^{32}, c'est-à-dire plus de 4 milliards), mais il n'est pas infini. Compte tenu de l'explosion d'Internet et de l'augmentation exponentielle du nombre d'ordinateurs dans le monde, nous tendons, à l'heure actuelle, vers la saturation. Il a donc fallu trouver des moyens pour remédier à ce problème.

L'une des solutions proposées, la traduction d'adresses (ou NAT pour Network Address Translation), repose sur un constat d'une simplicité déconcertante : pour accéder à Internet et échanger des messages avec n'importe quel ordinateur de la planète, tout le monde n'a pas forcément besoin d'une adresse IP connue publiquement. Par exemple, l'intranet d'une entreprise, ou votre réseau domestique à la maison, peut très bien se contenter d'utiliser des adresses IP privées, ignorées par les routeurs publics.

Dans ce cas, comment échanger des messages via Internet, si l'adresse de votre poste est inconnue du fournisseur d'accès ou des routeurs de l'opérateur télécoms ? La réponse est très simple : il suffit qu'un seul de vos équipements, par exemple votre routeur assurant l'interface avec le réseau public, dispose d'une adresse IP « publique », attribuée officiellement par le fournisseur d'accès, selon son propre plan d'adressage. Supposons que le FAI vous attribue l'unique adresse *213.228.60.166* (voir figure 5-15). Vous attribuez cette adresse au routeur d'interface jouant le rôle de passerelle. Cette adresse est tout à fait officielle, elle est unique, reconnue de tous les routeurs du monde entier, et si un ordinateur envoie un message IP à cette adresse, votre passerelle le recevra.

Supposons maintenant que vous ayez plusieurs ordinateurs à la maison (*Rachmaninoff*, *Liszt*, *Brahms*), tous connectés via un réseau Ethernet. Comment relier tous vos ordinateurs à Internet en même temps et leur permettre d'échanger de l'information ? Il suffit de distribuer des adresses IP uniques à tous vos ordinateurs, dans une plage d'adresses privées « non routables », par exemple *192.168.y.z*.

C'est ici que l'astuce de la traduction d'adresses intervient. Supposons par exemple que l'ordinateur *Rachmaninoff*, dont l'adresse non routable est *192.168.0.4*, souhaite interroger un serveur web situé à l'adresse *212.27.32.5* sur Internet. Le message IP, qui contient les deux adresses *192.168.0.4* (source) et *212.27.32.5* (destination), va bien entendu transiter par la passerelle, puisque c'est le seul chemin qu'il puisse emprunter. La passerelle reçoit le message, l'analyse pour déterminer ce qu'il faut en

JARGON NAT

L'acronyme NAT, pour Network Address Translation, se traduit par « Traduction d'adresse réseau ». Toutefois, par abus de langage, vous trouverez également l'anglicisme « Translation d'adresse réseau ».

Adresses non routables

Certaines adresses sont dites non routables car tous les routeurs publics sont programmés pour les ignorer. En revanche, votre routeur privé sait parfaitement les gérer en local, et les ordinateurs situés sur votre réseau domestique peuvent tous se « voir » les uns les autres.

Les adresses non routables sont les suivantes :

- 10.x.x.x (réseau de classe A) ;
- 172.16.x.x (réseau de classe B) ;
- 192.168.x.x (réseau de classe C).

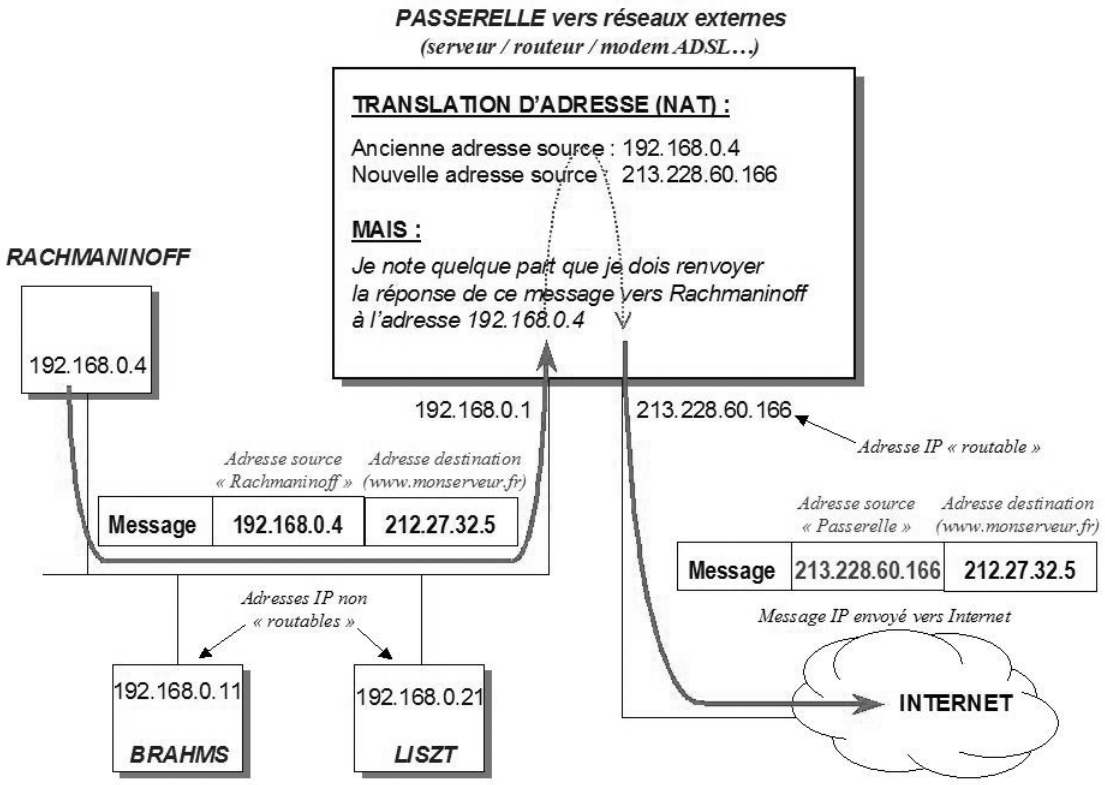


Figure 5–15 Principe de la traduction d'adresse

faire et comprend que le poste `Rachmaninoff` est invisible du réseau extérieur. Elle établit alors la connexion en son nom ; pour ce faire, elle modifie le champ d'adresse IP source du message en y incorporant sa propre adresse IP routable `213.228.60.166`, et ouvre elle-même la session avec le serveur web. Évidemment, elle note intérieurement que les messages IP en provenance de ce serveur sont en fait destinés à `Rachmaninoff` et s'apprête donc à effectuer le même tour de passe-passe dans l'autre sens. La passerelle routable agit comme une sorte de « relais » en transmettant la requête de l'ordinateur non routable à ce serveur et en passant les messages dans un sens et dans l'autre. Le serveur distant ne sait pas que le véritable client se trouve à l'adresse non routable `192.168.0.4` ; en ce qui le concerne, il communique avec `213.228.60.166`.

Quel est l'intérêt d'une telle complication ? Tout d'abord, les opérateurs et les particuliers ou les entreprises y voient un intérêt mutuel. Grâce à cette petite astuce, vous pouvez installer votre propre réseau privé avec

autant d'ordinateurs que vous voulez, tout en ne « consommant » qu'une seule adresse IP officielle. Cela évite à l'opérateur de gâcher ces précieuses adresses IP, et pour vous le coût est bien moindre.

Toutefois, vous gagnez surtout (et c'était plus inattendu !) en sécurité. Imaginez qu'un pirate décide de vous attaquer. Avant de passer à l'action, tout pirate qui se respecte commence par établir une cartographie précise de votre réseau, c'est-à-dire la liste des ordinateurs connectés (identifiables par leurs adresses IP), les ports ouverts, les services actifs, etc. Les techniques employées pour obtenir ces informations mettent généralement en jeu un dialogue direct entre le poste de l'attaquant et les postes attaqués, d'où la nécessité pour le pirate de disposer de l'adresse IP de ces derniers. Supposons, par exemple, qu'il espionne vos échanges pour déterminer ces adresses. La figure 5-16 vous montre l'exemple d'une interception de votre trafic par ce pirate. Que constatez-vous ? L'adresse source de tous les messages n'est autre que l'adresse NAT de la passerelle ; aucune adresse IP de votre réseau interne n'est divulguée sur Internet !

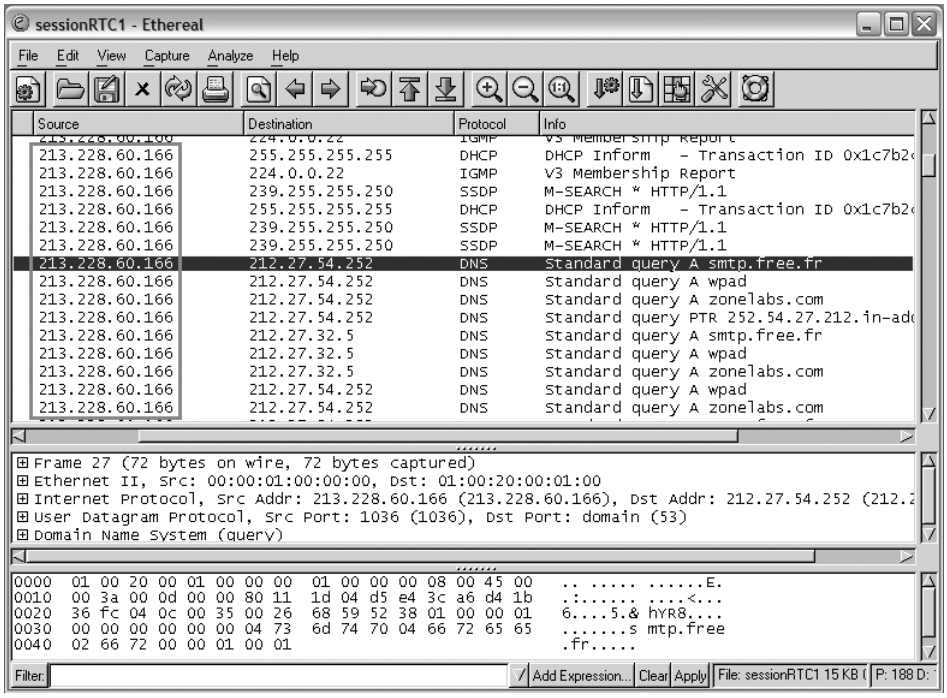


Figure 5–16
Exemple d'une interception

C'est ce qui s'appelle faire une bonne farce au pirate. Nanti de cette information, il pourra toujours utiliser tous les outils d'intrusion dont il dispose, il aura peut-être une chance de malmener un peu votre modem ADSL, mais aller plus loin est une autre paire de manches. Bel effort !

Bien entendu, vis-à-vis des problèmes de sécurité, la traduction d'adresses n'est pas un mécanisme d'une fiabilité à toute épreuve. Il reste contournable, mais attaquer un réseau protégé par une fonction NAT fait appel à un savoir-faire nettement supérieur.

Aussi, si votre modem câble, votre modem ADSL, votre routeur, votre pare-feu ou le serveur agissant à titre de passerelle sur votre réseau, dispose d'une fonction de traduction d'adresses, n'hésitez surtout pas à l'activer. Vous découragerez tous les pirates en herbe, ce qui veut dire, par expérience, presque toutes les attaques.

Créer ses propres règles de filtrage

Il se peut, c'est même d'ailleurs fréquent, que les règles génériques proposées par les pare-feux ne suffisent pas pour couvrir tous les cas de figure que vous allez rencontrer. Votre installation comporte inévitablement des spécificités dont vous souhaiterez tirer parti. Vous pouvez également chercher à affiner votre politique de filtrage afin de répondre à des exigences précises. Vous aurez par exemple besoin d'autoriser certains flux entre des machines clairement identifiées de votre réseau local, sans que les autres puissent prendre part aux échanges. Vous souhaiterez peut-être également adopter une politique restrictive vis-à-vis d'Internet tout en autorisant des sessions sur certains protocoles avec des serveurs bien définis.

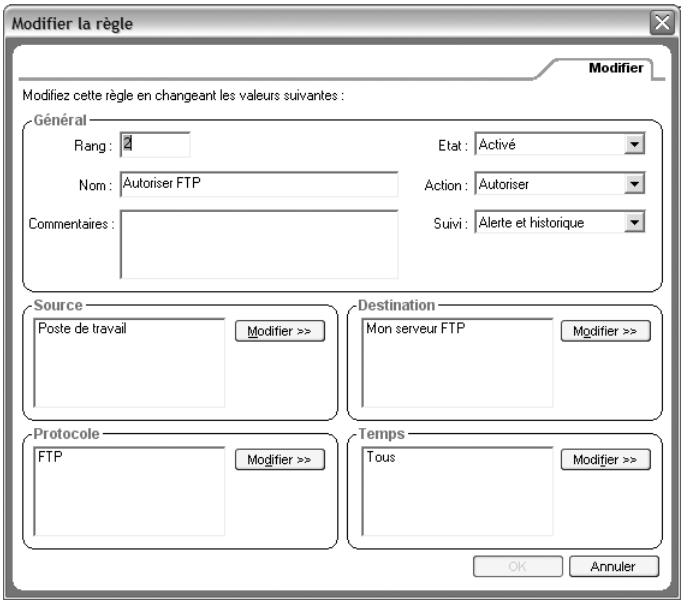


Figure 5–17
Définir une règle spécifique de filtrage

Les pare-feux élaborés vous proposent des mécanismes répondant à ces besoins particuliers. Prenons un exemple : supposons que vous souhai-

tiez autoriser le transfert de fichiers entre votre poste et un serveur FTP (File Transfer Protocole) situé sur Internet, sans forcément ouvrir votre pare-feu à tous vents (c'est malheureusement ce qui se produit lorsque les ports FTP, TCP 20 et 21, sont ouverts). Vous pouvez définir cette règle très simplement en cliquant sur l'onglet *Expert* à partir de l'écran *Firewall* de ZoneAlarm Pro.

Si vous observez la figure 5-17, vous définissez une règle de la manière suivante :

1 Spécifiez les adresses source et/ou destination des machines concernées par cette règle. Vous constaterez qu'en cliquant sur le bouton *Modifier* de la zone source ou destination, vous pouvez désigner ces adresses selon plusieurs formats différents (figure 5-18). Ce paramètre signifie que la nouvelle règle s'appliquera si le trafic réseau provient et/ou est à destination de votre ordinateur, d'un nom de domaine spécifié (*Hôte/site*), d'une adresse ou d'une plage d'adresses IP spécifiées, d'une passerelle ou d'un sous-réseau spécifié.

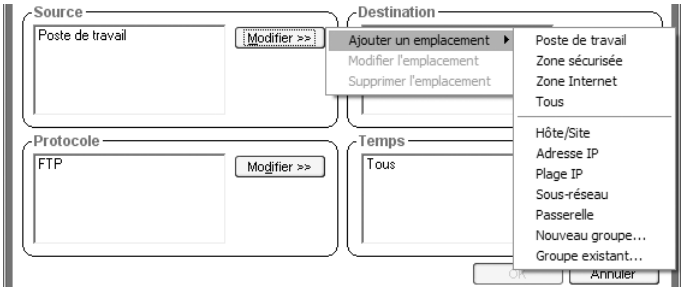


Figure 5–18
Définir les adresses source et destination de la règle.

Par exemple, admettons que le nom de domaine du serveur distant soit ftp.monserveur.com. Il vous suffit de sélectionner *Hôte/site* dans le menu contextuel de la zone *Destination* et de spécifier le nom de votre serveur FTP, comme le montre la figure 5-19.

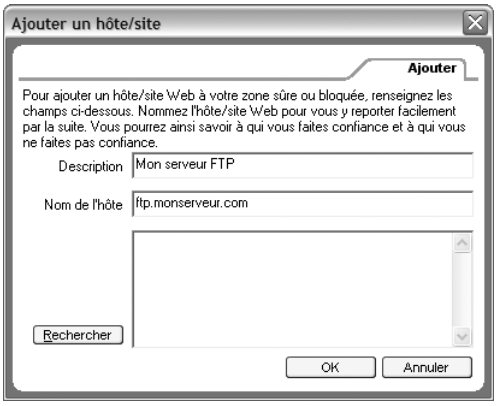


Figure 5–19
Spécifier un nom de domaine.

2 Spécifiez ensuite le protocole sur lequel s'applique la règle, en l'occurrence ici, FTP.

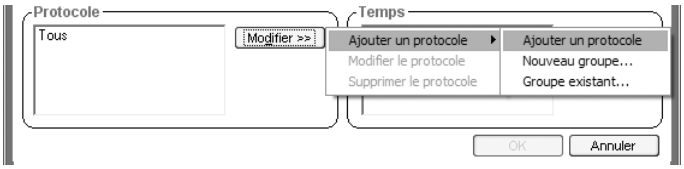


Figure 5–20
Définir le protocole sur lequel s'applique la règle.

Dans la zone *Protocole*, cliquez sur le bouton *Modifier* (figure 5-20) et sélectionnez *Ajouter un protocole*. Dans la boîte de dialogue affichée à la figure 5-21, sélectionnez *FTP* dans le menu déroulant *Port de destination*. Votre règle est maintenant presque entièrement définie.

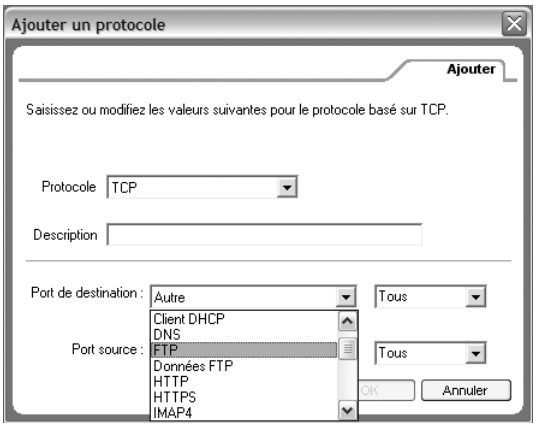


Figure 5–21
Spécifier qu'il s'agit du protocole FTP.

3 Vous avez en outre la possibilité de définir une plage temporelle (jour, heure, etc.) pendant laquelle la règle est définie. Cliquez sur le bouton *Modifier* de la zone *Temps* et entrez les valeurs correspondantes.

N'oubliez pas de spécifier l'action que doit réaliser la règle (*Autoriser* = autorise le protocole à entrer ou sortir, *Bloquer* = interdit le protocole), ainsi que son état (*Activé* = la règle fonctionne, *Désactivé* = elle ne fonctionne pas).

Pour déterminer le rang d'une règle experte, c'est-à-dire la position qu'elle occupe dans l'ordre d'évaluation des règles, il faut avoir en tête la manière dont procède le pare-feu lorsqu'il analyse le trafic. Une règle experte a priorité sur les règles affectées à une zone : si le pare-feu détermine qu'une règle experte s'applique, il ignore les règles de la zone pour cette communication.

Le but de cet ouvrage n'est pas d'entrer dans le détail des riches possibilités offertes par les règles de filtrage des pare-feux. Il est recommandé

de lire attentivement la documentation fournie par l'éditeur, voire de s'abonner aux forums de discussion spécialisés, et de se familiariser progressivement avec leur fonctionnement. La définition de règles spécifiques n'est pas une activité extrêmement ludique, mais ne ménagez pas votre peine car la sécurité réelle délivrée par un pare-feu dépend en grande partie de la précision de ses règles de filtrage.

Réagir aux alertes affichées par les pare-feux

Les pare-feux vous mettent souvent dans des situations embarrassantes : ils éprouvent un malin plaisir à afficher de façon intempestive des messages épouvantables, laissant perplexe l'utilisateur non averti (… mais aussi parfois, l'utilisateur averti !). Prenez le cas de cette alerte (apparemment d'ordre viral) de la suite PC-cillin (figure 5-22).

Figure 5–22 Le pare-feu vous informe qu'il vient de bloquer une attaque.

Si vous vous documentez sur ce message, vous apprendrez que le processus `lsass.exe` renferme une vulnérabilité exploitable par l'attaquant. Sachant cela, vous n'êtes cependant pas très avancé, et vous serez nombreux à refermer bien vite cette fenêtre en espérant l'incident clos. Certains utilisateurs, lassés par les apparitions régulières de ce message, désactivent même la suite logicielle ! C'est effectivement une façon de ménager sa tranquillité (en apparence...).

Si vous décidez de prendre la sécurité de votre poste au sérieux, il faut prendre en compte ces alertes. Cependant, elles font pour la plupart appel à des notions d'administration de système et sont inaccessibles à l'utilisateur non informaticien. Il faudra donc vous familiariser petit à petit avec ces alertes, et apprendre à les traiter. Pour cela, vous allez acquérir quelques notions ciblées en matière d'informatique système.

Voici quelques pistes qui devraient vous aider à mieux traiter les alertes de votre pare-feu :

- N'hésitez pas à consulter l'aide en ligne de votre produit, c'est souvent une mine de renseignements.
- Certains éditeurs proposent un lien dans la fenêtre affichée. Si vous cliquez dessus, vous accéderez à une page web donnant une information détaillée à propos de l'alerte affichée. Sachez toutefois que, la plupart du temps, cette page est en anglais.
- Le cas échéant, n'hésitez pas à effectuer vous-même quelques recherches sur Internet. Vous obtiendrez rapidement l'information pertinente et, de surcroît, en français.

Prenons l'exemple simple de la figure 5-23 : votre pare-feu a détecté que l'application `PcCltCom.exe` sollicitait les droits de serveur pour accéder à Internet, et vous demande votre accord.

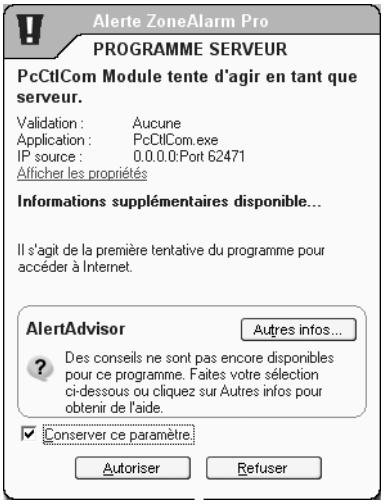


Figure 5–23 Votre pare-feu affiche une alerte. Que faire ?

Si le nom `PcCltCom.exe` ne vous dit rien, suivez la piste : cliquez sur le lien *Afficher les propriétés* ou lancez une recherche rapide sur Google. Dans ce cas précis, vous découvrirez vite qu'il s'agit d'un processus de l'antivirus PC-cillin de TrendMicro ; vous pouvez donc, exceptionnellement, accorder à ce processus l'autorisation d'agir en temps que serveur.

Les pare-feux puissants disposent souvent d'une panoplie étendue d'alertes de niveaux variés. L'objectif ici n'est pas de fournir une explication sur tous les cas de figure rencontrés, ce serait trop long. En revanche, il est primordial que vous vous familiarisiez avec la démarche de prise en compte des alertes :

1. Ne laissez pas le ver dans le fruit : ne négligez jamais une alerte de votre pare-feu ou de votre antivirus.
2. Prenez le temps de comprendre l'alerte affichée. N'hésitez pas à vous documenter ; éventuellement, demandez des explications si quelqu'un de votre entourage maîtrise mieux l'outil informatique que vous.
3. Apprenez les gestes qui sauvent : modifiez la configuration de votre pare-feu (restriction des droits). Supprimez toute application douteuse ; mettez à jour les modules logiciels incriminés.

Tout cela vous paraîtra contraignant au début, mais vous vous y ferez.

Journaux du pare-feu

Les journaux du pare-feu sont l'un des éléments fondamentaux de la sécurité de votre système. Ils sont incontournables, et pourtant si souvent délaissés ; quelle erreur !

Le journal de sécurité est votre service de contre-espionnage. Il enregistre toutes les attaques lancées à votre encontre, les tentatives d'intrusion, les anomalies, les alertes et toutes sortes d'événements qu'il juge suspects ; il permet de suivre les pirates à la trace. Il est votre compagnon et vous aidera à identifier les prémices d'une action et à prendre les mesures susceptibles d'empêcher une attaque ou de combler un trou dans votre cuirasse.

Vous trouverez dans ce journal l'information qui vous renseignera sur les paquets mis en cause : le type d'événement, les adresses IP source et destination, le type de protocole utilisé, la direction du trafic, l'heure et la date, etc… (figure 5-24).

Bien sûr, il faut apprendre à se familiariser avec le contenu du journal, car il n'est pas toujours très clair, surtout quand il s'agit de journaux édités au format texte.

D'autre part, il faut aussi apprendre à l'interpréter, et cela ne s'improvise pas ; là encore, quelques notions sur les protocoles IP seront utiles.

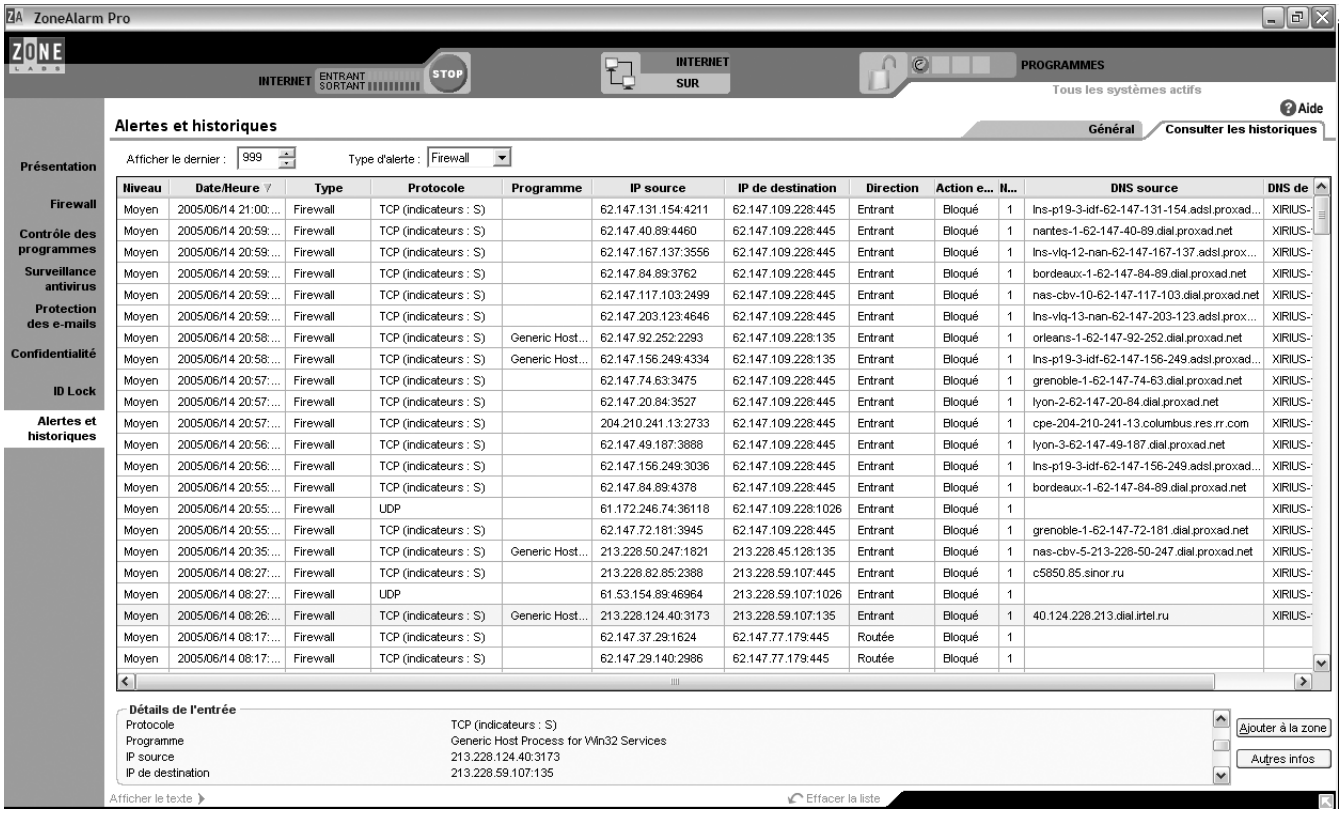


Figure 5–24 Visualisation du contenu du journal des événements de sécurité du pare-feu

Observez par exemple la figure 5-24 et constatez à quel point les ports 135 et 445 sont visés : rappelez-vous ce que l'on avait dit précédemment à propos des ports NetBIOS 135, 137 à 139 et 445. En d'autres termes, mesurez combien il est salutaire de bloquer ces ports, surtout sur Internet.

CONSEIL **Consultez les journaux d'activité du pare-feu**

Il est absolument vital de surveiller son journal d'activité. Surveiller le trafic bloqué vous renseigne sur les attaques que vous avez subies, en vous donnant toutes sortes d'indications sur l'origine et la nature de ces attaques. L'observation de l'historique peut aussi vous aider à personnaliser ou à optimiser les règles de filtrage du pare-feu. Revenir de temps à autre, à tête reposée, sur les alertes passées est un petit sacrifice qui vous évitera de gros soucis.

Trouver le juste équilibre entre le niveau de protection délivré par un pare-feu et la facilité d'emploi

Voici une question délicate et, en même temps, cruciale.

Vous noterez à l'usage qu'une politique trop restrictive du pare-feu aboutit inévitablement à une limitation, voire à une impossibilité de fonctionnement de tout ou partie de certaines applications. Si, par exemple, le pare-feu impose la fermeture du port TCP ou UDP d'un logiciel d'échange poste à poste ou du programme chargé d'effectuer la mise à jour d'un antivirus, vous n'obtiendrez pas le service que vous attendez et en serez probablement frustré.

Vous aurez donc généralement tendance à relâcher progressivement les protections de votre pare-feu en autorisant de plus en plus d'applications à accéder à Internet, ou à agir en tant que serveur. Vous serez également tenté d'ouvrir en sortie ou en entrée les ports qui vous empêchent de communiquer comme vous le désirez.

Attention, gardez en tête les risques que vous encourez lorsque vous autorisez une exception. Dès lors que vous acceptez l'ouverture d'un port, quel qu'il soit, vous offrez aux pirates un moyen d'exploiter ce canal à leur profit et d'infiltrer votre poste. Si votre pare-feu ne sait pas analyser le contenu des messages transmis à travers les ports ouverts, ce qui est le cas de la plupart, voire de tous les pare-feux personnels, les attaques visant à exploiter les vulnérabilités d'un protocole applicatif (par exemple HTTP, SMTP, DNS, etc.) ou d'une application (par exemple un client Kazaa, ICQ, etc.), ne seront jamais détectées.

Conseil **Recommandations pour la configuration du pare-feu**

Il est recommandé de suivre les grandes directives suivantes :

- De manière générale, autorisez un strict minimum d'applications à accéder à Internet.
- Afin d'éviter les attaques exploitant les bogues de ces applications et des protocoles qu'elles mettent en œuvre, veillez à maintenir ces logiciels à jour ; n'hésitez pas, par exemple, à recourir au site Windows Update.
- Méfiez-vous comme de la peste des applications qui agissent en tant que serveur ; c'est la porte ouverte à la prise de contrôle à distance.
- Si vous devez ouvrir le champ des applications susceptibles d'utiliser Internet, ou bien ouvrir certains ports TCP ou UDP, faites-le seulement si c'est nécessaire, et en ayant conscience des risques potentiels.
- Contrôlez de temps en temps la configuration de votre pare-feu, et si leur utilisation ne s'impose plus, n'hésitez pas à fermer des accès autorisés par le passé.

Dans tous les cas de figure, restez vigilant, quoi qu'il arrive.

Protéger l'accès aux fonctions d'administration du pare-feu

En général, il faut définir un mot de passe pour protéger l'accès à votre pare-feu. Cela évite d'éventuelles modifications intempestives de la part d'autres utilisateurs du PC, qui veulent, par exemple, accéder à Internet en se servant de logiciels que vous ne souhaitez pas mettre en œuvre ; cela permet aussi d'éviter des désagréments lorsqu'un code malveillant tente de modifier le comportement du pare-feu ou même de l'arrêter purement et simplement.

Figure 5–25
Pensez à définir un mot de passe pour restreindre l'accès à votre pare-feu.

Si vous ne protégez pas l'accès au pare-feu avec un mot de passe, l'édifice global que vous construisez pour protéger votre installation risque d'être fragilisé.

Les pare-feux matériels

Nécessité d'un pare-feu matériel

Une entreprise doit impérativement placer un pare-feu matériel à l'entrée de son site. Même si la structure est modeste (moins de 10 personnes), il est ridicule d'économiser les 1 500 euros nécessaires à

l'acquisition d'un pare-feu : sans vous en rendre compte, vous dépenserez bien plus pour gérer les problèmes causés par les pirates. Peut-être allez-vous dire que vos données ne sont pas confidentielles, que vos concurrents connaissent déjà vos prix, ou que votre secteur d'activité n'a rien de stratégique… Certes, mais lorsque l'on évoque la sécurité informatique, il n'est pas toujours question de confidentialité. Beaucoup de pirates agissent par jeu ou par défi, certains par dépit, d'autres aiment tout simplement fouiner dans les affaires d'autrui ou, pour se donner l'illusion de l'importance, s'excitent rageusement sur votre réseau tant qu'ils n'ont pas obtenu leur ration de pouvoir sur vos serveurs ; tout cela sans parler des erreurs commises par les utilisateurs, qui ignorent souvent les dangers d'Internet. Au bout du compte, le résultat est navrant : des postes de travail contaminés par toutes sortes de saletés attrapées sur Internet, qui vous espionnent et vous empoisonnent en consommant, par exemple, une bonne proportion de votre bande passante, des machines qui subissent des blocages intempestifs, des applications dont les configurations ont été altérées et qui ne fonctionnent plus très bien, tout un tas de problèmes bizarres qui obligent, à défaut de savoir éradiquer le problème, à procéder régulièrement à des réinstallations complètes. La liste est longue, que de temps perdu ! La facture est lourde pour le chef d'entreprise. Ne pas installer de pare-feu, c'est un peu comme si n'importe qui pouvait pénétrer librement, de jour comme de nuit, à l'intérieur de vos locaux, fouiller et examiner le contenu de vos dossiers, modifier l'organisation de votre rangement, corrompre vos données… Un réseau d'entreprise raccordé en permanence à Internet et non protégé avec un pare-feu, est ouvert à tous les vents.

Emplacement du pare-feu matériel

Il faut placer le pare-feu matériel en entrée de site, en aval du point de raccordement avec le réseau public (modem ADSL par exemple), en amont de votre réseau local ou du premier routeur de votre installation.

Si votre réseau comporte plusieurs sous-réseaux que vous souhaitez protéger, vous pouvez le faire à l'aide de pare-feux situés aux points de raccordement des sous-réseaux avec le réseau fédérateur.

Avantages d'un pare-feu matériel par rapport à un pare-feu logiciel

Tout d'abord, les pare-feux matériels se distinguent essentiellement par des capacités de filtrage extrêmement fines et élaborées. Non seulement vous pouvez filtrer selon la source, la destination, le type de protocole, le sens, l'utilisateur ou les horaires, mais il vous est possible de limiter, voire

d'interdire nominativement, les commandes que vous jugez dangereuses au sein même d'un protocole.

Ensuite, les pare-feux matériels peuvent agir en tant que relais (proxy). Lorsque vous établissez une session avec un service Internet (par exemple avec un serveur web, un serveur FTP ou un serveur de messagerie), le pare-feu crée en réalité deux communications IP distinctes : l'une entre votre poste et le proxy, l'autre entre le proxy et le serveur sur Internet. À elle seule, cette fonction vous apporte une part non négligeable de protection car, outre le fait que votre poste n'est plus en prise directe avec le réseau Internet, le pare-feu effectue de nombreux contrôles et a le pouvoir de bloquer la session s'il détecte une attaque. La technologie de proxy vous apporte :

- l'assurance – dans une large mesure – que les pirates ne réussiront pas à détourner le fonctionnement des protocoles dans le but d'infiltrer votre installation :
  - balayages de port et recensements à travers les pare-feux ;
  - attaques par saturation (déni de service) ;
  - débordements de tampons par utilisation, par exemple, d'URL très longues ;
  - prise en main à distance de votre site web (*directory traversal*) ;
  - toutes sortes de comportements intrusifs, comme l'insertion de scripts cachés dans les requêtes HTTP ;
- une protection contre les pourriels à l'entrée du site (contrôles antispam) ;
- le contrôle des contenus vous offrant un bouclier contre l'import malencontreux de chevaux de Troie, de contrôles ActiveX, de scripts malveillants, ou de logiciels espions qui foisonnent au sein des protocoles P2P encapsulés, des messageries instantanées ou autres programmes ;
- un contrôle antivirus sur les flux entrants et sortants. Ce type de service est très intéressant : le virus est éradiqué à la source, avant même d'avoir atteint la première machine de votre réseau privé. Conjugué à un deuxième système antivirus présent sur les postes utilisateurs (choisir de préférence un autre éditeur – voir chapitre 3), une telle solution vous assure une protection quasi intégrale contre la menace virale.

Il est remarquable de noter que toutes ces politiques agissent en un seul point, par exemple le point de raccordement du réseau sur le réseau Internet, et protègent du même coup l'ensemble des flux de l'entreprise.

En outre, les pare-feux matériels vont bien au delà de la seule problématique (pourtant complexe !) de filtrage des flux et de détection d'intrusion. À mesure que leurs fonctionnalités s'étendent, ces équipements

deviennent petit à petit des unités complètes prenant globalement en charge la sécurité périmétrique et des communications.

Ainsi les pare-feux matériels sont dotés d'infrastructures de gestion de clés (PKI – Public Key Infrastructure) qui vous permettent d'élaborer de façon fiable vos propres certificats et de déployer, éventuellement, une PKI à l'échelle de votre entreprise (voir à ce sujet le chapitre 6). En effet, la présence d'une PKI signifie la possibilité d'avoir recours à des mécanismes cryptologiques, c'est-à-dire à des mécanismes forts pour assurer l'authentification des utilisateurs et de l'origine des communications ainsi que l'intégrité et la confidentialité des données. À ce titre, les pare-feux matériels sont généralement dotés d'un serveur de VPN intégré.

Pour terminer, les pare-feux matériels offrent de riches fonctionnalités de suivi, grâce notamment à la présence de journaux détaillés, de dispositif d'alertes automatiques, ainsi que d'applications de visualisation en temps réel, et à distance, de l'activité en cours. Les pare-feux matériels peuvent aussi être administrés à distance, de façon centralisée et sécurisée, à travers un poste de travail authentifié.

AVANCÉ VPN (Virtual Private Network)

Derrière la notion de VPN, se cache un ensemble de services fondés sur des mécanismes cryptologiques, permettant essentiellement :

- l'établissement de tunnels chiffrés entre passerelles VPN (en l'occurrence des pare-feux), garantissant le chiffrement des échanges entre plusieurs sites d'une même entreprise à travers des réseaux non sûrs ;
- l'établissement de tunnels chiffrés entre pare-feux et postes nomades désirant accéder à distance aux ressources de l'entreprise en mode sécurisé ;
- l'authentification forte des utilisateurs.

Principaux pare-feux matériels disponibles sur le marché

Les constructeurs de pare-feux sont nombreux. À titre indicatif, voici une liste succincte donnant quelques uns des meilleurs équipements du marché :

- Cyberguard Firewall (Cyberguard Corporation, US) ;
- les produits Arkoon (Arkoon Network Security, France) ;
- les produits Netasq (Netasq, France) ;
- FireWall-1 (Check Point, Israël) ;
- Cisco PIX Firewal (Cisco, US).

Cyberguard Firewall (US)

La société Cyberguard Corporation (www.cyberguard.com), un des leaders mondiaux en matière de solutions de sécurité réseau, dispose d'une gamme d'outils qui couvre aussi bien les réseaux des petites entreprises que les infrastructures des grandes multinationales.

Les pare-feux Cyberguard fonctionnent en mode *stateful inspection* et offrent une large panoplie de fonctionnalités complémentaires, parmi lesquelles on peut citer :

- un système de connections VPN IPsec par câble ou ADSL ;
- un service de traduction d'adresses et de ports (NAT/PAT) ;
- une sonde intégrée de détection et de prévention anti-intrusion.

Suite au récent rachat de la société Webwasher, spécialisée dans le contrôle de contenu sur Internet, les pare-feux Cyberguard intègrent un logiciel antivirus effectuant un contrôle des flux HTTP, HTTPS, FTP et SMTP (les principaux vecteurs de transmission de virus), un système de filtrage des pourriels (Webwasher Anti Spam), un système anti-phishing et des fonctions très étendues de contrôle de l'activité et de l'accès des utilisateurs internes aux services Internet (en un mot, l'œil de Moscou).

Les pare-feux Cyberguard offrent en outre de riches capacités d'analyse des menaces véhiculées par les protocoles du Web, de la messagerie ou de certaines applications Internet, comme IM (Instant Messaging) et les applications Peer-to-Peer. Ils peuvent procéder à un blocage sélectif des flux de messagerie instantanées et des échanges poste à poste jugés « à risque ».

Point qui n'est pas sans intérêt, le pare-feu Cyberguard Firewall existe aussi sous forme embarquée : carte PCI enfichable sur poste de travail (Windows 2000 ou XP, Linux) ou serveur (Windows Server 2000/2003, Linux). Cette approche a pour avantage d'étendre la fonction pare-feu jusqu'au niveau des postes utilisateurs (empiétant ainsi clairement sur les prérogatives des pare-feux logiciels) et permet notamment l'établissement des tunnels VPN chiffrés entre chaque poste d'un même réseau local.

Arkoon Network Security (France)

Arkoon Network Security (www.arkoon.net/) propose une gamme de pare-feux dotés d'une grande diversité de fonctions de sécurité et dimensionnés pour protéger des réseaux de dix à plusieurs milliers de postes de travail.

Les pare-feux Arkoon entrent dans la catégorie des pare-feux applicatifs, c'est-à-dire qu'ils décodent et analysent en temps réel les protocoles jusqu'au niveau 7 (HTTP, FTP, SMTP, POP, DNS, NETBIOS, RSTP, NNTP, IMAP, H323, SQLNET, RPC, SNMP). Ils peuvent donc bloquer les attaques traditionnelles de niveau « réseau », et les attaques de niveau supérieur exploitant les vulnérabilités d'applications (non respect des standards RFC, violations protocolaires, commandes mal formées). Ainsi, ils peuvent pallier les débordements de tampons, les violations de répertoires par émission d'URL mal formées (*directory traversal*), le vol des paramètres d'identification de session (*cross site scripting*), ou, plus généralement, les attaques mettant en œuvre des données applicatives malveillantes injectées au sein des protocoles d'Internet. Ils sont notamment capables de filtrer les logiciels P2P (Kazaa, Emule) et la messagerie instantanée.

Grâce à un partenariat établi avec l'éditeur Sophos (voir chapitre 3), ces pare-feux intègrent un antivirus en ligne capable de bloquer virus, vers et chevaux de Troie transmis via les protocoles HTTP, SMTP, POP3 et FTP ; l'analyse s'effectue sur la base d'un fichier de définitions de virus situé à

l'intérieur du pare-feu, mis à jour automatiquement et de façon transparente par le constructeur, à travers Internet et un lien sécurisé SSL v3.

Les équipements Arkoon disposent en outre d'un dispositif de détection et prévention d'intrusion (IDPS), fondé sur le concept de signatures contextuelles, une technologie conçue pour optimiser les temps de traitement et réduire les risques de fausses alertes. La base de signatures utilise le même canal de mise à jour que pour les bases antivirus. Il s'agit d'un canal authentifié par certificat, et sécurisé. Chose intéressante, vous avez la possibilité de créer et d'ajouter vos propres signatures d'attaque.

Ces équipements fournissent aussi une fonction relais HTTP/FTP/SMTP/POP. Les fonctions relais HTTP/SMTP comprennent un système de filtrage d'URL et antispam basé sur une liste noire remise à jour automatiquement. Ils offrent également une fonction de filtrage des codes mobiles hostiles – modules Javascript, Applets Java, contrôles ActiveX et autres paradigmes (voir à ce sujet le chapitre 7).

Les boîtiers Arkoon fournissent un service VPN doté d'une infrastructure de gestion de clés (PKI) embarquée. Vous pouvez ainsi créer et déployer une véritable Autorité de Certification au niveau de l'entreprise (voir chapitre 6), gérer vos propres certificats X.509 v3, établir des tunnels sécurisés (DES, 3DES et AES 256 bits) permettant de raccorder plusieurs sites ou plusieurs nomades à un même site par l'intermédiaire de canaux chiffrés, et authentifier les utilisateurs à l'aide de mécanismes cryptologiques.

Ces pare-feux intègrent aussi des fonctions de routage dynamique (OSPF, RIP V2 et BGP 4) et de gestion de la bande passante (Qualité de service), pouvant ainsi faire office de routeur.

Netasq (France)

Au même titre que Arkoon, Netasq (www.netasq.com/fr/index.php) est le deuxième grand nom français des dispositifs de sécurité. Comme son concurrent, Netasq développe et commercialise des solutions pare-feux réseau et applicatifs, adaptées à toutes les tailles d'entreprises.

Les équipements Netasq délivrent un service VPN SSL permettant aux utilisateurs distants de se connecter aux réseaux d'entreprise de manière sécurisée avec un simple navigateur Internet ; ils fournissent VPN IPsec pour la mise en œuvre de tunnels chiffrés de pare-feu à pare-feu à travers des réseaux non sécurisés (le pare-feu jouant alors le rôle de passerelle de sécurité), et l'établissement de liens chiffrés ouvrant un accès sécurisé aux utilisateurs distants sur les ressources internes du réseau (postes nomades). Ces équipements sont dotés d'un module PKI embarqué servant à l'élaboration et à la gestion des certificats numériques X.509 v3 et offrant des mécanismes d'authentification forte des utilisateurs au moyen de certificats numériques et d'algorithmes cryptologiques.

Les boîtiers Netasq délivrent tous les services proposés par les matériels actuels et qui contribuent à renforcer significativement la sécurité de votre site. Ils sont par exemple dotés de l'antivirus Kaspersky (voir au chapitre 3) qui effectue en temps réel un contrôle systématique des flux entrants et sortants, et d'un système de prévention d'intrusion en temps réel fondé sur la technologie ASQ.

Les produits Netasq offrent en outre plusieurs mécanismes additionnels, comme un dispositif intégré de contrôle antispam basé sur les listes noires DNS mises à jour en temps réel, un tueur de logiciels espions, et le filtrage d'URL sur la base d'une liste noire répertoriant des millions de sites web classés par thèmes.

Comme les produits Arkoon, les équipements Netasq ont reçu plusieurs certifications par le gouvernement français (dont la certification Critères Communs au niveau EAL2+).

Check Point (Israël)

Check Point Software Technologies (www.checkpoint.com) est le leader mondial en matière de sécurité sur Internet ; les solutions pare-feu (Firewall-1) et VPN (VPN-1) sont les plus distribuées dans le monde.

Le produit FireWall-1 est un pare-feu réseau et applicatif très complet, capable d'analyser et de décoder plus de deux cents protocoles applicatifs ; on peut citer notamment les protocoles HTTP, FTP, SMTP, POP3, IMAP4, SSH, SSL, Microsoft/Oracle SQL, SOAP/XML, Windows Media, services H323, et bien d'autres.

Il ne faut toutefois pas oublier que les services de sécurité qui reposent sur des fonctions cryptologiques (comme VPN-1) mettent en œuvre des mécanismes qui ne sont pas développés en France.

Check Point Software Technologies commercialise désormais le pare-feu logiciel ZoneAlarm Pro, depuis sa récente acquisition de Zone Labs.

Choisir un pare-feu matériel

Si vous pensez que la sécurité est pour vous un enjeu majeur (par exemple, vous êtes patron ou administrateur informatique d'une entreprise à forte valeur ajoutée ou positionnée sur un secteur stratégique), il est bon de ne pas ignorer quelques principes de base en sécurité informatique.

Qu'il s'agisse de matériels, comme les postes de travail, les serveurs, les routeurs ou les pare-feux, ou de logiciels, comme les systèmes d'exploitation, les services ou les applications informatiques, sachez que tous ces composants recèlent des failles de sécurité et des accès cachés, susceptibles d'ouvrir l'accès complet à des tiers « initiés ». Les chapitres 3 et 7 montrent com-

ment l'exploitation des failles et des portes dérobées permet à un inconnu de s'introduire à distance dans un système informatique, de prendre discrètement son contrôle et d'accéder ainsi à toutes vos données sensibles. Plus généralement, certaines institutions sont passées maîtres dans l'art de fabriquer des modules logiciels dont l'analyse est tellement complexe qu'il est impossible de savoir si le code recèle ou non des failles cachées.

HISTOIRE Contrôle de l'information

De tous temps, les gouvernements se sont livrés à des combats feutrés, mais acharnés, dont le but était le contrôle de l'information de l'adversaire. L'excellent et passionnant ouvrage de Simon Singh, « Histoire des codes secrets », nous en livre un témoignage édifiant. Bien comprendre la cryptologie et les mécanismes de sécurité en général commence par admettre que ce principe reste toujours vrai.

À l'heure où certaines agences gouvernementales introduisent massivement des modules secrets au sein des composants, visant à ménager des points d'accès pour visiter ou agir sur n'importe quel système informatique n'importe quand, le réseau Echelon, qui a tant défrayé la chronique il y a peu de temps, pourrait presque faire figure de cornet acoustique du Professeur Tournesol dans un monde de plus en plus sous la domination de l'informatique.

En bon expert sécurité, paranoïaque à outrance comme il se doit, il serait maladroit de feindre l'ignorance à propos de la vraie finalité d'un composant informatique ou de communication (et a fortiori de sécurité informatique), à savoir l'instrument d'une chaîne d'intelligence économique servant le gouvernement qui l'a conçue. Ne nous méprenons pas, cette démarche est tout à fait respectable, c'est de bonne guerre, mais il faut savoir aussi effectuer les choix technologiques en connaissance de cause.

Il est clair que la dépendance technologique est devenue en France un facteur de risque pour les grands secteurs de l'économie, comme la Défense, la Finance, l'Industrie ou les grandes administrations. Aujourd'hui, sur le plan de la sécurité, on peut réellement déplorer la disparition des grands constructeurs et éditeurs français de l'informatique.

Tout au long de cet ouvrage, nous nous sommes efforcé de ne pas exprimer d'opinion personnelle, nous contentant de vous donner les éléments de comparaison, afin que vous puissiez effectuer vos propres choix. Nous ferons exception ici. Les grands pare-feux du marché, tout au moins ceux qui sont cités dans cet ouvrage, offrent une liste impressionnante de fonctions de sécurité, et chacun de ces produits vous apportera une haute protection contre la menace des *hackers*. Toutefois, nous avons la chance d'avoir sur notre territoire deux constructeurs, Netasq et Arkoon, qui, de surcroît, fabriquent des produits de tout premier plan. Si vos données revêtent un caractère sensible au plan national ou international, nous ne saurions trop vous conseiller de faire appel à l'un ou l'autre de ces fournisseurs pour le choix de votre pare-feu.

De façon générale, si vos exigences de sécurité sont élevées, une excellente solution consiste à mettre en œuvre deux pare-feux issus de deux constructeurs différents (comme pour les antivirus, les défaillances de l'un seront comblées par l'autre). Cela permet de conjuguer protection « stratégique » avec Arkoon ou Netasq (au plus près de votre installation) et richesse des fonctionnalités avec CheckPoint, CyberGuard ou autre. Une telle architecture n'est d'ailleurs pas toujours complexe à mettre en œuvre : beaucoup d'opérateurs ou de FAI utilisent déjà les grands pare-feux de type CheckPoint ; il vous suffit d'installer un Netasq ou un Arkoon à l'entrée de votre site pour satisfaire cette règle.

Détection et prévention d'intrusion

Détecter une tentative d'intrusion

Certains pare-feux vous alertent directement lorsqu'ils détectent ou bloquent une tentative d'intrusion sur votre poste. À l'image du pare-feu inclus dans le logiciel Panda Titanium Antivirus (voir figure 5-26), vous verrez dans certains cas, et selon la configuration de votre pare-feu, surgir une fenêtre indiquant qu'une tentative d'intrusion a été bloquée sur votre poste, sa nature, ainsi que son origine, matérialisée le plus souvent par l'adresse IP du poste source de l'attaque. Dans cet exemple, il s'agit d'une banale tentative de balayage de ports. En suivant les instructions du pare-feu, vous pourrez en savoir plus sur cette intrusion.

Figure 5–26
Détection d'une tentative d'intrusion

Une autre façon de détecter les tentatives d'intrusion consiste à analyser les journaux du pare-feu. L'analyse des journaux de bord est quelque chose de très ennuyeux, au point que même les administrateurs Système préfèrent éviter de se plonger dans ces hiéroglyphes, à supposer d'ailleurs qu'ils puissent trouver du temps pour ça ! Encore une fois, négliger cet aspect est un grand tort car ces journaux sont une source de renseignements fort utile.

En observant attentivement la figure 5-27, vous pouvez noter que la machine située à l'adresse IP *172.20.4.63* – la source – vous a bombardé de toute une série de trames TCP (votre machine – la destination – est située à l'adresse *172.20.4.70*). Vous constatez en outre que le numéro de port destination varie à chaque fois (il figure à la suite de l'adresse *172.20.4.70*, juste après le signe « : »). Il s'agit ni plus ni moins, là aussi, d'un balayage de ports, la fameuse étape préparatoire à toutes les intrusions. Dans ce cas, le pare-feu n'avait pas affiché d'alerte (il est configuré pour ne pas vous déranger dans votre travail à chaque battement de cil), mais l'exploitation du journal vous apprend qu'une machine située sur votre réseau local a tout de même tenté une action de reconnaissance sur votre poste. C'est toujours bon à savoir.

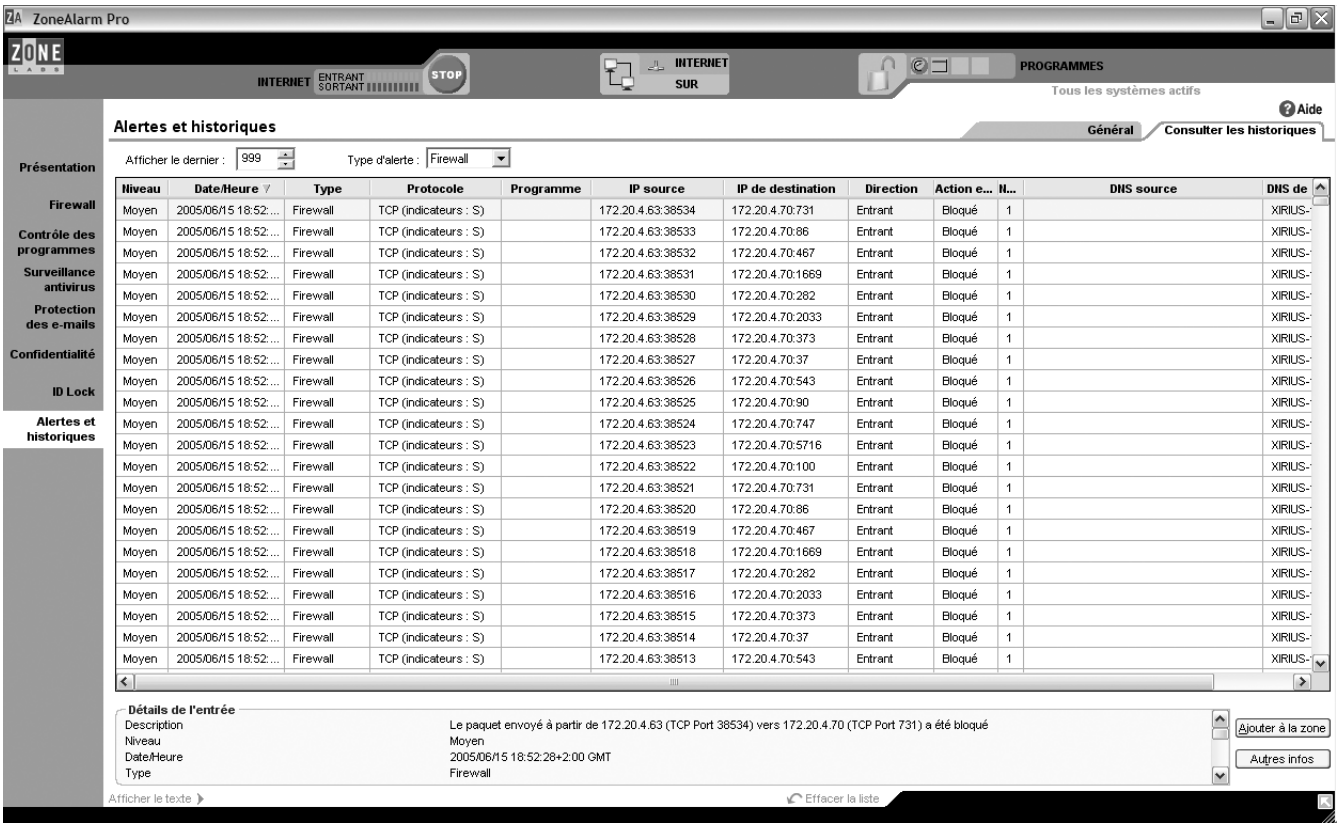


Figure 5–27 Trace d'une tentative d'intrusion

Restez attentif, consultez votre journal, vérifiez les attaques dont vous avez été la cible, analysez leurs conséquences réelles ou potentielles. Vous pourrez comme cela optimiser et valider la configuration de votre pare-feu, et prendre éventuellement les mesures conservatoires pour éviter des attaques plus dévastatrices.

Apport d'un logiciel spécifique de détection et de prévention d'intrusion en complément du pare-feu

Si vous disposez d'un pare-feu matériel, il est évident que les fonctions IDPS (Intrusion Detection and Prevention Systems) sont présentes dans votre équipement et qu'il n'y a pas lieu d'investir dans un outil supplémentaire.

Si vous ne possédez qu'un pare-feu logiciel, votre niveau de protection est moindre ; cependant, si ce produit est performant et correctement configuré, vous pouvez, à la rigueur, envisager de vous passer d'un outil spéci-

CONSEIL **Préférez le pare-feu matériel**

Si vos données sont vitales pour le bon déroulement de votre activité, n'hésitez pas à préférer la solution du pare-feu matériel.

fique de détection et de prévention d'intrusions, à condition bien sûr de mettre en œuvre les autres mesures de protection décrites dans cet ouvrage, à commencer par un bon antivirus. Toutefois, si votre environnement est sensible, ou si vous êtes paranoïaque, l'utilisation d'une fonction additionnelle de détection et de prévention d'intrusion ajoutera indubitablement une couche de sécurité supplémentaire, et ce à moindre coût.

Principales sondes en matière de détection et de prévention d'intrusion

Comme nous l'avons évoqué plus haut dans ce chapitre, tous les grands pare-feux matériels (Check Point, Cyberguard, Arkoon, Netasq, etc.) sont dotés d'un IDPS intégré. Pour des questions de performance, les traitements IDPS s'effectuent au cœur même du noyau de leur système d'exploitation, ces contrôles ne doivent donc pas dégrader outre mesure le débit de votre réseau.

Si vous vous orientez plutôt vers une solution logicielle, l'un des meilleurs choix à l'heure actuelle se porte sur le logiciel Snort, téléchargeable gratuitement à l'adresse www.snort.org.

Snort est reconnu par la profession comme l'une des sondes de détection d'intrusions les plus efficaces du marché ; certains spécialistes ont même tendance à la préférer à d'autres sondes commerciales. Cependant, si vous souhaitez réellement tirer parti de ses riches possibilités, cet outil s'adresse indiscutablement aux initiés : l'interface et la documentation sont en anglais, l'outil est en ligne de commande et son utilisation nécessite une connaissance approfondie des protocoles TCP/IP et des méthodologies d'attaques des pirates. Il réjouira sans conteste les as de la programmation ; si ce n'est pas votre cas mais si vous avez un tantinet de patience et de courage, vous mettrez en œuvre, en conjonction avec votre pare-feu, un tandem efficace.

Règles natives des IDPS

Dans le cas des pare-feux matériels, les signatures d'attaques sont mises à jour automatiquement par le constructeur ; vous n'avez donc pas à vous soucier de définir de règle particulière, d'autant que vous avez déjà spécifié de nombreuses règles de filtrage lors de la configuration du pare-feu.

Pour sa part, Snort est livré avec une base de plusieurs centaines de règles et de signatures d'attaques, qui, au passage, constitue un standard utilisé par de nombreux produits du commerce (par exemple, le module IDPS d'Arkoon se base sur les règles Snort).

Cependant, il est souvent indispensable d'affiner l'analyse de certains événements ou de mettre en œuvre des procédures spécifiques. Sachez par exemple que certaines alertes remontées par les règles standards de Snort sont fausses. Faire le tri ou la corrélation entre les événements nécessite une attention particulière et une expérience confirmée. Si vous désirez optimiser votre IDPS, vous serez donc confronté tôt ou tard au problème de l'écriture de nouvelles règles de détection d'intrusion.

Écrire une règle de détection d'intrusion avec Snort

Snort peut fonctionner selon trois modes : analyseur de réseau, enregistreur de trafic et sonde de détection d'intrusion (NIDS pour Network Intrusion Detection System). Nous nous intéresserons ici à cette dernière.

Avec Snort, vous pouvez écrire et ajouter de puissantes règles de filtrage afin de tenir compte des spécificités de votre installation. Néanmoins, elles sont complexes à paramétrer : une règle Snort se présente sous la forme d'une ligne de commande et d'un langage conçus par un développeur qui, manifestement, aime partager avec les utilisateurs ses migraines infernales.

Voici un exemple simple (règle n°1) :

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING
NMAP"; dsize:0; itype:8; reference:arachnids,162;
classtype:attempted-recon; sid:469; rev:3;)
```

Type d'action

Une règle vous permet tout d'abord de définir une action. Dans le cas présent, Snort remontera une alerte lorsque les éléments dans cette composition de règle sont vrais. Les cinq principaux types d'actions définis par Snort sont `alert`, `log` (enregistrer le paquet), `pass` (ignore le paquet), `activate` et `dynamic`.

Type de protocole

Vous spécifiez ensuite le protocole que Snort doit analyser. Dans notre exemple, il s'agit d'ICMP. Toutefois, Snort sait également analyser les protocoles TCP, UDP et IP. Il est en outre tout à fait possible de créer des règles se rapportant aux protocoles des couches supérieures ; il suffit pour cela de spécifier le numéro de port correspondant dans le champ `any`, comme le montre l'exemple qui suit (règle n°2) :

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS zone
transfer TCP"; flow:to_server,established; content:"|00 00
FC|"; offset:15;)
```

Le port 53 correspond au protocole DNS, l'une des premières sources de renseignement pour un pirate. La requête DNS dite de « Transfert de Zone » permet au pirate de recueillir l'intégralité des données figurant dans les fichiers de zone d'un domaine, c'est-à-dire les noms des serveurs et la liste des utilisateurs du domaine. À éviter absolument !

Adresses IP, ports source et destination

Vous précisez les adresses IP et ports source et destination concernés par la règle. Une adresse IP peut se référer à une adresse unique ou à une plage d'adresses. Pour plus de convivialité, il est possible d'associer une adresse à une variable. C'est le cas dans les exemples précédents, la variable `$HOME_NET` recevant l'adresse du réseau local au moment du lancement de Snort. La commande de lancement du logiciel prend la forme suivante :

```
snort -dev -l ..\log -h 192.168.10.0/24
```

Ici, `$HOME_NET` prendra la valeur *192.168.10.0/24*, qui désigne le réseau local de classe C dont les adresses sont comprises entre *192.168.10.1* et *192.168.10.255*. La variable `$EXTERNAL_NET` désigne par exemple le réseau Internet.

Opérateur de direction

L'opérateur -> indique le sens du trafic concerné par la règle en question. Les adresses IP et les numéros de ports situés à gauche de l'opérateur sont considérés comme trafic source, les informations d'adresses et de ports situées sur le côté droit de l'opérateur désignent le système destination. Traduit en français, l'exemple de la règle n°2 s'exprime de la façon suivante : lorsqu'un paquet TCP en provenance du réseau extérieur (`$EXTERNAL_NET`), attaché à n'importe quel port source (désigné par le mot-clé `any`), est transmis vers un ordinateur du réseau privé sur le port 53, provoquer une alerte. Voici un autre exemple (règle n°3) :

```
log tcp any any -> 192.168.1.0/24 :6000
```

Avec cette règle, vous demandez à Snort de journaliser l'ensemble du trafic TCP à destination du réseau local *192.168.1.0/24*, à condition que le port destination soit inférieur ou égal à 6000.

Options

À chaque règle, vous pouvez définir des options détaillées pour effectuer des contrôles très fins sur les paquets entrants et sortants. Ces options sont contenues à l'intérieur de la section entourée par les parenthèses ; elles sont séparées par des points-virgules et les mots-clés de chaque

option sont séparés de leurs arguments par un caractère « deux points ». Les options portent – entre autres – sur :

- `content` : recherche un motif caractéristique d'une attaque (signature) dans le contenu à l'intérieur d'un paquet. Par exemple : « `content:"|00 00 FC|"` ».
- `msg` : affiche un message dans les alertes et journalise les paquets. Par exemple : « `msg:"DNS zone transfer TCP"` ».
- `itype` : teste si la valeur du champ type ICMP est égale à une valeur spécifiée (par exemple un type ICMP égal à 8 caractérise une trame ICMP `ECHO`, trahissant l'existence potentielle d'un balayage Ping).

Il existe bien d'autres options qu'il n'est pas utile de présenter dans le cadre de cet ouvrage.

Cette rapide présentation a simplement pour but de démystifier – partiellement – le problème complexe de l'écriture des règles en matière de détection d'intrusion, mais elle est tout à fait succincte. Vous disposez maintenant de quelques notions qui vous permettront sans doute de comprendre le millier de règles contenues dans l'outil Snort. Cependant, si vous envisagez sérieusement d'écrire de nouvelles règles, nous ne saurions trop vous conseiller de vous reporter au manuel utilisateur de Snort et de lire très attentivement le chapitre dédié à l'écriture de ces règles.

Récapitulatif

Les attaques dirigées contre les couches basses des protocoles de communication (IP, TCP, UDP) sont devenues depuis longtemps monnaie courante, à cause, notamment, de la publication tous azimuts d'outils d'intrusion prêts à l'emploi, et d'une efficacité remarquable. Contrairement à ce que prétendent certains experts, mentionnant des problèmes d'efficacité rencontrés avec les outils de filtrage actuels, ce serait une grave erreur de ne pas protéger son installation avec un pare-feu, logiciel ou matériel, voire les deux.

Toutefois, il faut être conscient des limites d'un pare-feu. Les pirates chevronnés focalisent aujourd'hui leurs attaques vers les couches hautes du modèle OSI (couches présentation/application), voire les applications elles-mêmes, naviguant ainsi quasiment au-delà de la zone d'influence des pare-feux. Un pare-feu efficace doit obligatoirement être doté de modules d'inspection applicative capables d'analyser finement les protocoles de plus en plus complexes transportés, voire de comprendre la sémantique des données échangées entre applications. Cependant, il est illusoire d'imaginer que les pare-feux, même les plus puissants, sauront

un jour analyser complètement tous ces protocoles, étant données leur diversité, leur spécificité et leur complexité. Les trous de sécurité subsisteront. Comment en effet assurer que tel paramètre PHP/MySQL ne va pas déclencher un débordement de tampon sur l'application du serveur Apache qui l'héberge ? Comment déjouer l'injection d'une DLL visant à tirer parti d'un logiciel autorisé doté de droits élevés, ou assurer que tel script ou contrôle ActiveX n'a pas été conçu à des fins d'espionnage ? Sécuriser un poste ou un site revient à prendre les mesures nécessaires pour réduire les opportunités d'attaque. Il est bien évident que la sécurisation résulte d'un faisceau de mesures cohérentes et complémentaires appliquées à plusieurs niveaux, dont le pare-feu n'est qu'une composante.

À RETENIR Mesures de sécurité

En tout état de cause, pensez à prendre les mesures suivantes :

- Dans le cas d'une entreprise, même modeste, installez impérativement un pare-feu matériel à l'entrée de votre site.
- Déployez un pare-feu logiciel sur tous vos postes reliés à Internet.
- Veillez à ce que votre pare-feu soit capable d'analyser les protocoles applicatifs courants (HTTP, SMTP, POP3, IMAP4, FTP, DNS, etc.).
- Configurez rigoureusement votre pare-feu de manière à n'autoriser que les services nécessaires.
- Veillez à ce que tous les ports correspondant à des services que vous n'utilisez pas soient fermés. Prenez garde notamment à ne pas ouvrir les ports NetBIOS (135, 137 à 139, 445) aux réseaux non sûrs.
- Interdisez le protocole ICMP à l'entrée de votre site.
- Soyez extrêmement prudent si vous autorisez une connexion entrante sur un port donné. Idéalement, cette autorisation ne devrait jamais être accordée.
- N'hésitez pas, si besoin, à créer vos propres règles de filtrage afin d'adapter les filtres de votre pare-feu à vos cas d'utilisation spécifiques.
- Passez en revue régulièrement la configuration de votre pare-feu.
- Ne négligez en aucun cas une alerte affichée par votre pare-feu. Si besoin, prenez du temps pour comprendre de quoi il s'agit et résolvez le problème.
- Analysez régulièrement les journaux de vos pare-feux et cherchez à comprendre pourquoi et comment vous avez subi telle ou telle attaque. Modifiez la configuration du pare-feu en conséquence.
- N'oubliez jamais que la protection assurée par un pare-feu ne résout pas tous les problèmes.
- Protégez l'accès à votre pare-feu avec un mot de passe.
- Activez la fonction de traduction d'adresses au niveau du point de raccordement à Internet.
- Si vous utilisez un outil de détection d'intrusion complémentaire, soyez prêt à consacrer du temps à son paramétrage et à l'analyse des alertes.
- Ne téléchargez pas n'importe quoi sur Internet ; méfiez-vous des logiciels freeware, des clients P2P et des messageries instantanées.

chapitre 6

Reconnaître l'authenticité sur Internet avec les certificats

Comment être sûr de l'authenticité d'un site web, d'un document électronique ou de la clé publique d'un correspondant ? Ce chapitre expose les grands principes de la certification qui vous seront nécessaires pour comprendre la sécurisation de la messagerie, des transactions électroniques et compléter la configuration de votre navigateur Internet.

SOMMAIRE

- Certifier une clé publique
- Certificat, signature et autorité de certification
- Déchiffrer un certificat
- Réseaux de confiance
- Listes de révocation

MOTS-CLÉS

- clé publique/privée
- certificat
- signature électronique
- autorité de certification
- réseau de confiance
- liste de révocation

EN PRATIQUE Connexion sécurisée

Lorsque la connexion est sécurisée (URL commençant par `https://`), Internet Explorer affiche un petit cadenas en bas à droite de l'écran. Firefox, quant à lui, colore de plus la barre de navigation en jaune.

C'est bientôt l'anniversaire de votre fils et vous décidez de lui offrir le dernier opus des aventures de Harry Potter, en anglais pour parfaire sa connaissance de la langue de Shakespeare. Vous établissez donc une connexion Internet avec votre site préféré de vente en ligne aux États-Unis et lancez la commande pour l'achat de ce livre.

Après avoir rempli quelques formulaires vous demandant de saisir votre adresse électronique, quelques informations personnelles et, éventuellement, un mot de passe (attention aux cookies ! - voir chapitre suivant), vous lancez l'ordre d'achat. Soudain, une alerte de sécurité surgit sur votre écran (voir figure 6-1) vous indiquant que votre connexion est désormais sécurisée et que les informations échangées sur le site seront chiffrées.

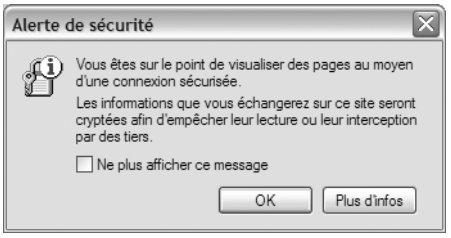


Figure 6–1
Ouverture d'une session chiffrée

À ce moment précis, votre objectif est de réaliser cet achat. Vous cliquerez donc probablement sur le bouton *OK* et continuerez la session en présumant de la sécurité effective de la connexion. Malgré tout, une fois l'achat terminé, vous ne pourrez vous empêcher de nourrir secrètement quelques doutes sur la sécurité réelle de cette transaction car, enfin, vous venez tout de même d'envoyer votre numéro de carte de crédit sur Internet, et vous l'avez confié à une page web !

Il est tentant d'interrompre la transaction avant de confier des données confidentielles au réseau, mais dans ce cas vous ne réaliserez pas votre achat. Alors, peut-être chercherez-vous à savoir ce que signifie réellement « connexion sécurisée » en cliquant sur le bouton *Plus d'infos*. Toutefois, apprendre que le site web dispose d'un certificat valide, c'est sans doute très bien… sauf lorsqu'on ignore ce qu'est un certificat, qui est habilité à déclarer un certificat valide et le degré de confiance attribuable à un tel outil.

Est-ce vraiment rassurant de savoir qu'un certificat garantit l'authenticité d'un site ? Cela ne laisse-t-il pas supposer que d'autres ne sont pas authentiques, qu'un site web peut usurper l'identité d'un autre ? La lecture de ce texte explicatif n'est pas très explicite sur la sécurité réelle du protocole.

Tâchons donc de voir ensemble ce que sont un certificat, une connexion sécurisée avec un site web distant, les niveaux de sécurité réels qu'ils assurent et les risques auxquels vous êtes confrontés. Toutefois, avant d'aborder ce chapitre, la lecture de l'annexe A vous permettra de bien

comprendre le fonctionnement et la mise en œuvre des algorithmes cryptologiques à clés publiques, des fonctions de hachage et des signatures électroniques.

Certifier une clé publique

Si vous souhaitez envoyer un message chiffré, il faut utiliser pour le chiffrement la clé publique *de votre correspondant*. Lui seul en effet, en possession de la clé privée associée, peut ainsi déchiffrer ce message et accéder au secret qu'il renferme (voir annexe A).

Supposons que vous deviez envoyer à l'un de vos collègues le rapport confidentiel que vous êtes en train de rédiger. Pour en garantir la confidentialité absolue, vous décidez de chiffrer votre message et pour cela, il vous faut obtenir la clé publique du collègue. La solution la plus simple consiste à appeler ce dernier au téléphone et à la lui demander. Il vous la donne, vous chiffrez le message et vous le lui envoyez. Dans ce cas précis, il n'y a pas de confusion possible : vous avez eu votre collègue au téléphone, vous avez reconnu sa voix, vous êtes donc sûr que la clé qu'il vous a communiquée est bien la sienne. Sa voix a, en quelque sorte, authentifié cette clé.

Supposons maintenant que vous ne connaissiez pas votre correspondant. Pour obtenir sa clé publique, vous pouvez par exemple la lui demander par courrier électronique, ou la télécharger à partir d'un annuaire. Seulement voilà, qui vous assure que la réponse provient bien de votre correspondant et que la clé fournie est bien la sienne ? Nous verrons au chapitre 8 que l'adresse électronique d'un internaute n'authentifie nullement cette clé.

Lorsque vous souhaitez acheter en ligne un produit vendu sur le site eyrolles.com, vous espérez légitimement que la transaction sera protégée afin de préserver la confidentialité de vos coordonnées bancaires ; c'est d'ailleurs ce que clament haut et fort la plupart des sites web marchands lorsqu'ils brandissent l'arme de la connexion sécurisée. Comme l'expliquera le chapitre 9, la session sécurisée vous protège effectivement de « l'homme du milieu » qui espionne le trafic sur Internet. Néanmoins, êtes-vous sûr de ne pas avoir été piégé par un faux site web dont les pages ressemblent à s'y méprendre à celles de eyrolles.com, et dont l'unique objectif est de récupérer votre numéro de carte de crédit ? Connaissez-vous la clé publique de eyrolles.com ? Évidemment non et, avouons-le, personne ne souhaite avoir à mémoriser une information aussi ennuyeuse !

Pour être sûr que vos informations secrètes seront effectivement protégées avec la clé du vrai destinataire, les cryptologues ont apporté une

À RETENIR Authentification des clés

C'est là un des talons d'Achille des systèmes à clés publiques. Ce n'est pas parce que vous trouvez sur un individu plusieurs cartes de visite au nom de Monsieur Durand que cette personne est effectivement Monsieur Durand. De même, disposer d'une clé publique ne suffit pas. Encore faut-il être sûr que cette clé appartient bien à celui qui prétend la posséder.

réponse efficace : il faut associer à chaque clé publique un mécanisme permettant d'affirmer sans confusion possible, autrement dit de *certifier*, qu'elle appartient bien à son prétendu propriétaire. Un tel mécanisme, associé à la valeur de la clé publique et à d'autres informations que nous allons détailler, s'appelle *le certificat*.

Certificat, signature et autorité de certification

Le mécanisme de certification d'une clé publique fait intervenir un troisième acteur (les deux premiers étant vous et votre correspondant) : un organisme tiers auquel nous allons tous accorder une certaine confiance.

Cet organisme va tout d'abord se charger d'élaborer pour nous, ou pour les sites marchands comme eyrolles.com, les paires de clés publique et privée dont nous avons besoin. Jusque-là, son rôle n'est pas très original car nous pouvons tous très facilement engendrer deux nombres aléatoires p et q. Par exemple, pour obtenir p, vous pouvez tirer 512 fois à pile ou face. C'est un peu long et fastidieux, mais la qualité de l'aléa obtenu n'est pas mauvaise. En supposant que vous cherchiez à utiliser RSA, il ne vous reste plus qu'à effectuer les calculs nécessaires à l'élaboration de n, de e et de d, aboutissant ainsi aux valeurs numériques de la clé publique et de la clé privée (voir annexe A). Cependant, ces traitements font appel à des logiciels spécifiques et, si vous n'êtes pas vous-même informaticien, ces procédures vous paraîtront sans doute très compliquées. Pour plus de simplicité, laissez donc un organisme tiers effectuer ces calculs à votre place.

En revanche, lorsqu'il a élaboré une paire de clés publique et privée RSA, l'organisme de certification apporte une valeur ajoutée indiscutable. En effet, il joint à la clé publique le nom de son propriétaire (par exemple eyrolles.com), ainsi que quelques données d'identification supplémentaires (comme le nom de l'organisme émetteur de la clé, un numéro de série). Il associe également des données d'administration (comme les dates de validité de la clé), et surtout l'information capitale que lui seul est capable de produire, *sa signature*. Toutes ces informations sont regroupées en un unique petit fichier : *le certificat* (figure 6-2).

Un certificat est en quelque sorte l'équivalent d'une pièce officielle délivrée par la Préfecture de Police, comme le passeport ou le permis de conduire, à la différence qu'il existe sous forme électronique. La signature de l'organisme ayant émis le certificat permet de lier ensemble les informations qu'il contient (notamment le nom du propriétaire et la clé publique associée), et de *certifier* l'exactitude de ces informations, donc de garantir que

EN COULISSES Signature

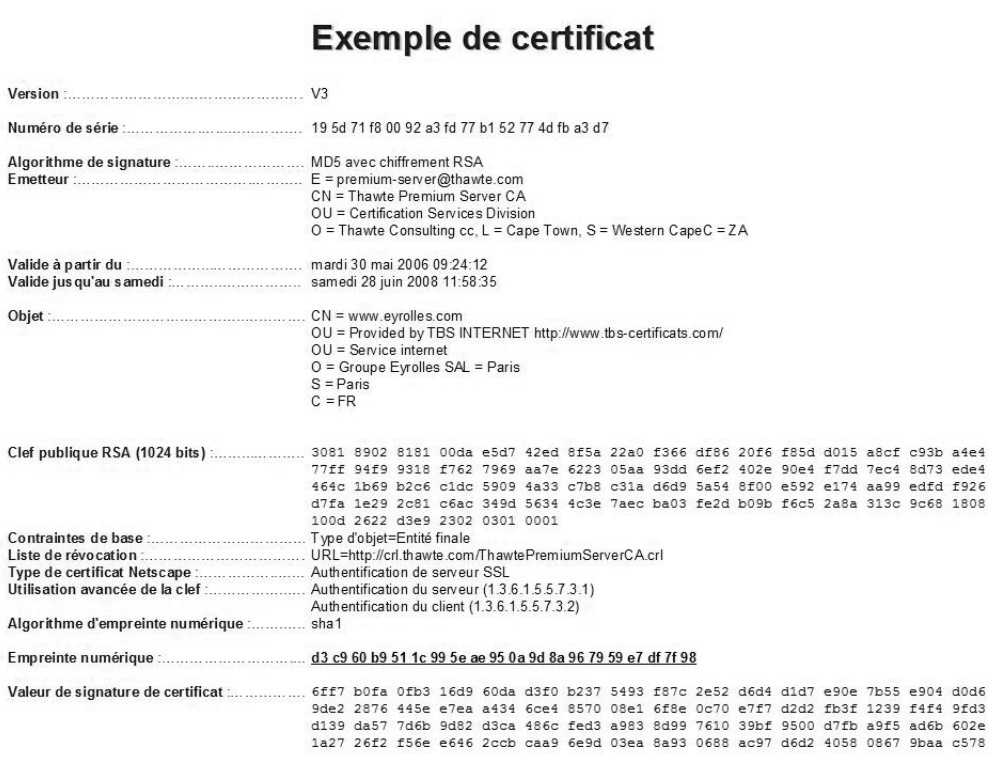
Pour établir une signature, l'organisme de certification calcule simplement l'empreinte numérique de toutes les informations citées - clé publique, données d'identification, données d'administration - (il peut utiliser par exemple MD5, SHA-1 ou d'autres algorithmes de hachage), et chiffre ce condensé avec sa propre clé privée en utilisant le plus souvent l'algorithme RSA. N'oubliez pas que lui seul est capable de calculer cette valeur chiffrée, car lui seul connaît la valeur de sa clé privée. En revanche, tout le monde est capable de déchiffrer la signature, car tout le monde connaît, ou peut rapidement connaître, sa clé publique, et vérifier que la valeur déchiffrée correspond bien à l'empreinte numérique recalculée du certificat.

CONCRÈTEMENT Certificat

Le certificat est un petit fichier contenant :
- la clé publique ;
- les données d'identification du propriétaire de la clé ;
- la période de validité de la clé ;
- les données d'identification de l'organisme émetteur ;
- la signature de cet organisme.

Autorité de certification

À l'image de la Préfecture vis-à-vis des passeports, l'Autorité de Certification est un service qui délivre des certificats. Il se porte garant de l'authenticité des données contenues dans le certificat, et ajoute sa propre signature.



Exemple de certificat

Version	V3
Numéro de série	19 5d 71 f8 00 92 a3 fd 77 b1 52 77 4d fb a3 d7
Algorithme de signature	MD5 avec chiffrement RSA
Emetteur	E = premium-server@thawte.com CN = Thawte Premium Server CA OU = Certification Services Division O = Thawte Consulting cc, L = Cape Town, S = Western CapeC = ZA
Valide à partir du	mardi 30 mai 2006 09:24:12
Valide jusqu'au samedi	samedi 28 juin 2008 11:58:35
Objet	CN = www.eyrolles.com OU = Provided by TBS INTERNET http://www.tbs-certificats.com/ OU = Service internet O = Groupe Eyrolles SAL = Paris S = Paris C = FR
Clef publique RSA (1024 bits)	3081 8902 8181 00da e5d7 42ed 8f5a 22a0 f366 df86 20f6 f85d d015 a8cf c93b a4e4 77ff 94f9 9318 f762 7969 aa7e 6223 05aa 93dd 6ef2 402e 90e4 f7dd 7ec4 8d73 ede4 464c 1b69 b2c6 c1dc 5909 4a33 c7b8 c31a d6d9 5a54 8f00 e592 e174 aa99 edfd f926 d7fa 1e29 2c81 c6ac 349d 5634 4c3e 7aec ba03 fe2d b09b f6c5 2a8a 313c 9c68 1808 100d 2622 d3e9 2302 0301 0001
Contraintes de base	Type d'objet=Entité finale
Liste de révocation	URL=http://crl.thawte.com/ThawtePremiumServerCA.crl
Type de certificat Netscape	Authentification de serveur SSL
Utilisation avancée de la clef	Authentification du serveur (1.3.6.1.5.5.7.3.1) Authentification du client (1.3.6.1.5.5.7.3.2)
Algorithme d'empreinte numérique	sha1
Empreinte numérique	d3 c9 60 b9 51 1c 99 5e ae 95 0a 9d 8a 96 79 59 e7 df 7f 98
Valeur de signature de certificat	6ff7 b0fa 0fb3 16d9 60da d3f0 b237 5493 f87c 2e52 d6d4 d1d7 e90e 7b55 e904 d0d6 9de2 2876 445e e7ea a434 6ce4 8570 08e1 6f8e 0c70 e7f7 d2d2 fb3f 1239 f4f4 9fd3 d139 da57 7d6b 9d82 d3ca 486c fed3 a983 8d99 7610 39bf 9500 d7fb a9f5 ad6b 602e 1a27 26f2 f56e e646 2ccb caa9 6e9d 03ea 8a93 0688 ac97 d6d2 4058 0867 9baa c578

Figure 6–2
Exemple type de certificat mis en œuvre pour sécuriser les achats en ligne

ce certificat et les informations qu'il contient sont authentiques. Pour cette raison, cet organisme est communément désigné sous le nom d'*Autorité de Certification* (AC ou CA = Certification Authority en anglais).

Déchiffrer un certificat

Exemple concret

Voyons concrètement comment utiliser un certificat avec un exemple simple basé sur une implémentation très artisanale de RSA sous Excel. Imaginons que l'auteur de ces lignes soit une autorité de certification reconnue dont vous connaissez la clé publique, en laquelle tout le monde s'accorde à avoir confiance : n=3041, e=1427. Supposons que vous receviez un message électronique provenant d'Alice, contenant une valeur chiffrée par cette autorité de certification reconnue :

```
« Š4R\? R^<-H‰G%H?!ý!rQCÜRí)\< Ißa–
@À ]!Qæl:77"ëœGOÛ>vüI!]#bQ] »
```

En temps normal, votre navigateur s'emploierait à déchiffrer cette information, car il dispose de tous les outils nécessaires. Toutefois, comme il s'agit d'un exemple pédagogique, vous pouvez vous-même faire ce calcul de déchiffrement. Si l'on écrit la partie utile de ce message avec les nombre décimaux qu'il représente, on obtient la suite :

```
« 1148 1672 2082 2723 728 419 2603 2732 2397 1516 419 2329 3338
1230 1082 858 2755 2755 1482 35 1567 1482 1962 118 2527 3332 693
35 1272 698 268 1093 ».
```

Certes, pour retrouver le message clair, il faut une petite dose de courage et beaucoup de chance, car notre logiciel de chiffrement respecte à peu près tout, sauf les standards ; vous allez donc développer une petite fonction sous Excel vous calculant automatiquement, pour chaque nombre k du message, la valeur $k^e \bmod n$, soit $1148^{1427} \bmod 3041$, $1672^{1427} \bmod 3041$, etc. Si vous réussissez à démêler cet écheveau et à retrouver les caractères ASCII se cachant derrière les nombres déchiffrés, vous retrouverez peut être un message intelligible :

```
« Alice n=869 e=463 Emetteur P. Legand ».
```

Vous constatez plusieurs choses. D'une part, si après avoir déchiffré un tel charabia, vous tombez sur un message intelligible en totalité, vous êtes sûr que ce n'est pas un hasard : ce message déchiffré correspond bien au message clair que l'entité détentrice de la clé privée associée avait chiffré au préalable. D'autre part, vous êtes sûr que c'est bien P. Legand qui a chiffré ce message, puisque vous l'avez déchiffré avec sa clé publique à laquelle vous faites confiance. Ce message signifie donc : « P. Legand, autorité de certification reconnue, déclare que la clé publique d'Alice est bien n=869 e=463 ».

Processus d'authentification d'un correspondant

Analysons succinctement ce qui se passe lorsque vous établissez un lien sécurisé avec un serveur web distant. Reprenons notre exemple de eyrolles.com.

1. **Le site marchand envoie son certificat** – Lorsque vous établissez un lien sécurisé avec eyrolles.com, plusieurs échanges ont lieu en début de session. Entre autres, comme vient de le faire Alice, eyrolles.com envoie à votre navigateur son certificat numérique.
2. **Le navigateur effectue quelques contrôles rapides** – Le navigateur cherche à savoir si ce certificat est valide et authentique. Il effectue tout d'abord quelques contrôles rapides, notamment sur les dates de validité. Si ces contrôles sont satisfaisants, il se lance dans le processus de vérification de la signature.

EN PRATIQUE Connexion sécurisée

Le navigateur établit automatiquement une connexion sécurisée lorsque vous cliquez sur un lien dont l'URL commence par `https://` (« s » pour « sécurisé »).

3 **Le navigateur calcule le condensé cryptologique des informations du certificat** – Il utilise pour cela le même algorithme que l'autorité de certification (cet algorithme est présent sur votre poste, et l'autorité de certification avait soigneusement rangé son nom dans les champs d'administration du certificat).

4 **Le navigateur déchiffre la signature** – Le navigateur utilise pour ce faire la clé publique de l'autorité de certification ; la signature déchiffrée doit être égale au condensé cryptologique recalculé.

Seulement voilà, où trouver cette clé publique ? Rassurez-vous, elle a de bonnes chances d'être stockée sur votre poste : votre navigateur est livré avec une liste des certificats de la plupart des autorités de certification commerciales. Si le certificat de l'autorité signataire n'est pas présent sur votre poste, le navigateur vous indique qu'il ne peut pas vérifier le certificat de eyrolles.com.

5 **Le navigateur compare la signature déchiffrée au condensé cryptologique recalculé** – Les deux valeurs doivent être égales.

COMPRENDRE **Que conclure de l'analyse du certificat ?**

Si la signature déchiffrée est égale à l'empreinte numérique recalculée à partir des données du certificat, on peut établir plusieurs conclusions :

- **Intégrité** - Si le certificat envoyé par eyrolles.com avait subi une quelconque altération (une modification d'un champ, même minime), jamais le condensé cryptologique recalculé par le navigateur n'aurait été égal à la valeur de la signature déchiffrée. Vous êtes donc sûr que ce certificat est intègre.
- **Authenticité** -Toutes les informations d'un certificat sont liées entre elles, grâce à la signature. Si donc ce certificat est intègre, on peut affirmer, sans confusion possible, que la clé publique qu'il contient a délibérément été associée au nom du propriétaire du certificat (en l'occurrence eyrolles.com) lors de sa génération.
- **Non-répudiation** - Le certificat a bien été émis par l'Autorité de Certification qui prétend en être l'origine, car tout le monde connaît la valeur de la clé publique de cette autorité, et c'est cette même clé publique qui a servi à vérifier la validité de la signature. L'Autorité de Certification a donc délibérément associé le nom de eyrolles.com à la clé publique contenue dans le certificat. En outre, cette autorité ne peut plus nier avoir émis le certificat au nom de eyrolles.com.

C'est tout, mais… c'est déjà beaucoup !

Principe de confiance

Nous sommes presque au bout de nos peines. En effet, si nous posons enfin la question qui se trouve derrière toute cette discussion : la clé publique présente dans ce certificat est-elle bien celle de eyrolles.com ? Quel crédit accorder à ce certificat ? En d'autres termes, qu'est-ce qui vous garantit qu'une autorité de certification véreuse n'a pas fabriqué un faux certificat au nom de eyrolles.com, en espérant récupérer vos numéros de carte bancaire ? La réponse est simple : en présence d'une signature valide, la notoriété de l'autorité de certification est le garant de l'exactitude des informations contenues dans les certificats qu'elle émet.

Vous allez très vite comprendre en revenant à notre exemple. Le certificat de sécurité utilisé par eyrolles.com pour sécuriser les échanges est émis par la société Thawte Premium Server CA (vous pouvez le vérifier très facilement à partir de votre navigateur en consultant le contenu de ce certificat). Si vous n'êtes pas dans la profession, ce nom ne vous dira probablement rien. Néanmoins, il s'agit en fait de la société Thawte, l'une des principales autorités de certification au monde. Imaginons que Thawte émette un certificat frauduleux, que se passerait-il ? Quelqu'un finirait rapidement par découvrir la supercherie, une crise de confiance porterait un coup au secteur du commerce électronique et cette société verrait sa crédibilité ébranlée. Ce n'est évidemment pas son intérêt. Le fait que Thawte signe le certificat de eyrolles.com engage sa propre réputation et, en conséquence, apporte son crédit au certificat. Si vous effectuez des opérations d'achat à partir des pages web sécurisées par ce certificat, vous êtes sûr que votre interlocuteur est bien eyrolles.com.

EN PRATIQUE Confiance

En présence d'une signature valide, la notoriété de l'autorité de certification est le garant de l'exactitude des informations contenues dans les certificats qu'elle émet.

RENVOI Et Vista ?

Si l'utilisateur est en quelque sorte forcé de faire confiance aux commerçants du Web, via les certificats qui sont réputés en garantir le sérieux, l'inverse est loin d'être vrai. Nous en voulons pour preuve les nouvelles dispositions technologiques mises en place par Vista pour limiter la marge de manœuvre des internautes (signatures de pilotes, « licences » pour appliquer les DRM...). Voir à ce sujet la discussion du chapitre 10.

Réseaux de confiance

En tant qu'utilisateur, vous n'êtes pas censé savoir que Thawte est une autorité de confiance. Si vous êtes inquiet à l'idée qu'il va falloir vous familiariser avec les méandres politico-technico-organisationnels du fonctionnement des autorités de certification avant de vous lancer dans le prochain achat, rassurez-vous : dans la pratique, à l'exception du problème de l'intégration du certificat racine que nous développerons plus loin, c'est le navigateur qui prendra à votre place la décision de faire confiance ou non à un certificat. Pour cela, il fait appel à une notion dont vous commencez peut-être à subodorer l'existence, celle de « réseau de confiance ».

RENVOI Certificat racine

Nous fournirons au chapitre 9 l'exemple de l'intégration du certificat racine MINEFI-AC-RACINE.

Infrastructures centralisées X.509

X.509 désignait à l'origine un groupe de travail de l'ITU-T (International Telecommunications Union - Telecommunication) chargé de définir le format d'un certificat électronique. Ce groupe de travail publia en 1988 une première recommandation X.509, modifiée par la suite en 1993 et en 1996 pour conférer aux certificats une flexibilité adaptée à leur utilisation au sein des protocoles sécurisés, tels que SSL ou IPsec, ou des applications Internet, comme le courrier électronique. La version actuelle, X.509 version 3 – ou X.509v3 – définit une structure de données complexe composée de nombreux champs obligatoires (version, numéro de série, émetteur, détenteur, dates de validité, clé publique) et optionnels (points de distribution de la liste de révocation, utilisation de la clé, etc.). À titre d'exemple, vous pouvez aisément visualiser le détail du contenu d'un certificat X.509v3 à partir du magasin de certificats de votre navigateur ; vous retrouverez un contenu analogue à celui de la figure 6-2. Par extension, X.509 désigne les infrastructures à clés publiques basées sur les certificats X.509.

COMPRENDRE X.509 : contrôle centralisé de l'information

Les infrastructures de type X.509 correspondent assez bien au modèle entreprise/état, où le caractère centralisé du processus d'élaboration et de gestion des clés confère à l'autorité supérieure un contrôle à peu près total sur l'information (il ne faut pas oublier que, engendrant elles-mêmes le couple clé publique/clé privée, les autorités de certification ont une parfaite connaissance de ces dernières).

Organismes habilités à établir un certificat

Qui peut délivrer des certificats ? Question cruciale. Pour simplifier, effectuons dans un premier temps une incursion dans un monde idéal, sans tricherie, constitué uniquement d'acteurs honnêtes. Faisons une réponse simple et pleine de bon sens : est habilitée à établir un certificat une entité dont les intentions sont louables, disposant de la compétence technique nécessaire, et dans laquelle nous avons tous confiance.

Autorité de certification racine

Revenons quelques années en arrière et supposons qu'un groupe d'hommes avisés ait décidé de créer une société appelée à devenir la première autorité de certification. En raison du caractère stratégique que représente la gestion de secrets en général, et plus particulièrement en cryptologie, tout le monde ne peut prétendre à jouer ce rôle. Il faut donc que cette société offre des garanties de probité et, accessoirement (ou principalement…), d'allégeance au gouvernement du pays dans lequel elle doit opérer.

À RETENIR Cryptologie et gouvernements

Gardez constamment à l'esprit que la cryptologie a toujours été considérée par les gouvernements comme une arme de guerre. C'est pourquoi ces derniers tâchent d'assurer un contrôle sur les principales autorités de certification (à travers, par exemple, des exigences précises du cahier des charges, ou une participation plus ou moins importante des institutions gouvernementales dans le capital de l'entreprise).

Il faut également que la société en question dispose d'une compétence technique pointue, car la gestion de certificats implique de :

- créer lesdits certificats ;
- garantir une haute protection des clés privées de certification ;

- assurer une haute disponibilité des certificats de clés publiques des utilisateurs ;
- gérer les listes de révocation (cette notion sera présentée plus loin) ;
- et, pour être un brin provocateur, être capable de remettre séance tenante n'importe quelle clé privée établie au cours de son activité à l'entité gouvernementale qualifiée qui en fait la demande.

Créer cette société ne pose pas de problème. En revanche, comment la confiance peut-elle s'établir ? En fait, nous faisons confiance à une autorité de certification *parce que nous savons qu'une autorité de certification digne de ce nom ne délivrera jamais de certificats frauduleux*. Délivrer un certificat frauduleux serait contraire à son éthique. C'est l'hypothèse de départ communément admise, parfaitement recevable dans notre monde idéal, recevable dans le monde réel sous certaines conditions, que nous analyserons plus loin.

À ce stade, nous sommes donc en mesure d'accorder notre confiance à une autorité de certification, et, grâce au mécanisme de signature, d'en déduire que tout certificat émis par cette autorité est fiable. Nous avons pour cela besoin de connaître la clé publique de cette autorité de certification.

Il y a toutefois dans ce schéma un problème que nous n'avons pas encore résolu. Même si nous faisons tous confiance à la clé publique de l'autorité racine, qui peut prétendre en connaître la valeur, sachant qu'il s'agit en général d'un nombre de plus de six cents chiffres ? Lorsqu'on vérifie la signature d'un certificat émis par cette autorité racine, qu'est-ce qui nous permet d'affirmer sans confusion possible que nous utilisons bien la clé publique de ladite autorité de certification ? En d'autres termes, comment être sûr que la clé publique de l'autorité racine n'a pas elle-même été corrompue et remplacée par celle d'un escroc ?

La réponse est très simple : le mécanisme de certification lui-même. La clé publique de l'autorité de certification signataire des certificats d'utilisateurs doit, elle aussi, être certifiée. Seulement, il n'existe pour le moment aucune instance située au dessus de notre première autorité de certification ; la seule entité capable de certifier son certificat est l'autorité de certification elle-même. C'est la raison pour laquelle on dit que ce certificat est *autosigné* et que notre première autorité de certification est une autorité de certification *racine* ou autorité de certification *principale*.

Chaîne de certification

Osons donc un premier bilan ; nous avons vu en détail comment l'autorité de certification racine était capable de certifier les certificats qu'elle émettait, et, par là même, de créer un réseau de confiance entre tous les membres du club des possesseurs d'un certificat. Dans un tel schéma,

À RETENIR Tout le monde fait confiance au certificat d'une autorité de certification racine

L'un des principaux axiomes des infrastructures X.509 est le suivant : le certificat d'une autorité de certification racine est un objet dans lequel tout le monde a confiance et constitue la fondation même des réseaux mis en place au sein de ces infrastructures.

Autorité de certification racine ou principale

On appelle *racine* (ou *principale*) une autorité de certification (AC) qui établit elle-même son certificat ; ce dernier est donc *autosigné*.
Un tel organisme est habilité à délivrer des certificats pour d'autres autorités de certification auxquelles il délègue une partie de son activité.

COMPLÉMENT
Certification des autorités racines

Dans la réalité, les certificats d'autorités racines sont signés par plusieurs organismes officiels (Greffe du Tribunal de Commerce, Direction Centrale de la Sécurité des Systèmes d'Information, autres autorités de certification reconnues, etc.).

À RETENIR Fiabilité du certificat principal de l'autorité racine

Le mécanisme de certification suffit à garantir la fiabilité du certificat principal de l'autorité racine. En effet, si une entité véreuse publiait un faux certificat contenant sa propre clé publique associée au nom de l'autorité racine, elle serait très rapidement découverte. Les certificats principaux des autorités racines sont connus, largement publiés sur Internet, tant sur les sites des autorités de certification que dans les navigateurs, ainsi que dans plusieurs organes officiels (le Journal Officiel par exemple). Le faux certificat serait alors rapidement identifié, inséré dans une liste de révocation et deviendrait ainsi non utilisable.

n'importe qui peut aisément vérifier l'authenticité du certificat d'un membre de ce club.

On imagine sans peine un tel schéma fonctionner à merveille lorsque le club compte une trentaine de membres. Cependant, que se passe-t-il à grande échelle, lorsque les utilisateurs se comptent par millions ? Dans ce cas, l'AC racine ne peut gérer seule un tel volume d'informations : il faut qu'elle délègue à d'autres AC la capacité de créer des certificats.

EN PRATIQUE Délégation de l'habilitation à émettre des certificats

Dans un schéma à plusieurs autorités de certification, comment garder intacte la confiance acquise avec une AC unique ? Une réponse à cette question consiste en la publication par l'AC racine d'un document authentique, que personne ne peut contester, disant à peu près ceci : *« En ma qualité d'autorité de certification racine, je déclare solennellement que la société SubCert a toute ma confiance et la proclame en conséquence autorité de certification. À ce titre, elle est désormais parfaitement habilitée à délivrer en son nom des certificats numériques en lesquels vous pouvez avoir toute confiance. En cas de litige, il pourra être établi que le certificat incriminé, émis par SubCert, a été émis avec mon consentement explicite »*. De toute évidence, une telle déclaration a de quoi rassurer et nous pourrons désormais faire confiance à la société SubCert pour délivrer des certificats. Il y a eu transfert de la confiance et, par conséquent, création de l'embryon d'une *chaîne de certification*.

Dans la pratique, cette délégation de pouvoirs est matérialisée par un certificat délivré par l'AC racine à la société SubCert. Ce certificat inclut le nom de la société, le texte de la déclaration que tout le monde peut lire, la clé publique de la nouvelle autorité et, surtout, la signature de l'AC racine. Cette signature prouve l'authenticité du certificat, baptisé « certificat d'autorité de certification intermédiaire ».

Certificat d'autorité de certification intermédiaire

Il s'agit du certificat délivré par l'AC racine à un organisme auquel elle délègue ses pouvoirs de certification. Cette nouvelle autorité de certification est dite *subordonnée* ou *intermédiaire*.

Nous sommes donc à l'intérieur d'un modèle hiérarchique et pyramidal, où l'AC principale occupe le sommet, et dans lequel il est possible de *chaîner la confiance* de l'AC principale jusqu'aux détenteurs de certificats, à travers un réseau de sociétés similaires à SubCert, que nous allons désormais appeler AC « subordonnées » ou AC « intermédiaires ». Il peut y avoir plusieurs niveaux d'AC subordonnées entre une AC racine et un utilisateur. Par exemple, sur la figure 6-3, vous pouvez remarquer que le certificat d'Eyrolles dépend hiérarchiquement de Thawte Premium Server CA. Il s'agit ici d'un exemple simple car il existe des cas où deux ou trois autorités de certification intermédiaires apparaissent dans la chaîne de certification, entre l'autorité principale et le détenteur final du certificat.

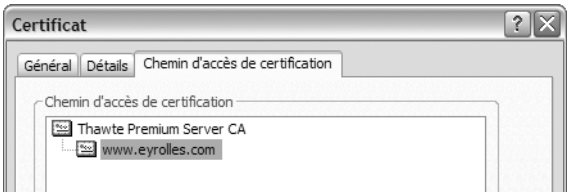


Figure 6–3
Chaîne de certification d'une AC subordonnée

Modèle réel composé de nombreuses autorités de certification

Dans la réalité, de nombreuses sociétés se sont établies autorités de certification, et ce, dans plusieurs pays. Le modèle actuel d'organisation et de fonctionnement des infrastructures X.509 repose donc sur une myriade d'autorités de certification racines réparties à travers le monde, certaines étant publiques, d'autres privées. Ces AC racines ont engendré chacune son lot d'AC subordonnées qui, à leur tour, émettent sans cesse des certificats aux particuliers ou aux sociétés de tous les horizons. On estime aujourd'hui à plusieurs centaines de millions le nombre de certificats en circulation de par le monde.

Bien entendu, le modèle idéal que nous venons de décrire ne correspond pas exactement à celui de la réalité. Avant tout, il convient de bien comprendre comment un certificat est accepté ou refusé au niveau d'un ordinateur.

Nous aborderons ce sujet plus en détail au cours du chapitre 7, mais il faut retenir que les certificats sont gérés à l'intérieur de ce que l'on appelle le magasin de certificats, qui dépend du navigateur. En quelques mots, le navigateur est capable vérifier l'authenticité d'un certificat s'il est capable de remonter la chaîne de certification. En d'autres termes, si les certificats d'autorités racines et subordonnées, directement ou indirectement signataires de ce certificat, se trouvent présents dans votre magasin, le certificat pourra être vérifié ; si sa signature est valide, il sera accepté par le navigateur. C'est ici que le bât blesse. On s'aperçoit en effet que des certificats racines d'origines très diverses sont livrés avec

votre navigateur et l'on est en droit de s'interroger sur la rigueur des pratiques de certification de certaines autorités. Si celles-ci ont pu effectivement s'établir AC par des moyens qui leur sont propres, le principe selon lequel nous avons tous confiance en ces autorités apparaît subitement quelque peu ébranlé.

De façon générale, gérer la liste des autorités racines présentes dans votre navigateur est une composante essentielle de la sécurité de vos futurs échanges. Si vous êtes particulièrement soupçonneux, faites le vide complet de votre magasin de certificats, quitte à réinstaller ultérieurement ceux dont vous aurez effectivement besoin. Ces opérations seront décrites avec moult exemples au cours des chapitres suivants. Sachez toutefois que l'intégration d'un certificat racine dans un navigateur est une opération sensible qu'il convient d'exécuter avec une extrême rigueur (voir à ce sujet la démarche proposée au chapitre 9).

Aller plus loin **Infrastructures X.509 ou confiance mutuelle OpenPGP ?**

Les certificats et OpenPGP sont basés sur les mêmes fonctionnements cryptologiques fondamentaux à clés asymétriques et garantissent, par le chiffrement et la signature électronique, les mêmes services : authentification forte, confidentialité, intégrité et non-répudiation. Toutefois, leurs formats ne sont pas compatibles (une donnée chiffrée par l'un ne sera pas déchiffrable par l'autre) et, surtout, leurs réseaux de confiance sont diamétralement opposés.

Les infrastructures X.509 sont pyramidales, inféodées aux Autorités de Certification (et aux gouvernements). À l'opposé, OpenPGP repose sur un système de confiance mutuelle, où chaque utilisateur est apte à délivrer ses propres certificats et à gérer ses propres réseaux de confiance.

OpenPGP propose un schéma très intéressant, permettant de s'affranchir de l'Autorité (de Certification, bien sûr !). En effet, son concept est basé sur un modèle où chaque utilisateur attribue lui-même, et selon des critères qui lui sont propres, des niveaux de confiance à d'autres utilisateurs. Il se crée ainsi une myriade de petits réseaux imbriqués : chacun peut décider de faire confiance à ses amis, puis aux amis de ses amis, et ainsi de suite. Voir au chapitre 8 une présentation plus détaillée du modèle de confiance mutuelle proposé par OpenPGP.

En fait, les deux approches sont complémentaires et vous utiliserez peut-être un réseau de confiance privé pour toutes vos activités personnelles ou activités professionnelles sensibles, tandis que vous vous servirez de certificats pour des transactions officielles (privées ou professionnelles) ou vos achats.

Renvoi **Liste de certificats dans le navigateur**

Il faut faire du ménage dans la liste des certificats fournis par défaut, et même, peut-être, le vide complet. Ce point sera traité au chapitre 7.

Listes de révocation

CONCRÈTEMENT Listes de révocation

Il s'agit de listes publiées périodiquement sur les sites des autorités de certification ou sur des sites prévus à cet effet. Elles répertorient les certificats valides que les AC ont émis, mais qui ne doivent plus être utilisés.

Nous avons vu que les infrastructures X.509 du monde entier géraient des millions de certificats. Évidemment, une telle profusion d'objets ne va pas sans son lot de brebis galeuses. Ainsi, de nombreux certificats sont utilisés à des fins plus que troubles. Pour remédier à cela, les autorités de certification ont mis au point le concept de *listes de révocation*, des listes publiées périodiquement sur leurs sites ou sur des sites prévus à cet effet, répertoriant les certificats valides mais qui, pour diverses raisons (certificat compromis, utilisation frauduleuse), ne doivent plus être utilisés. Pour éviter de vous faire piéger, votre seul recours est d'avoir accès à ces listes. Vous devez donc configurer votre navigateur de manière à ce qu'il puisse accéder périodiquement aux listes de révocation régulièrement mises à jour (voir chapitre 7).

Récapitulatif

Un certificat électronique est l'équivalent d'un passeport : regroupant l'identité de son propriétaire (nom, prénom, adresse électronique, etc.), sa clé publique et des données administratives telles que dates de validité et nom de l'autorité émettrice, le certificat est l'élément sans lequel aucune opération sécurisée ne peut avoir lieu sur Internet.

Dans un modèle X.509, un certificat est créé par une entité tierce appelée Autorité de Certification. Aucune donnée présente à l'intérieur d'un certificat n'est accidentellement ou intentionnellement modifiable, car toutes sont scellées grâce à la présence de la signature de l'autorité de certification.

Cette signature engage la réputation de l'autorité émettrice, qui ne peut nier ultérieurement avoir établi tel ou tel certificat. La valeur juridique d'un certificat dépend, entre autres, de la valeur de la signature de l'autorité de certification, elle-même fonction du degré de confiance qu'on lui accorde.

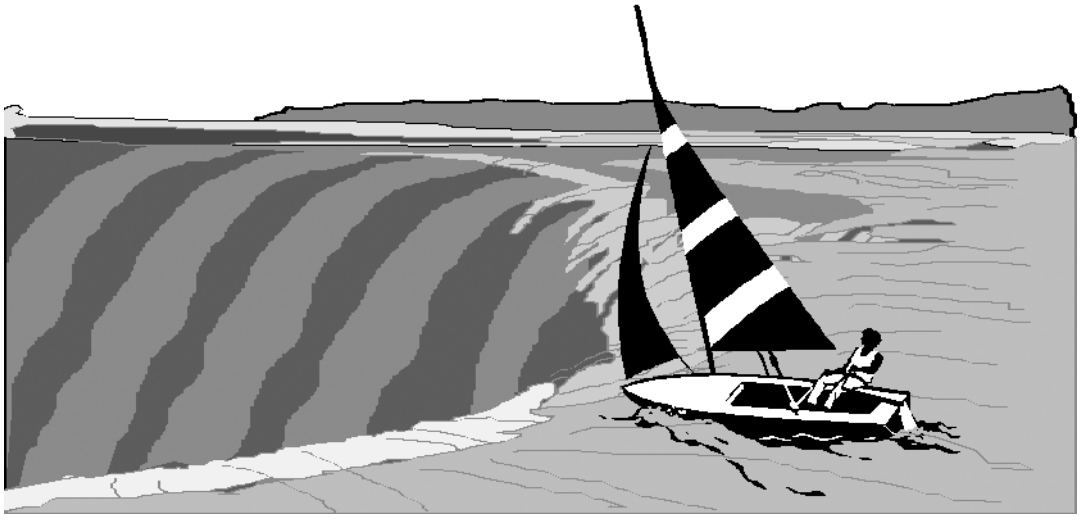
À l'exception de cryptosystèmes comme OpenPGP, fondés sur un modèle de confiance mutuelle, les autorités de certification sur Internet sont pour la plupart structurées sous la forme d'arborescences hiérarchiques dépendant chacune d'une autorité racine. Le degré de confiance associé à une autorité de certification dépend en grande partie du sérieux et de la notoriété de l'autorité racine.

Les navigateurs et les applications spécialisées dans le commerce électronique sont conçus pour vérifier automatiquement la validité de tout certificat utilisé lors des échanges sécurisés. Ils s'attachent notamment à contrôler la valeur des champs contenus à l'intérieur du certificat (les dates

de validité, l'URL d'un site web, etc.), et, surtout, à vérifier la signature apposée par l'autorité de certification émettrice. Pour vérifier cette signature, ils doivent disposer du certificat de clé publique de ladite autorité, ainsi que des certificats de clé publique de toutes les autorités de certification de niveau supérieur dont elle dépend, jusqu'au certificat de l'autorité racine (ce qui représente rarement plus de cinq certificats).

L'insertion du certificat d'une autorité racine dans un magasin de certificats est par conséquent une opération sensible. C'est pourquoi il convient de vérifier rigoureusement l'authenticité d'un certificat racine avant de l'accepter. Il faut pour cela s'assurer auprès d'une source sûre, de préférence par un canal autre que celui d'Internet, que l'empreinte numérique du certificat téléchargé correspond bien à celle du vrai certificat. Cette opération est peut-être fastidieuse, elle mais n'est réalisée qu'une seule fois.

chapitre 7



Configurer son navigateur Internet de façon sécurisée

Avec votre navigateur Internet, vous risquez d'ouvrir votre bergerie à de nombreux loups. Il faut donc le sécuriser très sérieusement. Cependant, pas de panique... votre navigateur contient déjà de nombreux mécanismes de protection ; le tout est d'accepter de consacrer un peu de temps à sa configuration.

SOMMAIRE

- Risques liés aux navigateurs
- Codes mobiles
- Cookies
- Sécuriser Internet Explorer, Netscape Navigator et Firefox
- Gérer les certificats

MOTS-CLÉS

- codes mobiles
- ActiveX
- applets Java
- scripts
- plug-ins
- cookies
- zones de sécurité
- certificat
- autorité de certification
- liste de révocation

Un pare-feu et un antivirus ne sont pas suffisants

Depuis quelques années, on voit apparaître une nouvelle génération d'attaques d'une efficacité ahurissante : les attaques dirigées contre les applications. De quoi s'agit-il ? À un instant donné (et avec votre consentement !), une application s'exécute sur votre machine. Elle s'accapare les ressources de votre processeur, accède en lecture et en écriture à votre système de fichiers, communique avec l'extérieur par l'intermédiaire de canaux que vous avez autorisés, utilise de nombreux privilèges élevés ; en bref, elle contrôle votre ordinateur. Imaginez maintenant un individu malveillant, en faction quelque part sur Internet, et donc bien entendu très loin de chez vous. Cette personne peut détourner les mécanismes logiciels de votre application pour exécuter son propre code, accéder à votre système de fichiers, implanter ses propres exécutables..., autrement dit, prendre le contrôle de votre ordinateur. Dès qu'une application communique avec l'extérieur, ce mécanisme peut être mis en œuvre. Ce type d'attaque connaît un succès exponentiel.

Pour mettre au point une attaque dirigée contre une application, il est d'abord primordial de disposer du code source de cette dernière ou, à la rigueur, de son code exécutable. Il faut ensuite mener une campagne d'analyse du code afin d'identifier les zones de vulnérabilité, puis concevoir et mettre au point l'attaque. Une attaque de ce type est intimement dépendante de l'application ; elle est élaborée à l'aide d'un microscope et d'un scalpel. La conséquence majeure de cette haute technicité est que les moyens de protection à mettre en place sont eux aussi intimement dépendants de l'application et relèvent de la microchirurgie.

Dans un tel cas, les pare-feux et les antivirus avec lesquels vous pensez être protégé sont largement dépassés. La réalisation de ce genre d'attaque donne lieu à des échanges « d'égal à égal » entre l'attaquant et l'application, c'est-à-dire qu'elle met en jeu un flux applicatif qui repose sur un protocole non filtré par le pare-feu (souvent HTTP). Il n'y a aucune raison pour que le pare-feu intervienne et bloque les paquets de l'attaquant, puisqu'il ne sait pas analyser avec suffisamment de subtilité le contenu des flux de haut niveau. De même, comme une attaque dirigée contre une application n'est structurellement pas conçue comme un virus, les antivirus sont inopérants.

Il faut savoir que le navigateur Internet est de loin l'application la plus prisée par les attaquants de tous bords (pirates en herbe et chevronnés, concurrents, gouvernements).

B.A.-BA **Code source et code exécutable**

Le code source d'une application est constitué de toutes les commandes qu'elle doit exécuter, exprimées en un langage compréhensible par un humain.
Le code source est ensuite traduit en instructions simples compréhensibles par l'ordinateur ; on dit qu'il est compilé. Le code exécutable est le code source compilé, celui que vous faites fonctionner lorsque vous « lancez » l'application.

Bon sens **Internet = danger**

Il est très délicat de contrer les attaques dirigées contre une application. Même si vous mettez en œuvre toutes les défenses imaginables, vous ne serez jamais protégé à 100 %, sauf à couper le fil qui vous relie à Internet. Si vos ordinateurs hébergent des secrets importants (qui relèvent par exemple de la confidentialité de savoir-faire industriel), la seule protection efficace est la séparation physique.

Pour le protéger, vous avez trois possibilités :

- utiliser un pare-feu applicatif qui analyse le contenu sémantique des données transportées par le protocole HTTP (voir le chapitre sur les pare-feux) ;
- configurer votre navigateur de façon sécurisée ;
- maintenir le navigateur à jour, afin d'enrayer toute exploitation de vulnérabilités connues.

L'idéal est de mettre en œuvre les trois niveaux de protection simultanément.

Ce chapitre se focalise sur la deuxième possibilité. Avant de détailler le paramétrage de votre navigateur, nous allons tâcher de mieux comprendre le contenu des fonctions de sécurité qu'il propose. Dans cette optique, nous commencerons par un bref aperçu des principales menaces spécifiquement liées aux applications de navigation sur Internet.

Risques liés aux navigateurs

Codes mobiles présents dans les pages web

En naviguant sur Internet, vous avez dû constater le caractère dynamique des pages web : des bandeaux animés défilent, des zones s'activent à l'approche de la souris, les sites boursiers proposent des graphiques animés, etc. Comment une technologie conçue initialement pour la visualisation de documents statiques peut-elle lancer le déroulement de séquences multimédia, activer la lecture de bandes son ou appeler l'affichage de menus interactifs dans le navigateur ? Le concept de code mobile est apparu avec l'évolution des technologies d'Internet. Il a été défini pour présenter une vision dynamique d'Internet à partir du client web.

Code mobile

Un code mobile, appelé aussi contenu actif, est un script ou un exécutable de taille suffisamment modeste pour être intégré au code source d'une page HTML. Lorsque vous chargez la page à partir du serveur web, le code mobile, s'il n'est pas déjà présent sur votre ordinateur, est téléchargé en même temps que la page et exécuté par votre navigateur. Nous sommes en présence d'un modèle d'exécution côté client selon lequel le code source peut très bien résider sur un ou plusieurs serveur(s) distant(s), être rapatrié sur votre machine à travers le réseau, pour être finalement exécuté localement.

Les codes mobiles présentent des avantages évidents. Ils enrichissent considérablement les potentialités des serveurs et effectuent de façon autonome des opérations à distance. Le champ d'action des codes mobiles dépasse actuellement largement celui du Web. Il s'étend aux applications réparties, comme la télévision interactive, le commerce électronique, l'avionique et les applications en temps réel.

Ils posent cependant de réels problèmes de sécurité. En adoptant un langage volontairement provocateur, on pourrait très bien exprimer les choses de la façon suivante : là où, à partir d'un serveur web, vous pensez charger le contenu d'une page hypertexte, vous téléchargez en fait des programmes qui s'exécutent spontanément sur votre ordinateur… Or, un tel mécanisme peut devenir très dangereux lorsqu'il est placé entre les mains d'un individu mal intentionné. Le téléchargement de codes mobiles s'effectue dans la plus grande transparence, c'est-à-dire à peu près à votre insu. Vous n'avez pas la maîtrise de la provenance du code téléchargé, vous ne connaissez pas son contenu et vous n'avez aucune possibilité d'intervenir sur son déroulement. Un code mobile développé par une personne mal intentionnée est capable d'accéder à votre système de fichiers, de s'insérer dans le Registre, d'exécuter du code arbitraire sur votre système et peut même être employé comme agent de surveillance. Les codes mobiles sont partout. On les trouve dans les applets web ou dans les e-mails dynamiques, les newsletters.

Aujourd'hui, il existe trois principaux paradigmes en matière de code mobile : les ActiveX de Microsoft, les applets Java de Sun et les plug-ins de Firefox ou de Netscape. Examinons les solutions de sécurité proposées par chaque constructeur et voyons comment les mettre en œuvre.

AVANCÉ **ActiveX sous Firefox et Netscape Navigator**

Le chargement d'un plug-in permet l'exécution des contrôles ActiveX sous Firefox et Netscape Navigator.

DÉVELOPPEMENT **Bibliothèques de contrôles ActiveX**

Des bibliothèques entières de contrôles ActiveX sont disponibles et offrent aux développeurs d'applications d'innombrables possibilités d'intégration de services au sein des pages web : des mécanismes de lecture MP3, des fonctions de conversion de la parole en texte, des contrôles de validité des cartes de crédit, etc.

AVANCÉ **Fichiers ActiveX**

Les contrôles ActiveX sont le plus souvent représentés sous la forme de fichiers portant l'extension `.ocx` et sont en principe sauvegardés dans l'arborescence située sous le répertoire Windows, bien que cela ne soit pas toujours le cas.

Contrôles ActiveX

ActiveX est une technologie introduite par Microsoft. D'un concept similaire à celui des applets Java, les contrôles ActiveX ont l'ambition d'être une alternative à ces dernières. Ils offrent de riches fonctionnalités, mais sont limités à l'environnement Windows, alors que leurs concurrents fonctionnent sur toutes les plates-formes.

Un contrôle ActiveX peut être incorporé dans une page web en tant qu'objet au moyen de la balise `<OBJECT>` et de quelques attributs complémentaires. Ces derniers fournissent des renseignements comme l'identification du contrôle ActiveX, sa localisation sur Internet, et les paramètres nécessaires à sa bonne exécution. L'exemple suivant montre la simplicité avec laquelle un objet ActiveX s'insère dans un fichier HTML.

```
<OBJECT
   classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
   id=animation
   width=396
   height=101
   codebase="http://active.macromedia.com/flash2/
            ➥ cabs/swflash.cab#version=6,0,0,0>
   <param
     name="movie"
     value="http://www.unsiteweb.com/img/animation.swf">
</OBJECT>
```

Lorsque vous chargez la page HTML, le navigateur sait qu'il doit faire appel au contrôle ActiveX référencé par le paramètre `classid=`, dans le cas présent le lecteur multimedia Shockwave Player de la société Macromedia. Le paramètre `codebase=` donne l'adresse Internet à partir de laquelle peut être chargé le contrôle ActiveX si le navigateur web ne le trouve pas sur votre ordinateur. La syntaxe `<param name= value=>` transmet une série de paramètres au contrôle ActiveX, comme l'adresse Internet de la séquence vidéo que vous souhaitez afficher.

Avec cet exemple, vous constatez la puissance d'un tel concept, et en même temps, le danger potentiel qu'il représente : votre navigateur est un programme exécutable autonome capable d'insérer dans son processus n'importe quel composant logiciel additionnel compilé, situé sur n'importe quel serveur accessible sur Internet, et qui accepte en entrée une série d'arguments pointant sur des ressources situées, elles aussi, sur n'importe quel autre serveur accessible sur Internet.

Si vous utilisez votre poste pour naviguer régulièrement sur Internet, il est probable que plusieurs contrôles ActiveX soient déjà stockés sur votre disque dur. Vous pouvez donc légitimement vous poser la question suivante : avec tous ces programmes installés à votre insu, votre ordinateur est-il toujours sûr ?

Question délicate. La réponse, sans doute exacte, de l'expert en sécurité (souvent taxé par les incrédules de grand paranoïaque) est : « probablement non ». Toutefois, dans la plupart des cas, vous risquez tout au plus une attaque de votre petite sœur, ou, à la rigueur, de pirates désœuvrés ou non expérimentés. Par ailleurs, il ne faut pas oublier que si votre ordinateur n'est plus très sûr, les contrôles ActiveX ne peuvent pas, seuls, être mis en cause.

Alors, comment, dans cet océan de composants logiciels , faire la part entre les « bons » contrôles et les « mauvais » ? Il n'existe probablement pas de réponse rigoureuse à ce problème complexe, et il est peu probable que quelqu'un déploie un jour une solution fiable susceptible de fonctionner à grande échelle. Toutefois, Microsoft propose une solution

RAPPEL Chiffrement, clés, signatures

Toutes les notions de cryptologie nécessaires pour comprendre les mécanismes de sécurisation des navigateurs sont expliquées à l'annexe A, à laquelle vous pouvez vous reporter à tout moment.

intéressante et que nous allons tenter d'expliquer : il s'agit de la technologie Authenticode.

Protection par Authenticode

Comme son nom l'indique, cette technologie a pour objectif d'authentifier du code. Il existe plusieurs manières de certifier un code et Microsoft a cherché à concilier l'inconciliable : il s'agit pour lui de garantir la fiabilité des contrôles ActiveX, avec un mécanisme fonctionnant à grande échelle, et des coûts supplémentaires qui restent raisonnables. Authenticode semble répondre plutôt convenablement à ces contraintes.

Lorsqu'un éditeur de logiciels souhaite distribuer ou commercialiser un contrôle ActiveX, il a la possibilité d'apposer une signature cryptologique à ce composant grâce à Authenticode. Il commence d'abord par obtenir un certificat de signature auprès d'une Autorité de Certification reconnue, comme VeriSign ou GTE. Ce certificat contient toutes les informations nécessaires à l'identification du fournisseur, ainsi que sa clé publique et sa période de validité ; il est bien sûr signé par l'autorité de certification, garantissant ainsi la fiabilité des informations qu'il contient. À l'aide des outils Authenticode, le fournisseur calcule à partir de son propre code une empreinte MD5 ou SHA, qu'il chiffre au moyen de sa clé privée et de l'algorithme RSA ; il incorpore la signature ainsi obtenue et le certificat de clé publique à son contrôle ActiveX, qui devient prêt à commercialiser.

Ensuite, au moment ou vous rapatriez l'ActiveX sur le poste client, toute une série de mécanismes se déroulent de façon transparente. Lorsque vous chargez ce composant, vous chargez aussi sa signature Authenticode et le certificat de signature du fournisseur. Le navigateur vérifie d'abord si le certificat de signature a bien été émis par une autorité de certification de confiance ; il dispose pour cela de la signature de l'autorité de certification – qui se trouve à l'intérieur même du certificat de signature du fournisseur – ainsi que du certificat de clé publique de cette autorité de certification (nous verrons à la fin de ce chapitre que tous les navigateurs Internet sont livrés avec les certificats des principales autorités de certification). Il contrôle ensuite les dates de validité du certificat et entame le processus de vérification de la signature Authenticode. Pour cela, d'une part il recalcule l'empreinte MD5 ou SHA du contrôle ActiveX et, d'autre part il déchiffre la signature Authenticode au moyen de la clé publique contenue à l'intérieur du certificat de signature. Si les deux valeurs sont égales, la signature du contrôle ActiveX est valide.

Ensuite, selon les valeurs de vos paramètres de sécurité, le navigateur vous affiche une fenêtre similaire à celle de la figure 7-1, vous informant que vous allez installer un composant authentifié. Cette fenêtre vous indique le nom du composant, ainsi que sa société émettrice.

Figure 7–1
Chargement d'un composant signé par Authenticode

Vous pouvez considérer que les informations visualisées sur cet écran sont fiables, à moins bien sûr que quelqu'un ait réussi à monter une attaque cryptologique contre les protocoles de signature ou une attaque contre l'implémentation de ces protocoles dans Authenticode, ce qui est fort peu probable lorsque la motivation du pirate est crapuleuse. En toute rigueur, la confiance que vous pouvez accorder à ce message dépend de la confiance que vous inspire l'autorité de certification ; dans l'exemple de la figure 7-1, il s'agit de VeriSign, une autorité de certification internationalement reconnue.

Cependant, à la lumière de cette présentation schématique du fonctionnement d'Authenticode, peut-être commencez-vous à en percevoir les limites. Authenticode ne garantit absolument rien en ce qui concerne le contenu du composant signé, pour la bonne et simple raison que le fournisseur établit lui-même sa propre signature. Il serait intéressant qu'un organisme extérieur reconnu procède à l'évaluation du contenu et pose sa signature dans le cas où il juge que ce composant est sûr. Toutefois, une telle organisation serait sûrement trop complexe à mettre en place à l'échelle mondiale.

Authenticode garantit de façon sûre au moins deux choses :

- **l'authentification de l'origine**, c'est-à-dire la garantie que le contrôle ActiveX provient bien du fournisseur qui prétend l'avoir développé ;
- **l'intégrité**, c'est-à-dire la garantie que le composant que vous avez chargé sur votre machine correspond bien au composant développé par son fournisseur.

C'est tout.

En pratique **Quelle confiance accorder à un composant signé avec Authenticode ?**

De toute évidence, Authenticode engage la crédibilité du fournisseur du contrôle ActiveX signé. Dans l'exemple de la figure 7-1, nous pouvons faire confiance au composant chargé car la société Macromédia a la réputation de développer des produits sérieux ; Flash Player ne viendra sûrement pas endommager ou espionner votre ordinateur. Cependant, comment réagir si le message affiche : « Vous allez installer et exécuter « IngraViseur » signé le 12/08/2003 16:54 et distribué par Imocco Ltd » ? Bien que la société et le produit vous soient totalement inconnus, il y a de fortes chances que vous acceptiez ce contrôle ActiveX. Le cas d'Internet Exploder est toujours dans les mémoires. À l'époque, un programmeur avait obtenu une signature authentique de Verisign pour un contrôle ActiveX qui arrêtait le système. La démarche était essentiellement pédagogique, mais la preuve du contournement des mécanismes d'Authenticode était faite. La réaction d'ailleurs ne se fit pas attendre, VeriSign décida de révoquer le certificat de ce programmeur, qui perdit ainsi la signature de son contrôle ActiveX.

De façon générale, un contrôle ActiveX malveillant finit toujours par être identifié comme tel par la communauté des experts et cette information est publiée sur Internet. Un tel composant, s'il dispose d'une signature Authenticode, a de bonnes chances de vivre l'expérience d'Internet Exploder ; grâce à la signature Authenticode, le fournisseur du contrôle ne peut plus nier en être l'auteur, et il peut être tenu légalement responsable du préjudice subi par les utilisateurs en cas de dommage grave. Il est donc raisonnable de penser qu'une signature Authenticode soit un gage d'une certaine fiabilité, d'autant plus élevée que la société qui la fournit et l'autorité de certification sont reconnues ; mais ce procédé n'est pas totalement infaillible. Nous considérons qu'Authenticode protège efficacement contre les attaques crapuleuses. En revanche, il est tout à fait réaliste d'imaginer l'existence de contrôles ActiveX signés qui, sous couvert d'une activité officielle très louable, laissent « involontairement » une porte dérobée bien cachée, permettant, par exemple, une petite surveillance discrète de votre ordinateur, voire la remontée d'informations vers un destinataire intéresssé par ce que vous faites ; c'est techniquement faisable et, si le code est habilement conçu, pratiquement indécelable (via un débordement de tampon par exemple). Accepter de charger sur son poste uniquement les contrôles ActiveX signés avec Authenticode est évidemment plus sage que de charger tous les contrôles ActiveX, mais un risque demeure. Il vous appartient de rester vigilant et de décider, au moment opportun, s'il convient d'installer ou non le contrôle ActiveX sur votre poste. Cette décision dépend bien évidemment du contexte d'utilisation de votre machine. Vous ne prendrez pas la même décision pour un poste isolé dédié à la navigation sur Internet, pour un poste relié à votre réseau informatique, et pour un poste hébergeant des données sensibles.

Contrôle ActiveX reconnu sûr pour l'écriture de scripts

Il existe donc des mécanismes permettant de conclure à la sûreté d'un contrôle ActiveX. Cependant, si le contrôle ActiveX doit être utilisé à partir d'un script, surgit un autre problème de sécurité. Un ActiveX peut être par exemple doté d'une fonction légitime d'accès au système de fichiers ou au Registre de la machine. Or, si un tel composant est utilisé dans un processus automatisé qui exploite cette fonction à des fins malveillantes, il peut devenir un redoutable agent d'investigation ou de destruction. Le contrôle Scriptlet, livré en standard sur des millions d'ordinateurs, en est un exemple : conçu au départ avec des intentions louables, il est capable de créer, de modifier ou d'effacer des fichiers sur votre disque local. Malheureusement, des pirates ont montré qu'en exploitant simplement les fonctionnalités de Scriptlet, il était possible d'effacer à distance le contenu complet de votre disque dur.

Pour éviter ce type de désagrément, Microsoft a développé un mécanisme particulier : les éditeurs attachent un drapeau à chaque contrôle ActiveX pour signaler que ce dernier ne présente a priori aucun danger potentiel pour l'ordinateur, même s'il est appelé par un script. Si ce drapeau est activé, le contrôle ActiveX est qualifié de cette périphrase un peu mystérieuse : « reconnu sûr pour l'écriture de scripts ».

Les contrôles ActiveX dits « reconnus sûrs pour l'écriture de scripts » exécutent pour la plupart des fonctions inoffensives. En particulier, ces dernières n'essayent pas d'accéder aux ressources du système local, d'ouvrir des connexions sur le réseau ou de lancer des programmes. Cependant, il convient de rester prudent. D'une part, selon le même principe qu'avec Authenticode, l'apposition du marquage « reconnu sûr pour l'écriture de scripts » est du ressort du fournisseur. Ce dernier est censé évaluer lui même la sûreté de son code et doit s'assurer que l'utilisation de son contrôle à des fins malveillantes soit impossible. En quelque sorte, le fournisseur est juge et partie. Il n'est donc pas impossible que des contrôles ActiveX marqués soient tout de même vulnérables, en dépit de la volonté du constructeur ; Scriptlet, marqué « sûr pour l'écriture de scripts » en est un exemple. D'autre part, il faut savoir que les contrôles ActiveX reconnus sûrs pour l'écriture de scripts ne sont pas soumis à la vérification des signatures Authenticode et, selon le paramétrage de votre navigateur, ils peuvent être installés sans que vous en soyiez informés.

Les applets Java sont-elles sûres ?

Au même titre que les ActiveX de Microsoft ou les plug-ins de Netscape, les applets Java constituent l'un des paradigmes de code mobile les plus répandus sur Internet. À l'inverse toutefois de leurs modèles concurrents

Applet Java

Une applet Java est une petite application (une appliquette) écrite en Java, un langage de programmation développé par Sun Microsystems au cours des années 1990. Les concepteurs de ce langage cherchaient une solution destinée à contourner les éternels problèmes rencontrés par les informaticiens tenus de présenter une offre compatible avec les multiples architectures matérielles et logicielles du marché. Avec Java, le programme devait pouvoir fonctionner sur toutes les machines. Pour rendre cela possible, Sun a inventé une architecture novatrice, indépendante du système d'exploitation utilisé.

qui fonctionnent essentiellement dans leur environnement natif, les applets peuvent, grâce à la machine virtuelle Java, s'exécuter sur n'importe quelle plate-forme, qu'elle soit dotée de clients comme Internet Explorer, Firefox ou Netscape Navigator, ou qu'elle repose sur des systèmes d'exploitation comme Windows, Unix, Linux ou Macintosh.

AVANCÉ **Architecture basée sur la machine virtuelle Java**

Contrairement aux langages C ou C++, compilés directement dans le langage de la machine sur laquelle le source doit fonctionner, Java est compilé en un pseudo-code générique, ou « byte code », complètement indépendant du système. Pour s'exécuter sur l'ordinateur, ce programme compilé s'appuie sur un composant logiciel primordial qui, lui, est spécifique à la machine et dont le rôle est de traduire le byte code générique dans le langage spécifique de la machine. Ce composant essentiel s'appelle une machine virtuelle Java (JVM en anglais, pour Java Virtual Machine).

L'avantage d'une telle architecture est considérable. L'éditeur de logiciel doit toujours gérer les différentes versions de sa machine virtuelle, mais ce travail n'est accompli qu'une fois ; dès que la machine virtuelle Java est disponible pour une plate-forme donnée, n'importe quel programme Java peut s'exécuter sur cette plate-forme.

D'autre part, elle présente un intérêt particulier sur le plan de la sécurité : à la différence des contrôles ActiveX, les applets Java ne s'exécutent pas directement par le processeur de votre ordinateur, mais sous le contrôle de la machine virtuelle Java qui s'interpose donc entre l'applet et les ressources du système. Ceci est d'autant plus appréciable que Sun a développé Java avec un souci de sécurité élevée. Outre une gestion de mémoire rigoureuse et l'utilisation d'un langage fortement typé (robuste grâce à une définition stricte des variables), une machine virtuelle Java intègre le concept de « bac à sable », métaphore imagée pour désigner un artifice astucieux : imaginez-vous empêtré jusqu'aux genoux dans un bac à sable, cherchant désespérément à exécuter votre passe préférée de tango argentin. C'est à peu près la manière dont s'exécute une applet Java, lorsque le navigateur ne lui accorde aucune confiance particulière. Sa capacité potentielle de nuisance est terriblement limitée car il lui est impossible d'accéder en lecture ou en écriture à un fichier du disque dur, elle ne peut supprimer aucun fichier de votre disque dur, elle ne peut accéder au réseau ni lancer d'exécutable présent sur votre poste. Bref, elle ne peut exécuter aucune opération illégale faisant appel à des privilèges élevés.

En théorie, le modèle Java et son gestionnaire de sécurité intégré offrent, dans leur conception, un environnement particulièrement sûr, élément appréciable lorsque l'on s'expose aux affres de la navigation sur Internet. Cependant, ce modèle a ses limites. Il arrive en effet que, pour des raisons de performance ou d'efficacité, certaines applets aient besoin d'accéder à votre disque dur, dans le cas, par exemple, où un message

d'erreur doit être journalisé sur le poste client. Dans certains cas, il devenait donc nécessaire de passer outre les limitations du bac à sable, étant entendu que ce privilège particulier ne pouvait être accordé qu'aux applets Java identifiées comme étant de confiance.

Ici encore, on se heurte au problème complexe que nous connaissons déjà : comment évaluer un code de provenance externe ? Une applet est considérée ainsi par la machine virtuelle Java en fonction de sa provenance (par exemple son URL source), ou lorsqu'elle dispose d'une signature électronique garantissant l'authenticité de son émetteur et l'intégrité de son contenu. Vous reconnaîtrez exactement la problématique que nous avions évoquée précédemment avec les contrôles ActiveX : le concept de certificat de signature s'applique aussi aux applets Java et les mêmes types de solutions sont envisagés. Il existe plusieurs manières de signer une applet : par le biais de la technologie Authenticode et selon les mêmes procédures que celles mises en œuvre avec les contrôles ActiveX, ou alors en utilisant les outils fournis par Netscape, dont Signtool, là aussi selon les mêmes procédures.

Lorsqu'une applet est signée, la JVM autorise son exécution à l'extérieur du bac à sable. Il serait peut-être exagéré, et un brin provocateur, d'affirmer que signer une applet est un moyen de contourner le bac à sable, qu'un processus conçu initialement pour plus de sécurité ait pour résultat moins de sécurité. Cependant, la JVM ne fournit dans ce cas aucun contrôle sur les intentions du code Java utilisant des privilèges élevés, et les conclusions exposées dans le paragraphe traitant de la sécurité d'Authenticode restent valables.

Il existe un autre cas de figure où la protection du bac à sable peut, cette fois, être sérieusement mise à mal : la sécurité du modèle dépend de la sûreté de l'implémentation de la JVM. Comme tout composant logiciel, celle-ci est potentiellement sujette à des vulnérabilités, et des attaques ont montré dans le passé qu'une applet non identifiée comme étant de confiance pouvait s'échapper du bac à sable et exécuter le code arbitraire de son choix. Fort heureusement, les éditeurs publient les correctifs nécessaires, mais de telles attaques restent possibles.

Autres formes de risques liés aux contenus exécutables

Les navigateurs savent interpréter beaucoup plus que de l'HTML. Outre les contrôles ActiveX et les applets Java, les pages web contiennent plusieurs autres formes de contenus exécutables, tels que les modules externes (plug-ins) ou les scripts.

Modules externes ou plug-ins

Un peu à la manière des contrôles ActiveX et des applets Java, les modules externes (ou plug-ins) sont des applications auxiliaires qui étendent les fonctionnalités des navigateurs comme Firefox ou Netscape Navigator. Une fois votre navigateur opérationnel, un plug-in peut s'installer ultérieurement (en général lorsque vous consultez une page qui le requiert), et s'exécute dans le contexte même du navigateur. Parmi les modules auxiliaires connus, on peut citer par exemple Apple Quick Time, Flash Player et Shockwave de Macromedia, Adobe Acrobat Reader ou Sun Java. Tout comme les autres paradigmes de code mobile, les modules externes permettent d'exécuter de petites applications, comme des films, des animations et des jeux.

Scripts

Une autre forme de contenu exécutable souvent rencontré au sein des pages HTML est le script. Un script est un petit programme dont le code exécutable est rapatrié de la façon suivante à partir d'un serveur accessible sur Internet :

```
<script src="http://serveurDistant.com/scripts/bookmark.js"></
script>
```

Il peut également s'agir d'un petit programme dont le code source fait lui-même partie de la page HTML. Si vous visualisez le code source des pages web que vous consultez, vous avez toutes les chances de constater la présence de scripts semblables à celui-ci :

```
<script>
<!--
// Engendrer un nombre aléatoire
var time = new Date();
var ordval = (time.getTime());
//-->
</script>
```

Or, il ne faut jamais oublier qu'un code exécutable peut avoir été conçu à des fins malveillantes, et qu'il représente une porte d'accès potentielle pour un pirate désireux de lancer une attaque crapuleuse, d'espionner ou de prendre le contrôle à distance de votre système informatique. Même si cette phrase est encore une fois un symptôme de la paranoïa aiguë de l'expert, en prendre conscience est un premier pas vers plus de sécurité, et il ne faut pas négliger les réglages des paramètres de sécurité de votre navigateur (voir sections suivantes). Parfois, en fonction de votre contexte d'utilisation, il faut même aller jusqu'à déconnecter votre poste Internet de votre réseau interne.

B.A.-BA

Afficher le code source d'une page HTML

- *Affichage>Code source de la page* sous Firefox ;
- *Afficher>Source de la page* sous Netscape ;
- *Affichage>Source* sous IE.

Cookies

Si vous décidez de construire une application web de manière à ce qu'elle soit accessible à des millions d'utilisateurs, vous aurez certainement besoin, au cours de son exécution, de gérer des données entrées par ces utilisateurs. Il peut s'agir de la réponse à un questionnaire, du contenu d'un panier de commande, ou encore de données d'administration relatives à la session. Certaines auront un caractère volatil et un rôle limité à la durée de la session. En revanche, d'autres, comme le profil ou les préférences de l'utilisateur, pourraient être utiles pour optimiser ses prochaines visites. Vous allez donc essayer de mémoriser une partie de ces données. Cependant, vous vous heurtez à un problème de taille : HTTP, le protocole de transmission entre navigateurs clients et serveurs web, ne gère pas l'état d'une session. Il ne conserve aucun des résultats obtenus au cours des interactions entre un client et un serveur et ne permet donc d'exploiter aucune antériorité. En bref, il est amnésique !

Vous pourriez, par exemple, adjoindre une base de données à votre application, et gérer, ainsi, vous-même, les données de chaque utilisateur. En allouant un espace de 10 Ko par utilisateur, et en prévoyant dix millions de visiteurs, il vous faudrait créer une base de données d'environ 100 Go, ce qui est acceptable. Cependant, la gestion d'une telle base de données représente une contrainte non négligeable, d'autant que cette base hébergera en permanence des données qui ne serviront que très épisodiquement, voire plus du tout, si l'utilisateur ne revient plus sur le site.

Les cookies offrent une solution plus astucieuse. Les informations à conserver sont entièrement liées à l'utilisateur et lui profitent exclusivement. Aussi, pourquoi ne pas les stocker sur son poste ? Pourquoi ne pas se servir des ressources de son ordinateur pour héberger des données qui lui sont propres ?

En toute rigueur, il n'existe pas toujours une relation aussi simple entre le poste client et l'utilisateur. En effet, il arrive que le poste Internet du bureau soit accessible à plusieurs utilisateurs, ou que vous accédiez à vos sites favoris à la fois depuis le bureau et depuis votre domicile, en utilisant deux machines différentes. Il arrive également que des postes usagés disparaissent de la circulation. Le concept n'est pas parfait, mais ce n'est pas vraiment gênant étant donné le caractère éphémère du cookie. L'utilisation généralisée des cookies sur le Web montre clairement qu'une solution consistant à tirer parti de la puissance de calcul et de la capacité de stockage de millions d'ordinateurs est très simple et efficace. Plus de base de données, plus de fichiers gigantesques, juste quelques petits fichiers stockés ici et là sur les ordinateurs qui, justement, veulent accéder à votre application !

En définitive, un cookie est tout simplement un petit fichier texte hébergeant des informations grâce auxquelles l'application web personnalise et gère au mieux vos visites. Un cookie est la mémoire d'HTTP et ce protocole offre un mécanisme explicite permettant d'échanger, d'écrire et de gérer les cookies lors d'une session entre un serveur web et un client.

Évidemment, cet outil n'est pas sans danger. Les cookies fournissent un lien fort entre une application web et des millions de postes clients situés n'importe où dans le monde. Ce petit mécanisme représente potentiellement un formidable outil de contrôle. L'homme cherche toujours à détourner à son profit les moyens dont il dispose ; pourquoi le cookie ferait-il exception ? Du moment que des informations vous concernant sont mémorisables, qui empêche l'application serveur, pour des raisons de marketing par exemple, de mémoriser vos habitudes, vos préférences, vos goûts, vos moyens de paiement, bref, des informations personnelles, voire sensibles ? Certes, les cookies contiennent uniquement les informations que vous fournissez au serveur, mais êtes-vous sûr de pouvoir décider des informations stockées dans les cookies, comme vos clics de souris ou les pages que vous visitez ? En effet, les cookies peuvent mettre en jeu des données plus sensibles. Avez-vous déjà défini des éléments d'authentification pour accéder au site de votre banque ? Où pensez-vous que ces éléments ont été stockés ? Imaginez qu'un vilain pirate décide de s'emparer de vos cookies. S'il réussit à développer un site web suffisamment attractif, vous viendrez y consulter quelques pages HTML ; en fait, son objectif caché est d'injecter sur votre poste un script JavaScript, code mobile soigneusement développé par ses soins et qui contient, entre autres, un code spécialement conçu pour rapatrier vos cookies sur sa machine. L'attaque ayant réussi, il peut désormais se connecter en votre nom sur vos sites favoris, et cela, sans avoir à fournir votre mot de passe. Il peut donc rejouer vos sessions antérieures et, pourquoi pas, accéder à votre compte en banque.

AVANCÉ **Emplacement des cookies**

Selon la nature des informations auxquelles ils se rapportent, les cookies sont gérés en mémoire vive ou stockés sur le disque dur de l'utilisateur. Sous Windows, on les trouve le plus souvent dans `%userprofiles%\Cookies`.

Fonctions de sécurité offertes par les navigateurs

Les navigateurs offrent de nombreux outils pour renforcer la sécurité de votre poste et, par voie de conséquence, de votre site. Ces derniers contribuent de manière significative à élever le niveau de sécurité de votre installation et, surtout, couvrent un secteur que seuls les navigateurs sont capables de contrôler. Ils permettent notamment de :

- définir des politiques de sécurité en fonction des sites visités ;
- régler précisément de nombreux paramètres de sécurité ;

À RETENIR

Mécanismes de sécurité des navigateurs

En toute rigueur, il ne faut pas avoir une confiance aveugle en la robustesse des mécanismes implantés dans les navigateurs Internet. D'une part, ils apportent leur petit lot de vulnérabilités à votre système (comme tout composant logiciel). D'autre part, retenez que l'un des ennemis majeurs de la sécurité est le nombre de lignes de code.

- contrôler les accès aux sites Internet en fonction des types d'URL ou du contenu des sites ;
- activer et gérer vos certificats de sécurité ;
- lutter contre les messages non sollicités.

Nous allons maintenant expliquer concrètement comment configurer votre navigateur au mieux pour limiter les risques d'attaques.

Sécuriser Internet Explorer

En naviguant sur Internet, vous consulterez forcément, à un moment ou à un autre, des sites faisant appel aux codes mobiles. Après avoir consciencieusement lu les pages précédentes de cet ouvrage, il se peut que votre confiance se soit quelque peu émoussée, et que, par précaution, vous décidiez de désactiver totalement les codes mobiles dans votre navigateur ; c'est une approche radicale, mais qui a au moins le mérite d'être efficace. Cependant, désactiver les codes mobiles risque de vous poser problème lors de la consultation de sites basés essentiellement sur cette technologie. Par exemple, lorsque vous vous connectez au site Windows Update de Microsoft, des contrôles ActiveX analysent les logiciels installés sur votre machine et procèdent au téléchargement et à l'installation des correctifs nécessaires. Or, si les contrôles ActiveX sont désactivés dans votre navigateur, les mises à jour automatiques ne pourront pas avoir lieu. En revanche, pour explorer les sites que vous ne connaissez pas, vous voudrez peut-être restreindre, voire désactiver totalement, l'exécution des codes mobiles.

Idéalement, il faudrait pouvoir adapter le niveau de protection délivré par votre navigateur au risque potentiel du site visité. Cependant, vous en conviendrez, il serait fastidieux de modifier manuellement ces paramètres de sécurité pour chaque nouveau site web visité. En effet, votre navigation vous conduit inévitablement vers des sites inconnus, et vous expose donc à l'ingérence de sites tiers (publicité par exemple). Vous pouvez également avoir plusieurs sessions actives simultanément, chaque session impliquant un niveau de confiance différent.

C'est pourquoi Microsoft propose de définir des zones de sécurité. Ces dernières concilient une sécurisation graduée des sessions web interactives avec les impératifs de la navigation et la facilité de mise en œuvre et d'utilisation.

Internet Explorer propose, pour chaque zone, des paramètres par défaut. Cela vous permet donc de mettre tout de suite en œuvre les zones de sécurité sans avoir à vous soucier de leur configuration. Cependant, vous pouvez personnaliser le niveau de sécurité de votre poste en choisissant vous-même la valeur des paramètres pour chaque zone. Ainsi, vous adaptez votre niveau de protection à vos besoins spécifiques et à votre

contexte d'utilisation, et vous renforcez le niveau de sûreté de votre ordinateur relié à Internet.

> DÉFINITION **Zones de sécurité**
>
> Pour expliciter de façon simple ce concept, on peut dire qu'une zone de sécurité correspond à un niveau de sécurité prédéfini, que le navigateur applique automatiquement lorsque vous consultez les sites web affectés à cette zone.
> Vous disposez de plusieurs zones et le navigateur peut mettre en œuvre simultanément plusieurs politiques de sécurité et appliquer en temps réel des contrôles et des filtrages différents selon les sites visités.
> Autrement dit, vous pouvez explicitement répertorier le site Windows Update dans une zone dite « de confiance », dans laquelle vous autorisez les contrôles ActiveX, tandis que, par défaut, les autres sites seront rattachés à une autre zone (baptisons-la pour le moment « autres sites »), dans laquelle tous les codes mobiles seront filtrés. Lorsque vous naviguez sur Internet, vous bloquez donc les codes mobiles en provenance de sites inconnus, tout en autorisant ceux émanant de sites auxquels vous faites confiance.

Zones de sécurité prédéfinies

Internet Explorer gère cinq zones de sécurité : *Internet*, *Intranet local*, *Sites de confiance*, *Sites sensibles* et *Poste de travail*.

La configuration de la zone *Poste de travail* est accessible à partir d'un outil d'administration séparé. Il est recommandé que, seul, un administrateur averti procède à une modification éventuelle du réglage des paramètres de cette zone.

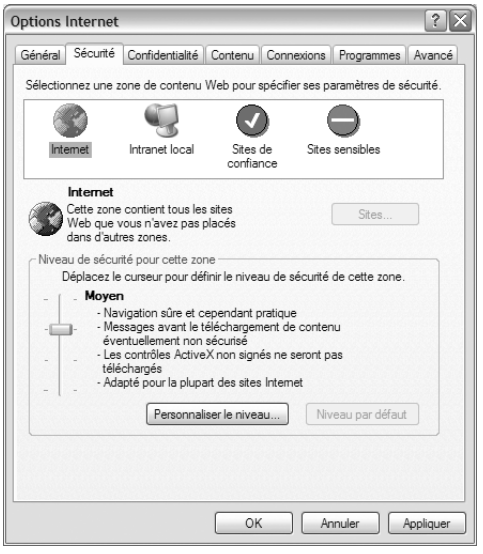


Figure 7–2
Zones de sécurité accessibles à l'utilisateur

Pour accéder aux zones de sécurité accessibles à l'utilisateur, choisissez *Outils>Options Internet* et cliquez sur l'onglet *Sécurité*.

- **Zone** *Sites sensibles* – Affectez à cette zone les sites en lesquels vous n'avez pas confiance, mais que vous consultez à la rigueur à condition d'être protégé par une barrière dissuasive, au détriment éventuel de la qualité de la navigation. Dans cette zone, le niveau de sécurité par défaut est positionné sur *Élevé*. Les paramètres de sécurité y sont réglés de manière à filtrer les contenus actifs : les composants signés ou non avec Authenticode, les contrôles ActiveX et les plug-ins sont désactivés. Par ailleurs, tous les cookies sont bloqués.
- **Zone** *Sites de confiance* – Affectez à cette zone les sites auxquels vous accordez une grande confiance (les sites qui n'ont pas vocation à manipuler d'objets malveillants). Par défaut, le niveau de sécurité est positionné sur *Faible* et aucun site n'est affecté à cette zone. Si vous affectez un site à la zone *Sites de confiance*, le chargement de contrôles ActiveX non signés et de scripts ActiveX non marqués est soumis à votre approbation. Par ailleurs, les cookies sont autorisés et enregistrés, les contenus actifs sont téléchargés et exécutés, sans qu'aucun message d'avertissement ne soit affiché à l'écran (il est peut-être judicieux de modifier ce paramétrage afin que vous soyez au moins averti au moment du téléchargement d'un contenu actif).
- **Zone** *Intranet local* – Cette zone concerne les sites web situés sur votre réseau intranet local et ceux dont les noms ne contiennent pas de points (http://local). Elle concerne aussi les connexions réseau établies en utilisant un chemin UNC (de la forme \\serveur\partage). Le niveau de sécurité par défaut est *Moyen* ou *Moyennement bas*. Il autorise l'exécution de composants signés ou non avec Authenticode, les contrôles ActiveX reconnus sûrs pour l'écriture de scripts, les scripts des applets Java et les cookies. Cependant, il désactive le téléchargement des contrôles ActiveX non signés.
- **Zone** *Internet* – Par défaut, le navigateur affecte à la zone *Internet* tous les sites que vous n'avez pas explicitement placés dans les zones précédentes. Par défaut, le niveau de sécurité de cette zone est positionné sur *Moyen*. On peut légitimement penser que ce choix a été guidé par le désir de faciliter une navigation plus conviviale. Avec Internet Explorer doté du Service Pack 2, les contrôles ActiveX non signés ne sont pas téléchargés par défaut, et le téléchargement de contrôles ActiveX signés est soumis à votre approbation. D'autre part, l'exécution des composants signés ou non avec Authenticode, des contrôles ActiveX reconnus sûrs pour l'écriture de scripts ainsi que des scripts d'applets Java est autorisée. En outre, la zone *Internet* ne bloque pas tous les cookies.

Bon sens **Sites « dangereux »**

Il n'y a qu'une seule manière de procéder avec les sites « dangereux » : les éviter. Si, pour une raison ou pour une autre, vous devez tout de même vous connecter à ce genre de site, affectez-les à la zone *Sites sensibles*.

Chemin UNC

Selon l'excellente définition proposée par le jargon français (www.linux-france.org) :
« *Universal Naming Convention. Convention de nommage universelle, mais seulement sous Windows, et tant qu'il n'est question que de nommer des disques partagés (et guère autre chose). Une adresse UNC a la forme :* « *\\Serveur\Partage* ».

Attention **Sites de la zone** *Internet*

Si vous ne gérez pas les zones de sécurité, vous accéderez à la grande majorité des sites web avec les paramètres de sécurité de la zone *Internet*. Il est donc fondamental de régler minutieusement ces paramètres.

Comme vous pouvez le constater, les zones de sécurité n'ont rien à voir avec les zones géographiques, elles ne représentent que des niveaux de sécurité. Aussi êtes-vous parfaitement libre d'affecter manuellement tel ou tel site web à la zone *Sites sensibles*, *Sites de confiance* ou *Intranet local*.

> **CONSEIL Personnalisez vos paramètres de sécurité**
>
> La configuration par défaut proposée par les navigateurs n'élimine pas tous les risques, mais représente un bon compromis entre niveau de sûreté et facilité d'utilisation. Cependant, si vous êtes familier des paramètres de sécurité, n'hésitez pas à modifier le réglage par défaut de toutes les zones afin de renforcer la sécurité de votre navigation.
> Si vous êtes paranoïaque (et en matière d'informatique en réseau, c'est loin d'être un défaut !), adoptez une politique de sécurité plus restrictive. Réglez les paramètres de sécurité de la zone *Internet* à ceux de la zone *Sites sensibles* (c'est-à-dire interdisez tout ou presque). Réglez les paramètres de la zone *Intranet local* à ceux de la zone *Internet*. Affectez nominativement les sites auxquels vous faites confiance à la zone *Intranet local* ou *Sites de confiance*.

Pour vous aider à modifier la valeur des paramètres de sécurité, la section suivante propose une explication succincte pour chacun d'eux.

Paramètres de sécurité affectés à chaque zone

Pour accéder aux zones de sécurité, choisissez *Outils>Options Internet* et cliquez sur l'onglet *Sécurité* (voir figure 7-2).

Pour chaque zone de sécurité, vous pouvez positionner le niveau de sécurité sur *Élevé*, *Moyen*, *Moyennement bas*, *Faible* ou *Personnalisé* : faites glisser la réglette jusqu'à atteindre le niveau désiré, puis cliquez sur *OK*.

Figure 7–3
Paramètres de sécurité de la zone Internet

Vous avez en outre la possibilité de modifier les paramètres d'un niveau de sécurité donné. Pour cela, choisissez la zone que vous souhaitez configurer, par exemple la zone *Internet* et cliquez sur le bouton *Personnaliser le niveau*. L'écran qui apparaît ressemble à celui de la figure 7-3.

Faites défiler la liste des paramètres et modifiez les valeurs à votre convenance en cliquant sur les boutons radio correspondants. Pour définir la politique de sécurité la mieux adaptée à votre façon de travailler, il n'y a pas de règle. En effet, les réglages optimaux seront différents suivant l'utilisation que vous faites de l'ordinateur qui vous permet d'accéder à Internet (machine dédiée ou non, machine reliée ou non à votre réseau informatique interne, présence ou non d'informations sensibles sur le disque dur, etc…).

Les paramètres sont répartis dans plusieurs rubriques (*Authentification utilisateur*, *Composants dépendants du .NET framework*, *Contrôles ActiveX et plugins*, *Divers*, *Microsoft VM*, *Script*, *Téléchargement*). Une première série de réglages concerne notamment les méthodes d'authentification de l'utilisateur par rapport aux sites web distants et les comportements des navigateurs vis-à-vis des codes mobiles (voir figure 7-3).

Pour la plupart des paramètres, vous avez le choix entre *activer* (par exemple activer automatiquement le téléchargement ou l'exécution du code mobile), *désactiver*, ou *demander* à être averti afin d'autoriser/refuser manuellement le téléchargement ou l'exécution.

IDÉALEMENT Machine dédiée à la navigation sur Internet

Une solution simple et sûre pour accéder à Internet consiste à utiliser une machine dédiée, ne contenant aucune donnée confidentielle, et qui ne soit pas reliée à votre réseau interne. Si vous pouvez vous permettre cela, empressez-vous d'oublier les zones de sécurité. La configuration par défaut proposée par le navigateur peut être utilisée sans souci.

Tableau 7–1 Paramètres de sécurité d'Internet Explorer

Paramètre de sécurité		Explication
Authentification utilisateur		Les serveurs auxquels vous vous connectez (serveurs Intranet, serveurs web externes) exigent parfois que vous vous authentifiiez lors de l'ouverture d'une session ou lors de l'accès à certaines pages protégées. Ces paramètres spécifient la manière dont le navigateur vous authentifie auprès des serveurs distants.
	Connexion automatique avec le nom d'utilisateur et le mot de passe actuel	Si vous activez cette option, le navigateur vous authentifie automatiquement auprès du serveur, en utilisant votre nom et votre mot de passe actuels. Cette méthode d'authentification est transparente pour vous, mais dévoile vos secrets. C'est un peu comme si vous confiiez les clés de votre propre maison à la consigne de la gare pour qu'on vous ouvre la porte au moment de déposer et de récupérer les bagages. Il est par conséquent fortement déconseillé d'employer cette méthode, surtout avec les sites web externes situés sur Internet. Attention, cette option est activée par défaut dans la zone *Sites de confiance*.
	Connexion automatique uniquement dans la zone intranet	Le navigateur procède à votre authentification automatique, seulement si le serveur qui en fait la demande est situé sur votre intranet local. Cette option est pratique. Si vous avez confiance dans votre intranet, ce qui est généralement le cas, vous pouvez envisager cette option (elle est positionnée par défaut dans la zone *Intranet local*).

Tableau 7–1 Paramètres de sécurité d'Internet Explorer (suite)

Paramètre de sécurité		Explication
	Demander le nom d'utilisateur et le mot de passe	Si vous choisissez cette option, le système vous invite à entrer un nom d'utilisateur et un mot de passe. C'est de loin l'option la plus sûre, à condition toutefois de ne pas choisir un identifiant et un mot de passe susceptibles de trahir un secret de votre machine ou de votre réseau ! N'oubliez pas que ces informations peuvent être interceptées sur Internet et que, de toutes façons, elles seront désormais connues du site distant.
	Ouverture de session anonyme	L'ouverture de session avec le site web distant s'effectue sans que vous fournissiez d'éléments d'authentification. Une session anonyme est alors ouverte, ce qui implique éventuellement un accès restreint au site distant.
Composants dépendants du .NET framework		
	Exécuter les composants non signés avec Authenticode	Un contrôle qui ne dispose pas d'un certificat d'éditeur valide peut être malveillant, il peut accéder et/ou modifier votre système de fichiers, installer des logiciels espions, etc. Pour une navigation plus sûre, et en dépit d'inconvénients possibles lors de l'affichage de certaines pages web, il est recommandé de choisir l'option *désactiver*. Attention, la zone *Internet* active par défaut l'exécution des composants non signés avec Authenticode.
	Exécuter les composants signés avec Authenticode	Les composants signés avec Authenticode sont réputés plus sûrs que les autres. N'oubliez pas toutefois que la technologie Authenticode authentifie **l'auteur** du contrôle ActiveX, mais ne fournit aucune garantie en ce qui concerne **le contenu** du contrôle ActiveX et les actions qu'il peut intenter sur votre machine. Vous pouvez à la rigueur accepter l'option *Activer*. Le paranoïaque choisira l'option *Demander*.
Contrôles ActiveX et plugins		
	Comportements de fichiers binaires et de scripts	Option désactivée dans la zone *Sites sensibles*.
	Contrôles ActiveX reconnus sûrs pour l'écriture de scripts	Option recommandée : *Demander*.
	Contrôles d'initialisation et de scripts ActiveX non marqués comme sécurisés	Option recommandée : *Désactiver*.
	Demander confirmation pour les contrôles ActiveX	Option recommandée : *Demander*.
	Exécuter les contrôles ActiveX et les plugins	Option recommandée : *Demander*.
	Télécharger les contrôles ActiveX non signés	La zone *Internet* désactive cette option par défaut. Ce choix est recommandé.
	Télécharger les contrôles ActiveX signés	Ce paramètre spécifie quelle doit être l'attitude du navigateur lorsqu'il s'apprête à télécharger un contrôle ActiveX qui dispose d'un certificat de signature Authenticode. Par défaut, la zone *Internet* demande votre accord avant de procéder au téléchargement.
Divers		
	Accès aux sources de données sur plusieurs domaines	Spécifie si le composant connecté à une source de données est autorisé ou non à accéder à des sources de données situées sur des domaines autres que celui de la page web visitée. Option recommandée : *Désactiver*.

Tableau 7–1 Paramètres de sécurité d'Internet Explorer (suite)

Paramètre de sécurité		Explication
	Affiche un contenu mixte	Spécifie si les pages web peuvent afficher des contenus en provenance de serveurs sécurisés et non sécurisés. Option recommandée : *Demander*.
	Glisser-déplacer ou copier-coller les fichiers	Détermine si l'utilisateur a le droit de glisser-déplacer ou de copier-coller des fichiers à l'intérieur de la zone. Option recommandée : *Activer* (il est fait l'hypothèse que les fichiers corrompus seront détectés par l'antivirus).
	Installation des éléments du Bureau	Détermine si l'utilisateur a ou non le droit d'installer des éléments du Bureau à partir d'une page web située à l'intérieur de la zone. Option recommandée dans la zone *Internet* : *Désactiver*.
	Lancement des programmes et des fichiers dans un IFRAME	Un IFRAME est un cadre qui s'affiche au milieu d'une page web, servant à visualiser un site extérieur sans obliger l'utilisateur à quitter la page en cours. Option recommandée : *Désactiver*.
	Navigation de sous-cadres sur différents domaines	Autorise ou non l'utilisateur à naviguer sur plusieurs domaines dans différents sous-cadres de la page. Option recommandée : *Activer*.
	Ne pas demander la sélection d'un certificat client lorsqu'il n'existe qu'un seul certificat ou aucun	Option recommandée : *Désactiver*. L'utilisateur sera invité à sélectionner un certificat.
	Permanence des données utilisateur	Autorise ou non les pages web de la zone à sauvegarder des informations personnelles sur le poste. Option recommandée : *Désactiver*.
	Soumettre les données de formulaire non codées	Autorise ou non les utilisateurs à soumettre des formulaires lorsque la liaison navigateur/serveur n'est pas chiffrée. Option recommandée : *Demander*.
	Utiliser le bloqueur de fenêtres publicitaires intempestives	Option recommandée : *Activer*.
Script		
	Active scripting	Détermine si IE peut ou non exécuter des scripts à partir de pages web de la zone. Pour une sécurité optimale, dans la zone *Internet* choisir *Désactiver*. Au besoin, inclure nominativement les sites non dangereux dans la zone *Sites de confiance* et activer cette option.
	Permettre les opérations de collage via le script	Option recommandée : *Désactiver*. Une page web ne doit pas pouvoir accéder en écriture au disque local de la machine.
	Script des applets Java (en anglais scripting of Java applets)	Option recommandée sur la zone *Internet* : *Désactiver*. Empêche les scripts d'accéder aux applets Java.
Téléchargement		
	Demander confirmation pour les téléchargements de fichiers	Option recommandée : *Désactivée*.
	Téléchargement de fichiers	Détermine si IE autorise ou non le téléchargement de fichiers à partir d'un serveur situé sur la zone. Option recommandée : *Activer* (l'antivirus empêchera le téléchargement en cas de fichier contaminé).
	Téléchargement de polices	Détermine si IE autorise ou non le téléchargement de polices HTML à partir d'un serveur situé sur la zone. Option recommandée : *Activer* (l'antivirus empêchera le téléchargement en cas de fichier contaminé).

Affecter un site web à une zone de sécurité

Pour affecter un site web à une zone de sécurité autre que *Internet*, choisissez la zone et cliquez sur le bouton *Sites* (voir figure 7-2). Sélectionnez l'adresse URL à partir de la liste déroulante ou saisissez-la dans le champ *Zone* et cliquez sur *Ajouter*. Si vous souhaitez assigner un site à la zone *Intranet local*, il faudra d'abord cliquer sur *Sites*, puis sur *Avancé*, et procéder de la même façon.

Vous pouvez restreindre une zone à des sites basés uniquement sur le protocole sécurisé HTTPS en cochant l'option *Nécessite un serveur sécurisé (https) pour tous les sites dans cette zone*.

Paramètres de « confidentialité »

Allez maintenant sous *Outils>Options Internet*, onglet *Confidentialité* ; vous devriez obtenir un écran semblable à celui de la figure 7-4.

Figure 7–4
Niveaux de confidentialité de la zone Internet

Une seconde série de paramètres concerne spécifiquement les cookies à l'intérieur de la zone *Internet*. Expliquons d'abord les termes utilisés par le navigateur (tableau 7-2).

VOCABULAIRE Confidentialité

Les navigateurs proposent généralement la terminologie un peu imprécise de « confidentialité ». Or, en réalité, le terme de confidentialité est plutôt réservé au domaine du chiffrement des données.

Cookie « tiers »

Lorsque vous consultez un site web, ce dernier est dit « nominatif ». Cependant, une partie du contenu qu'il fournit peut très bien provenir d'un autre site, notamment la publicité. Cet autre site est appelé site « tiers » ou « de tiers ». Le mécanisme de gestion des cookies fonctionnant avec tous les sites web, il n'y a pas de raison pour que les sites tiers s'interdisent d'échanger des cookies avec votre poste. Au contraire, ils en usent sans réserve… Il s'agit alors de cookies « tiers ».

Tableau 7–2 Les différents types de cookies

Types de cookies	Explication
Cookies tiers qui n'ont pas de stratégie de confidentialité compacte	Une stratégie de confidentialité compacte est conforme aux standards P3P (Platform for Privacy Preferences). Rassurez-vous, pas besoin de chercher à décrypter un tel jargon. Il existe une façon simple de se débarasser de ce genre de problème : bloquer.
Cookies tiers qui utilisent des informations d'identification personnelles sans votre consentement	Les cookies tiers peuvent utiliser, sans votre consentement (à des fins de marketing par exemple), des informations telles que votre nom, vos numéros de téléphone, l'adresse de votre domicile, votre adresse de messagerie ou d'autres informations privées.
Cookies internes qui utilisent des informations d'identification personnelles sans votre consentement	Même type de cookie, sauf qu'ils proviennent du site nominatif.

Pour gérer les cookies, vous avez le choix d'affecter à la zone *Internet* plusieurs niveaux de sécurité (ou niveaux de « confidentialité »). La zone *Internet* est configurée par défaut à un niveau de confidentialité *Moyen* : seuls les cookies tiers sont bloqués, et les cookies utilisant des informations personnelles sans votre consentement sont simplement restreints. Pour modifier le niveau de protection, faites coulisser le curseur sur la réglette et cliquez sur *OK*. Le bouton *Avancé* vous permettra en outre de préciser explicitement ce que le navigateur doit faire des cookies internes et des cookies tiers.

ASTUCE **Cookies « tiers »**

Une façon simple de gérer les cookies tiers : les bloquer sans restriction.

Tableau 7–3 Niveaux de confidentialité proposés pour la zone Internet

Niveaux de confidentialité de la zone Internet	Paramétrage du navigateur
Bloquer tous les cookies	Les cookies de tous les sites web seront bloqués. Les cookies existants sur votre ordinateur ne peuvent pas être lus par les sites web.
Haute	Bloque les cookies qui n'ont pas de stratégie de confidentialité compacte. Bloque les cookies qui utilisent des informations d'identification personnelles sans votre consentement.
Moyennement haute	Bloque les cookies tiers qui n'ont pas de stratégie de confidentialité compacte. Bloque les cookies tiers qui utilisent des informations d'identification personnelles sans votre consentement. Bloque les cookies internes qui utilisent des informations d'identification personnelles sans votre consentement.
Moyenne	Bloque les cookies tiers qui n'ont pas de stratégie de confidentialité compacte. Bloque les cookies tiers qui utilisent des informations d'identification personnelles sans votre consentement. Restreint les cookies internes qui utilisent des informations d'identification personnelles sans votre consentement.
Basse	Restreint les cookies tiers qui n'ont pas de stratégie de confidentialité compacte. Restreint les cookies tiers qui utilisent des informations d'identification personnelles sans votre consentement.
Accepter tous les cookies	Tous les cookies seront sauvegardés sur cet ordinateur. Les cookies existants sur cet ordinateur peuvent être lus par les sites web qui les ont créés.

ASTUCE **Durée de vie des cookies**

Dans les cas où un site vous oblige à accepter les cookies, une parade consiste à accepter uniquement les cookies de session (*Outils>Options Internet>Confidentialité>Avancé*).

AVANCÉ
Politique de confidentialité des sites

Idéalement, il faudrait que vous lisiez la politique de confidentialité publiée par les sites que vous visitez (accessible dans *Afficher>Infos page>Confidentialité>Politique*) avant de définir de façon pertinente certains paramètres. Il semble illusoire de penser qu'une telle démarche soit adoptée par la plupart des utilisateurs ; par ailleurs, il n'est pas fréquent de voir un site publier sa politique de confidentialité et, à supposer qu'elle existe, il s'agit souvent d'une simple déclaration d'intention.

À NOTER **Option Demander avant de mémoriser un cookie**

Elle présente au moins un intérêt : vous faire prendre conscience à quel point l'écriture et la modification d'un cookie sur votre poste est une opération fréquente. Pour avoir la paix, vous la désactiverez bien vite !

Le paranoïaque choisira probablement l'option *Bloquer tous les cookies*. En cas de gêne de navigation, l'option *Haute* pourra être sélectionnée ou, à la rigueur, *Moyennement haute*, mais pas en deça.

Sécuriser Netscape Navigator

Comme vous l'avez probablement constaté, le paramétrage de sécurité d'IE est très puissant, mais il provoque de légères migraines. Netscape aborde la gestion des paramètres de sécurité de façon plus simple et plus directe.

Préférences concernant les cookies

Pour définir vos préférences en matière de gestion des cookies :

- sélectionnez le menu *Édition* et choisissez *Préférences* ;
- dans la catégorie *Confidentialité et sécurité*, cliquez sur *Cookies*. Vous devriez voir apparaître l'écran présenté à la figure 7-5.

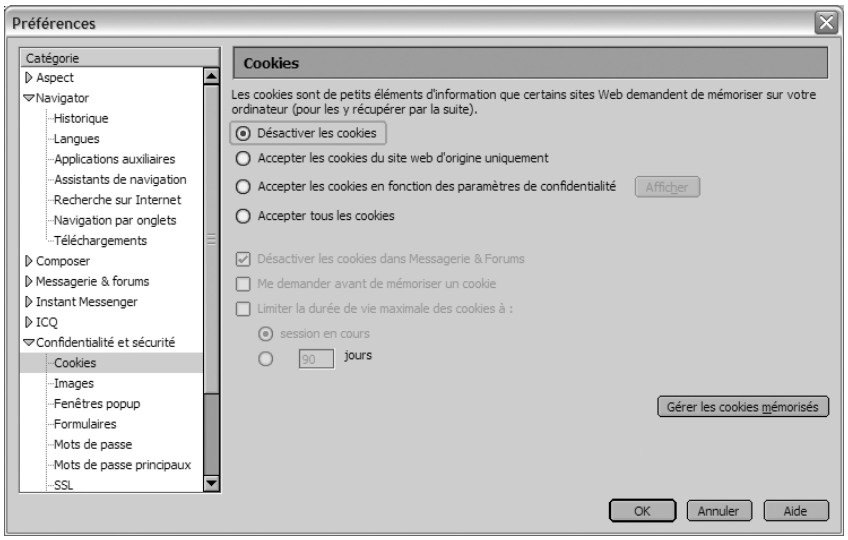


Figure 7–5
Gestion des cookies sous Netscape Navigator

Tableau 7–4 Paramètres de sécurité de Netscape Navigator

Paramètres de sécurité	Explication
Accepter tous les cookies	Attention, cette option est cochée par défaut.
Accepter les cookies en fonction des paramètres de confidentialité	Cette option vous permet de régler plus finement vos critères de filtrage. Certains sites web publient en effet une « politique de confidentialité », décrivant le type d'informations personnelles qu'ils collectent, à qui ils les communiquent, et comment ils les utilisent. En fonction de cela, vous avez la possibilité de définir votre politique d'acceptation des cookies pour les cookies uniques (correspondant aux cookies internes dans la terminologie Microsoft) et les cookies de tiers (cliquez pour cela sur le bouton *Afficher*).

Tableau 7–4 Paramètres de sécurité de Netscape Navigator (suite)

Paramètres de sécurité	Explication
Accepter les cookies du site web d'origine uniquement	Si vous cochez cette option, les cookies de tiers seront rejetés, seuls les cookies originaires du site que vous visitez seront acceptés.
Désactiver les cookies	Il s'agit d'une option simple mais efficace pour préserver la sécurité de votre poste.
Désactiver les cookies dans Messagerie & Forums	Cette option concerne votre messagerie. Si vous n'avez pas désactivé complètement les cookies, il vous est toutefois possible de désactiver ceux que vous recevez avec un message contenant une page web.
Me demander avant de mémoriser un cookie	Sans commentaire.
Limiter la durée de vie maximale des cookies à	Cette option peut servir à limiter la durée de vie d'un cookie à celle de la session. Cette option est intéressante si vous ne bloquez pas tous les cookies.

Vous avez la possibilité de visualiser le contenu des cookies stockés sur votre ordinateur et de les supprimer. Pour cela, cliquez sur le bouton *Gérer les cookies mémorisés*.

Selon la valeur de vos paramètres de confidentialité, une icône de notification de cookie peut apparaître dans la barre d'état, près de l'angle inférieur droit de la fenêtre du navigateur (voir figure 7-6).

Figure 7–6
Notification de blocage d'un cookie

Si vous cliquez sur cette icône, vous accéderez au rapport de confidentialité regroupant les informations complémentaires relatives aux sites concernés (figure 7-7).

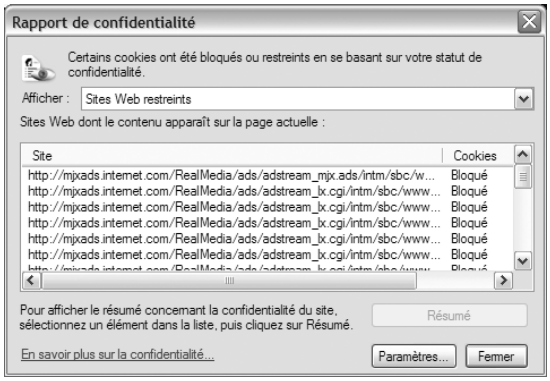


Figure 7–7
Rapport de confidentialité

Préférences concernant les scripts et plug-ins

Lorsque vous chargez une page web qui requiert l'installation d'un module externe sur votre poste, vous pouvez configurer Netscape pour qu'il procède selon l'une des deux méthodes exposées ci-après. Dans le menu *Édition>Préférences*, cliquez sur *Navigator*, puis sur *Applications auxiliaires* (voir figure 7-8).

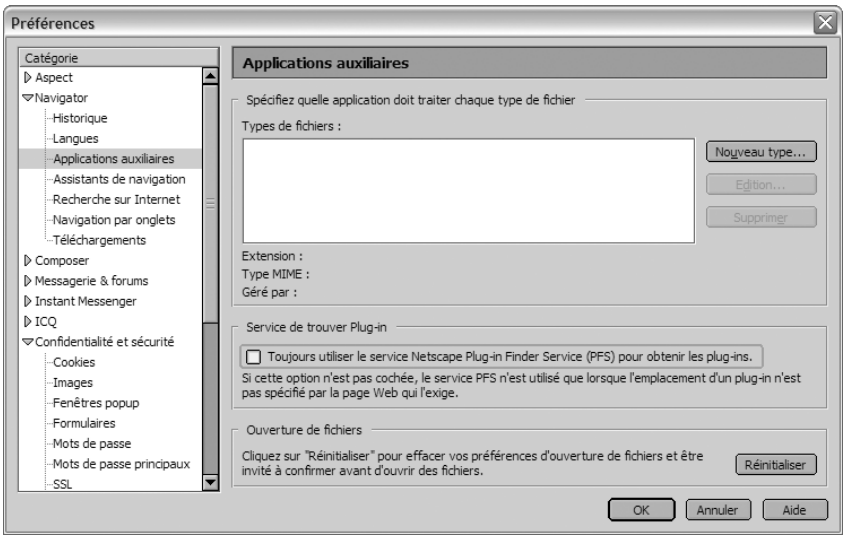


Figure 7–8
Mode de téléchargement des modules externes

Netscape dispose d'un service automatique de recherche de plug-ins (Netscape Plug-in Finder Service). Si vous cochez l'option *Toujours utiliser le service Netscape Plug-in Finder Service (PFS) pour obtenir les plug-ins*, Netscape lance une requête vers un script CGI situé sur le site netscape.com, chargé d'obtenir l'URL du site auprès duquel votre navigateur procédera lui-même à l'installation du nouveau module. Si vous ne cochez pas cette case, le téléchargement du module externe s'effectuera, après confirmation de votre part, auprès du site spécifié dans la page web que vous consultez.

Bien entendu, le paranoïaque aura tendance à faire confiance à Netscape pour trouver le bon plug-in, plutôt qu'à un site inconnu. Cependant, n'oubliez pas qu'il s'agit d'un code exécutable. Idéalement, la meilleure option serait, au préalable, d'installer manuellement les modules externes auxquels vous faites confiance, et de vous limiter à ceux-ci.

Préférences liées à l'interprétation des pages web

Ouvrez le menu *Édition>Préférences*, cliquez ensuite sur la catégorie *Avancé* (voir figure 7-9).

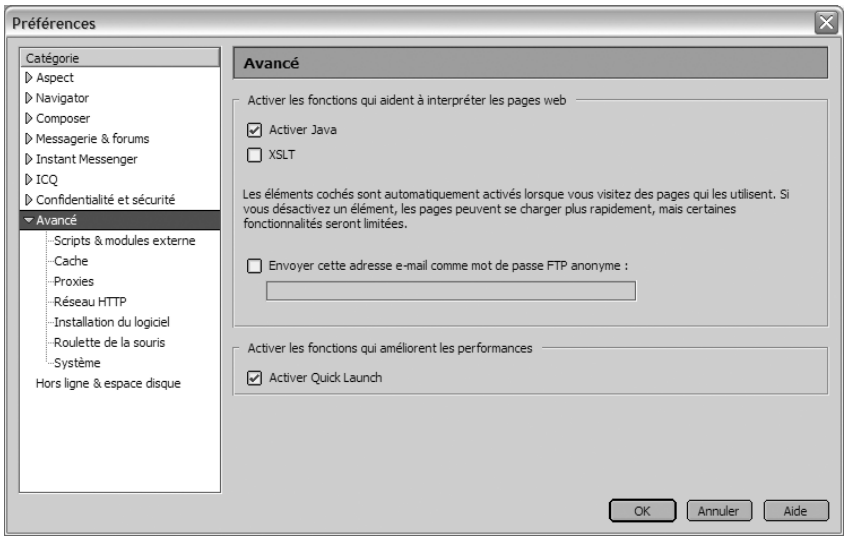


Figure 7–9
Paramètres de sécurité liés à l'interprétation des pages web

Étant donné le modèle de sécurité de Java, vous pourrez activer ce langage dans votre navigateur, sauf, bien entendu, si vous considérez que les risques résiduels exposés plus haut sont incompatibles avec le niveau de protection exigé pour votre poste.

En revanche, XSLT, un langage utilisé pour convertir les documents au format XML vers un autre format, comme HTML, devrait être désactivé, en raison du manque de connaissances actuel concernant son modèle de sécurité.

Préférences concernant les scripts

Il vous est possible de restreindre JavaScript et les modules externes sous Netscape. Ouvrez le menu *Édition>Préférences*. Cliquez ensuite sur la catégorie *Avancé*, puis sur *Scripts & modules externes*. L'écran de la figure 7-10 apparaît.

Netscape a été conçu de manière à interdire aux scripts d'appeler des fonctions susceptibles de mettre en danger votre ordinateur. Il existe toutefois des risques résiduels, principalement liés aux défauts d'implémentation de JavaScript ou aux attaques de type Cross Site Scripting. Cependant, désactiver JavaScript vous gênerait considérablement au cours de vos navigations. Il est donc recommandé d'activer JavaScript dans Navigator.

En revanche, nous vous conseillons de désactiver les codes mobiles dans *Messagerie & forums*.

RENVOI **Attaque de type Cross Site Scripting (XSS)**

Reportez-vous à l'annexe B pour toutes les définitions d'attaques.

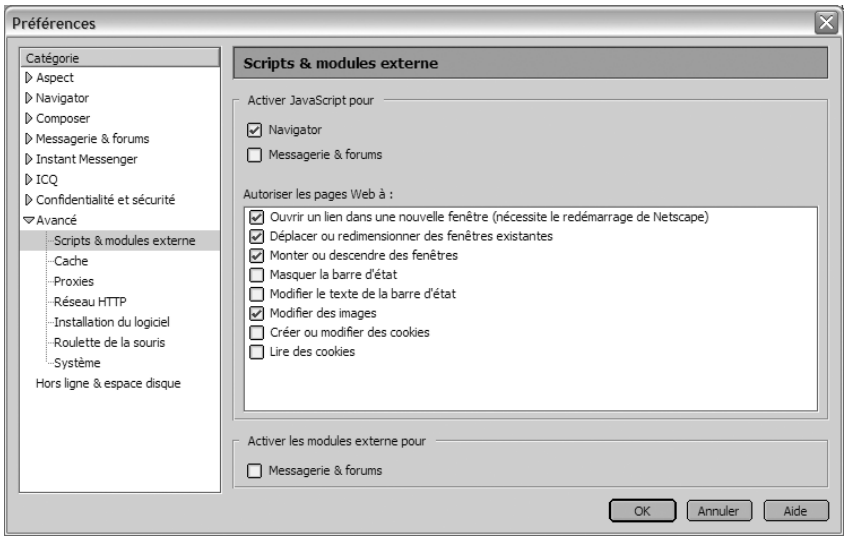


Figure 7–10
Paramètres de contrôle de l'utilisation de Javascript et des modules externes sous Netscape

En outre, il est recommandé d'interdire aux scripts contenus dans les pages web de masquer ou de modifier le texte de la barre d'état – qui sert notamment à afficher des informations sur le site que vous êtes en train de visiter. En effet, certaines attaques, notamment lorsque vous effectuez un paiement sur Internet, peuvent vous faire croire que vous êtes sur le bon site, alors qu'en réalité, vous donnez votre numéro de carte à un site pirate.

De même, activer les options *Créer ou modifier les cookies* et *Lire les cookies* vous expose aux attaques de type Cross Site Scripting. Par conséquent, il est recommandé de les désactiver.

Si vous souhaitez de plus amples informations sur les possibilités de réglage des paramètres de sécurité de Netscape, une aide détaillée est accessible en ligne directement sur chaque écran, via le bouton *Aide*.

Sécuriser Mozilla Firefox

C'est la rançon de la gloire : de plus en plus utilisé, Firefox devient lui aussi une cible de choix des pirates du monde entier. Considéré un temps comme l'un des navigateurs les plus sécurisés au monde, Firefox est à son tour affecté par un nombre croissant de failles de sécurité, dont certaines sont jugées critiques.

Toutefois, la Mozilla Foundation fait preuve d'une forte réactivité et publie généralement ses correctifs dans un laps de temps très court (plus court en tous cas que certains de ses concurrents).

Par ailleurs, de nombreuses exigences de sécurité liées au danger de la navigation sur Internet ont été prises en compte lors de la conception de

Firefox. Par défaut, Firefox ne prend pas en charge les contrôles ActiveX et bloque tout exécutable en provenance d'un site distant.

Firefox représente donc une alternative intéressante du point de vue de la sécurité, à condition de le maintenir à jour et de veiller soigneusement au choix des options de sécurité.

La gestion des cookies

Ouvrez le gestionnaire des cookies : dans le menu *Outils>Options*, cliquez sur *Vie privée*, puis sur *Cookies*.

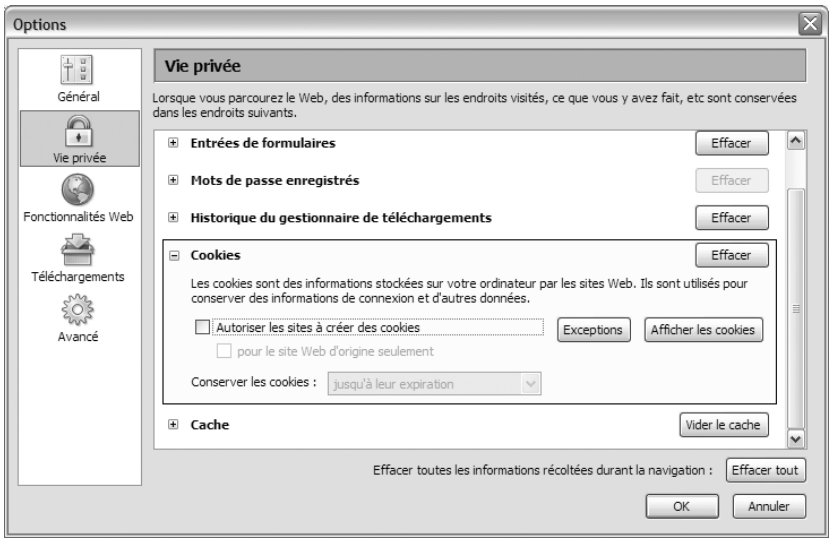


Figure 7–11
Gérer les cookies sous Firefox

Une manière simple pour durcir la sécurité consiste à désactiver la case *Autoriser les sites à créer des cookies*. Si cette option gêne votre navigation, notamment lorsque vous naviguez sur des sites de confiance, n'oubliez pas que vous pouvez définir des exceptions : cliquez sur le bouton *Exceptions*, et saisissez l'URL des sites concernés.

Si cette configuration est encore trop contraignante, cochez à la rigueur la case *Autoriser les sites à créer des cookies*, mais restreignez ce choix en cochant la case *pour le site Web d'origine seulement*. En outre, agissez aussi sur le paramètre *Conserver les cookies jusqu'à leur expiration* ou *jusqu'à la fermeture de Firefox* (préférez ce dernier paramètre).

En cliquant sur le bouton *Afficher les cookies*, vous accédez à une fenêtre donnant la liste de ceux déjà enregistrés sur votre poste. Cette fenêtre dispose aussi d'un bouton absolument fantastique : *Supprimez tous les cookies*. Amenez calmement la souris sur ce bouton et pressez la détente !

ASTUCE Durée de vie des cookies

Dans les cas où un site vous oblige à accepter les cookies, une parade consiste à limiter leur durée de vie à celle de la session (*Outils>Options>Vie privée*).

Gestion des mots de passe de sites web

Pour vous éviter de ressaisir vos authentifiants à chaque ouverture de session avec un site protégé, Firefox propose de mémoriser vos noms d'utilisateur et mots de passe. Cette fonctionnalité est en effet très conviviale, mais dangereuse du point de vue de la sécurité : par défaut, les mots de passe en clair sont accessibles en cliquant sur le simple bouton *Voir les mots de passe enregistrés* !

Un moyen radical pour éviter les problèmes consiste tout simplement à ouvrir le menu *Outils>Options>Vie privée>Mots de passe enregistrés* et à désactiver la case *Retenir les mots de passe* (voir figure 7-12).

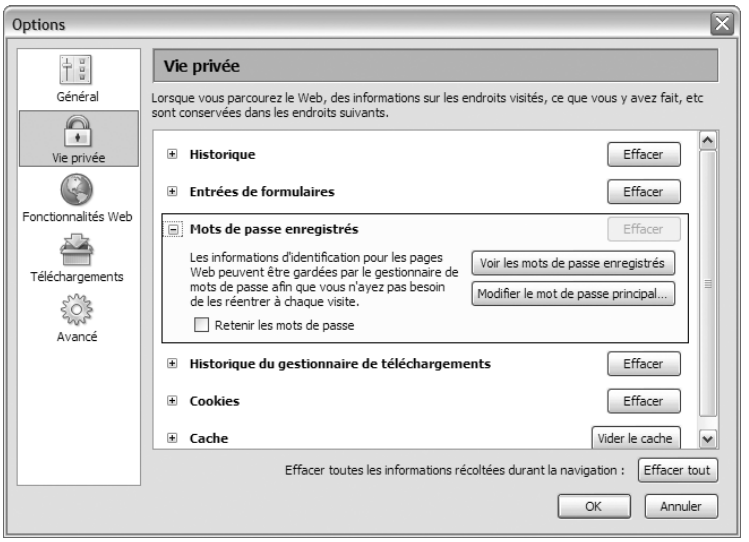


Figure 7–12
Évitez de mémoriser les mots de passe de sites web protégés.

ASTUCE DU PIRATE Variez les mots de passe

Les utilisateurs ont toujours tendance à utiliser les mêmes mots de passe, et les pirates le savent ! La visualisation du mot de passe d'une page web peut conduire à l'ouverture de nombreuses portes, à commencer par le compte de l'utilisateur sur la machine !

ATTENTION Mot de passe principal

N'oubliez pas ce mot de passe. Notez le bien soigneusement !

Si vous tenez absolument à mémoriser les mots de passe de certains sites, définissez au moins un mot de passe principal : il vous sera demandé pour visualiser les mots de passe enregistrés. Il suffit pour cela de cliquer sur *Modifier le mot de passe principal* et de suivre les instructions.

Paramètres de sécurité liés aux fonctionnalités web

Ouvrez le menu *Outils>Options>Fonctionnalités Web*. À travers cet écran, vous pouvez régler quelques paramètres de sécurité :

- Bloquer les fenêtres popup (« surgissantes »).

  Attention toutefois, certains sites web ont recours à ces fenêtres pour gérer des fonctionnalités utiles (vous inviter par exemple à saisir un mot de passe), et leur blocage peut nuire au fonctionnement du site. Dans ce cas, autorisez nominativement les sites de confiance en cliquant sur le bouton *Sites autorisés*.

- Réglementer l'installation de logiciels par les sites web.
  Il s'agit d'un des paramètres de sécurité les plus intéressants de Firefox. Par défaut, la case *Permettre aux sites Web d'installer des logiciels* est activée, ce qui ne veut pas dire pour autant que l'installation aura lieu automatiquement : Firefox vous demandera toujours confirmation. Cependant, si vous voulez interdire l'installation de logiciels, il suffit de désactiver cette option.
- Empêcher ou limiter le chargement d'images selon la provenance.
  Vous réduirez ainsi les risques d'attaques basées sur l'utilisation d'images « piégées ».
- Désactiver le chargement d'applets Java ou de code Javascript.
  Cela constitue une parade à de nombreuses attaques. Cependant, choisir cette option peut gêner votre navigation, voire empêcher certains sites de fonctionner.

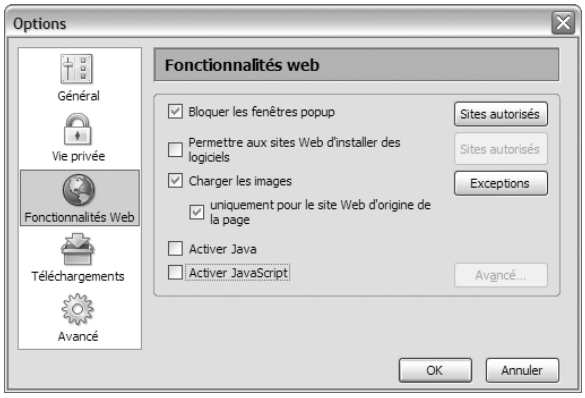


Figure 7–13
Réglage des paramètres de sécurité liés aux fonctionnalités web

Si vous décidez d'autoriser les scripts Javascript, restreignez toutefois le champ d'action des scripts. Cliquez sur le bouton *Avancé* (figure 7-14). Les options disponibles sont détaillées au tableau 7-5.

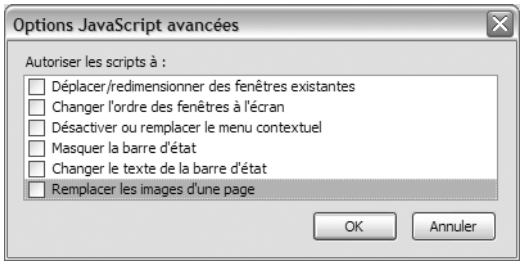


Figure 7–14
Options Javascript avancées

Tableau 7–5 Options Javascript

Paramètre	Recommandation
Déplacer/redimensionner des fenêtres existantes	De nombreuses attaques agissent sur la dimension des fenêtres pour leurrer l'utilisateur. Cette option doit être désactivée.
Changer l'ordre des fenêtres à l'écran	De même, cette option doit être désactivée.
Désactiver ou remplacer le menu contextuel	Option à désactiver.
Masquer la barre d'état	La barre d'état affiche à l'utilisateur de précieuses informations (le cadenas indiquant une connexion sécurisée, l'adresse du site, etc.). Masquer, éditer et recréer une fausse barre d'état sont des subterfuges employés par les pirates lorsqu'ils tentent d'usurper l'identité d'un site authentique. Il faut donc interdire aux scripts de masquer la barre d'état.
Changer le texte de la barre d'état	Pour les mêmes raisons que précédemment, il ne faut pas que les scripts puissent changer le texte de la barre d'état. Cette option doit être désactivée.
Remplacer les images d'une page	Option à désactiver.

Gérer les certificats

Même si vous êtes un utilisateur acharné d'Internet, vous ne vous êtes probablement jamais soucié des problèmes de certificats. Le chapitre précédent a montré que ce sujet a largement de quoi rebuter l'internaute le plus motivé par les problèmes de sécurité. Pourtant, ces petits fichiers ont un rôle essentiel dans la sécurité des échanges sur Internet. Si, par exemple, vous souhaitez accéder aux téléservices proposés de plus en plus fréquemment par les administrations, comme la télédéclaration d'impôts, ou le télépaiement de la TVA, vous serez nécessairement amené à vous intéresser à la gestion des certificats. Et même si vous y renoncez, vous serez certainement confronté tôt ou tard à des alertes de sécurité de votre navigateur, vous indiquant par exemple que tel certificat ne peut pas être vérifié, ou vous demandant si vous décidez de faire confiance à tel autre certificat.

Si enfin vous souhaitez avoir recours à des services d'authentification, de chiffrement, d'intégrité ou de non-répudiation sur Internet, ne serait-ce que pour protéger votre messagerie électronique, vous aurez besoin de faire établir un certificat numérique pour vous-même, de l'installer et de le gérer dans votre navigateur.

En définitive, si vous désirez pleinement bénéficier des riches possibilités que vous offre Internet dans des domaines aussi diversifiés que l'achat en ligne ou la dématérialisation des procédures administratives (entre autres), vous ne pourrez pas échapper à la gestion des certificats. Le chapitre précédent vous a décrit comment fonctionne le processus de certification. Les sections qui suivent vous expliquent maintenant comment gérer les situations les plus courantes.

Afficher la liste des certificats stockés dans votre navigateur

Sous Internet Explorer

Le magasin de certificats est accessible à partir du menu *Outils>Options Internet>Contenu>Certificats* (voir figure 7-15). En parcourant cet écran, vous vous familiariserez avec le nom des principaux acteurs de la distribution de certificats, ce qui vous sera très utile lorsqu'il faudra accepter ou refuser l'installation de certificats au cours de vos transactions sur Internet.

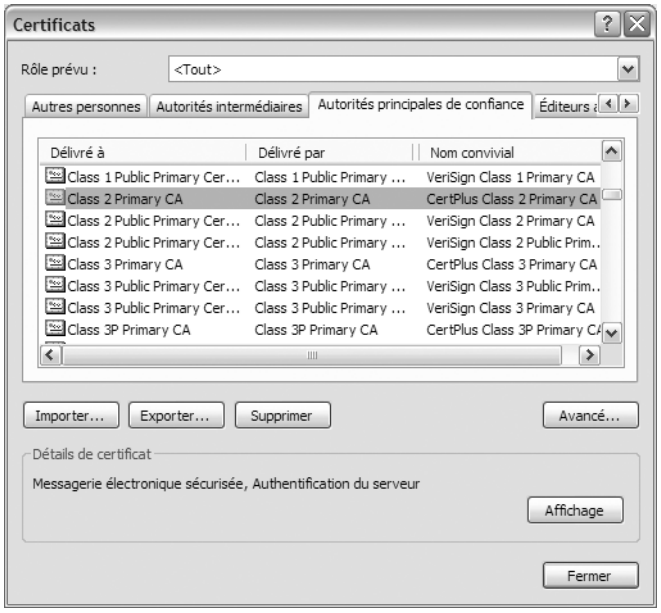


Figure 7–15
Magasin de certificats sous Internet Explorer

Après lecture du chapitre 6, vous comprendrez sans peine la signification des deux onglets *Autorités principales de confiance* et *Autorités intermédiaires*. Si vous cliquez sur le bouton *Affichage*, vous visualiserez la valeur des champs du certificat sélectionné.

Sous Netscape

Ouvrez le menu *Édition>Préférences*, déroulez la liste *Confidentialité et sécurité* et cliquez sur *Certificats*. Cliquez ensuite sur le bouton *Gérer les certificats* et faites apparaître le *Gestionnaire de certificats* représenté à la figure 7-16.

En cliquant sur l'onglet *Autorités*, vous afficherez les certificats des autorités de certification installés par défaut dans votre navigateur.

À RETENIR

Autorités de certification réputées

Pour votre information, sachez que les sociétés les plus connues en matière de certification sur Internet sont essentiellement anglo-saxonnes (donc subordonnées au gouvernement des États-Unis) et se nomment, entre autres, VeriSign, Thawte, RSA Security, GlogalSign, Entrust, ValiCert, GTE Corporation ou Baltimore.

À RETENIR

Autorités de certification françaises

Pour votre gouverne, le certificat sélectionné sur la figure 7-15, `CertPlus Class 2 Primary CA`, est émis par la société CertPlus, une autorité de certification située en France. Il s'agit du certificat autosigné d'une autorité de certification principale.

Il existe très peu d'autorités de certification françaises délivrant des certificats destinés à sécuriser les échanges personnels, comme le courrier électronique. Soit on a affaire à des autorités délivrant gratuitement des certificats dédiés à la réalisation de tâches administratives précises (telec@rtegrise, déclaration des revenus, etc.), soit il s'agit d'autorités à caractère professionnel, spécialisées chacune dans un secteur métier bien spécifique (recherche, avocats, universités, etc.) ; le plus souvent, les certificats sont payants. Citons par exemple ChamberSign (réseau des Chambres de Commerce et d'Industrie), le Greffe du Tribunal de Commerce de Paris, Certinomis, le CNRS, etc.

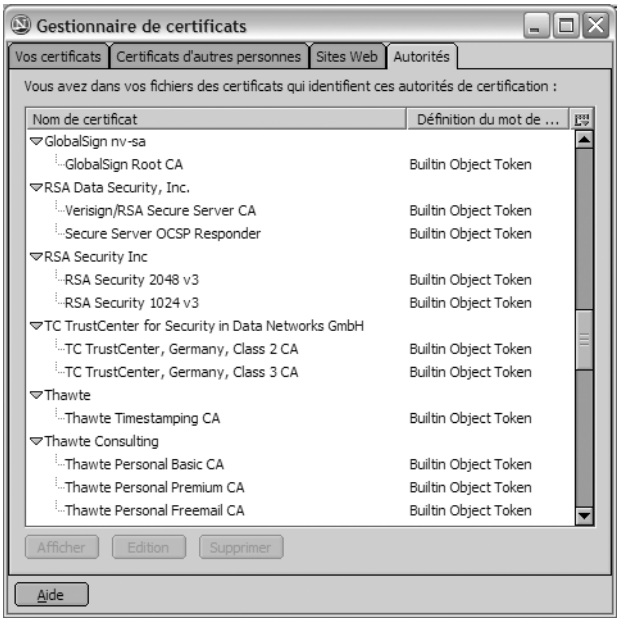


Figure 7–16
Liste des certificats installés par défaut dans Netscape

Sous Firefox

La gestion des certificats sous Firefox s'effectue à partir du menu *Outils>Options>Avancé>Certificats*. Cliquez sur le bouton *Gérer les certificats* et sur l'onglet *Autorités*.

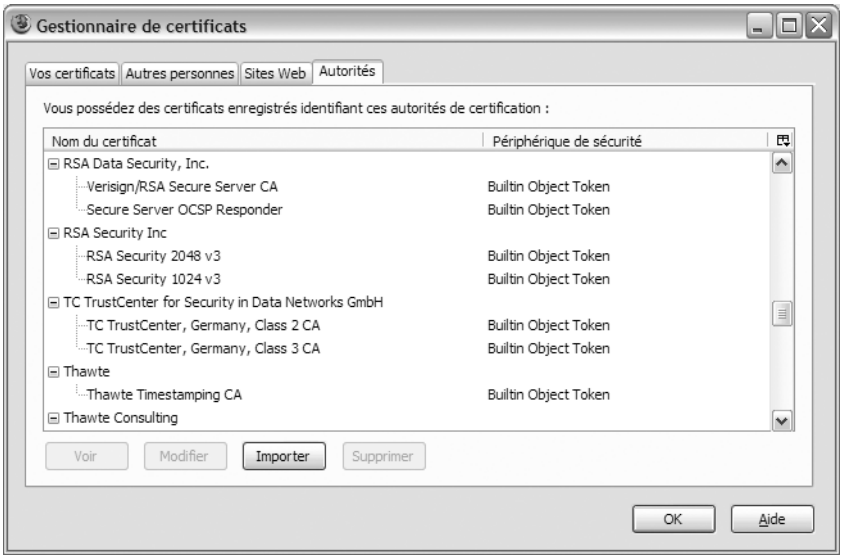


Figure 7–17
Liste des certificats installés par défaut sous Firefox

Modifier la liste des certificats présents par défaut dans le navigateur

Il est important que vous compreniez le rôle crucial joué par cette liste dans le processus d'évaluation d'un certificat. Le réseau de confiance est tout bonnement matérialisé par le magasin, ou le gestionnaire, de certificats. Tant qu'un certificat (de site web par exemple) est valide et a été signé par une autorité de certification présente dans le magasin, le navigateur considère que son détenteur (le site web) est authentifié et digne de confiance, même si le certificat de l'autorité signataire est douteux.

Imaginez que, pour une raison quelconque, le certificat d'une entité distante ait été révoqué (souvenez-vous du cas d'Internet Exploder par exemple, voir la section Authenticode évoquée plus tôt au cours de ce chapitre). Si votre navigateur n'a pas eu connaissance du contenu de la liste de révocation dans laquelle il figure, il n'a aucune raison de ne pas lui faire confiance, et il le considère comme valide. Et vous, inconsidérément rassuré, effectuerez des échanges sécurisés avec un site frauduleux.

Supposons maintenant, autre cas, qu'un certificat valide, appartenant à un utilisateur honnête, ait été émis par une autorité de certification qui ne figure pas dans votre magasin de certificats. Ce certificat pourra être utilisé. Toutefois, le navigateur vous indiquera que le certificat ne peut pas être vérifié car l'autorité émettrice est inconnue (voir chapitre 9), et vous serez déconcerté.

> CONSEIL **Triez la liste de certificats**
>
> Le contenu de cette liste est déterminant pour vos futures relations dites « sécurisées » avec les sites web. Vous avez notamment sérieusement intérêt à éliminer les certificats d'autorités racines dont vous n'avez pas explicitement besoin ou dont vous n'êtes pas sûr. Examinez pour cela les champs des certificats et recherchez d'éventuelles anomalies :
> - certificats sans numéro de série ;
> - clés RSA de 512 bits (on sait actuellement casser une clé de 512 bits) ;
> - validité jusqu'en 2040 (ce n'est pas sérieux !) ;
> - absence de listes de révocation...
>
> Une méthode simple et radicale consiste à supprimer tous les certificats, quitte à réinstaller vous-même ceux dont vous aurez réellement besoin au cours de votre navigation.

Le magasin, ou le gestionnaire, de certificats contient donc des éléments qui détermineront directement le niveau de sécurité de vos échanges. S'il contient des certificats racines non dignes de confiance, la sécurité de votre poste et de vos données sensibles (données bancaires par exemple) risque de chuter de façon dramatique. Les sections suivantes donnent

quelques recommandations précieuses, en se basant sur des exemples de situations concrètes rencontrées lors de visites sur différents sites Internet.

Attitude à adopter lorsqu'un certificat ne peut être vérifié

Prenons un premier exemple. Vous parcourez par curiosité votre magasin de certificats et vous affichez le contenu de la figure 7-18.

Figure 7–18
Exemple de certificat douteux

Que faire d'un tel certificat ? Faut-il activer la confiance et l'installer dans le magasin d'autorités de certification racines ? Faut-il au contraire vous en méfier ? Dans un premier temps, vous avez toujours la ressource d'explorer les autres onglets. Si vous cliquez par exemple sur l'onglet *Détails* (IE, Netscape et Firefox), vous verrez certainement l'information qui laisse peu de place à l'hésitation : la clé publique contenue dans ce certificat est une clé RSA de 512 bits. Elle n'est donc pas sûre et il est vivement déconseillé de suivre l'instruction affichée à l'écran. L'exploration des autres champs confirme nos présomptions : il a été émis en 1996, âge glaciaire d'Internet, et le champ « CN » vous indique explicitement qu'il s'agit d'un certificat de test. Vous pouvez donc, sans état d'âme, le supprimer de votre magasin.

RAPPEL Casser une clé de 512 bits

Depuis de nombreux mois déjà, les techniques de factorisation permettent de casser une clé RSA de 512 bits.
La longueur de la clé publique d'une autorité de certification racine doit être de 2 048 bits si la période de validité de ce certificat est grande. Reportez-vous à l'annexe A pour plus d'informations.

Autre cas, vous naviguez sur Internet et, subitement, l'écran de la figure 7-19 apparaît.

Figure 7–19
L'authenticité du certificat ne peut pas être vérifiée.

Voilà justement l'exemple type de la situation embarrassante à laquelle vous serez confronté si vous prévoyez d'utiliser pleinement Internet. Analysons point par point le contenu de cet écran, en commençant par le bas.

- *Le certificat de sécurité a un nom valide qui correspond au nom de la page que vous essayez d'afficher.*

  Voici déjà une bonne nouvelle. En effet, supposez un instant qu'un escroc, la société Naufrageurs SA par exemple, construise un site web ressemblant à celui de eyrolles.com dans le but d'extorquer votre numéro de carte bancaire. Notre escroc va devoir chiffrer les pages sécurisées avec *sa* clé publique (et non celle de eyrolles.com !). Bien sûr, il peut se faire établir un certificat au nom de eyrolles.com par une AC véreuse. Cependant, l'autorité racine sera inévitablement inconnue dans le navigateur et devra faire l'objet de l'attention que nous décrirons dans quelques lignes et un tel certificat sera très vite révoqué. Le pirate aura donc pris soin au préalable de se faire attribuer un certificat valide par une autorité de certification reconnue. Bien entendu, l'AC qui – dans ce cas présent – suit un code de déontologie absolument strict, ne lui délivrera jamais un certificat au nom de eyrolles.com. Le certificat sera donc établi au nom de l'escroc (Naufrageurs SA) et contiendra l'URL du site web de l'escroc, c'est-à-dire, pour fixer les idées, www.naufrageurs.com.

  Lorsque vous accédez à une page web sécurisée, le navigateur contrôle la cohérence entre le nom de cette page et le contenu du certificat qui la sécurise. Si vous tentez d'accéder au site de eyrolles.com (www.eyrolles.com) et êtes redirigé vers le site de cet escroc (sécurisé avec un certificat contenant le champ www.naufrageurs.com), soit vous allez vous en apercevoir (il y aura discordance entre les URL de la

RAPPEL Intégrité du certificat

N'oubliez pas que l'escroc ne peut pas modifier le contenu des champs de son certificat sans que cela soit détecté lors du contrôle de la signature.

barre d'adresse et celle de la barre d'état), soit le navigateur détectera lui-même la discordance et vous l'indiquera, à travers l'écran de la figure 7-19. Dans tous les cas, cela risque de tousser sérieusement et vous serez alerté. Dans le cas présent, il ne semble pas y avoir de problème de ce côté-là.

- *La date du certificat de sécurité est valide.*

  Cette information est, elle aussi, de bon augure ; elle vous indique que ce certificat n'a pas expiré.

- *Le certificat de sécurité a été émis par une société à laquelle vous n'avez pas choisi de faire confiance.*

  Attention, soyez vigilant avec ce message et considérez sa signification réelle : « *Le certificat de sécurité a été émis par une société à laquelle vous n'avez pas encore choisi de faire confiance* ». Ce point est capital, car il vous montre clairement de quelle manière vous êtes amené à intervenir dans le processus de l'évaluation de la confiance dans un certificat. Vous l'avez maintenant compris, l'écran de la figure 7-19 vous est affiché car l'autorité de certification émettrice de ce certificat ne fait tout simplement pas partie de votre magasin de certificats.

Pour que votre navigateur fasse confiance à ce certificat, vous devez installer dans son magasin le certificat de l'AC émettrice.

ATTENTION Installer dans son navigateur le certificat d'une AC racine

Encore une fois, cette opération est cruciale : si vous installez un certificat frauduleux… toutes les données transitant désormais entre votre poste et un site sécurisé à l'aide d'un certificat émis par cette AC seront protégées de tout le monde, sauf des escrocs ! D'autre part, un pan entier de votre schéma de confiance s'effondre ! Installer le certificat d'une AC racine dans votre magasin revient à ce que votre navigateur accorde sa confiance à une nouvelle pyramide de certificats. Cette décision est absolument capitale sur le plan de la sécurité et vous ne devez procéder à l'installation que si vous êtes sûr de la fiabilité de ce certificat. Nous verrons au chapitre 9 comment effectuer cette opération de façon sûre.

Déterminer si le certificat d'une nouvelle autorité de certification est fiable

Nous avons vu qu'il existait des cas où le certificat d'une autorité de certification n'était pas fiable (le certificat émis par Root Agency, figure 7-18, en est un exemple).

Pour évaluer la fiabilité d'un nouveau certificat, votre seule ressource est de l'examiner ; vous n'avez malheureusement pas d'autre choix. Sous IE, cliquez pour cela sur le bouton *Afficher le certificat* (voir figure 7-20). Avec Netscape, cliquez sur *Afficher* ; avec Firefox, cliquez sur *Voir*.

À première vue, ce certificat semble provenir d'une source sérieuse, le Ministère de l'Économie, des Finances et de l'Industrie, plus précisément la Direction Générale des Impôts (cette source n'est pas réputée pour ses canulars !) ; cependant, le navigateur n'est pas capable d'établir et de vérifier le chemin de confiance entre ce certificat et l'autorité de certification qui l'a émis. Et pour cause, le certificat de cette autorité ne figure pas, par défaut, dans votre navigateur.

Nous sommes donc, a priori, en présence d'un certificat émis par une AC de confiance, donc potentiellement fiable (si une AC véreuse avait publié un certificat frauduleux au nom de la Direction Générale des

À RETENIR Tous les certificats d'AC ne sont pas forcément dans votre navigateur.

Les éditeurs se contentent d'installer dans les navigateurs les certificats d'autorités de certification principales et intermédiaires les plus référencées dans le monde pour l'achat en ligne. Néanmoins, ils ne peuvent pas tous les installer. En effet, il n'est pas certain que les certificats utilisés dans les procédures franco-françaises de télédéclaration de la TVA intéressent les internautes situés au fin fond de la Mandchourie.

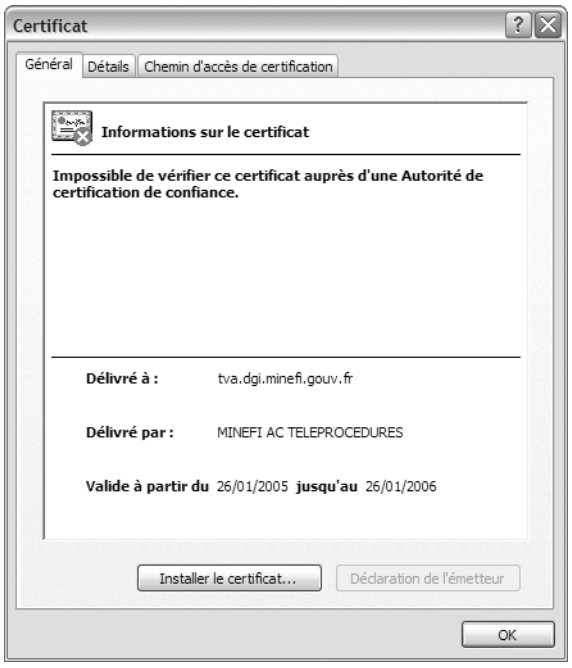


Figure 7–20
Visualisation des informations relatives à un certificat

Impôts, celle-ci aurait très vite réagi en insérant ce certificat dans sa liste de révocation). Vous pouvez donc l'installer (bouton visualisé à la figure 7-20), moyennant toutefois deux précautions :

- Pensez à vérifier auprès d'une autre source si les empreintes MD5 ou SHA-1 affichées dans l'onglet *Détail* correspondent bien aux empreintes réelles du certificat appartenant au ministère.
- N'oubliez pas d'activer la liste de révocation associée à ce certificat (voir plus loin).

Conseil Les AC que vous devez connaître

De façon générale, si vous décidez d'utiliser Internet comme support pour vos transactions officielles électroniques (procédures administratives, commerce électronique, actes juridiques), il est utile que vous vous familiarisiez avec les principaux fournisseurs de certificats des domaines concernés. Les certificats inclus par défaut dans votre navigateur sont plutôt orientés vers l'achat en ligne dans un contexte Internet. Le chapitre 9, traitant plus spécialement du commerce électronique et des procédures dématérialisées, vous donnera quelques points de repère supplémentaires à propos des autorités de certification que vous devez connaître.

Conseil Vérifier un certificat par courrier électronique

Vous pouvez par exemple envoyer un courrier électronique à l'administrateur du site émetteur du certificat, si l'autorité en question ne gère pas un volume important de certificats. Dans le cas du MINEFI, un serveur vocal est à disposition (voir chapitre 9). Faites-vous bien préciser les valeurs d'empreinte MD5/SHA-1 du certificat correspondant au numéro de série.

Gérer les listes de révocation

Le modèle de confiance mis en place par les infrastructures X.509 est bâti sur un foisonnement de réseaux pyramidaux : dans chaque réseau, une chaîne de confiance relie chaque certificat d'utilisateur à son sommet, l'AC racine, relayée à travers un ou plusieurs échelon(s) d'AC subordonnées (reportez-vous au chapitre 6 pour plus de détails).

Supposons que, pour une raison quelconque, la clé privée d'une AC de cette chaîne soit compromise, c'est-à-dire qu'elle tombe malencontreusement entre les mains d'une entité malhonnête. Tous les certificats qu'elle a délivrés depuis le début de son activité deviennent ainsi suspects, car il est désormais impossible de savoir si un certificat signé par cette autorité a été délivré par l'autorité elle même, ou par l'entité malhonnête.

Autre cas, supposons qu'un escroc se fasse établir un certificat valide par une autorité de certification de confiance, afin de monter une fraude (prenez le cas d'Internet Exploder par exemple). L'AC n'est pas censée connaître les intentions de cet escroc au moment où il effectue sa demande ; elle lui délivre donc le certificat, ouvrant ainsi la voie à ses activités malhonnêtes.

Ces deux cas, parmi d'autres, mettent en évidence le talon d'Achille d'un tel schéma de confiance. Vous devez informer votre navigateur du statut d'un certificat ; il est donc impératif d'avoir recours aux listes de révocation. Les navigateurs sont programmés pour rejeter tout certificat inséré dans une de ces listes. Aussi, pourquoi être aussi peu nombreux à en faire usage ?

Sous Internet Explorer

Les listes de révocation doivent être importées de la même manière que les certificats : *Outils>Options Internet>Contenu>Certificats>Importer*.

Sous Netscape Navigator

Vous accédez aux fonctions de validation des certificats dans le menu *Édition>Préférences>Confidentialité et sécurité>Validation*.

L'installation et la gestion des listes de révocation est accessible en cliquant sur le bouton *Gérer les CRL*. Si vous n'avez jamais explicitement configuré votre navigateur pour qu'il aille consulter les listes de révocation sur Internet, il se peut que votre écran ressemble à celui de la figure 7-22, c'est-à-dire un écran vide.

Netscape Navigator n'installe par défaut aucune liste de révocation. Vous constatez par vous-même à quel point vous êtes, dans ce cas, vulnérable à une des attaques précédemment citées.

À RETENIR Certificats frauduleux toujours en circulation

Il faut savoir qu'un malfrat, même découvert, continuera à faire usage de son certificat frauduleux. C'est pourquoi vous devez informer le navigateur que tel ou tel certificat, (apparemment valide) n'est en réalité que l'odieuse patte blanche d'un méchant loup embusqué quelque part sur Internet, qui attend patiemment que votre tour arrive.

AVENIR Vérification automatique des listes de révocation

Si vous êtes actuellement dans le camp des internautes n'utilisant pas ces listes, vous avez une circonstance atténuante car les navigateurs ne disposent à l'heure actuelle d'aucune fonction automatique assurant la coordination avec les autorités de certification, ce qui permettrait de vérifier automatiquement les listes de révocation.
Il s'agit là d'un manque incontestable, et il faut espérer que les éditeurs ajouteront cette fonctionnalité dans l'avenir. En attendant, vous êtes obligé de vous prendre par la main et de configurer vous-même votre navigateur pour qu'il fasse appel aux listes de révocation.

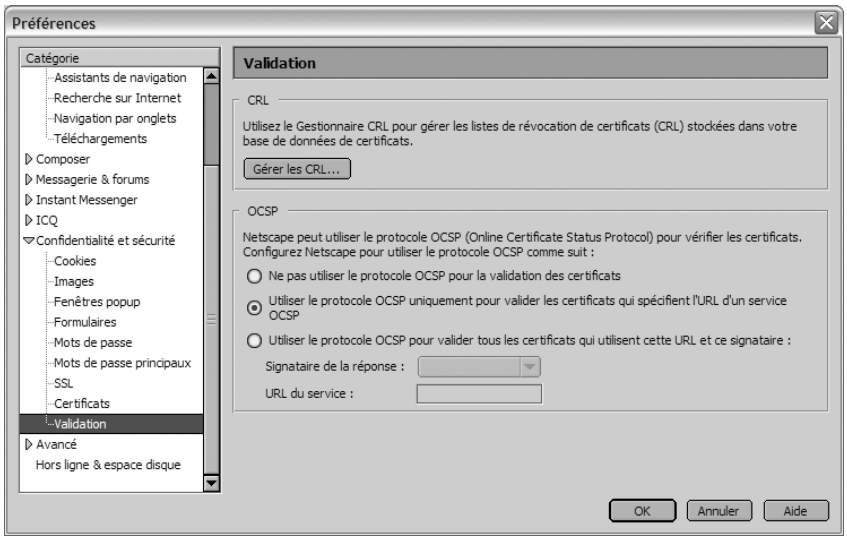


Figure 7–21
Gestion des listes de révocation sous Netscape

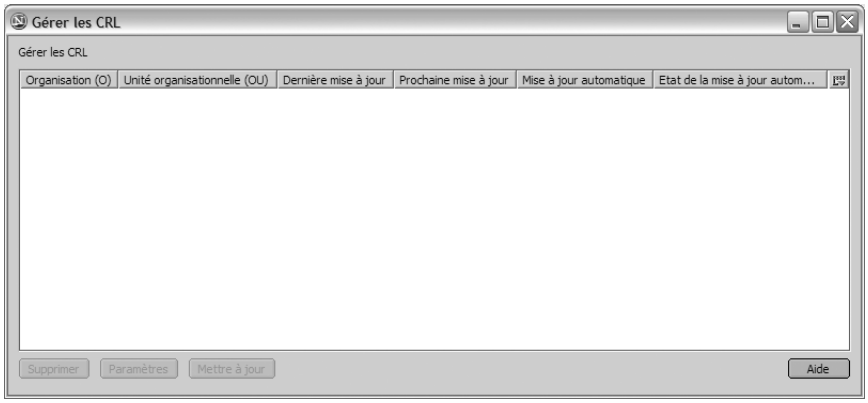


Figure 7–22
Listes de révocation de certificats

Pour renseigner le navigateur, vous devez vous connecter à l'URL d'une liste de révocation, par exemple http://crl.verisign.com, et l'importer vous-même en cliquant sur les liens de la page. Lorsqu'une liste de révocation a été correctement chargée sur votre machine, le message 7-23 est affiché :

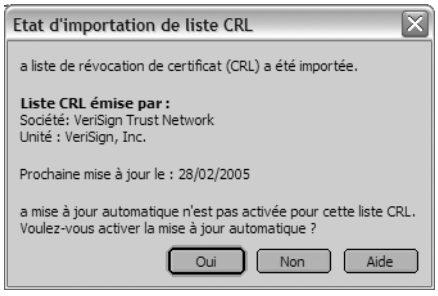


Figure 7–23
État d'importation d'une liste de révocation

Vous devez sélectionner le bouton *Oui* pour activer la mise à jour automatique de cette liste de révocation et accepter les préférences par défaut proposées par Netscape, visualisées à la figure 7-24.

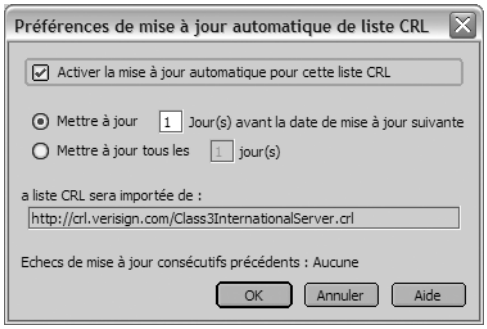


Figure 7–24
Préférences relatives aux mises à jour d'une liste de révocation

CONSEIL **Chargez les listes de révocation de toutes les AC identifiées dans votre navigateur.**

Pour que votre navigateur puisse vérifier en toute connaissance de cause le statut d'un certificat présenté, il faut, si vous êtes consciencieux, charger les listes de révocation publiées par toutes les autorités de certification dont vous possédez un certificat. Dans certains cas, l'URL de cette liste de révocation figure à l'intérieur même du certificat (voir figure 7-25).

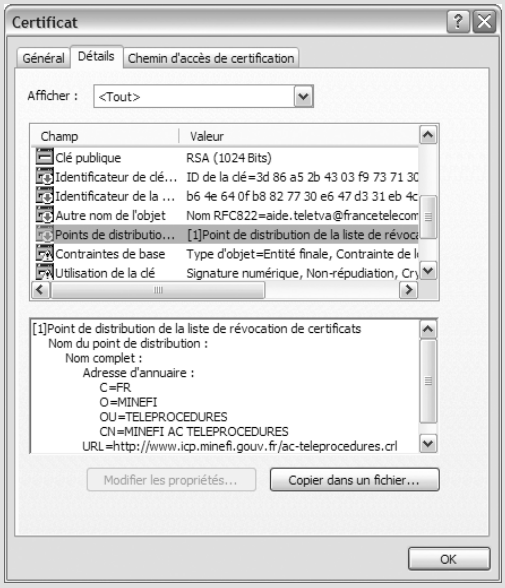


Figure 7–25 Point de distribution de la liste de révocation

Après avoir chargé toutes vos listes de révocation, l'écran de la figure 7-22 doit maintenant ressembler à celui de la figure 7-26.

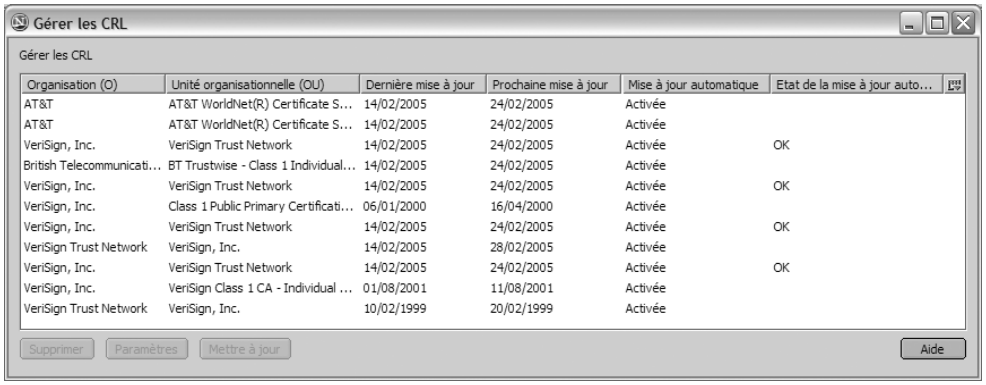


Figure 7–26
Listes de révocation de certificats installées sur votre ordinateur

Vous comprenez certainement à la lecture de ces lignes que la remontée de la révocation vers l'utilisateur via les listes de révocation est une procédure lourde. De plus, elle présente des lacunes. En effet, il existe une latence entre la révocation d'un certificat et la publication effective de cette révocation, qui survient à l'occasion de la mise à jour de la liste de révocation.

Pour remédier à ces problèmes, le protocole OCSP (Online Certificate Status Protocol) a été défini. Il constitue une alternative intéressante aux listes de révocation.

Protocole OCSP

Le protocole OCSP permet au Gestionnaire de certificats de vérifier la validité d'un certificat en ligne. Lorsqu'un certificat est présenté à votre navigateur, celui-ci émet une requête à destination du serveur OCSP, dont l'URL est spécifiée dans l'un des champs du certificat (si l'autorité de certification fournit le service OCSP). Cette requête contient notamment le numéro de série du certificat. Le serveur invoque alors son service OCSP chargé de collecter en temps réel la liste des certificats invalides, à partir de plusieurs listes de révocation ou d'autres serveurs OCSP. Il renvoie une réponse qui reflète la situation réelle à l'instant t : « certificat valide, révoqué ou inconnu ».

Les options relatives à l'utilisation du protocole OCSP par Netscape Navigator apparaissent à la figure 7-21. Il est recommandé d'utiliser l'option *Utiliser le protocole OCSP uniquement pour valider les certificats qui spécifient l'URL d'un service OCSP*. Notez que l'option par défaut, *Ne pas utiliser le protocole OCSP pour la validation des certificats*, ne devrait jamais être cochée.

Sous Firefox

La gestion des listes de révocation et l'utilisation du protocole OCSP s'effectuent exactement de la même manière que sous Netscape Navigator. Ouvrez le menu *Outils>Options>Avancé>Validation* (figure 7-27).

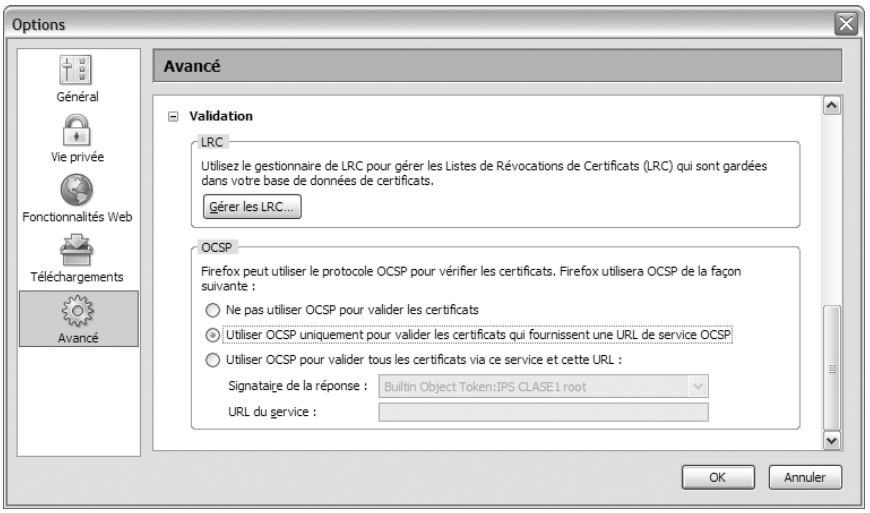


Figure 7–27
Listes de révocation et protocole OCSP avec Firefox

Récapitulatif

Le navigateur est l'outil grâce auquel l'utilisateur réalise la plupart des opérations sur Internet. Il est donc, logiquement, une cible d'attaques privilégiée des pirates de tous bords.

Malheureusement, la nature des flux applicatifs engendrés par un navigateur dépasse largement le champ d'action des pare-feux et des antivirus. Si des mesures complémentaires sont mises en œuvre à d'autres niveaux de l'installation, le navigateur doit absolument participer à l'établissement d'une stratégie de sécurité propre à la navigation.

Une menace redoutable rencontrée aujourd'hui provient des codes mobiles, ActiveX, Applets Java, scripts ou plug-ins. Ces petits exécutables, rapatriés continuellement lors du chargement de pages web, peuvent, lorsqu'ils sont malveillants, espionner, prendre le contrôle de la machine à distance, ou causer des dommages irrémédiables sur le poste de travail.

Il existe des technologies, comme Authenticode, permettant d'authentifier l'éditeur d'un code mobile et de garantir l'intégrité de l'exécutable. Bien qu'elles aient quelquefois montré leurs limites, les signatures de ce type représentent aujourd'hui un mécanisme viable pour un écrémage de premier niveau, et la mise à l'écart de composants à risque.

D'autres technologies, comme le concept de bac à sable dans l'environnement Java, restreignent considérablement, voire anihile, la capacité de nuisance des codes mobiles malveillants.

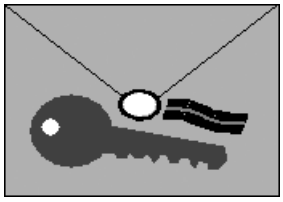
Pour tirer avantageusement parti de ces fonctionnalités, encore faut-il prendre le temps d'affiner les stratégies de sécurité proposées en natif par les navigateurs : ces logiciels disposent en effet de nombreux paramètres de sécurité, qui apportent une contribution incontestable au niveau de protection atteint par l'installation. Toutefois, il faut consacrer du temps à revoir et à optimiser la valeur de ces paramètres, car certains réglages par défaut sont notoirement laxistes !

Par ailleurs, il faut garder à l'esprit que la gestion des certificats, éléments fondateurs de tous les services de sécurité basés sur la cryptologie (sécurisation de la messagerie et des transactions électroniques sur Internet), a lieu à l'intérieur même du navigateur.

Pour cela, il faut veiller scrupuleusement à ce que la chaîne de confiance mise en place par le magasin de certificats ne soit pas affectée par la présence de certificats racines douteux. Il ne faut donc pas hésiter à supprimer les certificats racines dont on sait, à l'évidence, qu'ils ne seront d'aucune utilité. En outre, il est nécessaire de maîtriser les procédures d'installation de certificats d'autorités racines, en sachant surtout reconnaître l'authenticité du certificat que l'on installe.

Contrairement à ce que l'on pourrait imaginer, le navigateur Internet occupe une postion hautement stratégique dans l'édifice de sécurité d'un poste de travail. Une faiblesse dans son paramétrage et la machine se transforme en un superbe cheval de Troie, encore plus efficace si elle se situe sur le réseau – a priori sécurisé – d'une entreprise. Il convient donc de prendre très au sérieux le paramétrage d'une telle application, sinon l'impact néfaste sur la sécurité sera déterminant.

chapitre 8



Sécuriser son courrier électronique

Le courrier électronique est une des cibles préférées des pirates ; alors, débarrassez-vous de tous les pourriels qui envahissent votre boîte aux lettres et renforcez votre protection antivirus. Apprenez également à garantir la confidentialité et l'authenticité de vos courriers.

SOMMAIRE

- Reconnaître et éviter les messages indésirables
- Filtrer les messages indésirables
- Réduire les risques d'infection virale par la messagerie
- Obtenir des clés de chiffrement
- Chiffrer et signer un message
- Déchiffrer et authentifier un message

MOTS-CLÉS

- spam, pourriel
- phishing, hameçonnage
- clé de chiffrement
- algorithme symétrique/asymétrique
- certificat
- OpenPGP

À ce stade de l'ouvrage, nous avons abordé de nombreux sujets de sécurité. Si vous avez suivi nos conseils depuis le début du premier chapitre, on peut raisonnablement penser que votre ligne de défense est maintenant suffisamment robuste pour prévenir et contrer la plupart des menaces informatiques.

Cependant, apporter quelque attention à la messagerie électronique ajoutera incontestablement un niveau de protection supplémentaire. En effet, contrairement au Web et à de nombreuses applications sur Internet, qui frappent l'internaute anonyme un peu au hasard, votre adresse électronique constitue un moyen efficace d'atteindre votre machine en particulier, et parfois en dépit des moyens de protection mis en place.

C'est d'ailleurs pour cette raison que les virus et autres codes malveillants se sont très tôt servi de la messagerie électronique comme vecteur de propagation et de pénétration. C'est aussi à cause de la messagerie électronique que de grandes entreprises laissent imprudemment partir des informations sensibles en clair sur Internet et, au bout du compte, perdent des marchés importants.

Afin de remédier à ces problèmes et de renforcer le niveau général de protection, nous détaillerons dans ce chapitre quelques mesures de sécurité spécifiques à la messagerie électronique, et apprendrons comment tirer parti des fonctions de sécurité natives de cette application. Nous nous focaliserons notamment sur trois points :

- comment vous protéger contre le spam qui vient polluer votre boîte aux lettres ;
- comment mettre en œuvre des procédures pour renforcer votre protection contre les virus et les codes malveillants ;
- comment assurer la confidentialité et l'authenticité d'un courrier électronique et mettre en place une protection de chiffrement efficace.

Lutter contre les messages non sollicités

Le spam

Il suffit de lancer la réception de son courrier électronique pour qu'un flot de messages parasites déferle et vienne encombrer notre boîte aux lettres. Nous perdons un temps fou à supprimer des publicités pour des produits, des sites pornographiques ou des médicaments dont nous n'avons cure, que d'illustres inconnus, retranchés jusque dans les moindres recoins de la planète, prennent un malin plaisir à nous envoyer. En dépit de la nuisance causée et de l'inutilité apparente de ces messages, le mobile des annon-

ceurs du monde virtuel est guidé par des objectifs très concrets : vendre le plus souvent, extorquer quelquefois, infiltrer de temps en temps.

Il est fort probable que vous n'ayez jamais succombé à ces Sirènes modernes. Pourtant, le spam, ou pourriel, est un commerce plus que juteux. Contrairement aux courriers publicitaires traditionnels, envoyer un spam à des millions de gens ne coûte rien ; en revanche, il rapporte d'importantes sommes d'argent à ses commanditaires et ne semble donc pas prêt à se tarir. Il suffit qu'une infime partie de la population morde à l'hameçon pour que les « Golden-Nautes » se frottent les mains. L'une des tâches du spammeur consiste donc à établir des listes, à recenser et à toucher le plus de monde possible, par tous les moyens. Patience donc, vous n'êtes pas au bout de vos peines !

Spam ?

Un spam est un message électronique non sollicité, largement diffusé, émis par une source avec laquelle vous n'avez aucun lien particulier. La figure 8-1 en présente un exemple.

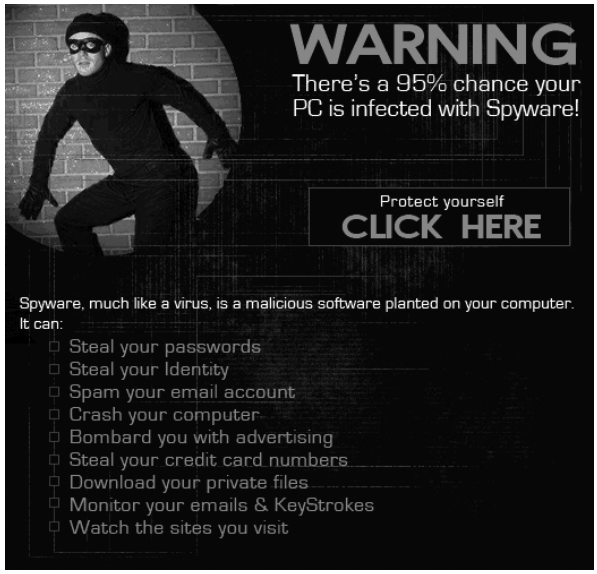


Figure 8–1 Exemple de spam

Le spam ne se présente pas systématiquement par le biais de la messagerie. Il apparaît aussi sous forme de pop-ups, fenêtres publicitaires qui surgissent inopinément à l'écran lorsque vous naviguez sur le Web.

Un courrier indésirable n'est pas toujours émis dans un but strictement commercial. Il peut très bien avoir un caractère politique, religieux ou, tout simplement, servir de vecteur d'infiltration pour vous inoculer un virus.

Divulgation de votre adresse de courrier électronique

Commençons par une lapalissade : si vous avez reçu un spam, c'est que l'émetteur a eu connaissance de votre adresse, par un moyen ou par un autre ; et justement, ces moyens sont nombreux.

Tout d'abord, il est toujours possible de deviner les adresses. En effet, qui empêche le spammeur de prendre le botin, ou de d'établir une liste exhaustive d'adresses en s'appuyant sur tous les noms associés à tous les prénoms de France et de Navarre ? En associant chaque doublet au nom d'un opérateur connu, il est très facile d'obtenir des adresses potentiellement valides telles que angelique.martin@wanadoo.fr ou dominique.blanc@free.fr. Comme cela ne coûte rien d'envoyer un message électronique, vous imaginez à quel point il est simple de vous spammer.

Cependant, l'annonceur peut aussi employer des méthodes plus subtiles. Considérez très sérieusement que les forums de discussion, les newsgroups, les messageries instantanées, les pages web (qui regorgent de quantités d'adresses valides) représentent une mine d'or pour les spammeurs. Sachez qu'il existe des automates performants capables de détecter systématiquement la présence d'adresses électroniques sur n'importe quelle page publiée sur Internet, et qui construisent automatiquement des listes de diffusion ciblées par thèmes.

Il existe encore d'autres moyens de collecter ce sésame. Lorsque vous souscrivez à certains services, vous êtes obligé de spécifier votre adresse électronique. S'il s'agit de votre banque, de la SNCF, ou d'un service à caractère professionnel, vous n'avez pas grand-chose à redouter. En revanche, s'il s'agit d'un site peer-to-peer, d'une messagerie instantanée ou d'un site pornographique, finie la tranquillité !

Bien entendu, toute liste s'affine amoureusement au fil du temps, en isolant toutes les adresses certifiées valides. Sachez que dans le monde des spammeurs, une liste thématique constituée d'adresses électroniques valides devient très vite un objet de valeur : elle finit tôt ou tard (très tôt en général) par s'échanger entre spammeurs contre compensations financières, non virtuelles celles-ci. C'en est à un tel point que l'élaboration de listes de diffusion devient un métier à part entière sur le Net, à votre grand dam d'ailleurs, pauvres futures victimes de bombardements massifs !

KESACO ? **Site peer-to-peer**

Logiciel d'échange de fichiers directement d'utilisateur à utilisateur à travers Internet. Les logiciels P2P les plus connus sont Kazaa et Emule.

📖 Fabrice Lefessant, *Peer-to-peer, comprendre et utiliser*, collection Connectez-moi, Éditions Eyrolles, 2006.

ATTENTION

Ne répondez surtout pas aux spams !

Si par exemple vous répondez à un spam en disant « fichez-moi donc la paix ! ! ! », le spammeur est content : il a maintenant la certitude qu'au bout de cette adresse hypothétique existe un vrai bipède et il va maintenant la conserver bien précieusement !

Protéger son adresse électronique contre le spam : quelques mesures simples

Un compte public et un compte privé

Commencez par vous établir une seconde adresse de messagerie, une adresse « publique », avec laquelle vous réaliserez toutes vos opérations

sur Internet : enregistrer et télécharger vos logiciels préférés (attention au cheval de Troie, ne téléchargez pas n'importe quoi !), effectuer des réservations, accéder à des sites en accès protégé, etc. Cette adresse deviendra probablement assez vite une cible pour les spammeurs, mais cela n'a pas d'importance, vous ne l'utiliserez pratiquement pas ; vous laisserez ainsi s'accumuler les spams avec le plus grand mépris. Éventuellement, de temps à autres, vous passerez un coup de broyeuse automatique afin de libérer l'espace. En revanche, vous continuerez d'échanger vos courriers électroniques avec votre adresse principale, laquelle sera connue uniquement de vos interlocuteurs.

Plusieurs portails vous offrent la possibilité de créer des adresses électroniques gratuitement (voir l'exemple de la figure 8-2). Cliquez sur le lien et suivez les instructions.

BON SENS Ne divulguez pas votre adresse électronique

Partez du principe que la publication d'une adresse électronique entraîne obligatoirement et sans délai l'insertion de celle-ci dans une liste de diffusion.
Pour vos démarches sur Internet, inscriptions à des forums et autres listes de diffusion, n'utilisez pas votre adresse personnelle ou professionnelle : faites-vous attribuer une adresse « jetable » que vous pourrez remplacer facilement.

Figure 8–2
Créez une adresse électronique « publique ».

Créez-vous ensuite un nouveau compte de messagerie correspondant à cette adresse. Avec Thunderbird par exemple, voici la marche à suivre :

- dans le menu *Outil*, cliquez sur *Paramètres des comptes* ;
- appuyez sur le bouton *Ajouter un compte*, activez le bouton radio *Compte courrier électronique* et cliquez sur *Suivant* ;
- entrez les paramètres de votre nouveau compte en suivant les instructions proposées par l'assistant (figure 8-3).

La procédure est exactement la même avec d'autres clients de messagerie, comme Outlook ou Outlook Express.

Lorsque vous commencez à recevoir trop de spams et que cette adresse publique devient « grillée », rien de vous empêche de l'abandonner et de vous en attribuer une nouvelle.

ATTENTION Réception des messages dans votre client de messagerie

Avec certains fournisseurs, vous accéderez gratuitement à votre messagerie uniquement via le Web ; la réception des messages avec le client de messagerie est un service payant.

Figure 8–3
Créez un compte associé à votre adresse électronique « publique ».

Une adresse résistant au spam

Écoutez ensuite votre bon sens : lorsque vous spécifiez une nouvelle adresse électronique, choisissez donc un nom d'utilisateur inhabituel, comme « m56rf4 » (m56fr4@wanadoo.fr) ou, si vous n'aimez pas les séquences aléatoires, une « phrase » d'utilisateur, comme « michelsanspourriel » (michelsanspourriel@hotmail.com). Avec un peu de chance, vous devriez recevoir moins de courriers indésirables.

Un domaine peu usité

En toute logique, plus votre FAI ou votre domaine est connu, plus il est ciblé par les annonceurs et plus vous risquez de recevoir du spam. Si en revanche vous choisissez un FAI ou un domaine sorti d'on ne sait où (janoticot@cyclopathes.fr), vous bénéficierez incontestablement d'une protection « naturelle » supplémentaire.

Plutôt l'image que le texte

Bien entendu, il ne sert à rien de prendre tant de précautions si vous êtes obligé malgré tout de publier votre adresse dans un forum, une page web ou tout ce qui est susceptible d'apparaître sur Internet. Pour déjouer les outils automatiques de recherche d'adresses électroniques, pensez à publier votre adresse sous la forme d'une image (figure 8-4), en évitant d'insérer un lien entre cette image et votre adresse !

Figure 8–4
Insérez plutôt votre adresse sous la forme d'une image.

ÉLÉMENTAIRE **Pièges à éviter lorsque l'on reçoit des pourriels**

- À l'exception bien sûr des messages envoyés par les sociétés en lesquelles vous avez confiance (qui vous offrent en général la possibilité de vous désabonner), ne répondez jamais à un spam. Répondre à un spam ne sert à rien parce que non seulement les spammeurs camouflent astucieusement leurs véritables adresses, mais encore cela confirme la validité de la vôtre !
- Ne cliquez jamais sur un lien HTML contenu à l'intérieur d'un spam. Cela indique bien entendu au spammeur que votre adresse est valide, et vous risquez en plus d'infecter votre machine avec un virus ou d'installer un logiciel espion.
- Ne cliquez pas non plus sur la pièce jointe d'un spam, probablement vecteur de virus. L'exemple de la figure 8-5 est bien tenté mais, heureusement, la physionomie de ce courriel est typique de ces pièges grossiers : en effet, en dépit de l'indication « +++ Attachment : No Virus Found » au bas du message (la ficelle est grosse !), la pièce jointe est porteuse d'un beau virus.

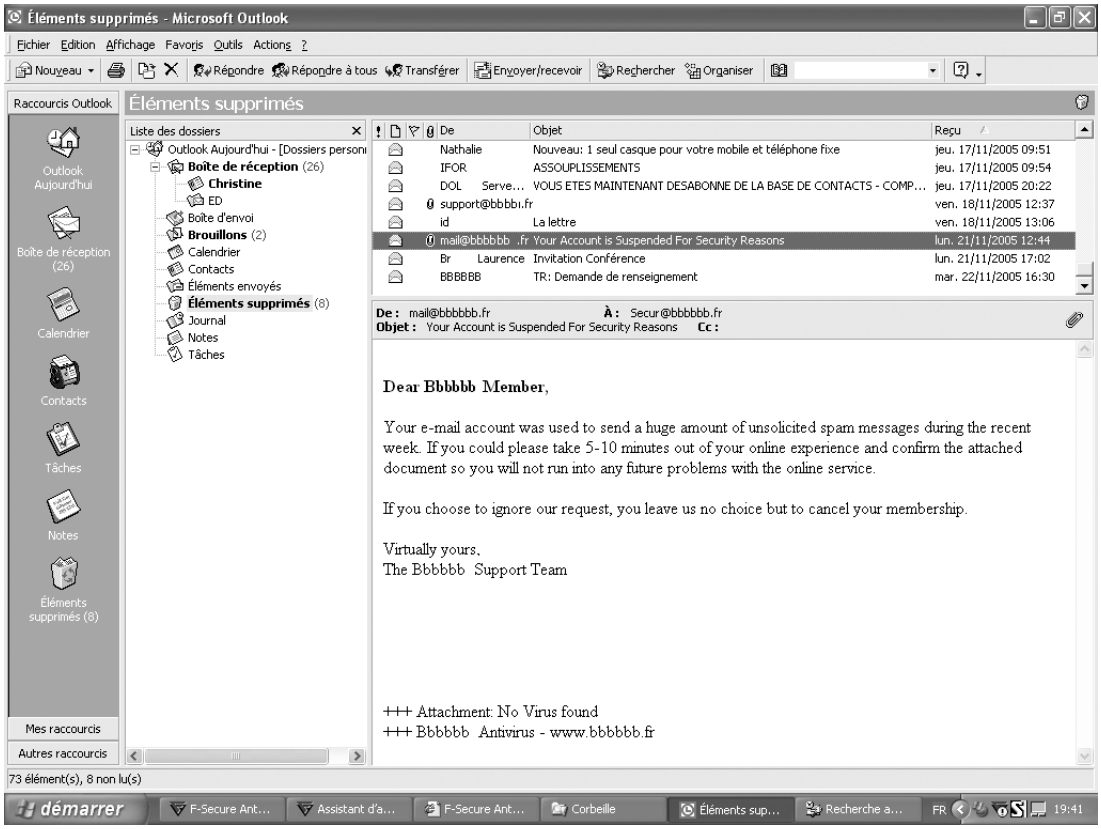


Figure 8–5 Ne cliquez jamais sur la pièce jointe d'un spam.

JARGON **Phishing**

Le terme « phishing », ou « hameçonnage » en français, est issu de la contraction de deux termes : « phreaking », le piratage des centraux téléphoniques, et « fishing », aller à la pêche.

Le phishing

Il existe une autre facette du spam, qui connaît actuellement un essor important : le « phishing ». Il s'agit d'une technique nouvelle mise au point pour vous escroquer.

L'objectif du phishing est de vous inciter – très habilement en général – à divulguer des informations confidentielles vous concernant : vos mots de passe, numéros de carte de crédit, numéros de compte ou toute autre forme d'information personnelle.

Pour y parvenir, le phishing allie deux procédés :

- ce que les anglo-saxons appellent le « social engineering », c'est-à-dire l'exploitation de la crédulité, le « baratinage » ;
- et la technique du message non sollicité.

Dans la plupart des cas, vous recevez un message qui provient manifestement de votre banque, de Microsoft ou de tout organisme officiel qui offre un service de gestion de compte en ligne, et en lequel vous avez confiance. Malgré son apparence crédible (il contient les logos, les polices de caractères de l'organisme en question, voire des liens vers des sites web copies conformes des sites officiels), ce message est frauduleux. Il contient généralement un discours extrêmement bien « huilé » qui, sous de faux prétextes, vous amène progressivement à renvoyer par courrier électronique des données personnelles sensibles, ou à saisir un mot de passe via une fenêtre contextuelle. Ou bien il vous invite à cliquer sur un lien conduisant à un formulaire que vous remplissez avec des codes d'accès personnels. La figure 8-6 en présente un exemple.

Figure 8–6
Exemple de courrier frauduleux

Le stratagème est tellement bien monté que beaucoup s'y trompent et confient de précieuses informations à des inconnus. Une fois collectées, ces données personnelles permettront aux escrocs d'accéder à votre compte en ligne à votre place.

Éviter de se faire piéger avec le phishing

Il existe des techniques pour reconnaître un faux message parmi les vrais. Par ailleurs, les éditeurs publient toutes sortes d'outils prétendus anti-phishing. Si vous êtes fortuné, vous pouvez toujours découvrir de nouveaux produits et satisfaire votre curiosité. Cependant, sachez qu'on peut se protéger très facilement et très efficacement sans débourser le moindre centime. Il suffit de suivre une règle d'une simplicité désarmante : un organisme sérieux, quel qu'il soit, ne vous demandera jamais d'informations personnelles et confidentielles par courrier électronique. Si vous recevez un message de ce type, c'est assurément un faux, ignorez-le systématiquement. Si tout le monde appliquait une règle aussi simple, les escrocs n'auraient plus qu'à retourner à leurs fourneaux, et mitonner des méthodes un peu plus sophistiquées. Sachez qu'un mot de passe est une information strictement personnelle, que personne d'autre que vous ne doit connaître – à commencer par l'organisme en question.

Bon sens Ne donnez jamais d'informations confidentielles

Quelle que soit l'apparence d'un message, d'un site web, des adresses électroniques ou des fenêtres contextuelles associées, ne répondez jamais à un courrier électronique dans lequel on vous demande des informations personnelles et confidentielles. La saisie de telles informations doit être le résultat d'un processus que vous avez vous-même engagé (un achat, la saisie du mot de passe sur un site protégé lorsque c'est vous qui prenez l'initiative d'ouvrir la session, etc.)

Filtrer les messages indésirables

Mode opératoire d'un filtre antispam

Lorsque vous recevez un courrier, le filtre antispam l'analyse et tente d'évaluer s'il s'agit d'un message légitime ou d'un courrier indésirable. Dans ce deuxième cas, le message est marqué et redirigé vers un dossier distinct. Cela libère ainsi votre boîte de réception et facilite considérablement votre travail d'élimination des messages.

Toutefois, le concept de filtre antispam n'est pas parfait. Tout d'abord, la phase d'analyse requiert un temps parfois pénalisant si vous recevez un grand nombre de messages ; ensuite, le filtre lui-même n'est pas toujours infaillible : il laisse passer des spams « déguisés » en messages légitimes, ou, au contraire, considère comme courriers indésirables certains messages que vous auriez souhaité lire.

Le problème vient de la méthode probabiliste utilisée pour effectuer cette évaluation : le filtre pondère de nombreux paramètres, comme la liste des expéditeurs autorisés ou filtrés, le contenu du message, la présence ou non de mots-clés caractérisant un spam, etc. Les bons filtres antispam utilisent des algorithmes à apprentissage.

Algorithme à apprentissage

Un filtre à apprentissage construit ses propres règles de filtrage au fil du temps, en fonction des indications que vous lui fournissez lorsque vous marquez tel ou tel message comme indésirable. L'efficacité des filtres à apprentissage est généralement très élevée.

Les filtres antispam évolués (généralement proposés par les pare-feux matériels) reposent sur l'utilisation de serveurs DNSBL (DNS based Blachhole Lists). Ces derniers publient des listes noires d'adresses IP connues pour propager du spam ; ces listes sont interrogeables à distance via le protocole DNS.

Bien entendu, malgré ces techniques avancées, les filtres antispam n'atteignent pas une fiabilité de 100 %. Il faut notamment toujours vérifier qu'aucun message valide n'a été malencontreusement dirigé vers le dossier du courrier indésirable.

Services proposés par les clients de messagerie pour filtrer les spams

Avant d'avoir recours à des outils spéciaux antispam, sachez que les clients de messagerie proposent des mécanismes qui peuvent déjà vous tirer quelques épines du pied.

Bloquez ou déplacez les indésirables

Si un gêneur a commis l'imprudence d'utiliser toujours la même adresse électronique source, vous avez la possibilité d'expédier automatiquement tous ses messages dans le dossier *Éléments supprimés*. Avec Outlook Express par exemple, dans le menu *Message*, il suffit de cliquer sur *Bloquer l'expéditeur* (figure 8-7). Vous pouvez accéder à tout moment à cette liste, visualiser et gérer les expéditeurs bloqués à partir du menu *Outil>Règles de message>Liste des expéditeurs bloqués*.

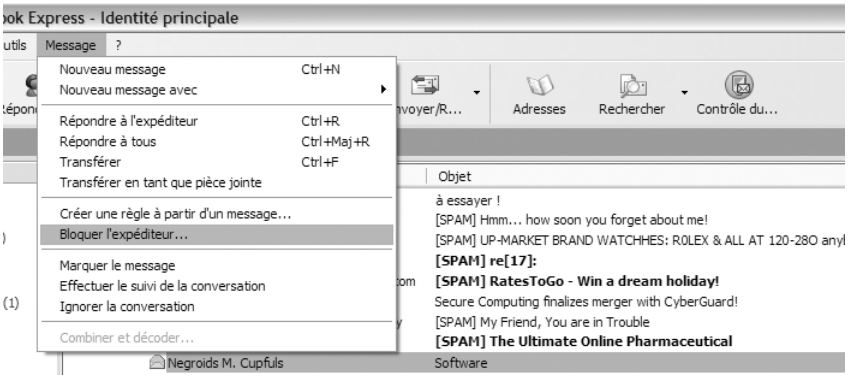


Figure 8–7
Bloquez les indésirables.

Thunderbird possède en outre un filtre antispam intégré dont l'efficacité dépasse largement celles de certains produits du commerce. Vous pouvez le configurer pour qu'il redirige automatiquement les messages qu'il juge indésirables vers un dossier spécifique. Dans le menu *Outils*, sélectionnez *Gestionnaire des indésirables* (figure 8-8). Activez l'option *Déplacer les*

messages entrants identifiés comme indésirables vers : et spécifiez le nom du dossier.

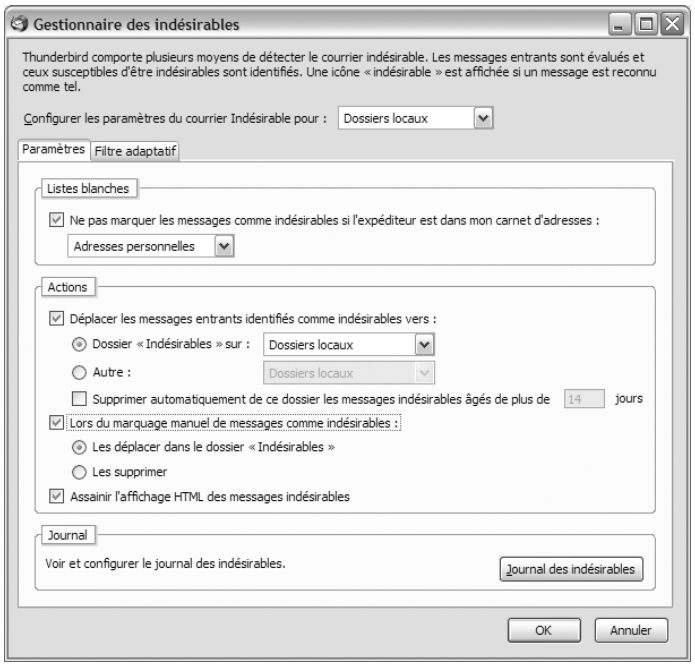


Figure 8–8
Déplacez les messages indésirables avec Mozilla Thunderbird.

Règles de filtrage des messages

Les clients de messagerie savent généralement trier et diriger les messages selon leur contenu. Pour cela, ils se basent sur des règles que vous pouvez très facilement élaborer.

Avec Outlook Express, dans le menu *Outils*, sélectionnez *Règles de message*, puis cliquez sur *Courrier*. Vous voyez apparaître un écran contenant toutes les règles qui s'appliquent à votre courrier électronique. Par exemple, la règle visualisée à la figure 8-9 demande à Outlook Express de rediriger automatiquement tous les messages dont la ligne « Objet » contient le mot « SPAM » vers le dossier *Éléments supprimés*.

Pour créer une nouvelle règle, cliquez sur *Nouveau*, et construisez votre propre politique de filtrage en fonction des nombreux paramétrage proposés. Sélectionnez une condition, une action et entrez les valeurs spécifiques en cliquant sur les liens affichés dans la zone description de la règle (figure 8-10).

Au besoin, affinez dans le temps la configuration en fonction des courriers indésirables reçus.

CONSEIL Supprimer ou déplacer ?

Faites attention avant de choisir l'action *Supprimer* : soyez sûr de vos conditions. Dans le cas contraire, choisissez plutôt de réorienter le message vers un dossier distinct, que vous inspecterez avant de procéder à la suppression définitive.

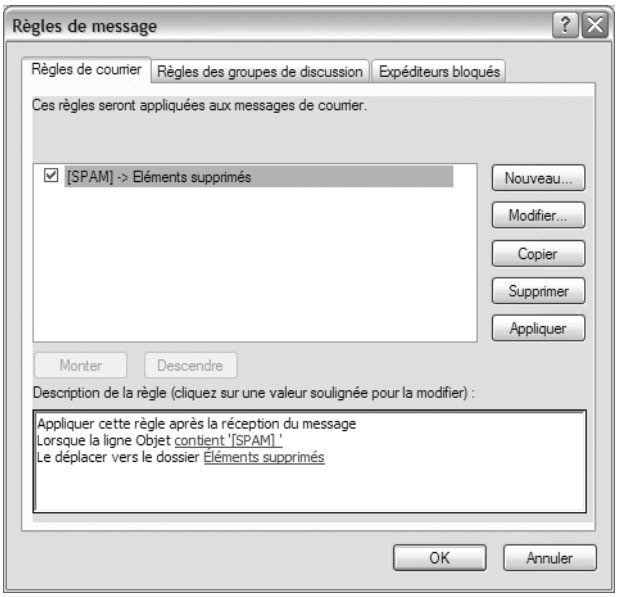


Figure 8–9
Règle de message d'Outlook Express

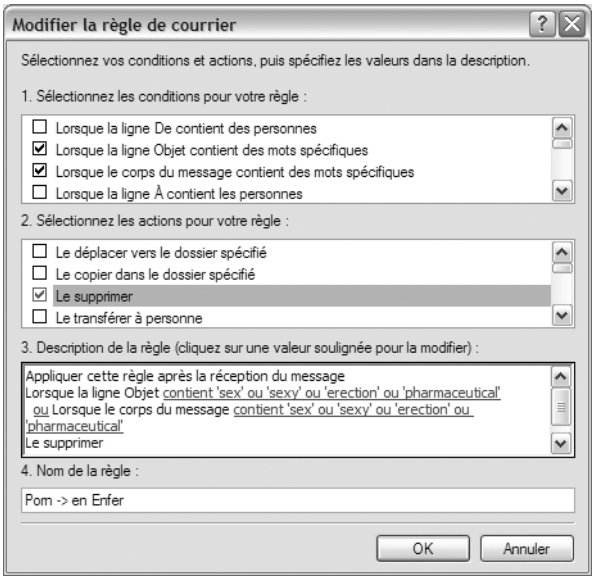


Figure 8–10
Modifier une règle de message avec Outlook Express

D'autres clients de messagerie, comme Thunderbird, Outlook 2003, Netscape ou Eudora Pro, permettent de créer et de gérer des règles de message de la même façon.

En outre, sachez que les services en ligne tels que AOL ou MSN disposent de mécanismes natifs antispam. N'hésitez pas à activer et à configurer ces fonctions de filtrage.

Installer un filtre antispam additionnel

Si vous recevez des quantités importantes de courrier indésirable, les règles que vous définissez manuellement ne suffiront peut-être plus à endiguer le fléau. Dans ce cas, vous serez obligé d'avoir recours à un filtre antispam : il enrichira votre politique de filtrage en place avec des moyens d'analyse et de filtrage généralement sophistiqués.

Principaux filtres antispam disponibles actuellement

L'une des meilleures recommandations que l'on puisse faire pour commencer, est de vous suggérer l'utilisation du client de messagerie Mozilla Thunderbird.

Thunderbird est un logiciel libre que vous pouvez télécharger et installer gratuitement à partir du site Mozilla-Europe, à l'adresse suivante : http://www.mozilla-europe.org/fr/products/thunderbird.

Outre le fait qu'il s'agisse d'un client très complet, léger (moins de 6 Mo) et facile à installer, Thunderbird est doté d'un filtre bayésien, capable de détecter la plupart des courriers indésirables et de vous protéger contre le phishing.

Si, à l'usage, vous vous rendez compte que ce type de solution ne suffit pas, là, seulement, vous pourrez envisager l'emploi d'un outil spécialisé.

Si vous disposez d'une suite logicielle antivirus, pare-feu, contrôle parental et ainsi de suite, il y a de fortes chances que vous soyiez déjà en possession d'un filtre antispam intégré. Toutefois, cela ne veut pas dire que vous êtes sauvé : le filtre antispam de certaines suites n'est pas toujours brillant !

En tenant compte de trois critères principaux, à savoir l'efficacité de la détection, les temps d'analyse et les erreurs commises, voici, à titre indicatif, quelques-uns des meilleurs produits du marché :

- le filtre antispam de la suite PC-cillin (Trend Micro), qui semble actuellement l'un des meilleurs, sinon le meilleur, mais n'est malheureusement pas commercialisé séparément ;
- Vade Retro (Goto Software) ;
- SafetyBar (Cloudmark) ;
- BitDefender SpamDeny (SoftWin).

Configurer un filtre antispam

Constituez d'abord votre liste d'expéditeurs autorisés (la fameuse « White List »). Elle repose généralement sur les contacts situés dans votre carnet d'adresses. Avec la suite logicielle F-Secure par exemple, dans la rubrique *Contrôle du courrier indésirable>Expéditeurs autorisés*, il vous suffit de cliquer sur *Importation* pour créer ou mettre cette liste à jour (figure 8-11).

QU'EST-CE QUE C'EST ? Filtre bayésien

Un filtre bayésien se caractérise par ses capacités d'apprentissage et le fait que son analyse s'appuie à la fois sur le contenu des messages indésirables, et sur celui des messages légitimes. Ainsi, il devient très difficile à un spammeur de déjouer ce type de filtre.

Figure 8–11
Créez et maintenez votre liste d'expéditeurs autorisés.

Constituez ensuite votre liste noire : au fur et à mesure que vous recevez des spams, faites entrer leurs expéditeurs dans la liste des expéditeurs filtrés. Avec certains filtres antispam, appuyer sur un bouton ou un simple clic droit suffit (voir figure 8-12).

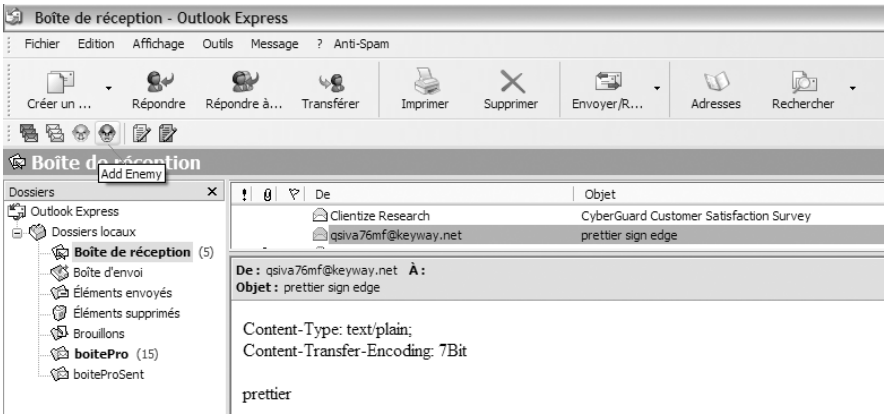


Figure 8–12
Constituez progressivement votre liste noire.

De façon générale, vous avez toujours la possibilité de gérer manuellement ces listes. Kaspersky Anti-Spam affiche plusieurs icônes dans la barre d'outils, à partir desquelles vous accédez directement aux fonctions de gestion (figures 8-12 et 8-13).

Figure 8–13
Gestion des listes

Lorsque vous recevez un spam, pensez à marquer le message comme tel avant de le détruire ; cela enrichit la base de connaissance de votre antispam, si celui-ci fonctionne par apprentissage. Avec Kaspersky Anti-Spam, un clic droit de la souris marque un message en tant que *Spam*, *Spam probable* ou *Obscène* (voir figure 8-14).

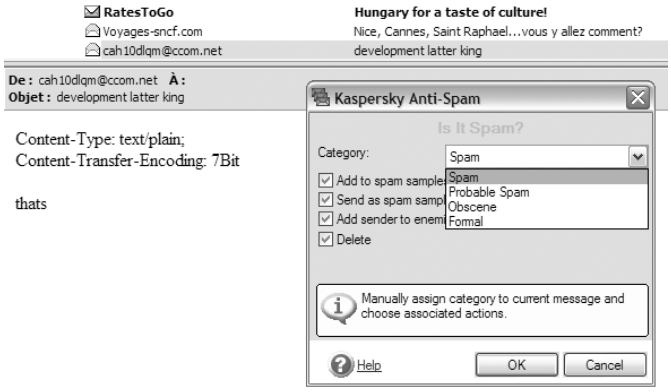


Figure 8–14
Marquez le courrier indésirable en tant que spam

Avec Thunderbird, un simple clic marque un message comme *Indésirable* (figure 8-15) ; ainsi s'enrichit son moteur d'analyse, basé sur un système à apprentissage.

📖 Daniel Garance, *Thunderbird, le mail sûr et sans spam*, collection Poche Accès Libre, Éditions Eyrolles, 2005

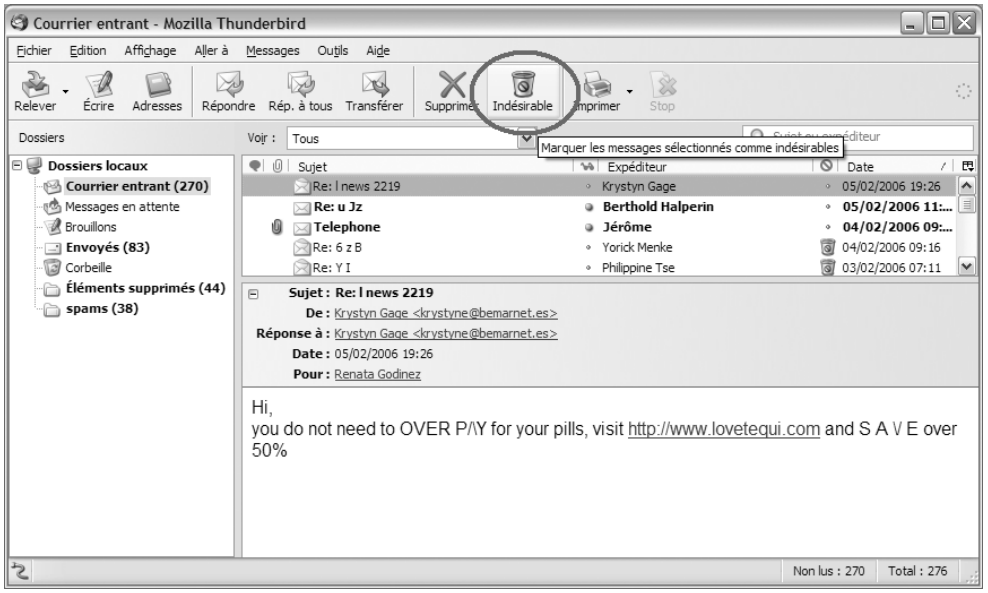


Figure 8–15 Un simple clic de souris marque le courrier comme indésirable.

Une solution simple pour une protection efficace

Les filtres basés sur les règles « manuelles » que vous définissez vous-même finiront tôt ou tard par se laisser berner par une bonne proportion de messages. Les annonceurs rivalisent d'astuces pour déjouer la sagacité de ces empêcheurs de tourner en rond, comme modifier l'orthographe des mots-clés susceptibles de déclencher une règle antispam. Par exemple, le « VIAGRA » se transformera en « V1AGRA » ou « VIAAGRRRA » et votre règle n'y verra que du feu. La figure 8-16 présente un exemple tout à fait classique de spam conçu pour tromper le filtre.

Figure 8–16
Type de spam conçu pour déjouer les règles des filtres

Par ailleurs, définir des règles de filtrage fondées sur la simple adresse source se révèlera très vite inefficace, car les spammeurs font en sorte de masquer leurs origines, ou s'appuient sur le carnet d'adresses de leurs victimes pour propager leurs publicités.

Si votre filtre antispam se laisse complètement déborder, ou si la politique de filtrage draconienne que vous êtes forcé de mettre en place provoque un nombre trop important de « faux positifs », cela veut dire qu'un filtre antispam représente de moins en moins la solution à votre problème. Pensez donc à changer d'adresse électronique et à repartir d'un bon pied.

CONSEIL Thunderbird pour les particuliers

Si vous êtes un particulier et si vous faites un usage raisonnable d'Internet, la solution qui répondra certainement le mieux à votre attente consiste à utiliser le client de messagerie Thunderbird. Non seulement ce logiciel est gratuit, mais son antispam est d'une efficacité étonnante ; comme il est activé dès l'installation du logiciel, vous n'avez plus qu'à marquer les messages indésirables comme tels pour instruire le filtre. Tous les courriers indésirables seront désormais expédiés dans un dossier spécial, sans intervention de votre part, le tout avec un taux d'erreur très faible !

- http://www.mozilla-europe.org/fr/products/thunderbird/

Réduire les risques d'infection virale ou de pénétration via la messagerie

La messagerie électronique est une des cibles préférées des pirates, ce qui en fait un important vecteur de virus et autres codes malveillants. Apprenez à la configurer de façon à limiter autant que possible ces risques.

Optimiser la configuration de son antivirus vis-à-vis de la messagerie électronique

Les programmes antivirus réputés offrent des fonctions dédiées spécifiquement à l'analyse du courrier électronique. Ces fonctions bloquent en amont tout courrier entrant associé à une pièce jointe porteuse de virus et font barrage à tout courrier sortant susceptible d'être émis par un ver.

Vous accédez généralement à l'option d'analyse du courrier électronique à partir de la fenêtre principale de l'antivirus (voir figure 8-17).

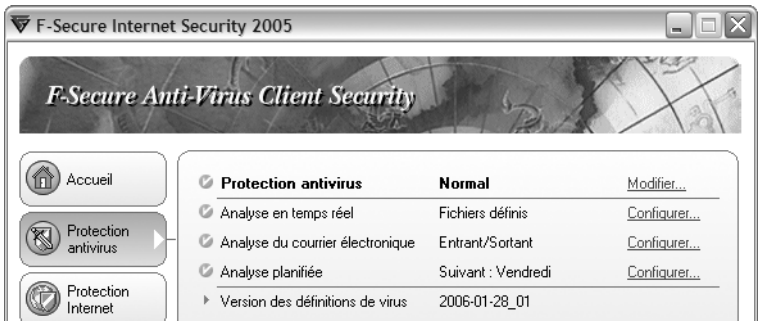


Figure 8–17
Activez l'analyse du courrier électronique avec l'antivirus.

Vous disposez généralement de plusieurs options pour définir les types de pièces jointes à analyser en fonction de leur extension (toutes les pièces jointes ou seulement celles dont les extensions figurent parmi une liste que vous gérez) ; vous pouvez en outre spécifier les types de fichiers compressés à analyser et, éventuellement, les exclusions.

Bien entendu, pour plus de sécurité, il faudrait laisser l'antivirus analyser toutes les pièces jointes. Cependant, plus les types de fichiers à analyser sont nombreux, plus les temps de traitement sont longs. Il vous appartient de définir, en fonction des capacités de votre machine, le meilleur compromis entre un niveau de sécurité optimal et des performances acceptables.

Bloquer images et contenus externes dans les messages HTML

En raison des risques d'installation de codes mobiles (voir à ce sujet le chapitre 7), les messages HTML constituent une source d'intrusion potentielle.

Afin de réduire les risques d'intrusion ou d'infection virale, prenez l'habitude de lire les messages de sources inconnues en texte brut :

- Avec Thunderbird, à partir du menu *Affichage*, sélectionnez *Corps du message en*, puis choisissez *Texte seul* (figure 8-18).

PRATIQUE Filtrez vos courriers électroniques avec votre antivirus

Ce type de protection apporte indiscutablement une couche de sécurité supplémentaire, et il serait dommage de ne pas en profiter : pensez à activer l'analyse du courrier électronique !

RAPPEL Analyse complète de l'ordinateur

N'oubliez pas qu'un logiciel antivirus bien configuré analysera régulièrement le contenu intégral de votre machine (tous les fichiers, sans exclusion). Donc, si une pièce jointe infectée parvenait à passer au travers des deux protections – messagerie et temps réel – de l'antivirus, elle serait de toute façon anéantie à la prochaine analyse complète.

LE CONSEIL DU PRO
Lisez vos messages en format texte

Lorsque l'expéditeur vous est inconnu, ne lisez pas un message en format HTML, mais en format texte. De cette façon, vous limitez le risque d'intrusion ou d'infection virale.

Figure 8–18
Lire les messages en texte seul.

- Avec Outlook Express, dans le menu *Outils*, sélectionnez *Options*, puis cliquez sur l'onglet *Lecture* et cochez la case *Lire tous les messages en texte clair* (figure 8-19).

Figure 8–19
Activez l'option Lire tous les messages en texte clair.

Avec ce paramétrage, vous pouvez tout de même lire un message individuel en HTML si vous faites confiance à son expéditeur. Lorsque le message est sélectionné, il vous suffit pour cela de cliquer sur le menu *Affichage*, puis sur *Message HTML* (figure 8-20).

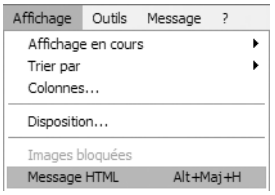


Figure 8–20
Si le message provient d'une source de confiance, vous pouvez revenir au mode HTML.

Préserver la confidentialité et garantir l'authenticité d'un message électronique

Avec l'utilisation croissante des technologies de l'information et la généralisation des échanges sous forme électronique, la protection du contenu d'un courrier électronique contre les regards indiscrets, ou l'assurance de l'authenticité d'un message et de son émetteur deviennent des exigences incontournables.

En effet, à l'heure où les Administrations françaises militent en faveur de la dématérialisation des procédures, où directives européennes et décrets gouvernementaux œuvrent conjointement pour mettre en place un cadre réglementaire relatif à la signature électronique, comment imaginer qu'un échange électronique falsifié soit à l'origine de contentieux importants en milieu professionnel, ou que la déclaration de revenus d'un particulier soit accessible par un tiers ?

Avoir recours aux procédés cryptologiques pour protéger la messagerie et les échanges électroniques devient une nécessité ; tout le monde, entreprises comme particuliers, y est de plus en plus confronté par la force des choses. Si signer et chiffrer un message sont des opérations simples à réaliser (une fois les services de sécurité correctement configurés, cela s'entend), le choix des solutions et le mode de gestion des secrets (principalement les certificats) sont délicats et influent considérablement sur le niveau de sécurité atteint.

C'est pourquoi nous allons étudier dans cette partie ce qu'implique la mise en œuvre des services cryptologiques de la messagerie et voir les types de solutions de sécurité à envisager, en fonction du contexte d'utilisation et du niveau de sécurité requis.

Principes de fonctionnement des échanges sécurisés

Avant toute chose, il faut savoir que les techniques de sécurisation de la messagerie électronique font appel à des mécanismes cryptologiques. En pratique, tous les mécanismes de sécurité décrits ci-après sont pris en charge par le système de messagerie et se déroulent de façon tout à fait transparente pour l'utilisateur.

Considérons deux acteurs principaux : Alice, l'émetteur du message sécurisé, et Bernard, le destinataire.

Chiffrement d'un message

Voici comment s'effectue l'émission d'un message chiffré :

- Votre client de messagerie commence d'abord par engendrer un nombre aléatoire, la clé secrète qui servira à chiffrer le message. Selon le type d'algorithme de chiffrement sélectionné, cette clé formera un nombre de 40, 56, 64, 128 ou 168 bits. Par ailleurs, cette clé secrète est à usage unique, c'est pourquoi on l'appelle « clé de session » (notée $K_{SESSION}$ sur le schéma de la figure 8-21).
- Le message M est ensuite chiffré à l'aide de l'algorithme symétrique sélectionné (DES, 3DES, RC2, etc.) et de $K_{SESSION}$.

RENVOI **Principes de la cryptologie**

Pour bien comprendre cette section, il est fortement conseillé de se remettre en tête les principes de fonctionnement des mécanismes cryptologiques. Relisez à ce sujet la présentation simplifiée d'éléments de cryptologie située en annexe, ainsi que le chapitre 6 concernant la gestion et l'utilisation des certificats.

- La clé de session est à son tour chiffrée avec l'algorithme RSA et la clé publique du destinataire, Bernard ($Kp_{Bernard}$). Pour réaliser cette opération, Alice doit nécessairement posséder une copie du certificat numérique de Bernard.
- L'ensemble est ensuite transmis à Bernard en un seul message.

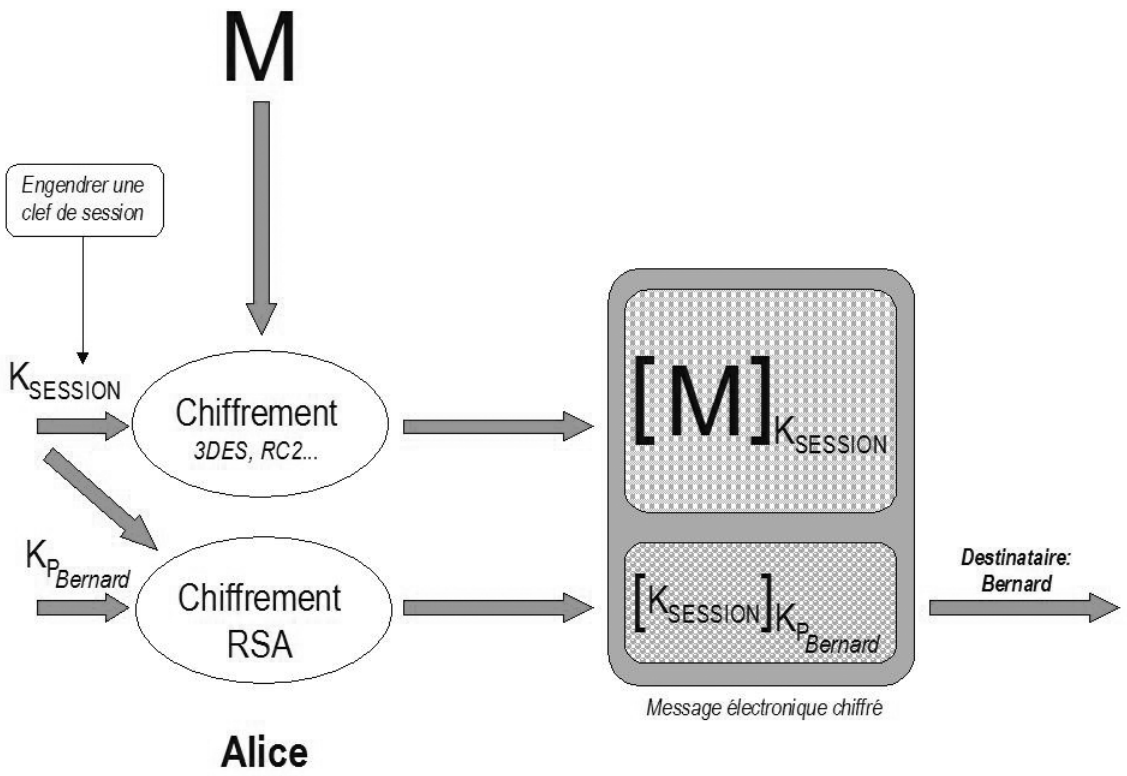


Figure 8–21 Principes mis en œuvre lors de l'échange d'un message chiffré.

- Lorsque Bernard reçoit le message, il commence par déchiffrer la clé de session $K_{SESSION}$. Lui seul peut effectuer cette opération car lui seul connaît sa propre clé privée, $Ks_{Bernard}$ associée à $Kp_{Bernard}$.
- Connaissant maintenant $K_{SESSION}$, il n'a plus qu'à déchiffrer le message chiffré par Alice, en utilisant le même algorithme (DES, 3DES, RC2, etc.). Optionnellement, il vérifie la signature et l'estampille temporelle.

AVANCÉ **Signature et estampille temporelle**

Dans la pratique, le message contient éventuellement une signature et une estampille temporelle, non représentées sur la figure 8-21 pour plus de clarté.

CRYPTOLOGIE Utilisation des différents types d'algorithmes

L'immense avantage des algorithmes à clés publiques est d'offrir la possibilité de chiffrer et de déchiffrer une information, *sans divulguer aucun secret au préalable* : le chiffrement s'effectue avec une clé que tout le monde connaît, la clé publique, alors que le déchiffrement est réalisé à l'aide d'une autre clé, la clé privée associée à cette clé publique, que seul le destinataire possède. Lorsqu'il s'agit de passer un appel téléphonique, vous devez connaître le numéro de votre correspondant ; de même, lorsque vous connaissez la clé publique du destinataire, chiffrer ou déchiffrer une information est une opération instantanée.

Ce n'est pas le cas des algorithmes symétriques (ou à clés secrètes), où une même clé est utilisée pour les opérations de chiffrement et de déchiffrement. Pour que l'émetteur et le destinataire puissent échanger une information chiffrée, ils doivent être en possession du même secret (la clé). Soit ils se mettent mutuellement d'accord sur une valeur secrète partagée, soit l'un des deux fixe cette valeur et la transmet à l'autre avant d'entamer les échanges sécurisés. Bien entendu, le secret ne doit jamais tomber entre les mains d'un tiers, sinon celui-ci pourra lire tous les messages protégés. Si un tel schéma est réaliste avec un nombre restreint d'utilisateurs (c'est le cas notamment des systèmes militaires, extrêmement rigoureux sur les procédures de « mise à la clé »), ce problème de transmission de la clé rend presque impossible l'utilisation des algorithmes symétriques à grande échelle. En effet, hormis le fait que la phase d'échange des clés secrètes nuise à l'interactivité de la communication, comment assurer la distribution de millions de clés secrètes sur Internet de façon sécurisée ?

Toutefois, les algorithmes symétriques présentent un avantage qui les rend incontournables : ils sont environ mille fois plus rapides que leur cousins asymétriques.

C'est pourquoi les messageries électroniques – et les applications sécurisées en général – combinent les deux types d'algorithmes. Pour des raisons de performances, le chiffrement du message, c'est-à-dire de l'information volumineuse, est réalisé avec un algorithme symétrique (comme DES, 3DES ou RC2). En ce qui concerne le problème de la transmission de la clé, les algorithmes asymétriques viennent à la rescousse : une clé est une information courte, qui est donc transmise de l'émetteur vers le destinataire, chiffrée avec un algorithme à clés publiques (comme RSA).

Signature d'un message

Alice souhaite expédier un message signé à Bernard, afin de prouver qu'elle seule a écrit ce message, et personne d'autre. Le principe de la signature d'un courrier électronique repose sur le chiffrement du message avec RSA et la clé privée de l'expéditeur.

Nous avons signalé précédemment que les algorithmes à clés publiques étaient lents. Afin d'optimiser les performances, les clients de messagerie ne chiffrent pas l'intégralité du message ; ils calculent tout d'abord ce

que l'on appelle un « résumé » du message, une empreinte numérique de type MD5 ou SHA-1.

MD5 et SHA-1 sont des fonctions dites de « hachage à sens unique », chargées de calculer une empreinte cryptologique de longueur fixe (128 bits avec MD5, 160 bits avec SHA-1), quelle que soit la longueur du message. Dans le contexte de la messagerie électronique sur Internet, on admet les hypothèses suivantes :

- Connaissant une empreinte numérique, il n'est pas possible de retrouver le message d'origine.
- Il est impossible de trouver deux messages différents dont les empreintes numériques soient identiques.

Partant de ces principes, Alice chiffre le résumé du message avec sa clé privée, notée Ks_{Alice} sur la figure 8-22. Ce résumé chiffré lie cryptologiquement le message et Alice : c'est donc ce que l'on appelle la signature du message par Alice.

Le client de messagerie envoie ainsi le message, auquel il adjoint la signature et, selon les paramètres de configuration du client de messagerie, le certificat d'Alice dans lequel se trouve la clé publique Kp_{Alice}.

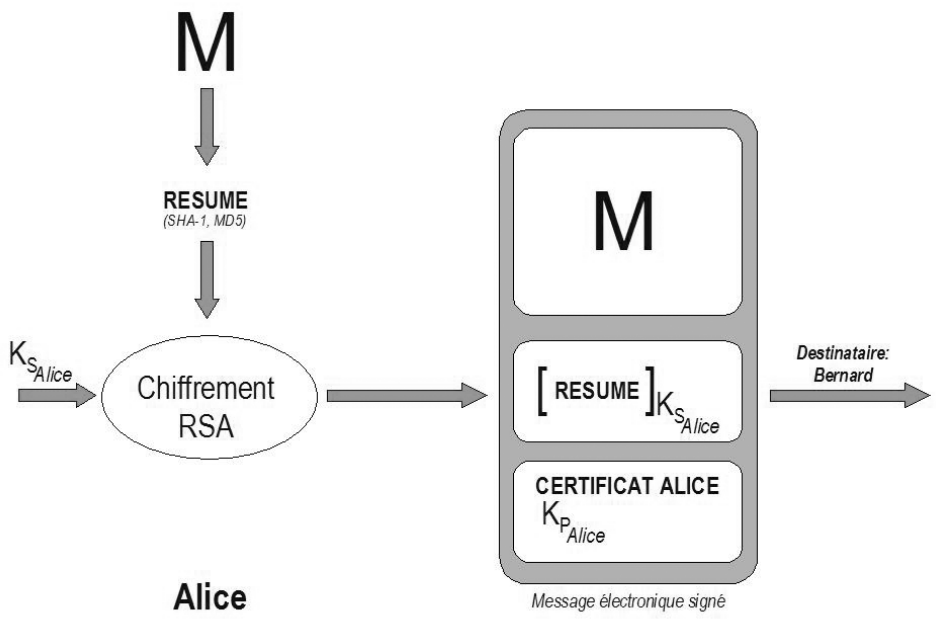


Figure 8–22 Principes mis en œuvre pour signer un message électronique

Pour vérifier cette signature, Bernard calcule l'empreinte numérique du message reçu, à l'aide de MD5 ou de SHA-1, selon l'algorithme utilisé par Alice.

Il déchiffre ensuite la valeur de la signature avec RSA et la clé publique d'Alice, KpAlice. Si les deux valeurs sont égales, cela prouve :

- que le message a bien été signé par Alice ;
- qu'il est intègre (il n'a pas été modifié durant son transfert).

RAPPEL Principes d'une signature

Le principe est très simple : il repose sur le fait qu'Alice chiffre une information *avec sa clé privée* ; elle seule est capable d'effectuer cette opération. En revanche, tout le monde peut déchiffrer l'information avec la clé publique d'Alice, et en conclure que cette dernière en est bien l'expediteur.
Exemple :
Alice prouve qu'elle seule, et personne d'autre, a joué la combinaison gagnante du loto : 24, 2, 47, 21, 3 et 39. Pour cela, au moment où elle effectue la mise, elle prend soin d'écrire au-dessous de chaque nombre, la valeur dudit nombre chiffrée avec l'algorithme RSA et sa clé privée ; au-dessous de 24, 2, 47, 21, 3 et 39 figurent donc les valeurs 23 998, 24 343, 7 778, 16 489, 37 405 et 34 281, que personne d'autre ne sait calculer.
Tout le monde sait que la clé publique (e=30 503, n=66 203) est bien celle d'Alice, puisqu'elle est certifiée par une Autorité de Certification. Chacun peut donc effectuer les calculs simples suivants :
- $23\,998^{30\,503} \bmod 66\,203 = 24$
- $24\,343^{30\,503} \bmod 66\,203 = 2$
- $7\,778^{30\,503} \bmod 66\,203 = 47$
- $16\,489^{30\,503} \bmod 66\,203 = 21$
- $37\,405^{30\,503} \bmod 66\,203 = 3$
- $34\,281^{30\,503} \bmod 66\,203 = 39$

et vérifier que cette combinaison provient bien d'Alice, et de personne d'autre.

Chiffrer et signer à l'aide des certificats

Examinons maintenant comment tout se déroule concrètement lorsque vous envoyez un courrier avec votre client de messagerie habituel.

Échanger des messages signés et/ou chiffrés avec un correspondant

La cryptologie offre des mécanismes de sécurité de très haut niveau, mais son utilisation exige une grande rigueur. Si vous intégrez bien les quelques notions qui suivent, le reste vous paraîtra simple comme bonjour.

Pour utiliser les services de chiffrement et de signature avec la messagerie, vous devez suivre les principes suivants :

- **Vous chiffrez un message avec la clé publique de votre correspondant** – Vous devez donc importer dans votre client de messagerie les certificats numériques de tous les correspondants vers lesquels vous voulez émettre des messages chiffrés.

  En corollaire, si vous souhaitez que quelqu'un vous adresse un message chiffré, vous devez avoir obtenu un certificat numérique et l'avoir publié ou diffusé à vos interlocuteurs.
- **Vous signez un message avec votre clé privée** – Vous êtes le seul à connaître et à posséder votre clé privée ; donc vous seul êtes capable de calculer cette signature. En revanche, tout le monde a accès à votre clé publique et peut vérifier cette signature.

  Pour signer, vous devez donc impérativement détenir votre propre certificat, l'intégrer à votre client de messagerie et le publier ou le diffuser à vos interlocuteurs.
- Ne signez **jamais** un message avec un certificat utilisé par vos interlocuteurs pour vous envoyer des messages chiffrés.

  En effet, des attaques cryptologiques risqueraient de dévoiler vos secrets.

  Si vous devez signer et chiffrer un message, utilisez un certificat de signature et un certificat de chiffrement distincts.

Pour utiliser les services de chiffrement et de signature offerts par la messagerie, il ne vous reste plus qu'à obtenir un certificat, à le diffuser ou le publier et à l'intégrer dans votre client de messagerie ; parallèlement à cela, vous devez intégrer les certificats numériques de vos correspondants.

Obtenir un certificat et l'intégrer dans votre client de messagerie

Vous pouvez obtenir un certificat – ou un identificateur numérique selon la terminologie employée – auprès de l'Autorité de Certification de votre choix (voir chapitre 6).

Si vous ne connaissez pas d'Autorité de Certification (AC) en particulier, consultez l'aide de votre client de messagerie ; certains vous proposent un lien direct vers un site qui vous aiguillera vers une Autorité de Certification reconnue (figure 8-23).

Avec Internet Explorer par exemple, cliquez sur *I want to get a digital ID* et suivez les instructions. Vous aurez juste à entrer un nom, un mot de passe destiné à protéger l'accès au certificat et votre adresse électronique.

Une fois votre certificat établi par l'AC, vous devez l'importer dans votre magasin de certificats. Avec certaines AC, il suffit de presser le bouton *INSTALL* pour que cette procédure se déroule automatiquement (figure 8-24).

ATTENTION **Certificat de messagerie et adresse électronique**

Ce certificat de messagerie est intimement lié à votre adresse électronique. Si vous vous trompez dans la saisie de cette adresse, vous ne pourrez pas vous servir du certificat.

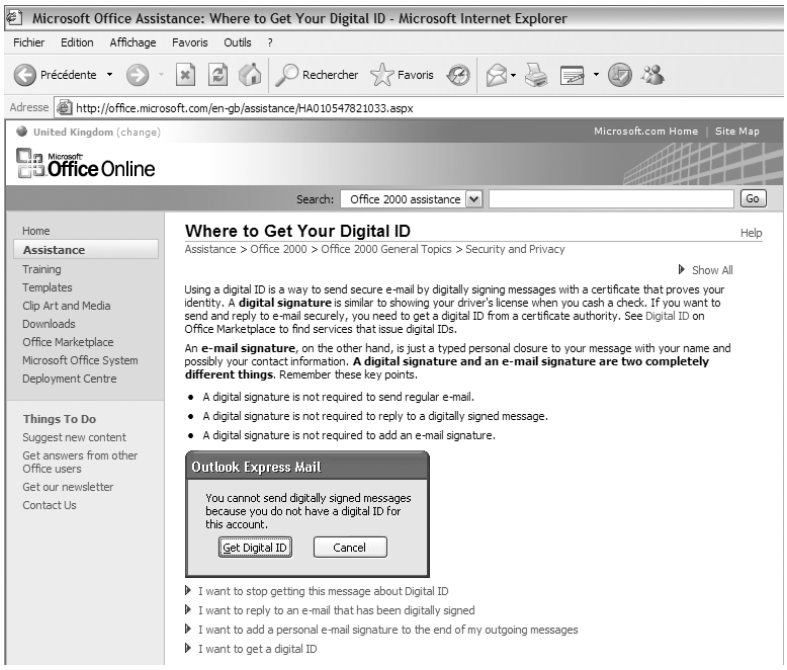


Figure 8–23
Obtenir un certificat auprès d'une Autorité de certification

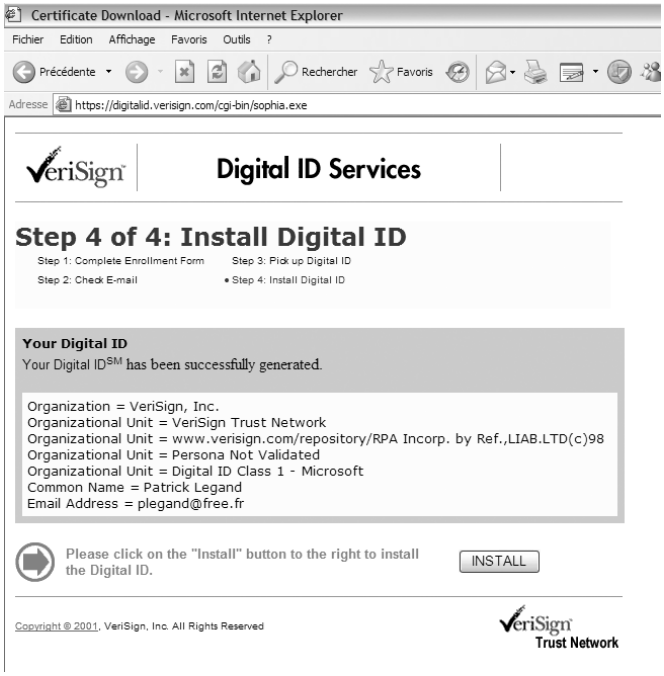


Figure 8–24
Installation du certificat dans votre magasin de certificats

Il ne vous reste plus qu'à associer le certificat à votre compte. Avec Thunderbird par exemple, dans le menu *Outils*, choisissez *Paramètres des comptes* et cliquez sur *Sécurité* (figure 8-25).

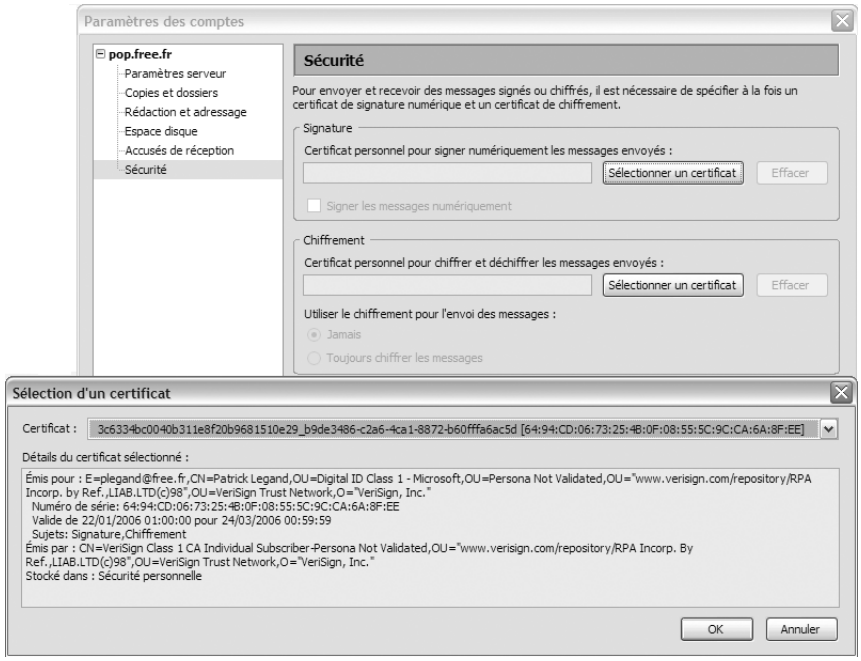


Figure 8–25
Association du certificat à votre client compte de messagerie

Si vous destinez ce certificat aux opérations de signature, cliquez sur le bouton *Sélectionner un certificat*, choisissez celui qui vous intéresse, puis cliquez sur *OK*. L'opération est terminée.

Attention toutefois à ne pas tomber dans le piège : le logiciel vous propose d'utiliser ce même certificat comme certificat de chiffrement (figure 8-26). Refusez cette option et faites-vous établir un autre certificat que vous destinerez aux opérations de chiffrement.

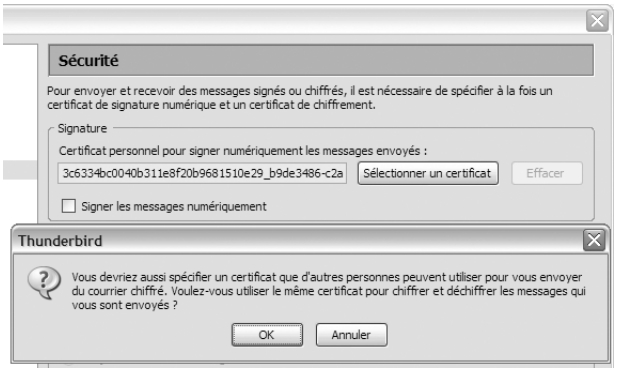


Figure 8–26
Attention à ne pas utiliser le même certificat pour signer et pour chiffrer.

Diffuser votre certificat à vos interlocuteurs

Allez dans votre magasin de certificats :

- Avec Firefox, depuis la barre de menus, choisissez *Outils*, puis sélectionnez *Options* et cliquez sur *Avancé*. Dans la fenêtre de droite, cliquez sur *Certificats*, puis sur le bouton *Gérer les certificats* (figure 8-27).

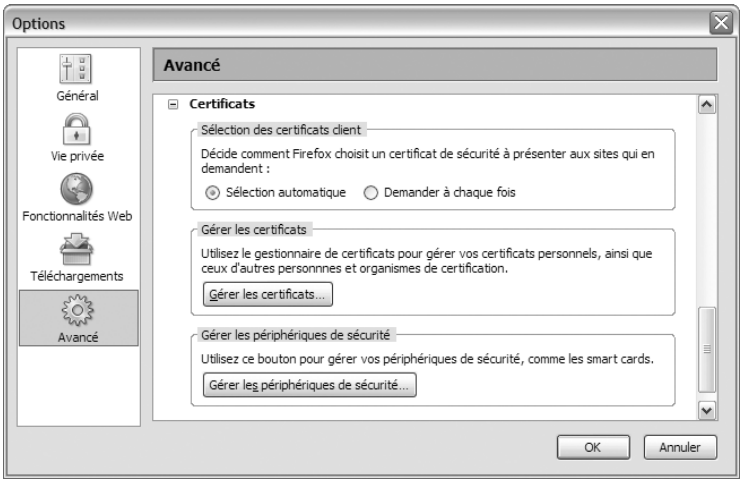


Figure 8–27
Allez dans votre magasin de certificats.

Sélectionnez le certificat que vous voulez diffuser, cliquez sur *Exporter* et suivez les instructions (figure 8-28).

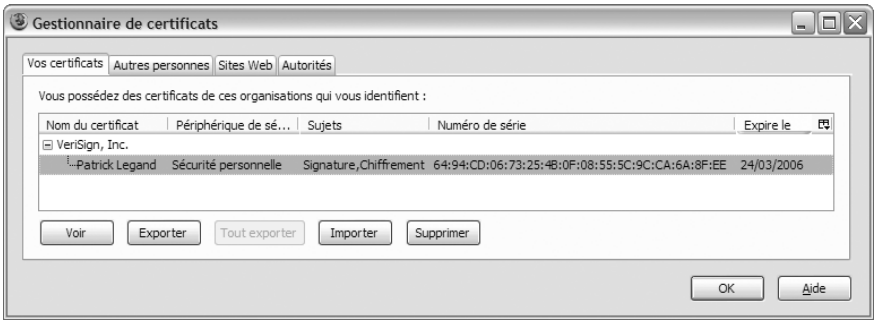


Figure 8–28
Exportez votre certificat avec Firefox.

- Avec Internet Explorer, dans le menu *Outil*, choisissez *Options Internet*, puis sélectionnez l'onglet *Contenu* et cliquez sur *Certificats* (figure 8-29).

  Dans l'onglet *Personnel*, sélectionnez le certificat que vous voulez diffuser, cliquez sur *Exporter* et suivez les instructions de l'assistant *Exportation de certificat* (figure 8-30). Bien entendu, choisissez l'option *Ne pas exporter la clef privée* !

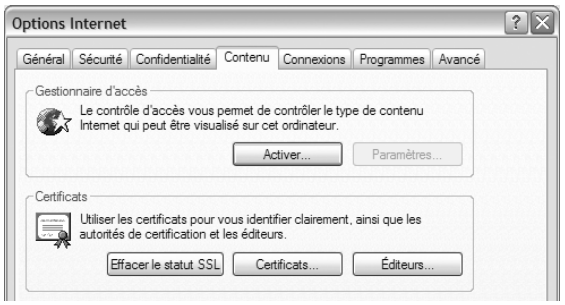


Figure 8–29
Allez dans votre magasin de certificats avec IE.

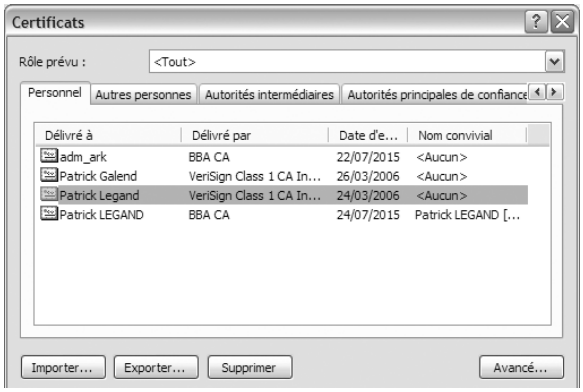


Figure 8–30
Exportez votre certificat avec Internet Explorer.

Vous obtenez un fichier à un format spécial, par exemple PKCS#7 ou PKCS#12 (vous avez le choix entre plusieurs formats). Transmettez-le à vos interlocuteurs, en utilisant les moyens à votre convenance (par télégraphe et en morse, ou tout simplement en tant que pièce jointe d'un courrier électronique).

Astuce **Ne faites rien !**

Une méthode bien plus simple consiste à ne rien faire. En effet, après vous avoir délivré un certificat, les Autorités de Certification le publient en général automatiquement dans leur annuaire. Si quelqu'un souhaite vous envoyer un message chiffré, c'est à lui de se débrouiller pour récupérer votre certificat. Nous verrons plus loin comment procéder.

Lorsque vous envoyez un message signé, c'est encore plus simple : le certificat contenant votre clé publique est émis avec le message. Pour vérifier la signature, votre correspondant n'a qu'à cliquer sur un bouton. Nous verrons aussi plus loin comment cela se passe.

Récupérer et intégrer le certificat d'un correspondant

Bien entendu, nous supposons que cette personne est déjà titulaire d'un certificat destiné exclusivement au chiffrement des messages.

Pour récupérer ce certificat, allez sur le serveur en ligne de l'Autorité de Certification qui l'a émis. À la figure 8-31, vous constatez par exemple que Verisign vous permet de retrouver un certificat très facilement, et vous offre même plusieurs critères de recherche (adresse électronique, numéro de série, etc.).

Le plus simple est d'entrer l'adresse électronique de votre correspondant et de lancer la recherche. Vous trouvez ainsi aisément le certificat que vous cherchez (figure 8-32).

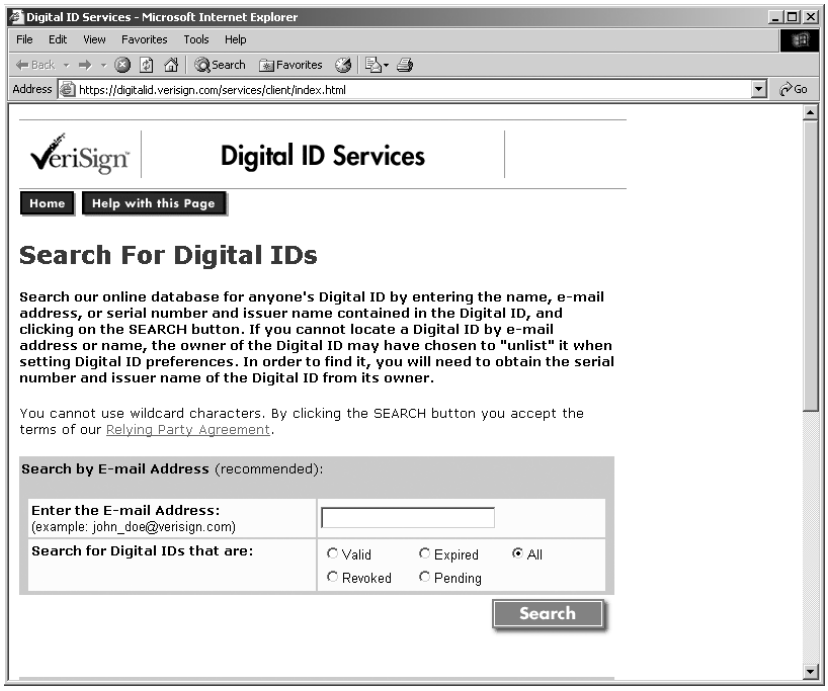


Figure 8–31
Retrouvez un certificat facilement à partir du site de l'Autorité de Certification.

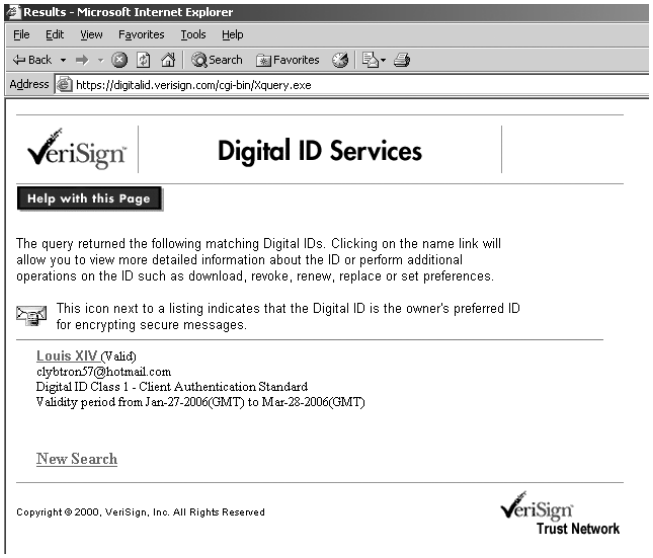


Figure 8–32
Cliquez sur le lien pour accéder au certificat et procéder au téléchargement.

Il vous suffit alors de cliquer sur le lien associé au détenteur de ce certificat pour accéder à la page de téléchargement. Rapatriez le certificat sur votre poste ; parmi les options proposées, choisissez le format *S/MIME Binary PKCS#7*.

Cette opération réussie, il ne vous reste plus qu'à associer ce certificat à son détenteur dans votre carnet d'adresses. Avec Outlook Express par exemple, dans votre carnet d'adresses, cliquez droit sur le nom de votre correspondant, sélectionnez *Propriétés*, cliquez ensuite sur le bouton *Identificateurs numériques*, puis sur le bouton *Importer* (figure 8-33).

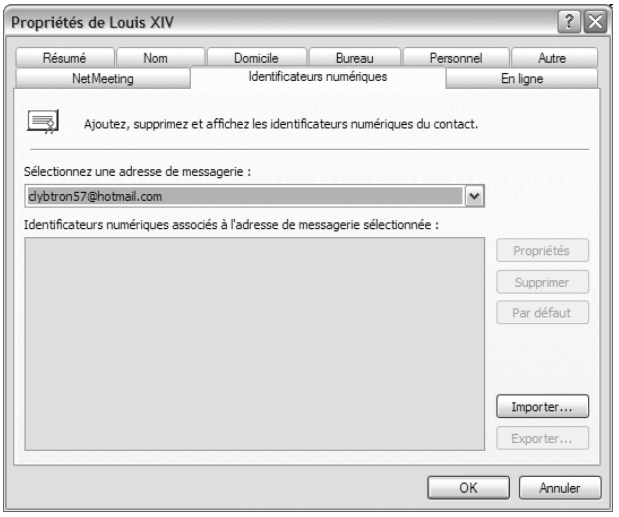


Figure 8–33
Dans votre carnet d'adresses, associez le certificat à son détenteur.

À partir de ce moment, si vous le désirez, vous pourrez chiffrer toute votre correspondance avec cet interlocuteur.

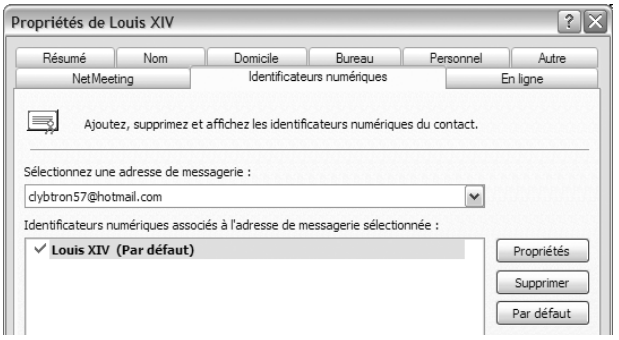


Figure 8–34
Vous êtes désormais prêt à émettre des messages chiffrés.

Signer ou chiffrer un message

Une fois ces opérations de configuration préliminaires accomplies, signer ou chiffrer un message devient extrêmement simple.

Commencez d'abord par vérifier que les boutons *Sécurité* (Thunderbird) ou *Signer* et *Crypter* (Outlook Express) sont bien présents sur la barre d'outils de votre client de messagerie. Si ce n'est pas le cas, avec Outlook Express, à partir du menu *Affichage*, choisissez *Barres d'outils* et cliquez

sur *Personnaliser* (figure 8-35). Sélectionnez ensuite les boutons *Signer* et *Crypter* qui apparaissent dans la zone des boutons disponibles à gauche de l'écran, puis cliquez sur *Ajouter*. Pressez éventuellement les boutons *Monter* ou *Descendre* selon la position souhaitée, puis cliquez sur *Fermer*. Les opérations de signature et de chiffrement vous sont désormais directement accessibles en un clic de souris.

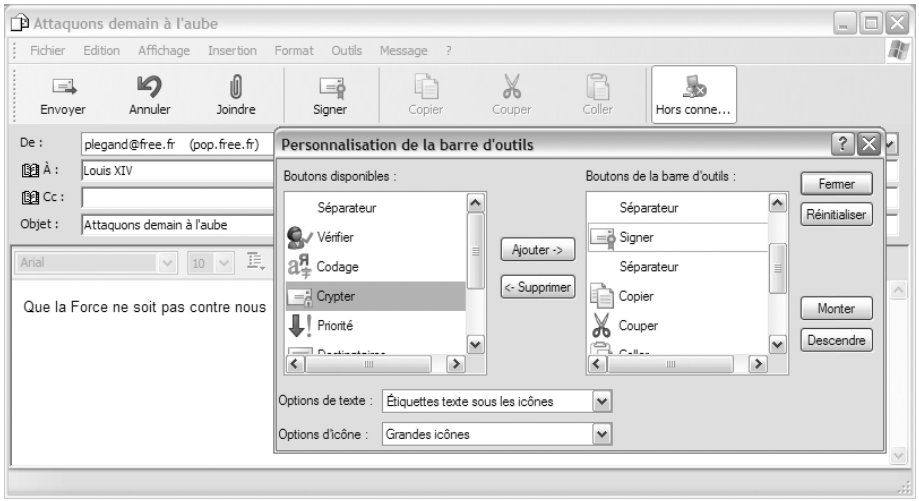


Figure 8–35
Personnalisez votre barre d'outils.

Si vous voulez chiffrer votre message, il vous suffit de cliquer sur le bouton *Crypter* (figure 8-36). Vous verrez apparaître à droite de l'expéditeur un petit cadenas qui symbolise le fait que le message sera chiffré avant l'envoi.

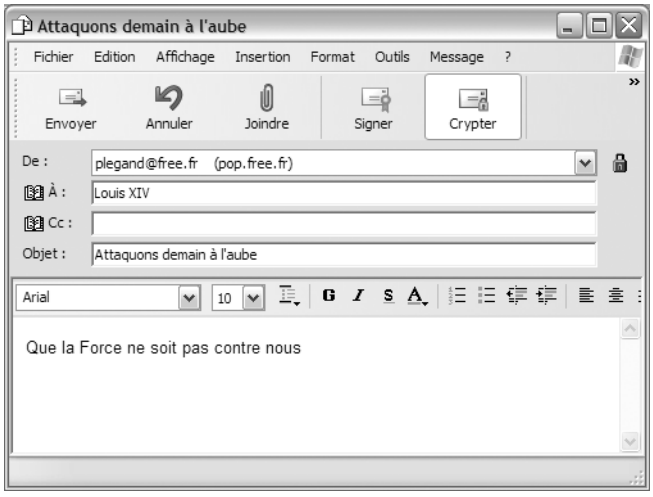


Figure 8–36
Pour chiffrer le message, cliquez sur Crypter.

ATTENTION Vous ne pourrez pas relire un message que vous avez chiffré

Personne d'autre que votre correspondant ne pourra relire le courrier chiffré que vous lui envoyez, pas même vous. En effet, il n'y a aucune raison pour que vous possédiez sa clé privée. Deux possibilités s'offrent à vous pour garder de votre correspondance une trace chiffrée mais lisible par vous :

- sauvegarder le message en clair, mais dans un dossier chiffré (voir chapitre 2) ;
- vous envoyer une copie à vous-même en chiffrant avec votre propre clé publique.

Vous n'avez plus qu'à cliquer sur *Envoi* pour faire partir le message chiffré. Votre client de messagerie ira chercher automatiquement le certificat du correspondant dans votre carnet d'adresses et, dès lors, plus personne ne pourra, en théorie, accéder au contenu de ce message, à part votre correspondant.

Pour signer le message, c'est très simple : il suffit de cliquer sur le bouton *Signer* avant de cliquer sur *Envoi*.

Bien entendu, vous pouvez signer d'abord le message et le chiffrer ensuite avant de procéder à l'envoi.

Lire un message chiffré par votre correspondant

Selon le client de messagerie utilisé ou les options de configuration sélectionnées, le message chiffré est reconnaissable par une marque spécifique. Avec Outlook Express, il s'agit par exemple d'une petite icône en forme de cadenas située sur l'enveloppe (figure 8-37).

Figure 8–37
Lire un message chiffré

L'opération de déchiffrement est extrêmement simple : vous cliquez sur le message, optionnellement vous autorisez le programme à accéder à votre clé privée, ou bien vous entrez le mot de passe qui protège celle-ci (cela dépend du niveau de sécurité que vous avez attribué à votre certificat au moment de sa création), et le message déchiffré apparaît à l'écran comme n'importe quel autre message. C'est tout.

Vérifier la signature et donc l'authenticité d'un message

Lorsque vous recevez un courrier électronique signé, l'icône qui symbolise l'enveloppe de ce message est revêtue du sceau indiquant la présence d'une signature (figure 8-38).

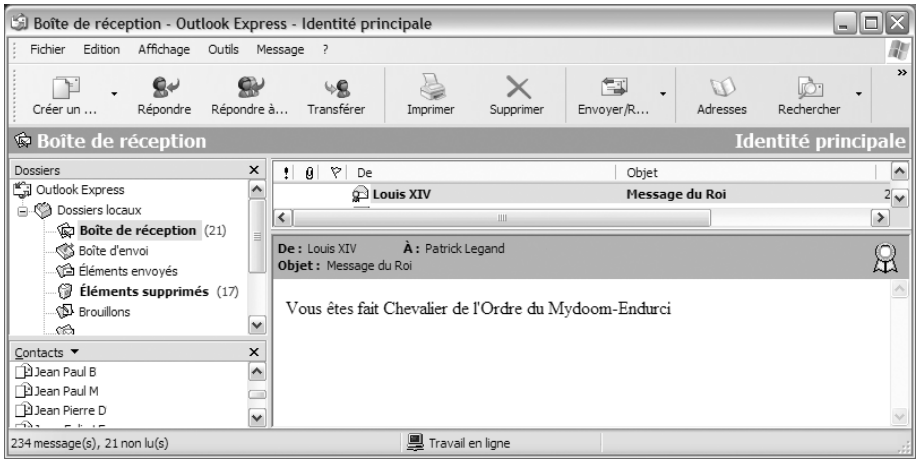


Figure 8–38
Réception d'un message signé

Une première vérification est réalisée automatiquement par votre client de messagerie. En effet, celui-ci effectue deux calculs distincts. D'une part, il recalcule l'empreinte numérique de ce message en utilisant l'algorithme spécifié à l'intérieur du certificat de l'émetteur, joint à ce message (MD5 ou SHA-1 le plus souvent). D'autre part, à l'aide de la clé publique contenue dans ce certificat, il déchiffre la signature calculée par l'expéditeur au moment de l'émission. Si les deux valeurs sont identiques, cela prouve que le message a bien été signé avec la clé privée associée au certificat de signature, et que le message n'a pas été altéré durant son transfert.

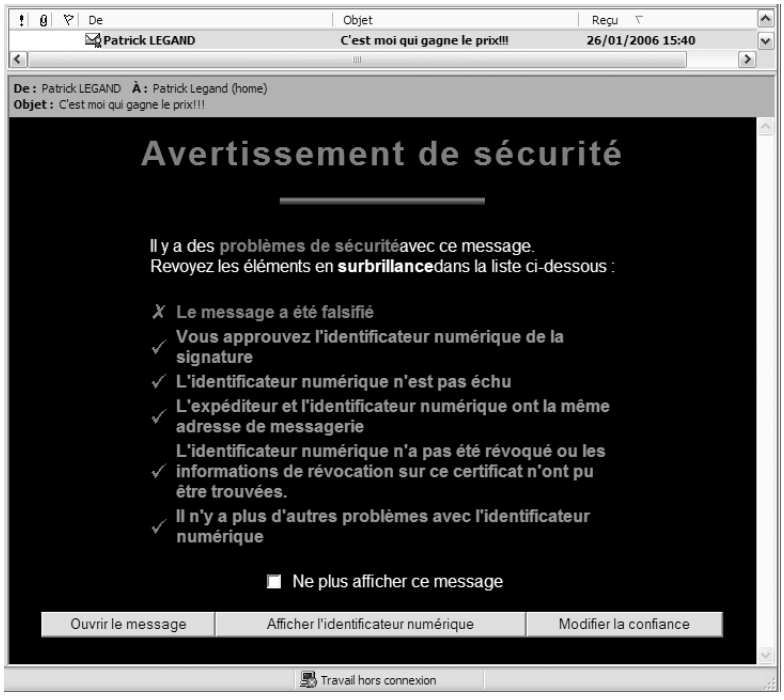


Figure 8–39
Exemple de problème de sécurité avec un message signé

Le client de messagerie vérifie aussi que l'adresse de la source du message est bien identique à celle présente à l'intérieur du certificat de signature. Cette mesure élimine le risque d'usurpation d'adresse source.

Il effectue en outre quelques vérifications supplémentaires, notamment les dates de validité du certificat, ou le fait qu'il n'ait pas été révoqué. Si tous ces contrôles se déroulent avec succès, vous aurez accès au contenu du message, à l'image de la figure 8-38. Sinon, votre client affichera un écran similaire à celui de la figure 8-39.

Authentification de l'expéditeur via un certificat

L'authentification par certificat n'est toutefois pas complète. Vous constatez que pour obtenir un certificat, à aucun moment il n'a été question de fournir une pièce justificative d'identité. Une simple requête anonyme sur un site web a été suffisante. Bien entendu, la simplicité d'une telle procédure facilite considérablement la vie de l'utilisateur. Cependant, dans le cas de figure que nous avons décrit, si le certificat garantit au moins l'adresse électronique de l'expéditeur (via le lien cryptologique fort qui existe entre les éléments qui le composent et le fait que l'Autorité de Certification ne délivre ce certificat par voie de messagerie qu'à cette adresse), il n'authentifie nullement la personne qui l'a envoyé. Nous n'avons eu par exemple aucun mal à attribuer un certificat à Louis XIV et à envoyer un message signé au nom du Roi de France. De même, des individus mal intentionnés peuvent tout à fait établir un certificat au nom de votre banquier, et, s'appuyant sur une signature censée vous mettre en confiance, vous extorquer des informations personnelles.

En toute rigueur, vous devriez toujours authentifier l'émetteur par rapport à son certificat. Pour cela, vous n'avez pas le choix : il faut aller consulter le contenu du certificat.

À RETENIR Le certificat authentifie l'adresse, mais pas l'identité de l'expéditeur

N'oubliez pas qu'aucune preuve tangible d'identité (passeport, carte d'identité nationale...) n'est demandée pour obtenir un certificat de ce type. Il est donc tout à fait possible d'usurper une identité.

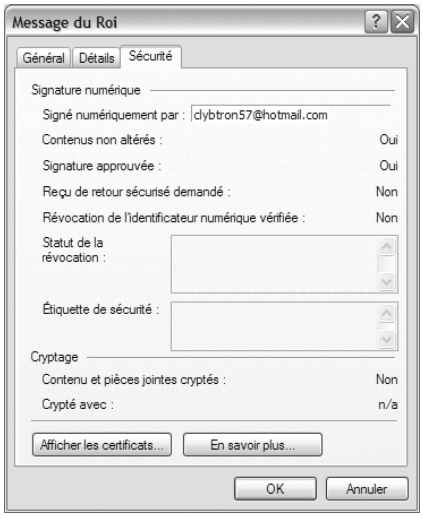


Figure 8–41 Affichez les certificats.

Figure 8–40
En cliquant sur l'un de ces boutons (Outlook Express, Thunderbird), vous accédez au détail des éléments de la signature.

Cliquez sur le « sceau » qui symbolise cette signature (figure 8-40). Dans la fenêtre qui apparaît (figure 8-41), cliquez sur le bouton *Afficher les certificats* (figure 8-42).

Lorsque vous cliquez sur *Certificat de signature*, vous accédez aux informations générales du certificat (figure 8-43).

Vous avez déjà une indication qui caractérise la valeur du certificat : il s'agit d'un certificat de classe 1 (« Class 1 CA Individual Subscriber-Persona Not Validated »), dénué de valeur juridique.

À NOTER Exemples présentés

Les écrans qui suivent s'appuient sur l'exemple d'Outlook Express. Cependant, avec Thunderbird, Outlook ou d'autres clients de messagerie, même si les écrans diffèrent, la procédure reste la même.

Figure 8–42 Cliquez sur Certificat de signature.

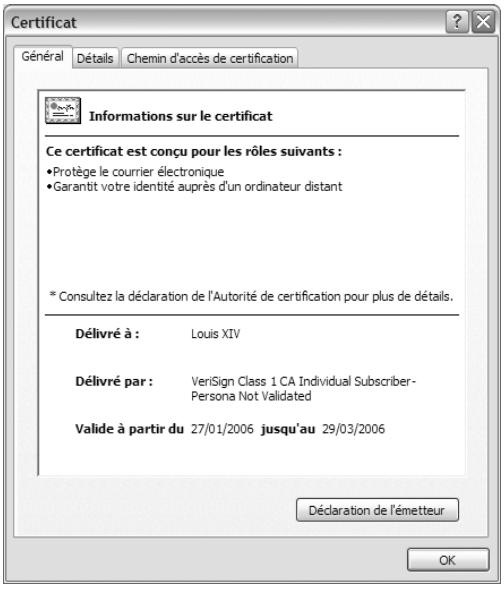


Figure 8–43 Inspectez le contenu du certificat de signature.

À RETENIR **Valeur juridique des certificats**

Les Autorités de Certification distinguent trois classes de certificats selon la précision des contrôles effectués lors de leur création :

- Classe 1 : certificats obtenus en ligne sur une base déclarative sans aucune vérification d'identité. Ils sont utilisés par les particuliers pour chiffrer le courrier électronique sur Internet. Seule, l'adresse de la messagerie électronique est validée par ces certificats.
- Classe 2 : les informations d'identification (nom, adresse, adresse de messagerie, etc.) font l'objet d'une vérification par l'Autorité de Certification. Ces certificats sont utilisés dans le cadre de transaction électroniques officielles (par exemple, le paiement électronique de l'impôt sur le revenu).
- Classe 3 : pour obtenir un certificat de Classe 3, vous devez vous présenter physiquement à l'Autorité d'Enregistrement et prouver votre identité. Un certificat de classe 3 garantit l'exactitude de l'information qu'il contient, à commencer par l'identité de son propriétaire.

Vous aurez probablement la plupart du temps affaire à des certificats de classe 1. Il vous est malgré tout possible d'authentifier leur propriétaire et de leur accorder ainsi un haut niveau de confiance.

Cliquez pour cela sur l'onglet *Détails* et faites dérouler la liste jusqu'à afficher la valeur de l'empreinte numérique (figure 8-44).

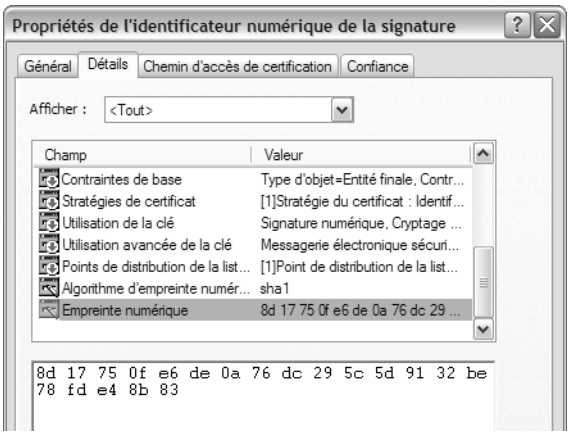


Figure 8–44
Valeur de l'empreinte numérique du certificat de signature

Il s'agit ici d'une empreinte SHA-1, le « résumé » du certificat, lié cryptologiquement à tous les champs que ce dernier contient. De plus, il est relativement facile à lire.

Partant du principe que deux certificats différents n'auront jamais la même empreinte numérique, rien ne vous empêche – si vous connaissez son propriétaire – de l'appeler au téléphone et de lui demander l'empreinte numérique de son certificat. Si les deux valeurs concordent, vous êtes sûr que le certificat de signature appartient à la bonne personne (sa voix authentifiant en quelque sorte cette empreinte numérique), et que le message est authentique.

Par exemple, vous vous rendrez vite compte que Louis XIV ne pouvait être l'émetteur du message : il n'a jamais utilisé SHA-1 et les calculs en hexadécimal lui donnaient des maux de tête épouvantables.

Certes, tout ceci paraît un tantinet contraignant ; sachez cependant que vous n'aurez à effectuer cette opération qu'une seule fois pour chaque nouveau certificat. Néanmoins, ne l'oubliez jamais, une bonne sécurité a un prix !

Niveau de protection réel délivré

Les mécanismes que nous venons de décrire renforcent incontestablement la sécurité de vos échanges. Avec de tels services de sécurité, il devient très difficile, voire impossible au commun des mortels, d'intercepter et de lire vos messages chiffrés. Cependant, il faut rester lucide. Tous les experts en sécurité vous le diront : les algorithmes cryptologiques mis en œuvre dans les cryptosystèmes du commerce (AES, 3DES, RC2, SHA-1, RSA, etc.) sont réputés fiables (jusqu'à preuve du contraire, aucun de ces algorithmes n'a été cassé à ce jour), mais c'est souvent l'implémentation des protocoles utilisant ces algorithmes qui pêche. Examinons les quelques faiblesses du modèle que nous venons d'évoquer.

Problème de la fiabilité des clés secrètes et privées

En règle générale, la sécurité d'un mécanisme cryptologique dépend de la solidité de l'algorithme et de la fiabilité de la clé. Comme nous venons de l'affirmer, le premier point est communément admis.

En revanche, qu'en est-il de la fiabilité des clés secrètes et privées ? Idéalement, une clé doit être engendrée de façon aléatoire, afin que l'attaquant ne puisse émettre aucune hypothèse sur sa valeur. Malheureusement, les générateurs aléatoires d'une grande fiabilité sont des mécanismes extrêmement difficiles à réaliser, à tel point qu'on les rencontre essentiellement dans des produits de sécurité haut de gamme, généralement à l'intérieur d'équipements matériels utilisés par des grandes Administrations, les banques ou la Défense. Ce que l'on peut dire des générateurs fonctionnant sur vos machines, c'est qu'ils sont à peu près tout, sauf aléatoires. Certes, il existe bien une part de hasard dans ces nombres (remuer la souris en donne probablement l'illusion), mais ils sont issus de valeurs contenues dans les registres de l'ordinateur, la mémoire ou dans des myriades de variables système qui, malheureusement, contiennent beaucoup de séquences prévisibles. En y regardant d'un peu près, on s'aperçoit par exemple que les fichiers dits « random » sont alimentés à partir de séquences semblables à celle-ci : « 00 00 00 45 00 00 00 FA 00 00 00 00 ». Que penser des générateurs utilisés par les Autorités de Certification pour délivrer à tour de bras des certificats de classe 1 « Individual Subscriber-Persona Not Validated » ? On peut imaginer qu'ils sont meilleurs, mais ils ne produisent probablement pas d'aléas véritables.

Ensuite, n'oubliez pas que vous n'êtes pas le seul à connaître votre clé privée. L'Autorité de Certification, qui l'a générée, la connaît aussi. Bien sur, les AC sont soumises à des règles déontologiques très strictes et n'iront jamais divulguer une telle information à n'importe quel tiers. Cependant, quand les enjeux deviennent importants, il n'est pas interdit d'imaginer qu'elles soient obligées – exceptionnellement, cela s'entend – de communiquer une clé privée au gouvernement dont elle dépend, ou à des services de police dans le cadre de la recherche d'un escroc ou d'un criminel. Soyez prudent donc, dans le cadre, par exemple, de grands appels d'offres internationaux. Si vos données ont de la valeur, conservez toujours la maîtrise de vos secrets.

N'oubliez pas non plus que, lorsque vous recevez le certificat de classe 1 calculé pour vous par l'Autorité de Certification, celui-ci transite sur Internet. Cela signifie que votre clé privée transite au moins une fois sur Internet. Certes, elle ne transite pas en clair, elle est chiffrée ; mais chiffrée avec quoi ? tout simplement à l'aide du mot de passe que vous avez fourni. Avez-vous pensé à la robustesse de ce dernier ? En tout état de

Conseil

Conservez la maîtrise de vos secrets

Si vous voulez être certain d'être le seul à connaître votre clé privée, le mieux est de créer vous-même une paire de clés et de rentrer dans un réseau de confiance mutuelle pour vous affranchir de la centralisation par les AC (voir la section sur GnuPG à la fin du chapitre).

cause, il est illusoire de croire que la protection d'une clé privée à l'intérieur d'un certificat est sécurisée par un mécanisme de niveau cryptologique. Dans les faits, seul le mot de passe assure sa protection !

D'autre part, cette clé privée est stockée sur votre ordinateur, dans un endroit bien connu (le magasin de certificats). Même si elle est protégée par ce fameux mot de passe, elle se trouvera tôt ou tard présente en clair dans la mémoire de votre ordinateur lorsque vous effectuerez les opérations de signature ou de déchiffrement. Bien sûr, réussir une attaque pour intercepter cette clé au bon moment demande un certain savoir-faire. Cependant, si le jeu en vaut la chandelle, un pirate expérimenté a de bonnes chances de la récupérer. Pour parer à cet inconvénient et atteindre une sécurité élevée, l'idéal est d'avoir recours à un équipement matériel supplémentaire (token, carte à puce) ; toutes les opérations sensibles (stockage de la clé privée, signature, déchiffrement) s'effectuent à l'intérieur de ce matériel, dans une zone non accessible physiquement par des moyens usuels.

Enfin, veillez à ce que vos messages soient chiffrés à l'aide d'algorithmes basés sur des clés de 128 bits ou plus (3DES, RC2 128 bits, AES, etc.). Votre navigateur pourra vous signaler l'usage de clés plus petites (figure 8-45).

ATTENTION

Ne confondez pas les types de clés

Ne confondez pas la longueur d'une clé symétrique, de l'ordre de 128 bits, avec celle des clés asymétriques mises en œuvre dans des algorithmes tels que RSA. Une clé asymétrique doit atteindre au minimum les 1 024 bits.

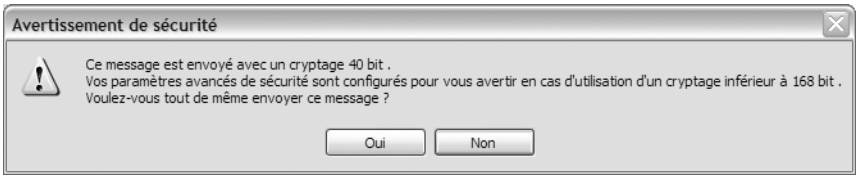


Figure 8–45
Méfiance, il se peut que votre client de messagerie utilise un chiffrement faible.

En effet, une manière de décrypter (c'est-à-dire retrouver le message clair sans posséder la clé) consiste à disposer d'un bout du message chiffré et à essayer toutes les clés possibles jusqu'à tomber sur le message en clair correspondant. Si votre clé a une longueur de 40 bits, le pirate devra effectuer 2^{40} opérations pour essayer toutes les clés (en moyenne, la moitié suffira) ; c'est la fameuse attaque exhaustive, l'attaque dite de « force brute ». Avec la technologie actuelle, casser une clé de 40 bits est très faisable. En revanche, si vous utilisez une clé de 128 bits, il faudrait en théorie « mouliner » pendant une durée supérieure à la durée de vie de l'Univers.

À RETENIR **Ne soyez jamais confiant à 100 %**

Pour votre information, sachez que ce discours théorique a ses limites. Cela suppose que votre machine produise des aléas vrais, ce qui n'est pas le cas ; d'autre part, derrière les messages tonitruants des éditeurs brandissant le 128 bits comme l'argument suprême de la sécurité, sommes-nous toujours sûrs que sur les 128 bits choisis par le logiciel, 80 ne sont pas déjà connus par le gouvernement dont dépend le concepteur du programme ?

Malgré quelques réserves (voir aparté), préférez toujours les clés de 128 bits à celles de 40 bits. Avec Outlook Express, à partir du menu *Outils*, sélectionnez *Comptes*, puis cliquez sur l'onglet *Courrier*, sélectionnez votre compte et cliquez sur le bouton *Propriétés*. Cliquez sur l'onglet *Sécurité* et, à l'image de la figure 8-46, choisissez vos préférences.

Figure 8–46
Sélectionnez un algorithme robuste utilisant des clés de 128 bits au minimum.

Renforcer la sécurité des échanges par voie de messagerie électronique

Lorsque les exigences de sécurité sont élevées, par exemple dans le cadre professionnel, il convient de respecter un certain nombre de règles en matière de choix technologiques et d'organisation de la gestion des certificats :

- Le certificat est délivré par un prestataire reconnu qualifié, ou, à défaut, par une Autorité de Certification reconnue dans la profession que vous exercez.
  - La procédure d'établissement du certificat garantit notamment l'authentification de son propriétaire et l'acheminement de la clé privée par un canal sûr (en particulier, elle ne doit pas circuler sur Internet).
  - Les opérations cryptologiques ainsi que le stockage des clés privées se déroulent à l'intérieur d'un dispositif matériel externe à crypto-processeur (clé USB, carte à puce, etc.).
  - Les procédures de chiffrement et de signature des documents électroniques sont réalisées à l'aide d'un logiciel agréé, voire certifié par la DCSSI.
- Le produit utilisé fournit un service d'horodatage et, éventuellement, d'accusé de réception.
- Le cryptosystème est doté d'un service de non-répudiation des messages, offrant ainsi l'assurance que ni la transaction, ni les informations transmises lors de cette transaction ne seront contestées ultérieurement par l'émetteur. En cas de contentieux, des procédures de rejeu de la transaction doivent permettre de vérifier a posteriori le contenu des transactions litigieuses.

Organisme qualifié

Est reconnu qualifié un organisme qui a apporté la preuve de sa conformité aux exigences portant sur la délivrance de certificats électroniques qualifiés. La qualification de ces prestataires s'effectue sous l'autorité de la DCSSI.

DCSSI (Direction centrale de la sécurité des systèmes d'information)

La DCSSI assure la fonction d'autorité nationale de régulation pour la SSI. Elle délivre notamment les agréments pour les systèmes d'information de l'État, les procédés et les produits cryptologiques employés par l'administration et les services publics. Elle tient à jour le catalogue des produits de sécurité certifiés.

EXEMPLE

Greffe du tribunal de commerce de Paris

Le greffe du tribunal de commerce de Paris impose l'achat d'un « token » vendu par un éditeur spécialisé, sélectionné par le Greffe.

C'est à ce prix que les services de signature et de chiffrement de la messagerie électronique seront efficaces.

Valeur juridique de la signature d'un message électronique

« La loi 2000-230 du 13 mars 2000 précise que toutes les signatures électroniques sont recevables en justice dès lors qu'elles assurent, à l'aide d'un procédé fiable, l'identification du signataire et l'intégrité de l'acte. »(DCSSI, www.ssi.gouv.fr/fr/faq/faq_sigelec.html).

Les conditions selon lesquelles le procédé de signature électronique est présumé fiable sont décrites au sein du décret 2001-272 du 30 mars 2001, que vous pouvez consulter sur le même site.

En particulier, la signature électronique est recevable en justice au titre de preuve si :

- La signature électronique est « sécurisée », c'est-à-dire :
- propre au signataire ;
- créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantissant avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.
- Elle est créée par un dispositif certifié de création de signature électronique.
- La vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

Il est donc possible d'établir des signatures électroniques ayant une valeur juridique, mais leur procédé d'élaboration doit reposer sur des matériels et des logiciels évalués et certifiés conformes aux exigences du décret 2001-272 du 30 mars 2001 :

- soit par les services du Premier ministre chargés de la sécurité des systèmes d'information, ou par des organismes agréés par ces services,
- soit par un organisme désigné à cet effet par un État membre de la Communauté européenne.

RÉFÉRENCE Signature électronique

Si vous souhaitez plus d'information sur la signature électronique, n'hésitez pas à consulter l'excellent site de la DCSSI :

- www.ssi.gouv.fr/fr/dcssi/

Sécuriser son courrier sous Thunderbird avec OpenPGP

Modèle de confiance d'OpenPGP

Réseau de confiance

Il existe une alternative intéressante au modèle basé sur les certificats et les autorités de certification, appelé aussi « PKI » (Public Key Infrastructure, ou IGC, Infrastructure de gestion de clés). En effet, une IGC se

caractérise essentiellement par le fait que les éléments secrets les plus sensibles, à savoir les clés de chiffrement et de signature, sont confiées, dès le départ, à un acteur tiers.

Un autre modèle a été instauré à l'origine par le système « dissident » PGP et est aujourd'hui relayé par le standard OpenPGP. Comme il a été rappelé au chapitre 2, PGP a été conçu pour apporter sa modique contribution à la défense des droits de l'Homme, dans la mesure où la robustesse des mécanismes cryptologiques qu'il implémente devaient servir à préserver la vie privée de l'individu, y compris contre les regards indiscrets de certains gouvernements.

À ce titre – c'est ici qu'il diffère radicalement du modèle de PKI, généralisé aujourd'hui dans le monde entier – tout élément secret attaché à un utilisateur est élaboré par l'utilisateur lui-même, sans aucune intervention extérieure et sans qu'aucun tiers n'ait connaissance, ou ne puisse deviner, la valeur du secret. Avec OpenPGP, la notion d'autorité de certification, au sens où nous l'avons décrite au chapitre 6, n'existe pas.

Évidemment, la question se posait alors de savoir comment bâtir un schéma de confiance qui permettrait à l'utilisateur OpenPGP de reconnaître de façon sûre la validité de la clé de n'importe quel autre utilisateur OpenPGP.

Le concepteur d'OpenPGP a répondu à cette question en imaginant un modèle formidablement astucieux, si l'on tient compte du contexte d'utilisation : le schéma de confiance est tout simplement basé sur la confiance mutuelle entre les individus (c'est la fameuse notion de « Web of Trust », ou toile de confiance). À l'inverse des PKI, où la responsabilité de valider tel ou tel certificat est déléguée aux autorités de certification, l'utilisateur joue un rôle direct dans le processus d'établissement de la confiance : en se basant sur des éléments irréfutables, il prend lui-même la décision d'attribuer un niveau de confiance donné à une clé publique, ou bien il délègue cette responsabilité aux personnes en qui il a confiance.

Raisonnons sur un cas concret. À l'origine, Alice élabore elle-même sa propre clé, en laquelle elle a donc une confiance absolue. Connaissant très bien Alice, Bernard peut être sûr que cette clé lui appartient vraiment, en vérifiant personnellement son empreinte numérique auprès d'elle. Il sait donc que cette clé est valide.

Bernard réalise donc une opération qui est habituellement plutôt du ressort des autorités de certification dans le modèle des PKI : il signe la clé d'Alice avec sa propre clé privée. C'est sa manière de déclarer à la communauté qu'il considère cette clé comme valide.

En admettant par ailleurs qu'Alice ait signé les clés de Béatrice et de Jean-Christophe (elle a pu vérifier par le même procédé qu'elles étaient

valides), Bernard peut être sûr à son tour de la validité de celles-ci, sans avoir rencontré personnellement leurs propriétaires : il a en effet une confiance absolue en Alice pour signer des clés et utilise la clé publique valide de cette dernière pour vérifier les signatures de celles de Béatrice et Jean-Christophe.

> TRANSITIVITÉ **Réseau de confiance mutuelle**
>
> Si vous faites confiance à une personne en particulier pour valider des clés, toute clé signée par une clé valide de cette personne est elle-même considérée comme valide.

Niveaux de confiance

Il convient de s'apesantir quelques instant sur une notion cruciale d'OpenPGP, qui n'existe pas dans les PKI : la confiance accordée à une personne pour signer des clés. Vous pouvez très bien considérer la clé de Fantômas valide, mais ne pas faire confiance à Fantômas lorsqu'il valide une clé. Dans ce cas, vous ne pouvez pas considérer comme valides les clés signées par Fantômas en vous appuyant exclusivement sur sa signature. C'est pourquoi OpenPGP vous offre la possibilité de déterminer explicitement le niveau de confiance attachée à la clé d'un utilisateur (figure 8-47).

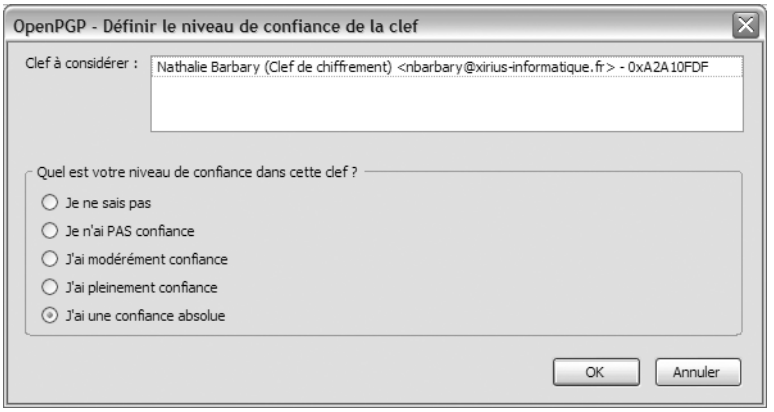


Figure 8–47
Attribution d'un niveau de confiance à la clé d'un utilisateur donné

Le niveau de confiance que l'on accorde à une clé dépend du niveau de confiance attribué aux utilisateurs qui ont signé cette clé, et de la validité de la signature.

Ce qui est un peu déroutant avec le modèle OpenPGP, et en même temps fondamentalement intéressant, c'est que vous attribuez vous-même un niveau de confiance à quelqu'un, selon des critères qui vous sont propres. En quelque sorte, vous avez votre mot à dire. C'est un avis subjectif, certes, mais il ne regarde que vous et influe sur un niveau de

sécurité qui ne concerne que vous. Cette considération est absente du modèle de PKI, où le navigateur prend la décision à votre place, en se basant sur la présence ou non du certificat racine dans le magasin de certificats, et sur la validité de la signature du certificat vérifié. En bref, avec une PKI, vous faites confiance ou vous ne faites pas confiance à une autorité racine ; vous ne pouvez pas attribuer une confiance modérée.

Avec OpenPGP, la question est de savoir quelle attitude adopter envers des personnes avec lesquelles on ne dispose d'aucun lien particulier. La réponse est simple, lorsqu'on ne sait rien sur le propriétaire de la clé, il existe un niveau de confiance absolument fantastique proposé par OpenPGP : « Je ne sais pas ». Par défaut, les clés de votre trousseau de clés publiques ont ce niveau de confiance. De façon générale, plus une clé a été signée par différents utilisateurs, plus elle est logiquement digne de confiance. Si vous devez utiliser la clé d'un inconnu, prenez le temps de regarder les signatures qui lui sont associées.

Bien entendu, on pourrait soulever des objections face à un tel schéma : par exemple, accepter dans son trousseau la clé publique d'utilisateurs inconnus en leur attribuant un faible niveau de confiance n'est-il pas un leurre pour contourner une problématique difficile à résoudre ? Pour fonctionner dans les meilleures conditions, un vrai réseau de confiance entre les utilisateurs (c'est-à-dire des utilisateurs ayant « pleinement confiance » entre eux, voire une « confiance absolue ») n'est-il pas préférable ? Le schéma de confiance d'OpenPGP serait-il limité car réellement applicable à une communauté restreinte d'utilisateurs qui se connaissent, soit personnellement, soit par l'intermédiaire d'amis communs ?

Tout d'abord, échanger de l'information avec un utilisateur dont on ne sait pas évaluer s'il est digne de confiance n'est pas plus dangereux que de converser avec un utilisateur dont le certificat a été élaboré par une autorité dont on ne sait rien.

Ensuite, en y réfléchissant bien, tant dans la vie professionnelle que dans notre vie privée, il est rare que nous échangions des informations à caractère sensible avec des interlocuteurs que nous ne connaissons pas. Les communications importantes (par exemple, les documents de travail) ont généralement lieu avec des personnes qui, par la nature même de leurs relations, constituent exactement ce que OpenPGP désigne par « réseau de confiance ».

Prenons le cas de grandes entreprises qui mettent en place des consortiums pour répondre ensemble à des appels d'offres internationaux. Même si les différents partenaires d'un même consortium sont largement disséminés, par exemple en Europe et aux États-Unis, les principaux intervenants se connaissent personnellement, au moins parce qu'ils se sont rencontrés dans une réunion. Autour de ce noyau dur gravitent

d'autres intervenants, qui ne se connaissent peut-être pas personnellement, mais qui, par l'intermédiaire de leurs collègues, se font confiance. Il s'agit typiquement d'un schéma de confiance OpenPGP. Au cours de la préparation de l'offre, tous ces intervenants vont échanger des informations ultra-sensibles vis-à-vis de la concurrence, à savoir des architectures techniques, des considérations stratégiques sur l'offre et sur le développement commercial de leur entreprise, ou des montants financiers. Idéalement, sécuriser efficacement de telles communications nécessite la mise en place de VPN, tunnels chiffrés dédiés reliant de bout en bout l'ensemble des intervenants. Malheureusement, dans la pratique ce n'est pas toujours le cas : la mise en place de VPN dédiés implique le déploiement d'équipements matériels sur chaque site, la configuration de ces matériels, la génération et la distribution de certificats numériques individuels et, par conséquent (ce qui coûte le plus cher !), la prestation d'un ou plusieurs ingénieur(s) spécialiste(s) en sécurité (souvent un sur chaque site). Non seulement le coût d'une telle opération n'est pas anodin, mais en plus le temps nécessaire pour convaincre les instances décisionnelles des entreprises sur le bien-fondé de l'opération elle-même est généralement incompatible avec les délais de réalisation de l'offre. Ceci explique peut-être pourquoi, aujourd'hui encore, beaucoup de communications stratégiques se font en clair.

VPN

Un VPN, ou Virtual Private Network, utilise un tunnel chiffré de bout en bout pour l'échange d'informations sur un réseau non fiable (Internet).

Cela est d'autant plus regrettable qu'OpenPGP représente une alternative tout à fait intéressante pour offrir une réelle sécurité et, de surcroît, est parfaitement adapté au contexte d'emploi : les échanges ont lieu au sein d'un réseau d'utilisateurs qui se connaissent et se font mutuellement confiance, les mécanismes d'OpenPGP sont robustes, l'installation, la configuration et la mise en œuvre d'OpenPGP sur le poste de l'utilisateur ne prend pas plus d'un quart d'heure, enfin chaque utilisateur peut élaborer son propre certificat, aucun ingénieur spécialiste en sécurité ne doit être mobilisé !

De nombreuses informations complémentaires sur les concepts d'OpenPGP, notamment la notion de « toile de confiance », sont accessibles à travers les multiples documents sur PGP et OpenPGP disponibles sur Internet. Citons par exemple le manuel d'utilisation d'OpenPGP, fourni avec le paquetage GnuPG.

Pour conclure cette rapide introduction, vous l'avez sûrement compris maintenant, OpenPGP est plus particulièrement adapté aux communications privées, qu'elles soient d'ordre personnel ou d'ordre professionnel. Si l'on devait comparer en une phrase OpenPGP et les PKI, l'on pourrait dire que OpenPGP fournit une sécurité forte pour des transactions non officielles, et les PKI, une sécurité sous contrôle pour transactions officielles. À vous de choisir les bons mécanismes au bon moment !

Installer les extensions de sécurité

Sous Thunderbird, vous pouvez très facilement bénéficier des excellentes fonctions de sécurité offertes par OpenPGP pour échanger des messages sécurisés. Pour cela, vous devez :

- installer au préalable le logiciel GnuPG, ainsi que son interface graphique WinPT ou GPGshell ;
- installer l'extension Enigmail de Thunderbird, qui offre l'accès aux fonctions de GnuPG directement depuis Thunderbird ;
- installer l'extension française d'Enigmail.

Nous ne reviendrons pas sur l'installation de GnuPG, déjà exposée au chapitre 2. En revanche, pour installer Enigmail et l'extension française, procédez comme suit :

1 Téléchargez les logiciels `enigmail-0.94.1-tb15-win32.xpi` et `enigmail-fr-FR-0.9x.xpi` (dernières versions à l'heure où nous écrivons ces lignes), depuis le site de Geckozone (http://www.geckozone.org).

2 Lancez ensuite Thunderbird et choisissez *Outils>Extensions*. Dans la boîte de dialogue qui apparaît (voir figure 8-48), cliquez sur le bouton *Installer*.

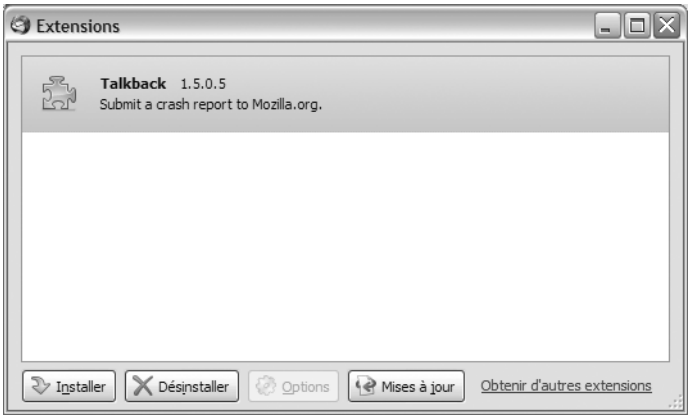


Figure 8–48
Lancez l'installation de nouvelles extensions.

3 Parcourez votre arborescence à la recherche du répertoire dans lequel vous avez enregistré les fichiers téléchargés. Sélectionnez le fichier `enigmail-0.94.1-tb15-win32.xpi` (extension Enigmail), puis cliquez sur *Ouvrir* et suivez les instructions. Réitérez la même opération avec le fichier `enigmail-fr-FR-0.9x.xpi` (figure 8-49).

Les deux logiciels s'affichent maintenant dans la liste des extensions prêtes pour l'installation automatique par Thunderbird (figure 8-50).

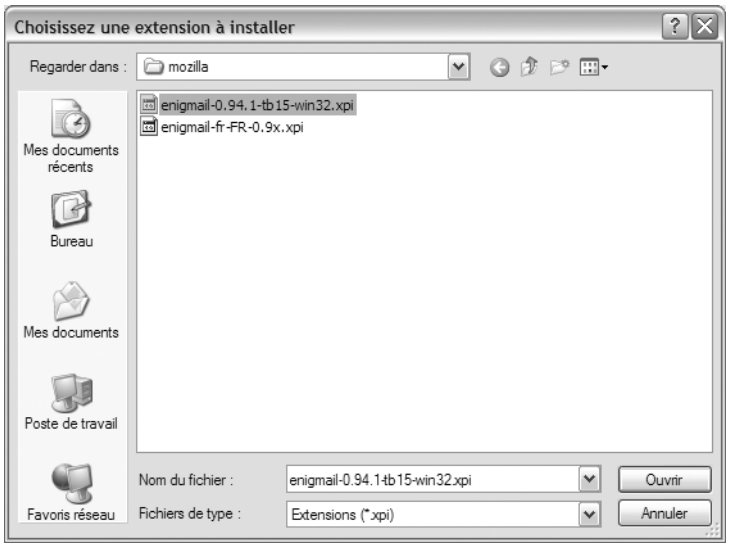


Figure 8–49
Installez de nouvelles extensions.

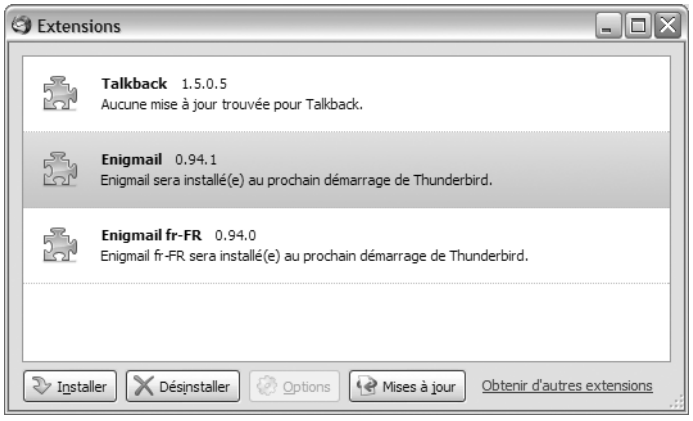


Figure 8–50
Les nouvelles extensions sont prêtes pour l'installation.

4 Refermez la boîte de dialogue et arrêtez votre client de messagerie. Vous n'avez rien d'autre à faire, à part relancer Thunderbird. Enigmail en français est maintenant opérationnel.

Configurer Enigmail

Vous disposez désormais d'un nouveau bouton dans la barre de menus de Thunderbird : l'accès direct à OpenPGP (figure 8-51). Il ne vous reste plus qu'à réaliser quelques modiques opérations de configuration pour que vous puissiez enfin signer et chiffrer vos messages avec OpenPGP.

Dans le menu OpenPGP, sélectionnez *Préférences*. Dans la boîte de dialogue qui s'affiche, cliquez sur l'onglet *Général* et, à l'aide du bouton *Parcourir*, indiquez le chemin d'accès au fichier exécutable `gpg.exe`. Ce

fichier devrait se trouver dans le répertoire `C:\Program Files\GNU\GnuPG`. Cliquez enfin sur *OK* (figure 8-52).

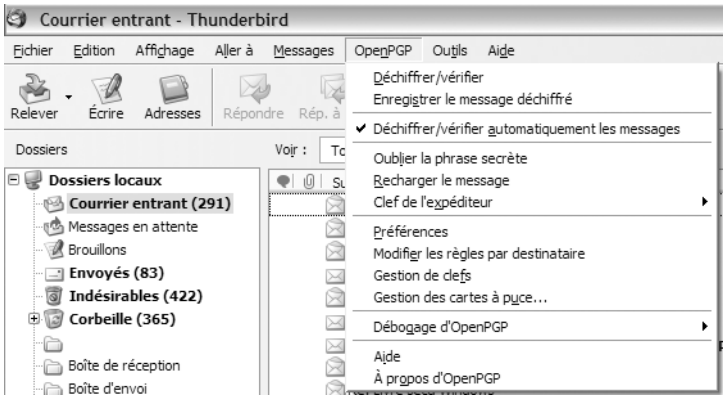


Figure 8–51
Aperçu des fonctions OpenPGP dans Thunderbird

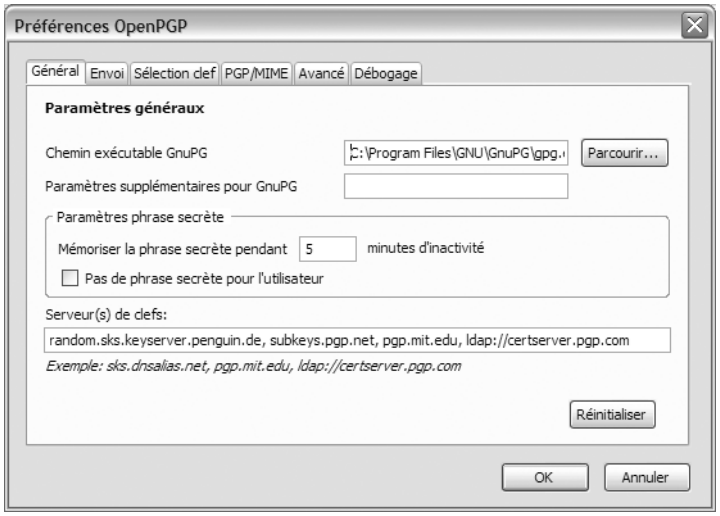


Figure 8–52
Indiquez le chemin d'accès à l'exécutable GnuPG.

Si vous avez consciencieusement effectué les opérations décrites au chapitre 2, vous disposez déjà au moins d'une paire de clés : dans le menu *OpenPGP*, cliquez sur *Gestion de clefs* et vous les verrez aussitôt apparaître.

Si ce n'est pas le cas, ce n'est pas grave, vous allez créer votre première paire de clés. Dans Thunderbird, choisissez *OpenPGP>Gestion de clefs* et sélectionnez *Générer>Nouvelle paire de clefs*.

Saisissez les principaux paramètres associés à votre nouvelle paire de clés (figure 8-53) :

- l'identité à laquelle se rattache la clé (ici il s'agit de votre adresse électronique) ;

- la phrase secrète qui protègera l'accès à votre clé privée (attention, choisissez-la convenablement : suffisamment complexe pour que personne ne puisse la deviner, facile à retenir car vous devrez la saisir fréquemment) ;
- un commentaire éventuel ;
- le délai d'expiration de la clé. Par défaut, OpenPGP vous propose une durée de validité de cinq ans. Si vous êtes rigoureux dans la manière de gérer vos clés privées, cinq ans est un assez bon choix. Une clé qui n'expire jamais n'est pas crédible, renouveler une clé trop fréquemment est pénible pour l'utilisateur.

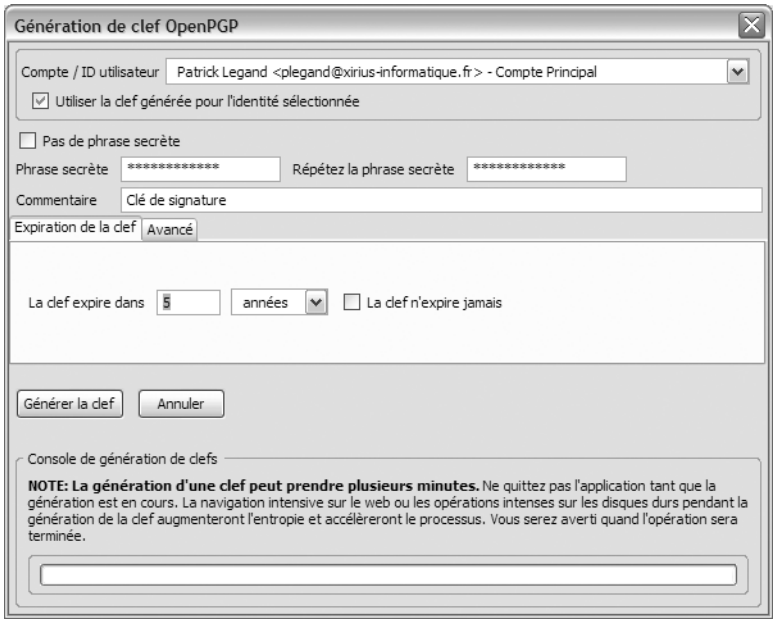


Figure 8–53
Créez votre première paire de clés.

Cliquez ensuite sur le bouton *Générer la clef*. Il se peut que cette génération prenne du temps. Cela est principalement dû aux raisons suivantes :

- Le logiciel OpenPGP doit générer plusieurs séquences aléatoires qui serviront à établir les nombres `p` et `q` (voir annexe A). Plus la qualité de l'aléa est élevée, plus cette génération est longue, surtout lorsque OpenPGP ne dispose pas de suffisamment de valeurs aléatoires en réserve.
- N'oubliez pas que ces nombres `p` et `q` doivent être premiers. OpenPGP doit réaliser plusieurs tests de primalité afin de déterminer si c'est effectivement le cas. Dans le cas contraire, il réitère le processus jusqu'à tomber sur deux occurrences qui satisfont effectivement à cette exigence.

Si ce calcul prend un peu de temps, consolez-vous en vous disant que votre clé sera de bonne qualité. Si le logiciel parvient toutefois à un résultat rapidement, cela ne veut pas dire que les clés sont mauvaises; peut-être le réservoir de valeurs aléatoires sur votre machine était-il déjà bien alimenté ; ou, tout simplement, votre ordinateur est très rapide !

Une fois cette paire de clés calculée (figure 8-54), Open PGP vous propose de créer un certificat de révocation. Ce dernier vous servira à invalider la clé dans le cas où elle serait perdue ou compromise. Acceptez cette option et enregistrez le certificat dans le dossier de votre choix. Attention, prenez soin de transférer le certificat de révocation sur un support externe (fiable et conservé en lieu sûr), sinon une personne malintentionnée, tombant sur ce certificat, pourrait invalider votre clé sans votre consentement.

Figure 8–54
Créez le certificat de révocation.

Diffuser votre clé publique OpenPGP

Il faut maintenant diffuser votre clé publique pour que les autres utilisateurs puissent vous envoyer des messages chiffrés.

Une méthode simple consiste à l'envoyer sur un serveur de clés OpenPGP. Rien n'est plus simple : ouvrez le gestionnaire de clés (dans Thunderbird, menu *OpenPGP>Gestion de clés*). Sélectionnez la clé à publier, choisissez *Serveur de clefs>Envoyez les clefs publiques* et, après avoir sélectionné le serveur de clés dans la liste déroulante, cliquez sur *OK* (figure 8-55).

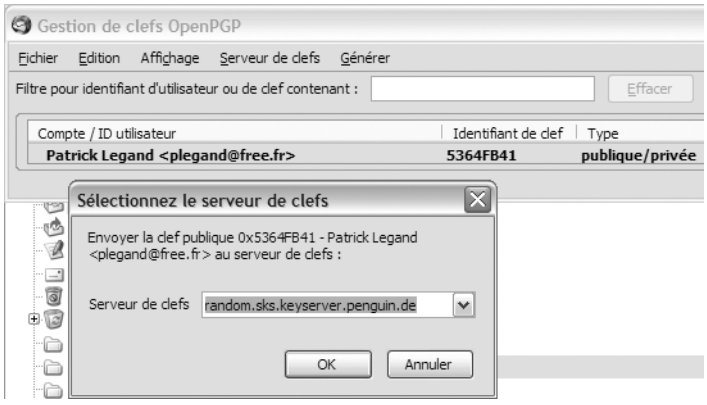


Figure 8–55
Publiez votre clé OpenPGP.

ASTUCE
Plusieurs identités pour une même clé

Afin d'éviter de gérer un trop grand nombre de clés, vous pouvez associer plusieurs adresses électroniques à une même clé. Dans la boîte de dialogue *Gestion de clefs OpenPGP*, sélectionnez la clé et choisissez le menu *Édition>Gérer les identifiants utilisateur*. Cliquez ensuite sur *Ajouter* et saisissez la nouvelle adresse électronique.

RAPPEL **Clés de signature et de chiffrement**

Établissez une clé que vous consacrerez au chiffrement, et une autre clé pour la signature.

Obtenir la clé OpenPGP d'un correspondant

Il y a plusieurs moyens d'obtenir la clé publique OpenPGP d'un correspondant. Si ce dernier est un habitué d'OpenPGP, il l'a certainement déjà publiée sur un serveur de clés. Étant relié à Internet, dans Thunderbird ouvrez le gestionnaire de clés OpenPGP (menu *OpenPGP>Gestion de clés*), cliquez sur *Serveur de clefs>Chercher des clefs* et, dans la boîte de dialogue de la figure 8-56, saisissez l'identifiant de votre correpondant (identifiant de la clé ou adresse électronique). Cliquez sur le bouton *OK*.

Figure 8–56
Téléchargez la clé d'un correspondant à partir d'un serveur de clés.

Un autre moyen consiste à importer le fichier de clé publique (un fichier `.asc`) que votre correspondant vous a communiqué par un autre moyen (par messagerie électronique par exemple). Enregistrez au préalable le fichier dans le dossier de votre choix. Dans le gestionnaire de clés publiques OpenPGP, choisissez *Fichier>Importer des clefs depuis un fichier* (figure 8-57). Parcourez votre arborescence jusqu'au dossier qui contient ce fichier et cliquez sur celui-ci. C'est tout, la clé figure maintenant dans votre trousseau.

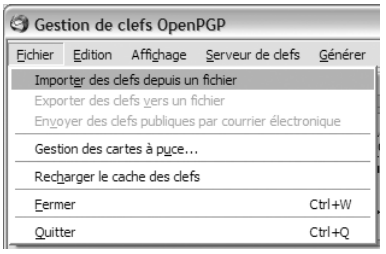


Figure 8–57
Importez directemet la clé de votre correspondant.

Signer ou chiffrer un message avec OpenPGP

Vous êtes maintenant prêt à utiliser les incomparables fonctions d'OpenPGP. La procédure est exactement la même que celle décrite plus haut pour les certificats.

Les fonctions de sécurité d'OpenPGP sont accessibles à partir du menu *OpenPGP*. Vous avez toutefois la possibilité d'ajouter le bouton OpenPGP sur la barre d'outils de votre client de messagerie. Pour cela,

cliquez droit sur cette barre d'outils et choisissez l'option *Personnaliser*. Dans la boîte de dialogue, sélectionnez l'icône OpenPGP et faites-la glisser sur la barre, à l'endroit de votre choix. Les opérations de signature et de chiffrement vous sont désormais directement accessibles en deux clics de souris (figure 8-58).

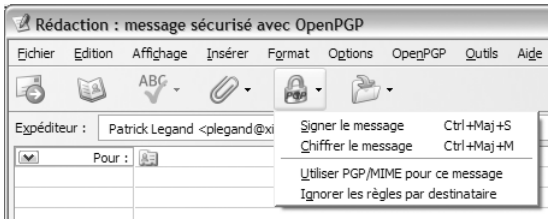


Figure 8–58
Les fonctions de signature et de chiffrement d'un message sont désormais accessibles immédiatement.

La suite des opérations est des plus simples :

1. Créez un nouveau message, comme à l'ordinaire.
2. Choisissez l'option *Signer le message* (vous pouvez aussi appuyer sur *Ctrl+Maj+S*).
3. Prenez ensuite l'option *Chiffrer le message* (ou *Ctrl+Maj+M*). Si la clé publique de votre correspondant n'est pas encore présente dans votre trousseau, OpenPGP vous offre la possibilité d'effectuer une recherche immédiate en affichant la boîte de dialogue *Sélection de clefs OpenPGP*. Sélectionnez le serveur de clés et appuyez sur le bouton *Télécharger les clefs manquantes* (figure 8-59).

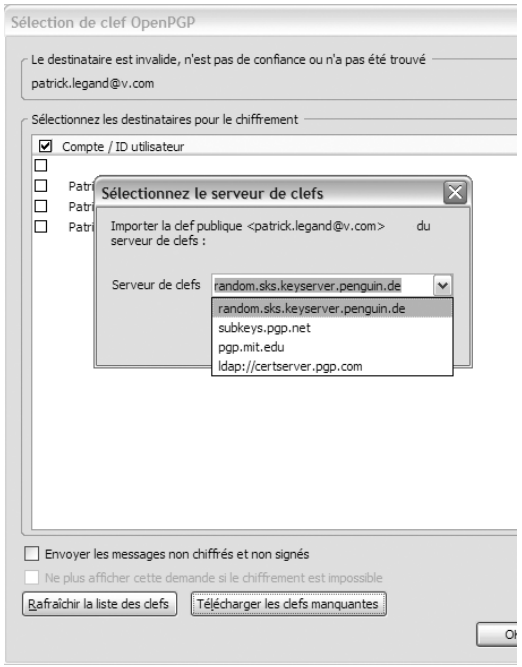


Figure 8–59
Télécharger les clés manquantes à partir d'un serveur de clés.

Si elles sont présentes sur le serveur, les clés manquantes seront alors insérées dans votre trousseau.

Un message sécurisé avec OpenPGP ressemble fortement à un message normal (figure 8-60). Dans le coin inférieur droit du message, vous pouvez distinguer deux petites icônes :

- une petite icône verte en forme de clé indiquant que le message est chiffré ;
- une petite icône en forme de stylo indiquant que le message est signé (si la signature est incorrecte, l'icône représente un stylo brisé).

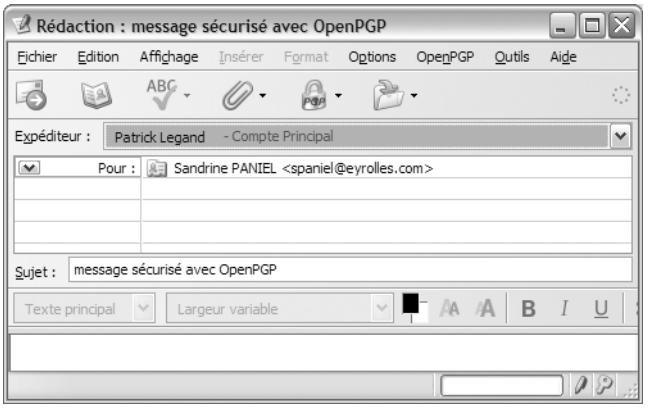


Figure 8–60
Physionomie d'un message sécurisé avec OpenPGP

Récapitulatif

Au cours de ce chapitre, nous avons présenté des solutions grâce auxquelles attaquer une messagerie devient une opération très difficile. Bien qu'il existe dans le commerce une profusion de produits dédiés à la sécurisation de la messagerie, quelques mesures extrêmement simples et non coûteuses répondront probablement à la plupart de vos attentes :

Pour vous protéger efficacement des spams :

- Envisagez l'utilisation du client de messagerie Thunderbird.
- Respectez quelques consignes de bon sens :
- Ne publiez pas votre adresse électronique sur une page web.
- Faites-vous attribuer une adresse « publique », que vous changerez en cas de besoin.
- Choisissez des adresses difficiles à deviner.

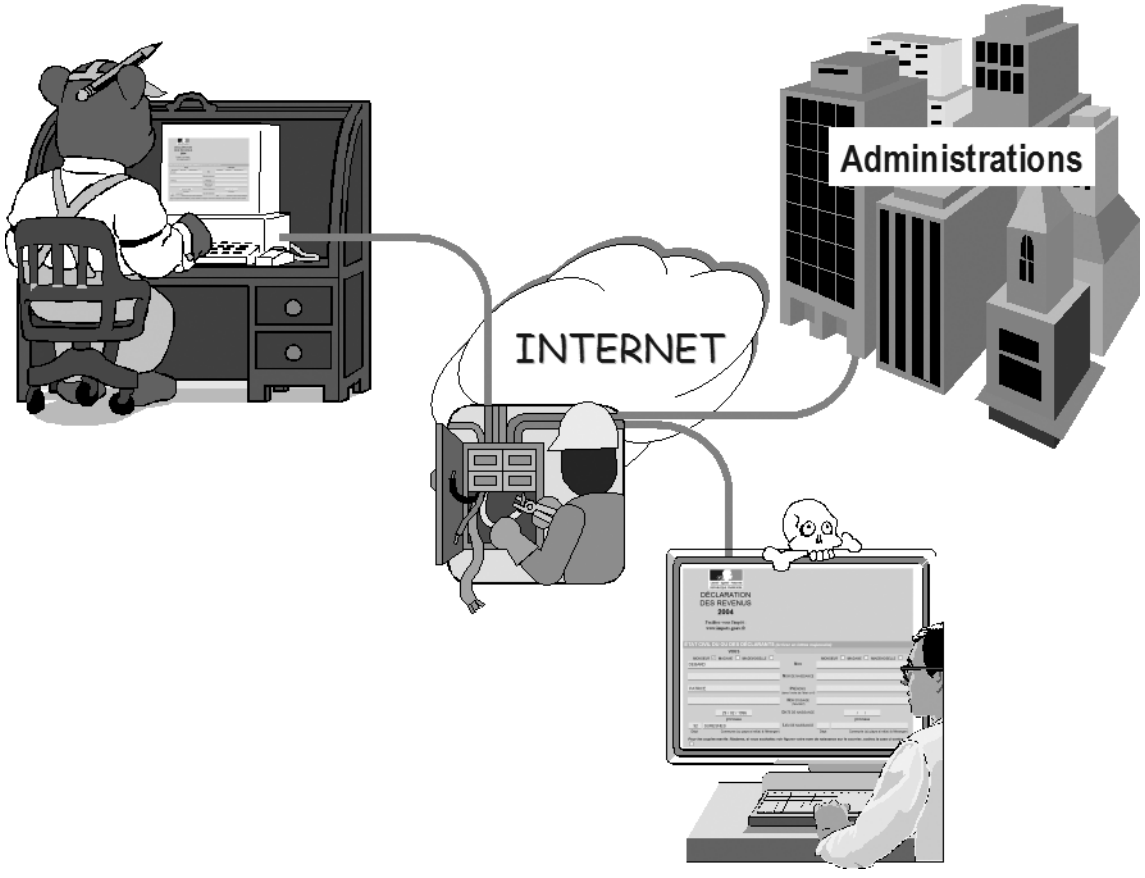
Pour en finir avec le phishing :

- Ne répondez jamais à un courrier électronique où l'on vous demande des informations personnelles.

Pour sécuriser les échanges de courriers électroniques :

- Envisagez l'installation d'OpenPGP intégré avec votre client de messagerie.
- Activez le cas échéant les mécanismes cryptologiques natifs de votre client de messagerie, et faites-vous attribuer les certificats nécessaires auprès de l'autorité de certification de votre choix.

chapitre 9



Transactions électroniques et paiement sur Internet

Payer sur Internet ? Oui, mais à quel prix ? Découvrez comment liaisons sécurisées et certificats vous protègent dans vos transactions avec des sites marchands ou des administrations.

SOMMAIRE

- Transaction électronique sécurisée
- Niveau de sécurité réel d'une transaction SSL
- Rendre les transactions plus sûres
- Transactions via un tiers de confiance
- Cas pratique : déclarer vos revenus par Internet

MOTS-CLÉS

- HTTPS
- SSL, SET, C-SET
- tiers de confiance
- législation

Évolution **Administrations en ligne**

Saluons au passage le formidable travail consenti par l'ensemble des administrations, qui rendent désormais accessibles sur Internet beaucoup de procédures qui nous faisaient jadis perdre un temps considérable !

Ce chapitre n'a pas pour objectif de traiter la vaste problématique du commerce électronique. Un seul livre n'y suffirait pas et ce domaine sort largement du cadre de notre ouvrage.

Cependant, nous sommes aujourd'hui de plus en plus nombreux à nous servir de notre ordinateur pour réaliser des transactions électroniques sur Internet : pour effectuer un achat en ligne, organiser nos vacances ou réaliser des démarches administratives, comme la demande d'un acte de naissance ou la déclaration des revenus.

Bien entendu, si elles nous simplifient la vie, les transactions électroniques s'accompagnent fatalement de la transmission de données personnelles, ou d'engagements financiers avec un tiers virtuel, ce qui ne manque pas de soulever de nombreuses interrogations en ce qui concerne la sécurité. Jusqu'à quel point les données personnelles restent-elles confidentielles ? Dans quelle mesure un acte d'achat ne dissimule-t-il pas une arnaque pour escroquer votre carte bancaire ?

Si ces questions se posent à nous tous, il faut reconnaître que la sécurité des transactions électroniques est un sujet dont la technicité a de quoi décourager la curiosité des plus motivés ; les rares initiés qui ont eu vent des protocoles dits sécurisés, tels que SSL ou HTTPS, peuvent légitimement se demander dans quelle mesure ils protègent réellement nos intérêts (sans parler de la logique obscure des certificats qui s'invitent invariablement dès que l'on évoque les protocoles sécurisés).

C'est pourquoi il n'aurait pas été convenable de terminer un livre traitant de la sécurité du poste de travail sans avoir dit quelques mots sur celle des transactions électroniques sur Internet, où le poste lui-même joue un rôle essentiel.

Nous allons donc, au cours de ce chapitre, expliquer succinctement l'anatomie d'une transaction électronique sécurisée. Cela vous permettra de mieux comprendre comment vous êtes protégé, et de faire désormais un usage plus éclairé des services d'Internet.

Sachez cependant que cette courte présentation a pour seul objectif de vous sensibiliser à l'une des nombreuses facettes de ce domaine ; si vous souhaitez acquérir une réelle connaissance en matière de commerce électronique, mieux vaut vous procurer un ouvrage spécialisé.

Toutefois, avant de commencer la lecture de ce chapitre, prenez soin de bien assimiler les techniques de sécurisation du courrier électronique, exposées au chapitre précédent. Tous les concepts et les principes cryptologiques mis en œuvre pour sécuriser la messagerie électronique s'appliquent de façon similaire à la sécurisation des transactions électroniques.

Acheter et payer sur Internet

Principes mis en œuvre au cours d'une transaction électronique sécurisée

Une session sécurisée avec un site web distant se distingue notamment grâce à l'URL affichée dans la barre d'adresses, de la forme https://www.site-sécurisé.fr/ (figure 9-1). Notez bien le « s » de « https », qui signifie HTTP sécurisé.

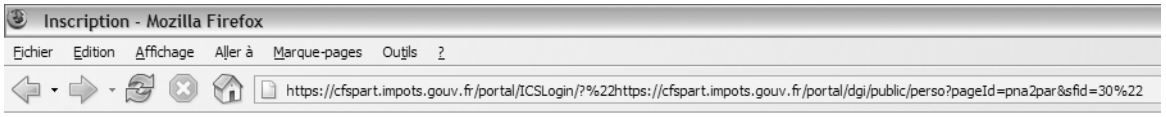


Figure 9–1 Le « s » de « https » caractérise une page sécurisée.

Lorsque vous déroulez une session en utilisant le protocole HTTPS, cela veut dire tout simplement que le flux qui transite entre votre navigateur et le serveur distant est chiffré de bout en bout, comme le montre la figure 9-2 : on dit que les informations circulent dans un tunnel chiffré. Au lieu d'attaquer directement les couches TCP/IP, comme le fait traditionnellement le protocole HTTP, le flux HTTPS passe tout d'abord par une couche intermédiaire, SSL (Secure Socket Layer) ou TLS (Transport Layer Security). Ces deux derniers protocoles de communication sont dotés de fonctions de sécurité chiffrant le contenu de l'information avant de l'envoyer sur le réseau.

AVANCÉ Fonctions de sécurité de SSL

SSL fournit en outre plusieurs autres fonctions de sécurité ; il offre notamment un service de signature assurant l'authenticité des émetteurs et des destinataires, et garantit l'intégrité des données au cours du transfert.

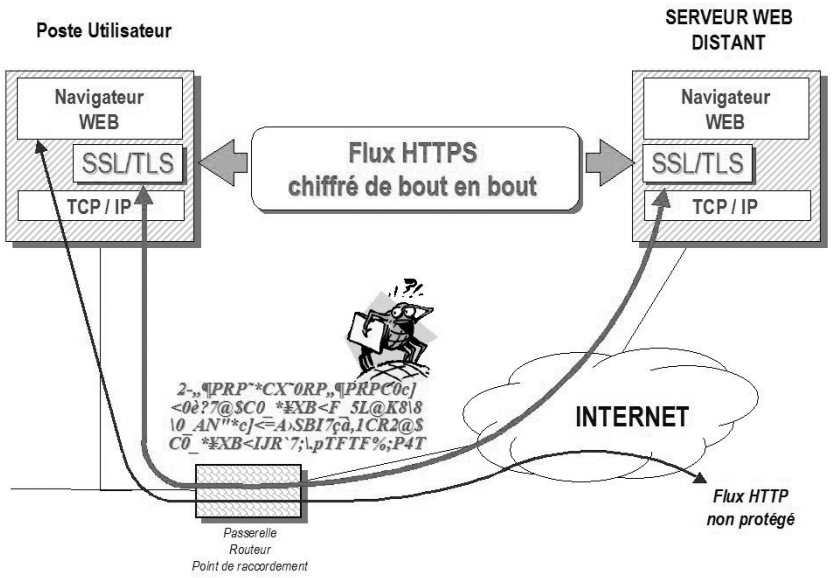


Figure 9–2
Sécurisation des flux entre poste Utilisateur et serveur distant avec HTTPS

Renvoi Attaque de l'homme du milieu

Reportez-vous à l'annexe B.

Ainsi, au moment où elles quittent physiquement votre poste ou le serveur distant, les données deviennent parfaitement inintelligibles. Tout espion qui manifesterait l'outrecuidance de jeter un regard indiscret sur le réseau pour capter votre conversation en serait pour ses frais : en guise de numéros de sécurité sociale ou de cartes bancaires, il ne lirait qu'un charabia indescriptible. Avec HTTPS, vous êtes protégé contre ce que l'on appelle « l'attaque de l'homme du milieu », (aussi appelée « attaque du singe intercepteur »).

Sachez que les principes mis en œuvre ici sont très proches de ceux de la messagerie électronique sécurisée. L'une des différences réside dans le fait que la messagerie chiffre le corps du message avant de l'émettre à l'intérieur d'un flux non chiffré, alors qu'avec HTTPS, vous chiffrez l'intégralité du flux HTTP à la volée, de bout en bout.

Le plus déroutant pour l'utilisateur, c'est que, a contrario de la messagerie, tous ces mécanismes se déroulent de façon transparente, vous n'avez pas à intervenir. En effet, serveurs web et navigateurs, entités qui, pourtant, ne se connaissent pas, sont conçus pour négocier et se mettre d'accord sur les paramètres cryptologiques nécessaires à l'établissement de tunnels chiffrés.

Déroulement d'une transaction électronique sécurisée

Examinons le mode opératoire pour mieux comprendre comment les choses se passent. Vous naviguez à loisir sur le site de votre choix ; comme vous avez pu le constater, vous visualisez la majeure partie du temps des pages non sécurisées dont l'URL est de la forme classique http://www.serveurdistant.com/pageLambda.htm. Dans ce cas, les informations transitent en clair entre votre poste et le serveur web, via le protocole HTTP.

À un moment donné, en général lorsque vous atteignez la phase de paiement ou de transfert de données personnelles, vous cliquez sur un lien qui, sans que vous le remarquiez, vous dirige vers une page dont l'URL est similaire à celle de la figure 9-1, de la forme https://www.serveurdistant.com/page-sécurisée.htm. Ce détail – « https » au lieu de « http » – est important mais ne saute pas forcément aux yeux ; c'est la raison pour laquelle, selon la configuration de votre navigateur, celui-ci vous affiche un message d'avertissement similaire à celui de la figure 9-3.

À cet instant s'engage entre serveur et navigateur un dialogue assez fourni, dont le succès est matérialisé par la montée du canal chiffré et l'affichage de la page web demandée. Ce dialogue a lieu, bien sûr, pendant un laps de temps très court, généralement le temps de l'affichage normal d'une page web ; c'est la raison pour laquelle cette couche de

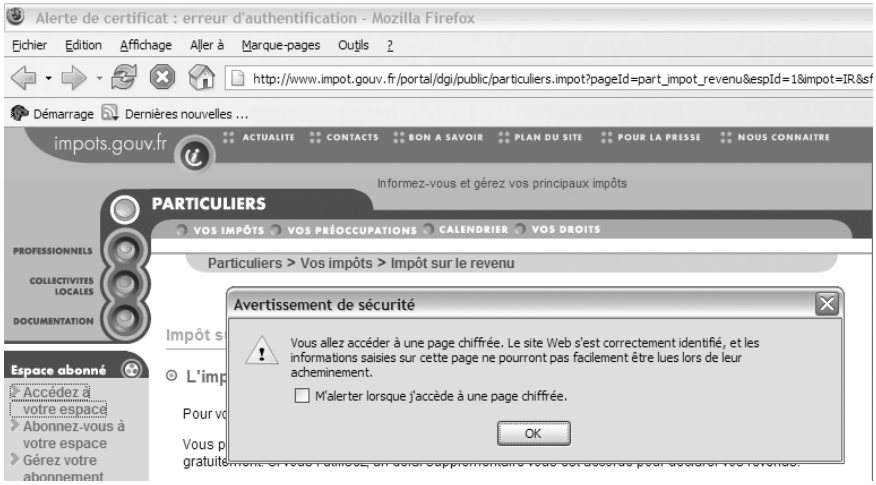


Figure 9–3
Le navigateur vous informe lorsque vous atteignez une page HTTPS et que vous entrez dans un mode sécurisé.

sécurité peut sembler transparente. Cependant, en dépit de cette relative rapidité, les dialogues sont intenses. Pour information, voici, très schématiquement, la teneur de ces échanges (voir figure 9-4) :

1. Le navigateur envoie une requête au serveur pour lui demander sa clé publique ; il profite de cet envoi pour lui transmettre des indications sur ses propres capacités cryptologiques et lui suggérer différents choix. Les principaux paramètres proposés par le navigateur concernent en particulier :
   - le type de protocole de sécurité sur lequel devra s'appuyer HTTPS (TLS, SSLv3 ou SSLv2) ;
   - les algorithmes de chiffrement reconnus par le navigateur (par exemple 3DES, RC4, RC2, DES, pour les algorithmes symétriques, RSA ou Diffie-Hellman pour les algorithmes asymétriques) et ceux qu'il préfère ;
   - les algorithmes utilisés pour effectuer le calcul des empreintes numériques (MD5, SHA-1) ;
   - d'autres paramètres, comme la méthode de compression des données.
2. Le serveur transmet au navigateur son certificat de clé publique. Il profite de cette réponse pour lui indiquer les paramètres cryptologiques qu'il a finalement sélectionnés et qui seront utilisés pour sécuriser l'ensemble de la conversation.
3. Lorsqu'il reçoit la réponse du serveur, le navigateur enchaîne plusieurs opérations :
   - Il commence tout d'abord par contrôler la validité du certificat du serveur, en vérifiant qu'il a bien été élaboré et signé par une Autorité de Certification reconnue.

RENVOI **Schéma de confiance des systèmes à clés publiques**

Vous pouvez vous reporter aux principes fondamentaux du schéma de confiance des systèmes à clés publiques, rappelés au chapitre 6.

RENVOI Et Vista ?

Il est à noter que la future version de Windows ajoutera quelques étapes à ce processus, dont le but avoué est de contrôler l'usage que fera l'internaute de ce qu'il aura acheté. Voir à ce sujet le chapitre 10.

– Il vérifie que le certificat n'a pas été altéré, accidentellement ou intentionnellement, durant son acheminement : pour cela, il recalcule l'empreinte numérique du certificat et la compare à la valeur de la signature déchiffrée à l'aide de la clé publique de l'autorité signataire. Au passage, il contrôle les dates de validité du certificat et, surtout, compare l'URL de la page visitée à celle du serveur web, présente dans l'un des champs du certificat. Cette simple vérification permet de déjouer les tentatives d'usurpation de sites web connus.
– Le navigateur engendre ensuite un nombre aléatoire, qui deviendra la clé de session. Cette dernière servira à chiffrer les échanges, à l'aide de l'algorithme symétrique sélectionné à l'étape 2.
– Il transmet cette clé de session au serveur, chiffrée, bien entendu, avec la clé publique de celui-ci.

4 Le serveur déchiffre cette clé avec sa clé privée. Lui seul est capable d'effectuer cette opération. Serveur et navigateur se retrouvent maintenant tous deux en possession de la copie d'un même secret, ils peuvent ainsi entamer les échanges sécurisés à travers le canal chiffré.

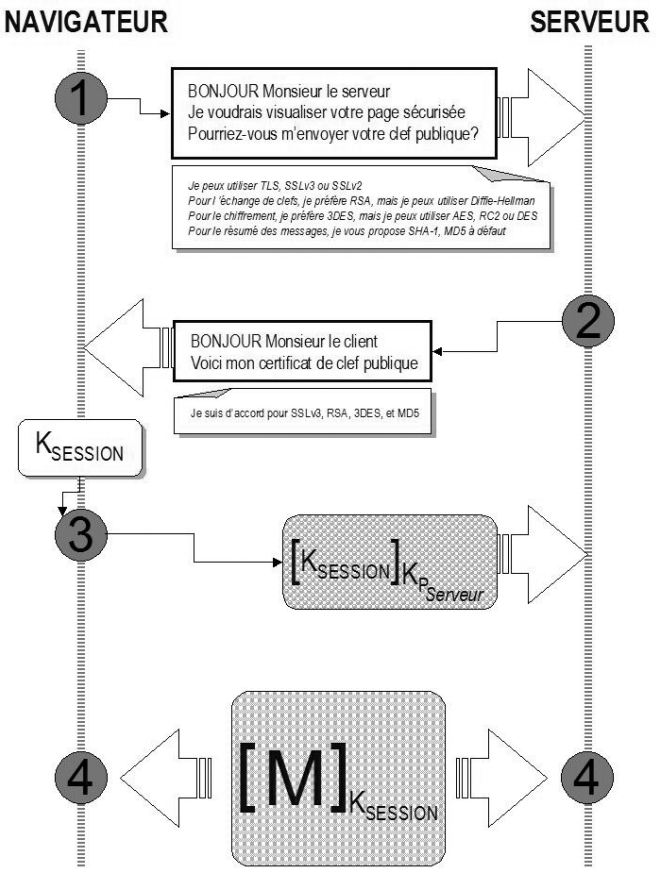


Figure 9–4
Schéma de principe de l'établissement d'une session SSL

Bien entendu, cette présentation est schématique, pour ne pas compliquer le discours. Dans la réalité, des mécanismes supplémentaires viennent se greffer autour de ces échanges, mais le principe reste le même et nous ne les aborderons pas. Nous avons toutefois omis un détail important : l'authentification du serveur. Ce point est capital aux yeux du consommateur : au moment de livrer son numéro de carte bancaire, il faut être sûr de dialoguer avec le bon serveur !

En réalité, cette authentification est implicite : le simple fait que le navigateur réussisse à échanger avec le serveur des informations chiffrées confirme son authenticité. Réfléchissons un peu : si le navigateur récupère du soi-disant serveur une information intelligible après déchiffrement, cela veut dire que le serveur a chiffré cette information avec la bonne clé de session, autrement dit, qu'il connaît cette clé. Comme le navigateur a engendré la clé de session, qu'il l'a transmise chiffrée avec la clé publique du serveur, cela prouve que l'entité qui a réussi à la déchiffrer possède forcément la clé privée du serveur. À moins bien sûr d'un piratage de celui-ci – nous écarterons cette hypothèse, grâce notamment aux listes de révocation – la seule entité au monde en possession de cette clé privée est bien le serveur en question ; il est donc authentifié par rapport au navigateur.

EN COULISSES

Le serveur, lui, ne vous authentifie pas

Avec un tel schéma, tout au moins dans la manière dont nous l'avons décrit, le navigateur authentifie le serveur web distant, mais la réciproque est fausse. Toutefois, il n'y a pas lieu de s'alarmer : ce modèle est bien adapté à la problématique de l'achat sur Internet, tout au moins du point de vue du consommateur : lorsque vous effectuez un achat, vous exigez l'authenticité du site web, et la confidentialité de vos coordonnées bancaires et autres données personnelles au cours de l'acheminement. Le serveur web ne dispose pas en revanche de moyens particuliers pour authentifier votre navigateur ; mais ce point est secondaire car le vendeur vous authentifiera grâce à votre numéro de carte de crédit (encore une raison supplémentaire pour ne pas galvauder cette information !).

Niveau de sécurité réel offert au consommateur lors d'une transaction SSL

Disons-le tout de suite, le consommateur bénéficie en France d'une réelle protection lorsqu'il achète sur Internet. Certes, les limitations techniques de SSL rendent la fraude toujours possible, mais la loi française est prévue pour combler les dommages éventuels causés au consommateur, le plus souvent au détriment des commerçants, des banques et des assurances. Pour mieux comprendre la nature des attaques rencontrées, tentons d'analyser techniquement d'où viennent les risques liés à une transaction électronique.

Plaçons-nous dans un premier temps dans le contexte des transactions dites « simples » que nous venons de décrire : l'internaute transmet au site marchand son numéro de carte de crédit, chiffré par SSL/HTTPS ; une fois en possession de cette information, le commerçant lance la véritable transaction de paiement avec la banque, en se servant d'un TPE classique. Ce genre de transaction, sans intermédiaire, est ce qu'il y a de plus répandu à l'heure actuelle.

TPE

Terminal de paiement électronique. Cet équipement électronique, utilisé par la plupart des commerçants, permet d'effectuer une transaction de paiement sécurisée, à l'aide – entres autres – d'une carte bancaire.

Pour commencer, il faut savoir que les réserves formulées au chapitre précédent à propos de la sécurité de la messagerie électronique s'appliquent de la même manière à la sécurité des transactions électroniques.

BON À SAVOIR **Chiffrement et gouvernements**

Les technologies employées n'empêcheront pas certains gouvernements d'accéder, si bon leur semble, au contenu de vos transactions. Cependant, là non plus vous ne risquez pas grand-chose. Tant que vous ne vous spécialisez pas dans le commerce du bicarbonate de soude, il y a peu de chance pour qu'ils s'intéressent à ce que vous achetez.

Concrètement, lorsque vous effectuez un achat par Internet, la confidentialité des flux transmis vous met à l'abri des escrocs, des fâcheux et des scrutateurs de trafic en tout genre, en quête de numéros de cartes bancaires. Vous êtes donc protégé pendant l'acheminement de vos données sur le réseau, ce qui constitue le seul vrai risque susceptible de vous menacer. Attention toutefois, vous n'êtes pas protégé à cent pour cent. En effet, rien n'empêche un pirate de récupérer vos coordonnées bancaires par un autre canal. Il peut faire appel au fameux « key logger » que nous avons déjà évoqué, ou voler un cookie ou, plus simplement, il peut subtiliser sur votre machine un fichier contenant ces précieuses informations que, par négligence, vous aurez omis d'effacer. Dans ce cas, SSL n'y est pour rien et, comme nous l'avons vu, les mesures à prévoir ne sont pas d'ordre cryptologique.

Dans ce type d'échanges, le vrai problème se situe ailleurs. En effet, le site marchand connaît à la fois votre identité et votre numéro de carte de crédit. C'est cette connaissance qui peut être la source de quelques petits désagréments. En voici deux types :

- **Site frauduleux** – Le premier, vous l'aurez deviné, peut venir d'un site frauduleux, dont la belle façade, respectable en apparence, n'a qu'une seule vocation : collecter les numéros de cartes de crédit. Le phishing, notamment, a abondamment recours à cette technique. De tels sites poussent tous les jours comme des champignons et disparaissent en général aussi vite, en ayant pris soin au passage de collecter quelques milliers de numéros de cartes, en prévision des bonnes œuvres au bénéfice des petits génies de la fraude. Prudence, donc, au moment de révéler vos coordonnées bancaires. Assurez-vous du sérieux du site avec lequel vous conversez. N'hésitez jamais à inspecter le contenu du certificat du site (voir chapitre 6 et plus loin dans ce chapitre).
- **Piratage des serveurs du marchand** – Le second est issu d'une menace plus sournoise, mais aussi plus probable, car elle fait appel à des techniques très classiques en matière d'attaques de sites web : il s'agit tout simplement du vol de votre numéro de carte de crédit suite à un piratage des serveurs du marchand. En effet, même s'ils ne sont pas censés stocker ces informations, les sites marchands ne s'en privent pas, ne serait-ce que pour des raisons administratives ou commerciales. Quand bien même ils s'abstiendraient de le faire, ils font pour la plupart appel à des prestataires externes (par exemple des hébergeurs), qui, pour des raisons techniques, sont amenés à stocker tout ou partie de leurs données – donc vos éléments financiers – pendant des mois, voire des années. La fiabilité du système de paiement dépend donc en grande partie de la façon dont ces intervenants gèrent vos données personnelles et des mesures de protection mises en œuvre au niveau du site marchand. Par exemple Paypal, prestataire

financier reconnu, conserve les données sur ses propres serveurs ; ceux-ci sont hautement surveillés, installés derrière un pare-feu et raccordés à des réseaux non directement connectés à Internet. Dans ce cas, le niveau de protection est significatif. Que dire en revanche de la sécurité mise en œuvre par la plupart des marchands en ligne, dont la compétence réside avant tout dans la vente de marchandises, de biens ou de services, et non dans le déploiement et l'administration de systèmes sécurisés ?

De nombreux rapports sur la fraude aux moyens de paiement sur Internet mettent en évidence l'augmentation notoire des transactions interdites, résultant de l'usurpation de numéros de cartes bancaires existantes. Il semblerait que la collecte frauduleuse des numéros de carte bancaire soit l'un des facteurs de risque recensés, et il est clair que le phishing et les techniques de piratage des sites de e-commerce n'y sont pas étrangers.

Moyens mis à votre disposition pour rendre vos transactions plus sûres

Malgré tous ces pièges, il ne s'agit pas d'abandonner définitivement l'idée de commercer sous forme électronique. Vous disposez d'un arsenal de mesures pour éviter les attaques, voire obtenir réparation en cas de préjudice.

Vigilance

Tout d'abord, votre vigilance doit être votre premier rempart ; soyez attentifs, nous pouvons vous assurer qu'une mesure aussi simple est vraiment efficace. De nombreuses attaques ont recours à une esbroufe dénuée de subtilité et ne doivent leur succès qu'à la crédulité, voire la naïveté, de l'utilisateur (c'est le fameux « social engineering » anglo-saxon). Ne tombez plus dans ces pièges grossiers, ni dans ceux du phishing. Dévoiler vos mots de passe et vos coordonnées bancaires sont des opérations sensibles qui résultent uniquement d'un processus que vous devez avoir initié vous-même. Si vous recevez inopinément une invitation à fournir ces données, pas d'hésitation possible, il s'agit d'une arnaque et vous ne devez jamais donner suite.

Conseil **Usez de votre bon sens**

Comment peut-on sérieusement croire au discours d'un soi-disant membre de la famille ex-princière d'un État qui a basculé dans le régime adverse, où l'on vous fait miroiter une commission mirifique si vous acceptez de « prêter » votre compte pour réaliser un transfert portant sur plusieurs millions de dollars ?

Législation française favorable au consommateur en ligne

Sachez que la loi française est très favorable au consommateur en ligne. Ceci résulte d'une démarche volontariste du gouvernement visant clairement à promouvoir le développement du commerce électronique en France. Pour commencer, l'objectif est clair : il s'agit d'élever le degré de

confiance des particuliers dans les technologies de paiement électronique. En cas d'utilisation frauduleuse d'une carte de crédit sur Internet, la loi prévoit que la responsabilité de l'utilisateur soit purement et simplement dégagée. Ceci est valable dans tous les cas, sauf peut-être lorsque le client a commis une négligence manifeste, comme laisser son code confidentiel apparent avec la carte. En dehors de ces cas particuliers, le consommateur bénéficie d'une couverture solide en cas de fraude sur sa carte.

Modèle de transaction avec tiers

Indépendamment des mesures législatives et organisationnelles, il existe des solutions de paiement sur Internet qui mettent en œuvre des concepts plus fiables que d'autres. Certains produits proposent en effet un modèle de transaction plus élaboré que celui présenté à la figure 9-4 : à la place du commerçant, un intermédiaire de confiance (prestataire financier accrédité ou organisme bancaire) prend entièrement en charge les opérations de paiement. Ce point est capital mais échappe malheureusement à beaucoup d'utilisateurs, auxquels les acteurs du e-commerce préfèrent vanter les mérites de SSL et du chiffrement à 128 bits.

Le principe d'une transaction électronique via un organisme bancaire est le suivant :

- Vous consultez le site marchand et établissez votre panier de commande en utilisant les procédures habituelles, éventuellement dans le contexte d'une session chiffrée HTTPS/SSL, comme exposé à la figure 9-4.
- Au moment de payer, le navigateur ouvre une session sécurisée avec le serveur en ligne soit d'une banque, soit d'un organisme financier ou d'un prestataire accrédité, pour prendre en charge la procédure de paiement auprès des banques du commerçant et du consommateur. Vos coordonnées bancaires sont chiffrées avec la clé publique de cet organisme officiel, et ne peuvent être lues par le site marchand.
- Le tiers financier effectue les vérifications nécessaires, débite votre compte, vire le montant de l'achat sur le compte du commerçant, puis délivre à celui-ci un numéro d'autorisation, lui confirmant ainsi que la transaction a eu lieu.
- Dès la réception de ce numéro d'autorisation, le marchand peut déclencher l'envoi de la marchandise.

Dans un tel schéma, la prise de commande et la saisie des informations bancaires ont été effectuées, la transaction a bien eu lieu, mais à aucun moment le commerçant n'a eu accès aux caractéristiques de vos moyens de paiement. Ceci vous protège contre la diffusion tous azimuts de ces données sensibles et réduit d'autant les risques de vol. De son côté, le marchand est libéré de la responsabilité de la gestion de ces données ; il

reçoit en outre de l'intermédiaire financier une garantie sur le paiement, ce qui réduit les risques d'impayés ou de répudiation des paiements. La sécurité du paiement a ainsi été assurée, à un double niveau : celui du marchand et celui du consommateur.

Ces solutions très avantageuses reposent sur les protocoles SSL ou SET (Secure Electronic Transaction). Le produit PaiementCIC (figure 9-5) proposé par le CIC en est un exemple, mais ce n'est pas le seul.

Figure 9–5
PaiementCIC, le tiers de paiement proposé par la banque CIC

Toutefois, sachez qu'en tant que consommateur, vous n'avez pas votre mot à dire concernant la technologie de paiement électronique utilisée lors d'un achat sur Internet. Celle-ci vous est imposée par le site du marchand. Tout au moins à l'avenir, vous saurez vous faire une meilleure idée de la fiabilité de la solution qui vous est offerte, sachant qu'en cas de litige, la loi sera en votre faveur.

Protocole SET

Avec le protocole spécialisé pour les paiements SET, le consommateur et le commerçant disposent chacun d'un certificat délivré par une Autorité de Certification habilitée. Les informations relatives à la commande sont chiffrées avec la clé publique du commerçant (ne peuvent donc être lues par la banque), les informations de paiement sont chiffrées avec la clé publique de la banque (ne peuvent être lues par le commerçant).

Étude de cas : la sécurité dans le cadre de la déclaration des revenus sur Internet

Vous disposez maintenant des éléments essentiels qui vous permettront d'évaluer, tout au moins du point de vue de l'utilisateur, le niveau de sécurité offert lors d'une transaction électronique. Examinons donc ce qui se passe sur un cas concret que nous affectionnons tous : la déclaration des revenus et le paiement de l'impôt sur Internet (non, non, c'est décidé, vous n'aurez plus d'excuse !).

Cette procédure est accessible très simplement à partir du site officiel de la Direction générale des impôts : http://www.impot.gouv.fr/.

SITE Direction générale des impôts

- http://www.impot.gouv.fr/

Une fois sur le site, si vous tentez d'accéder directement au service de déclaration des revenus, un détail d'importance ne manquera pas d'attirer votre attention : vous ne pouvez entamer de procédure officielle sans que la DGI ne vous ait attribué (gratuitement) un certificat électronique (figure 9-6).

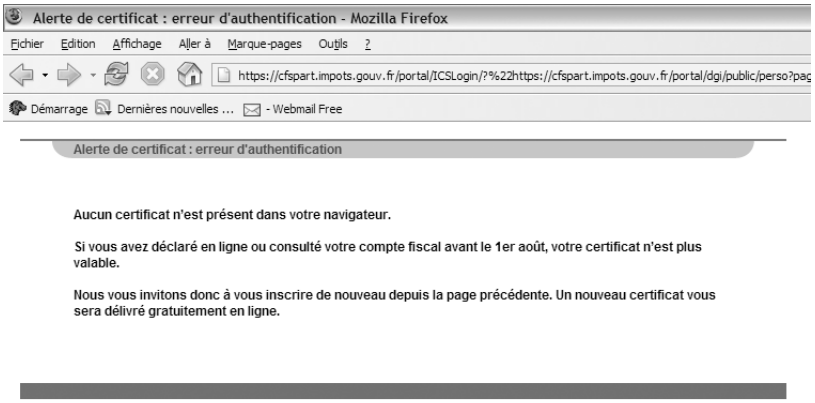


Figure 9–6
Pour déclarer vos revenus, vous devez posséder votre propre certificat.

Arrêtons-nous quelques instants sur ce point important. Le site de la DGI demande un certificat personnel au moment où vous accédez à votre espace privé : cela signifie que l'accès à l'espace privé d'un utilisateur est soumis à une authentification de cet utilisateur par des moyens cryptologiques. Si vous vous rappelez ce que l'on a dit à propos de l'authentification de l'origine des messages électroniques au chapitre précédent, vous comprendrez que ce certificat, délivré sous l'égide de la DGI (donc de confiance), servira à signer vos transactions ainsi que les requêtes que vous lancerez pour consulter votre compte : vous seul au monde serez capable d'élaborer une signature électronique que le site de la DGI reconnaîtra comme étant originaire de votre part. Donc, vous seul pourrez accéder à votre espace privé, en consultation ou en modifi-

BONNE PRATIQUE Protection du certificat

Vous seul pourrez accéder à votre espace privé, à condition toutefois de ne pas vous faire voler votre certificat, ainsi que le mot de passe qui le protège. Soyez donc très méticuleux lorsque vous manipulez cet objet sensible. Ne le laissez jamais traîner sur plusieurs ordinateurs et, éventuellement, pensez à le supprimer de votre poste une fois la procédure terminée (après l'avoir sauvegardé au préalable sur un support fiable, car vous en aurez besoin l'année suivante).

cation. Personne d'autre ne pourra mettre son nez dans vos affaires. Voilà déjà un point rassurant.

Vous noterez au passage, en déroulant la procédure, que ce certificat n'est pas établi sur une simple base déclarative, contrairement aux certificats de messagerie rencontrés au chapitre précédent (ne comptez donc pas obtenir un certificat au nom de votre patron, en espérant enfin connaître le montant de ses revenus !). Au moment de votre inscription, vous devez soumettre des éléments figurant sur votre déclaration de revenus et sur l'avis d'imposition des années précédentes. Ces valeurs vous sont propres et prouvent votre identité aux yeux de la DGI. Si vous entrez les bonnes valeurs, le site acceptera de vous attribuer un certificat personnel.

Obtenir votre certificat

Examinons rapidement cette procédure d'obtention de certificat : pour beaucoup d'entre vous, elle apparaît souvent pénible, contraignante et inutile, au point, d'ailleurs, d'en décourager certains. Cependant, soyez patient : cette procédure est très simple. Et surtout, n'oubliez pas que ce certificat est le passeport qui vous ouvre l'accès à vos données personnelles, et empêche les autres utilisateurs d'y accéder. À partir de la page d'accueil, en cliquant sur *Particuliers>Espace Abonné*, vous visualisez les différentes étapes (figure 9-7).

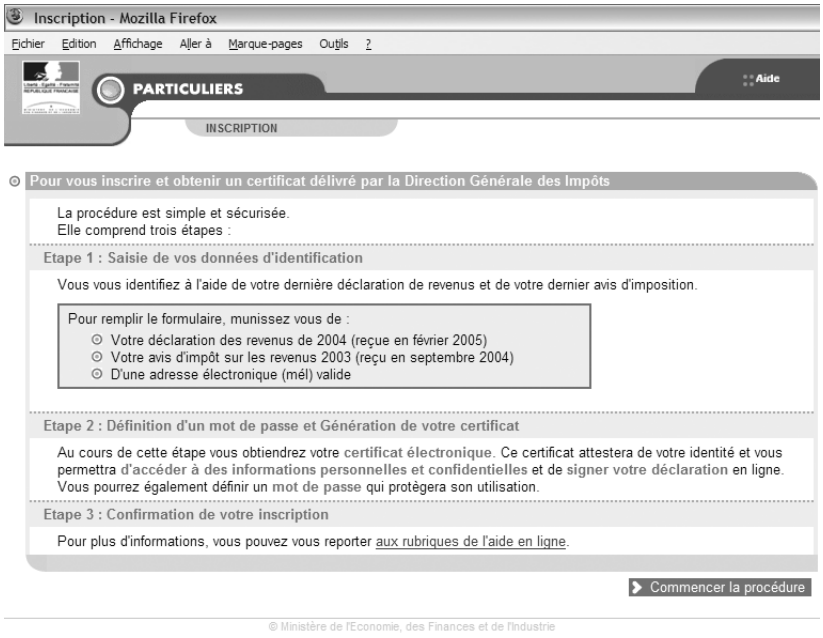


Figure 9–7
Procédure d'obtention de votre certificat personnel

1 Munissez-vous des documents demandés et déroulez la première étape : vous devez simplement saisir vos nom, adresse électronique, numéro fiscal, numéro de télédéclarant, revenu fiscal de référence. Ces trois dernières informations figurent sur vos déclarations de revenus et avis d'imposition ; attention donc à ne pas laisser traîner ces documents n'importe où !

2 À l'étape 2, on vous demande de choisir un mot de passe pour votre certificat (figure 9-8). Outre le fait qu'il protège votre clé privée, ce mot de passe est un peu l'équivalent du code PIN de votre carte bancaire : au moment de la transaction, il servira à prouver que l'utilisateur du certificat est bien son propriétaire, et non un pirate qui serait parvenu à subtiliser le certificat sur la machine. Bien que le logiciel du site semble ne pas accepter toutes les combinaisons (une séquence comme « 9s%Zme52va » n'est visiblement pas prise en compte), préférez toujours un mot de passe complexe ; une phrase courte et facilement mémorisable, comme la citation d'un auteur, fait parfaitement l'affaire (par ex. « *le public pardonne tout, sauf le génie* », Oscar Wilde).

RENVOI **Mot de passe robuste**

Reportez-vous aux conseils donnés au chapitre 2 pour choisir un mot de passe robuste.

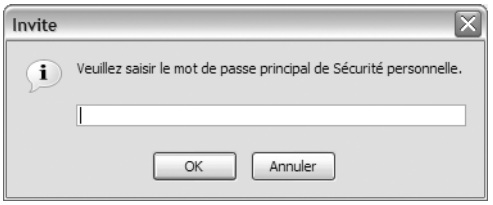


Figure 9–8
Choisissez un mot de passe robuste.

3 Une fois ce mot de passe entré, vous n'avez plus rien d'autre à faire, le site établit votre certificat (étape 3) et l'installe automatiquement dans votre magasin de certificats. Vous êtes maintenant prêt à accéder à tous les services en ligne offerts par la DGI.

ATTENTION **Gestion des certificats dans l'ordinateur**

N'oubliez pas que les certificats sont liés au navigateur, et non à l'ordinateur. Plus précisément, le certificat DGI est stocké dans le magasin de certificats du navigateur dont vous vous êtes servi lorsque vous l'avez fait établir. Si d'aventure vous changez de navigateur, il y a de bonnes chances pour que le site du MINEFI vous refuse l'accès à votre espace privé. La raison en est très simple : à moins d'avoir pensé à configurer le navigateur, votre certificat n'a aucune raison d'être présent dans le nouveau magasin. Par conséquent, pensez systématiquement à importer votre certificat (tous vos certificats personnels par la même occasion) dans le nouveau magasin de certificats !

Vérifier le certificat

Faisons une courte parenthèse et examinons le nouveau certificat. Avec Mozilla Firefox par exemple, dans le menu *Outils*, cliquez sur *Options*, choisissez *Avancé*, puis faites défiler la fenêtre principale jusqu'à atteindre l'option *Certificats* (figure 9-9).

Cliquez sur *Gérer les certificats* : vous constatez que vous disposez d'un nouveau certificat, émis par la Direction générale des impôts (figure 9-10).

Un détail peut sembler troublant à première vue : votre magasin indique que ce certificat a été émis par un inconnu (*Émetteur inconnu* indique la figure 9-10). Si vous ouvrez le certificat pour en savoir plus, le navigateur enfonce le clou : *Impossible de vérifier ce certificat car l'émetteur est inconnu* (figure 9-11).

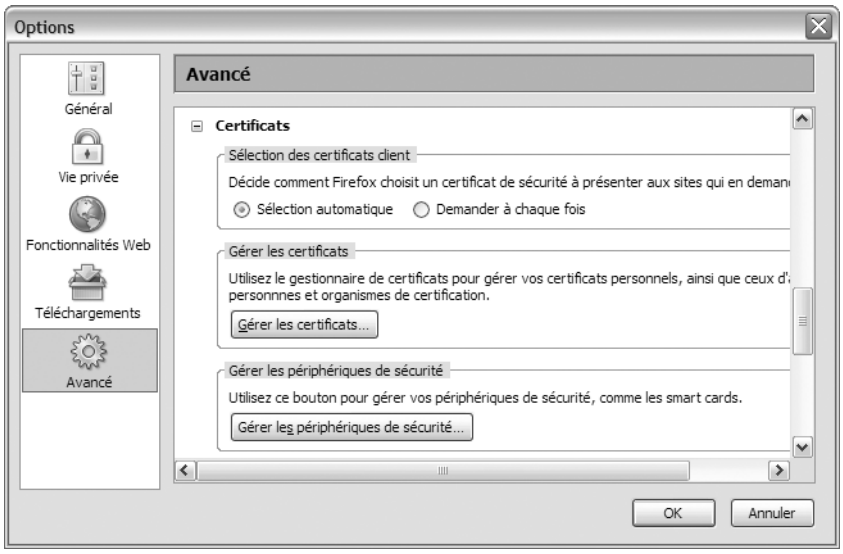


Figure 9–9
Consultez le contenu de votre magasin de certificats.

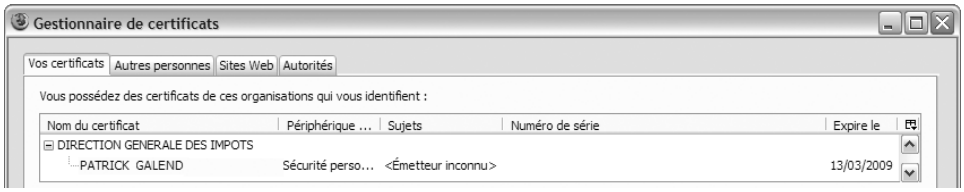


Figure 9–10
Le certificat de la DGI vous donne accès à votre espace privé.

Figure 9–11
Dans l'état de configuration actuel, votre certificat ne peut être vérifié.

Pourtant, il a semble-t-il été émis par la DGI. Avez-vous été abusé ? Êtes-vous tombé sur un site frauduleux essayant de se faire passer pour celui de la DGI ? A priori, la réponse est non. Souvenez-vous du chapitre 6 : un certificat digne de ce nom est toujours signé par l'Auto-

rité de Certification émettrice, elle-même liée, le cas échéant, à une AC de plus haut niveau, à laquelle tout le monde fait confiance. N'oubliez pas que la signature est le résultat du chiffrement de l'empreinte numérique SHA-1 du certificat avec la clé privée RSA de l'Autorité de Certification émettrice de la DGI. Pour vérifier cette signature, le navigateur a absolument besoin du certificat de clé publique de l'AC (en l'occurrence l'AC MINEFI B). Au fait, ce certificat est-il présent dans le navigateur ? Allez voir dans la liste des Autorités auxquelles le navigateur fait confiance par défaut (onglet *Autorités*, figure 9-10). Le certificat de clé publique de l'AC MINEFI B de la DGI figure-t-il parmi cette liste ? Vous constaterez probablement que non, ce qui explique pourquoi le navigateur ne peut pas vérifier la signature.

À RETENIR **Chargez les certificats des AC**

De façon générale (relire à ce sujet le chapitre 6), pour utiliser de façon optimale les services délivrés par un site sécurisé comme celui du MINEFI, il faut que les certificats des AC signataires des certificats de clés publiques utilisés par le site (au minimum le certificat racine) soient présents dans le navigateur. C'est grâce à eux que, lors de vos futurs échanges, vous serez sûr d'être en relation avec le bon site et que vos échanges seront sécurisés. Si ce n'est pas le cas, vous risquez de vous exposer à un message déstabilisant comme celui de la figure 9-12.

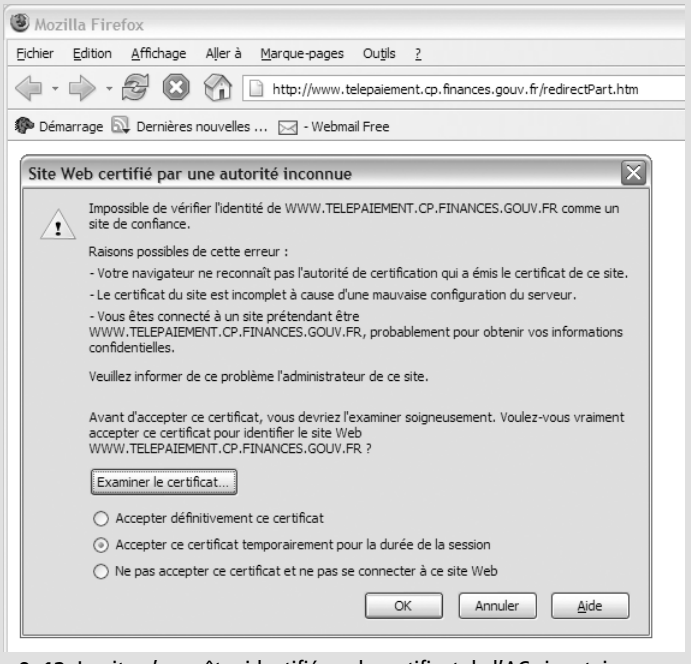


Figure 9–12 Le site n'a pu être identifié car le certificat de l'AC signataire n'est pas présent dans votre navigateur.

Dans l'exemple qui nous intéresse, le navigateur ne reconnaît pas l'AC qui a émis le certificat du site www.telepaiement.cp.finances.gouv.fr. En fait, la raison est très simple : tous les navigateurs sont livrés par défaut avec les certificats identifiant les principales Autorités de Certification rencontrées notamment dans le monde des achats sur Internet. En revanche, ceux du MINEFI n'y figurent pas. Il faut donc que vous les importiez vous-même.

Importer les certificats des AC signataires

Rendez-vous sur le site http://www.icp.minefi.gouv.fr. Suivez les instructions, l'installation se fait automatiquement (figure 9-13).

Figure 9–13
Téléchargez les certificats signés par le MINEFI dans votre navigateur.

Attention toutefois avant d'installer un certificat d'AC racine : vous devriez en toute rigueur vérifier, via une autre source (téléphone, courrier électronique…), que le certificat que vous allez enregistrer émane bien du MINEFI. En effet, qui vous dit que la page web visualisée à la figure 9-13 ne provient pas d'un faux site conçu pour vous faire installer son propre certificat et vous abuser ? Lorsque vous enregistrez un nouveau certificat dans la section *Autorités de confiance* de votre magasin, le navigateur vous demande toujours confirmation (figure 9-14).

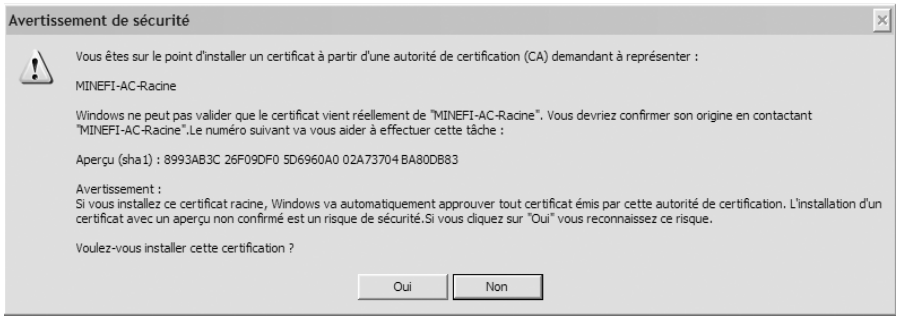


Figure 9–14 Pensez à vérifier l'origine d'un certificat avant de l'installer.

BON À SAVOIR **Certificats racines du MINEFI**

Pour vous faciliter la tâche, le MINEFI met à votre disposition un serveur vocal effectuant en trois langues (français, espagnol, anglais) une lecture de l'empreinte numérique de ses deux certificats racines (numéro AZUR 0 810 203 994). Notez attentivement l'empreinte SHA-1 du certificat MINEFI-AC-RACINE (« 8993AB3C 26F09DF0 5D6960A0 02A73704 BA80DB83 ») et vérifiez qu'elle est strictement identifique à la valeur contenue dans le certificat que vous installez. Évidemment, cette opération est contraignante, mais c'est la seule manière d'éviter les escroqueries. Sachez toutefois que l'intégration des certificats racines dans le navigateur ne se fait qu'une seule fois.
Les empreintes numériques des deux certificats racines de MINEFI sont en outre publiées au Journal Officiel de la République Française : JORF n°298 du 23 décembre 2004, page 21 848, texte n°85, NOR : ECOP0400995V. Ce texte est accessible en consultation sur le site de LegiFrance (www.legifrance.gouv.fr).

Utiliser les services sécurisés

Vous êtes donc maintenant en possession de votre certificat. Vous avez toute latitude pour accéder à votre espace abonné (après avoir dûment saisi le mot de passe associé à votre certificat) et enclencher les procédures de déclaration des revenus et du paiement de l'impôt (figure 9-15).

Figure 9–15
Vous accédez à votre espace privé.

Il est inutile de rentrer dans les détails des procédures proprement dites, ce n'est pas l'objet de cet ouvrage (de plus, elles sont très simples, vous ne pouvez pas vous tromper).

En revanche, jetons un œil rapide sur la sécurité de votre session lorsque vous déclarez vos revenus ou que vous payez votre impôt. Dès que vous entrez dans votre espace privé, vous naviguez sur des pages HTTPS, et les échanges sont sécurisés avec SSL. En somme, vous vous retrouvez exactement dans le cas de figure évoqué au début de ce chapitre : les échanges entre votre poste et le serveur de téléprocédures sont chiffrés de bout en bout.

Si vous voulez en savoir plus, vous pouvez aisément visualiser les caractéristiques de sécurité de chaque page visitée. Avec Firefox par exemple, un simple clic droit sur cette page vous affiche un menu contextuel dans le lequel vous pouvez sélectionner *Informations sur la page* (figure 9-16).

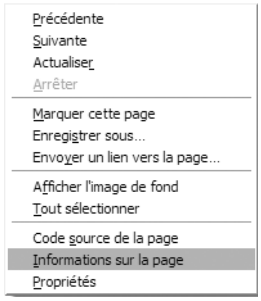


Figure 9–16 Visualisez les informations de sécurité associées à la page web.

Vous pouvez ainsi consulter les caractéristiques du niveau de sécurité associé à votre session (figures 9-17) :

- Vous êtes bien sur une page sécurisée de la forme https://....
- Vous êtes bien sur le bon site car son identité a pu être vérifiée par le navigateur : le certificat de l'AC émettrice (Thawte) est présent dans le navigateur (figure 9-18) et prouve que le certificat de serveur SSL qui sécurise cette page appartient bien à la DGI.
- Enfin, le flux échangé entre votre poste et le serveur de téléprocédure est chiffré à l'aide de l'algorithme RC4 (un bon algorithme) et d'une clé de 128 bits (figure 9-18). Comme cela vous est indiqué, cette con-

figuration rend « très difficile » l'accès d'une personne non autorisée au contenu de cette page durant son transfert. En clair, si le serveur de téléprocédures ne s'est pas fait pirater sa clé secrète (nous pouvons raisonnablement partir du principe que cette hypothèse est vraie), et si votre machine est saine (ce devrait être effectivement le cas après avoir suivi toutes les recommandations exposées dans cet ouvrage), aucun pirate ne peut en pratique accéder au contenu de ces informations.

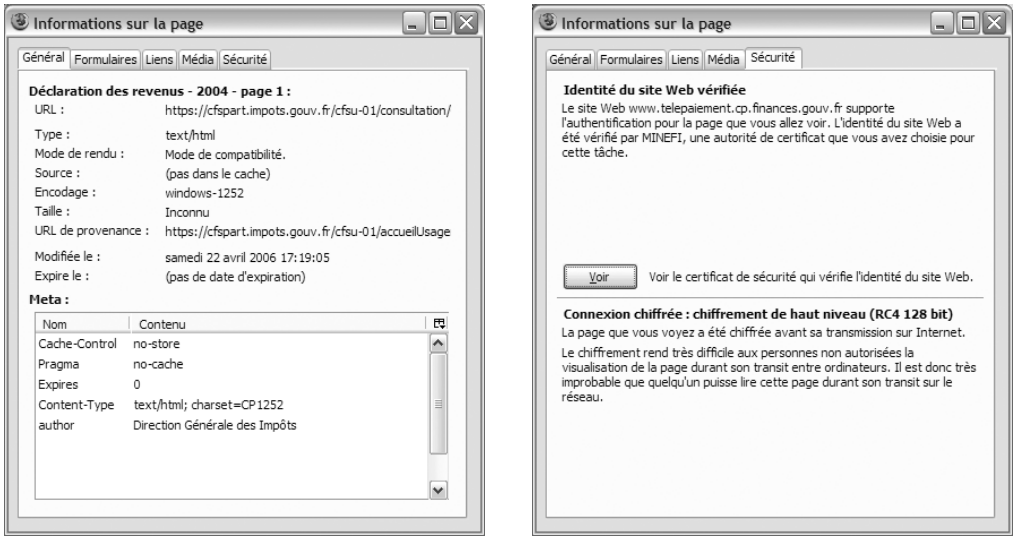


Figure 9–17 Visualisez les caractéristiques de sécurité de la session.

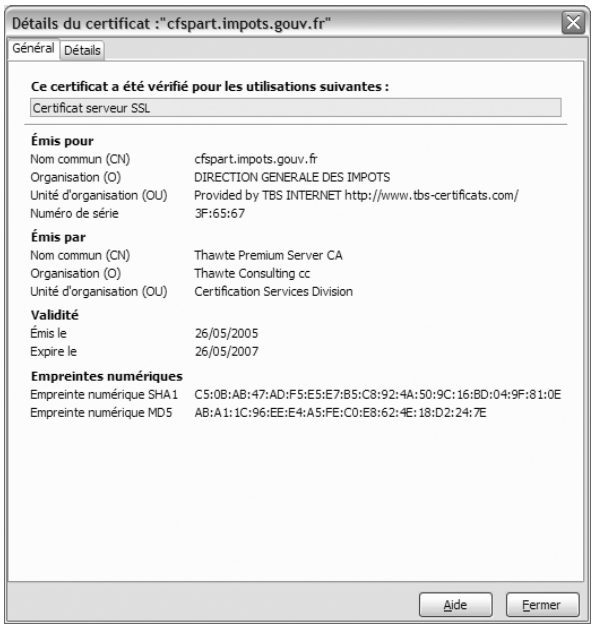


Figure 9–18
Détail du certificat qui a servi à sécuriser la session SSL avec le serveur de téléprocédure

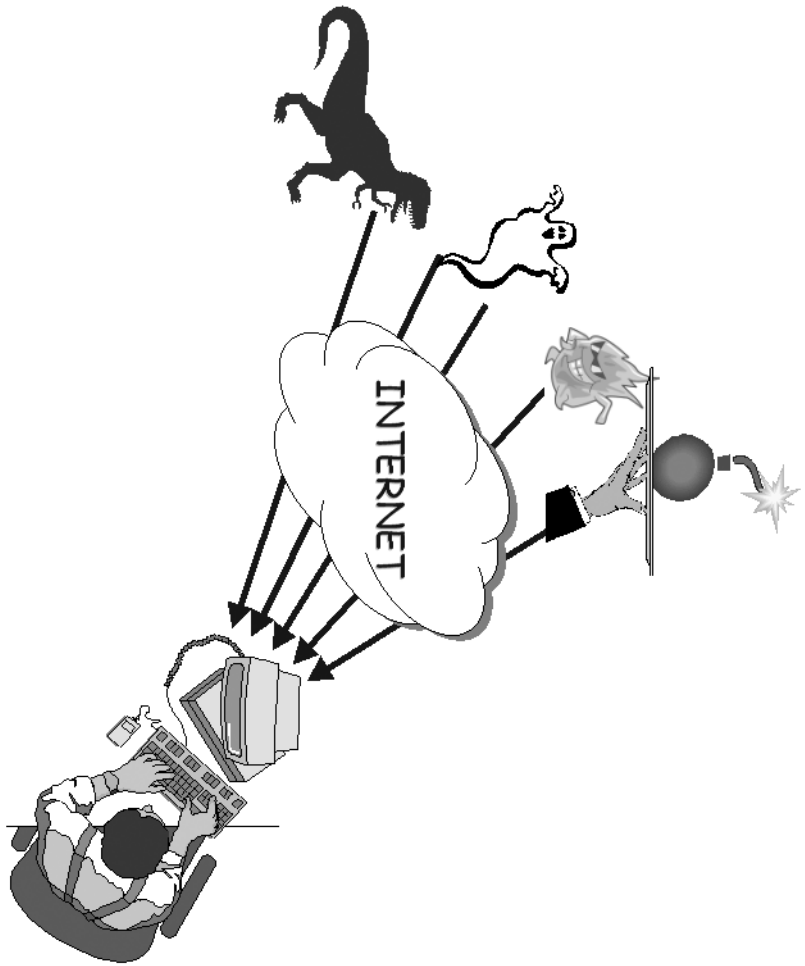
Récapitulatif

- L'accès à votre espace abonné est soumis à une authentification forte de l'utilisateur, réalisée à l'aide de moyens cryptologiques.
- Le site web du MINEFI est lui-même authentifié par votre navigateur grâce à son certificat.
- Les échanges entre votre ordinateur et le serveur de téléprocédures sont sécurisés avec le protocole SSL, un algorithme de chiffrement fiable et une clé de 128 bits.

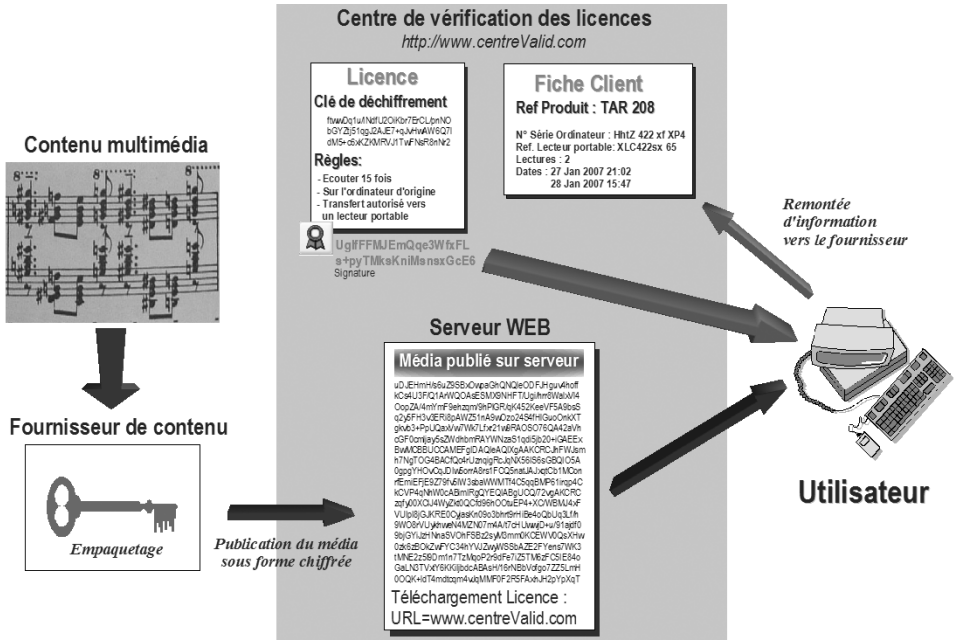
Disons que pour déclarer vos revenus et payer vos impôts sur Internet, vous bénéficiez d'un niveau de sécurité tout à fait compatible avec le besoin caractérisant ce type de transaction.

EXCELLENTE PRATIQUE **Protégez votre certificat**

On ne le répètera jamais assez : n'oubliez pas qu'une partie de la sécurité de cet édifice repose sur la protection de votre certificat, qui contient votre clé privée. Attachez-vous à en protéger l'accès avec un mot de passe que personne ne pourra deviner. Une fois la procédure terminée, ne le laissez pas traîner dans votre navigateur. Sauvegardez-le et supprimez-le de votre magasin de certificats. Vous aurez toujours la possibilité de le réinstaller ultérieurement si vous avez besoin de revenir vers ce site.



chapitre 10



Et Windows Vista ?

Avec l'arrivée de Windows Vista, la firme de Redmond se retouve une fois de plus au cœur de la polémique. Restant fidèle à la politique marketing affichée par Microsoft depuis plusieurs années, Vista propose des évolutions de sécurité importantes. Malheureusement, elles ne profiteront pas toujours à l'utilisateur.

SOMMAIRE

- Signature des pilotes et des exécutables
- Dépendance vis-à-vis du fournisseur
- Dépendance technologique et absence d'interopérabilité
- Solutions de sécurité intégrées
- Améliorations de la sécurité

MOTS-CLÉS

- DRM
- cryptologie « en dur »
- monopole
- choix technologiques
- interopérabilité
- TCPA
- Palladium-NGSCB

Référence **DADVSI**

La loi DADVSI (Droits d'auteurs et droits voisins dans la société de l'information) institue avec les DRM les mesures techniques de protection des contenus. Vous trouverez davantage d'informations concernant ses conséquences dans l'ouvrage suivant :

📖 *Peer-to-peer, comprendre et utiliser*, Fabrice Le Fessant, Éditions Eyrolles, 2006.

Avant d'évoquer les nouvelles fonctions de sécurité du système, remarquons d'emblée que Vista est le signe que les éditeurs veulent reprendre énergiquement en main la lutte contre le piratage de logiciels et le téléchargement sauvage de fichiers soumis à des droits.

Derrière le sigle DRM (Digital Rights Management), Microsoft propose en effet un nouveau mode de contrôle d'accès et d'usage des contenus (musique, vidéos...), de nature à révolutionner significativement le comportement des utilisateurs qui migreront vers Vista et les nouvelles architectures TCPA (Trusted Computer Platform Alliance), sur lesquelles le nouveau système va fonctionner.

Conséquences du contrôle d'accès généralisé aux contenus

Technologie **DRM**

Nous avons vu, tout au long de cet ouvrage, la puissance dont font preuve les mécanismes cryptologiques en ce qui concerne l'élaboration de documents infalsifiables et l'établissement de canaux chiffrés impénétrables entre la station de l'utilisateur et le serveur disant.
Faisant un usage massif de la cryptologie, les DRM sont fondés sur des mécanismes forts, qui bénéficient par ailleurs d'une robustesse d'autant plus élevée que les services cryptologiques sont désormais implantés profondément au cœur de la machine, à l'intérieur de puces matérielles soudées sur la carte mère.
Sans détailler le fonctionnement des DRM, tentons de comprendre la philosophie de ce concept à travers un cas d'utilisation : l'achat de musique sur Internet. Vous naviguez donc sur votre site marchand habituel, passez commande pour le morceau de musique de votre choix, réglez cette commande et lancez le téléchargement du fichier sur votre ordinateur. Très simple à première vue, cette opération cache une réalité plus complexe, car vont se dérouler en toile de fond plusieurs opérations dédiées à la gestion des droits d'accès :

1. Le fournisseur vous envoie non pas le fichier, mais un paquetage dans lequel se trouvent plusieurs éléments :
   - le fichier musical chiffré au moyen d'un algorithme symétrique et d'une clé secrète distribuée séparément ;
   - des informations diverses relatives au fournisseur ;
   - l'URL du centre de vérification des licences, à partir de laquelle la clé de déchiffrement peut être téléchargée.

Renvoi **Cryptologie**

Voir l'annexe A.

2. En utilisant un procédé assez similaire à celui mis en œuvre par les AC pour élaborer un certificat, le serveur établit un petit fichier qui contient la clé secrète de déchiffrement ainsi qu'une liste de règles décrivant précisément ce que l'utilisateur a le droit de faire avec le morceau de musique. Ce fichier s'appelle par exemple « licence » et le serveur le poste vers un centre de vérification spécial. Cette licence demeure aussi infalsifiable que le certificat émis par une AC : elle est signée cryptologiquement, donc si quelqu'un réussissait à modifier frauduleusement son contenu, par exemple pour étendre ses droits d'utilisation, ce serait peine perdue puisque le lecteur multimédia détecterait immédiatement la fraude en vérifiant la signature. Il refuserait donc de lire le morceau.
3. Vous recevez votre morceau de musique empaqueté et chiffré.
4. Vous souhaitez écouter votre morceau ; vous lancez donc un lecteur multimédia – attention, pas n'importe lequel comme nous allons le voir – par exemple Windows Media Player.
5. Constatant que le fichier est protégé par un DRM, le lecteur lance une requête auprès du centre de validation des licences afin qu'il lui fournisse la clé secrète nécessaire au déchiffrement. Bien entendu, le lecteur, qui a été conçu spécialement pour s'intégrer dans la chaîne de gestion des DRM, joint à cette requête toutes les informations nécessaires, par exemple le numéro de série de votre ordinateur.
6. Le serveur met alors à jour votre « fiche client », en inscrivant le numéro de série du morceau de musique et celui de l'ordinateur sur lequel vous voulez l'écouter.
7. Par un canal sûr (il faut protéger la clé secrète), le serveur envoie la licence à votre lecteur, qui la range bien soigneusement quelque part sur votre disque dur.
8. Exactement comme le navigateur lorsqu'il reçoit le certificat numérique d'un correspondant, le lecteur vérifie l'authenticité et l'intégrité de la licence et de son contenu, puis il finit par déchiffrer le fichier pour que vous puissiez l'écouter, s'il s'avère que vous avez effectivement ce droit.

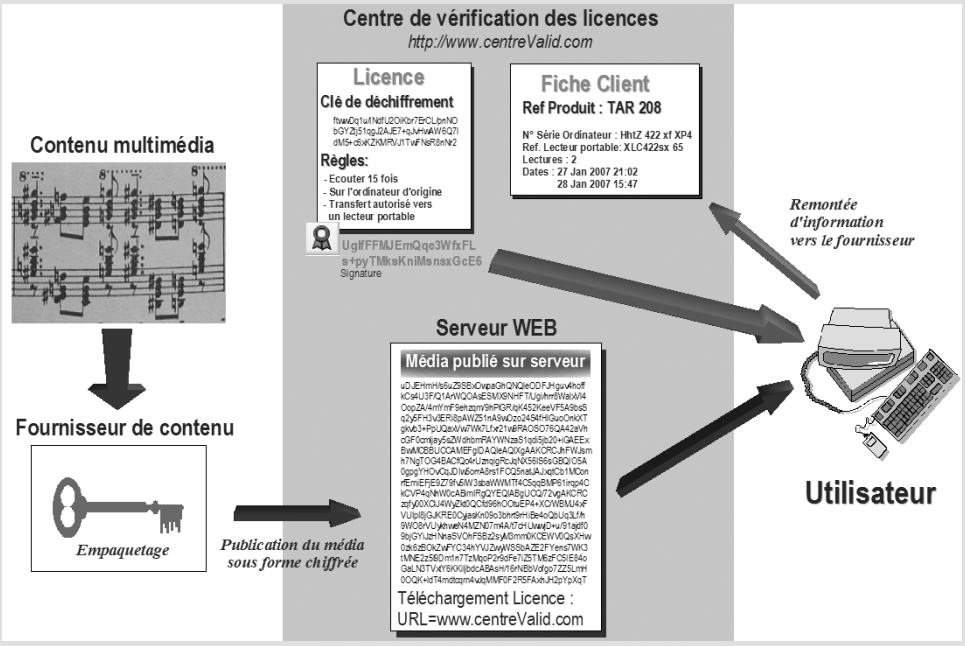


Figure 10–1 Principe de fonctionnement des DRM

Renvoi Certificats et autorités de certification

Voir le chapitre 6.

Vous pouvez d'ores et déjà constater les mécanismes plus « musclés » qu'il faut employer pour tenter de contourner ces protections. Franchement, on peut souhaiter bon courage aux as du piratage !
Maintenant, si vous transférez le morceau sur une autre machine, inutile de transférer aussi la licence car, en comparant les numéros de série, le lecteur saura tout de suite qu'elle n'a pas été attribuée à cet ordinateur. Le lecteur situé sur le nouvel ordinateur va donc recontacter le serveur pour obtenir une nouvelle licence. Votre « fiche client » sera ainsi mise à jour et le serveur tiendra soigneusement la comptabilité de ce que vous faites avec ce morceau.
Au bout d'un certain nombre de transferts, qui dépend du droit que vous avez acquis au moment de l'achat, le serveur refusera d'accorder une nouvelle licence. Il faudra soit « démonter » une licence sur un ordinateur pour la transférer sur une autre machine, le tout sous contrôle du serveur marchand, soit remettre la main à la poche.
Bien entendu, le fournisseur de contenu se réservera le droit de définir toutes les règles qu'il souhaite dans le fichier de licence, par exemple imposer un droit de lecture limité dans le temps, définir le nombre de lectures autorisées, autoriser ou interdire la gravure du morceau sur CD audio, etc.

En fermant les yeux sur certains détails gênants comme une certaine forme d'atteinte à la vie privée, il n'y a rien de vraiment choquant dans cette démarche, juste une réponse d'éditeur au piratage généralisé d'œuvres artistiques. Après tout, c'est de bonne guerre.

Plus préoccupantes en revanche sont les implications potentielles d'un tel modèle :

- la signature des pilotes et des exécutables ;
- la dépendance vis-à-vis du fournisseur ;
- la dépendance technologique et l'absence d'interopérabilité.

Signature des pilotes et des exécutables

Pour s'affranchir du modèle exposé précédemment, non pour cautionner le piratage mais simplement pour préserver une liberté individuelle au moins équivalente à celle que nous offrait le disque, on pourrait très bien imaginer avoir recours à un autre type de lecteur (Open Source ou autre), dans lequel les fonctions DRM seraient implémentées autrement. Bien entendu, les éditeurs et les majors n'y ont absolument aucun intérêt. Pour eux, l'enjeu est d'interdire l'exécution sur la machine de lecteurs multimédia « dissidents ». Ils tiennent absolument à ce que seuls des lecteurs en quelque sorte « agréés » DRM soient accessibles aux utilisateurs.

Il existe un moyen très simple et pratiquement incontournable pour parvenir à cet objectif : la signature numérique des pilotes et des exécutables.

Autrement dit, pour verrouiller ce modèle, le système d'exploitation – Vista en l'occurrence – est conçu spécialement pour autoriser sur la machine exclusivement les pilotes et les exécutables que Microsoft veut bien voir entre les mains de l'utilisateur, c'est-à-dire des composants auxquels il aura apposé sa signature. Ces principes sont exactement les mêmes que pour la technologie « Authenticode », à la différence que c'est Microsoft qui délivre la signature.

Renvoi Technologie Authenticode

Voir le chapitre 7.

En soi, obtenir une signature électronique de Microsoft n'est pas une procédure terriblement compliquée. Ce qui pose problème, c'est le fait que Microsoft et une poignée d'industriels, agissant à la fois en tant que juges et parties, s'arrogent le droit d'autoriser tel fournisseur, de mettre des bâtons dans les roues de tel autre, de faire barrage à telle ou telle technologie et de forcer l'utilisateur à n'exécuter sur sa machine que les applications souhaitées par lesdits industriels. C'est une nouveauté et elle est très mal perçue, notamment par la communauté du logiciel libre qui y voit clairement une menace.

Dépendance vis-à-vis du fournisseur

Comme le montre le cas d'utilisation précédent, un tel schéma impose à l'utilisateur, déjà en possession du produit (ou plus exactement du droit à sa lecture), de rester en relation avec son fournisseur via Internet s'il veut avoir une chance de jouir du produit. Par conception, cette nouvelle architecture obligera l'utilisateur à être en ligne beaucoup plus que par le passé, et à entretenir des relations beaucoup plus étroites avec son fournisseur, auquel, inévitablement, il rendra compte de ses faits et gestes.

S'il a été prévu de longue date que les nouvelles technologies réduiraient à terme l'espace de la vie privée, nous sommes ici en présence d'un modèle qui rend tout à fait possible le suivi à distance et en temps réel de ce que lit l'individu.

Cependant, il y a plus grave. Les communications entre le poste de l'utilisateur et le fournisseur s'effectuent à travers un tunnel chiffré, pour protéger les conversations. Pourtant, au-delà de l'échange de simples licences et de morceaux de musique, qui nous assure que ce canal opaque ne servira pas à transférer à des sociétés privées des informations beaucoup plus personnelles sur nos faits et gestes, les applications installées, éventuellement des fichiers personnels ou professionnels, des contenus de messagerie... Plusieurs chapitres dans ce livre ont montré l'existence de ce type de menace et des mécanismes pour les réaliser ; les dérives potentielles des DRM risquent d'en devenir le mécanisme légalisé.

Dépendance technologique et absence d'interopérabilité

On constate aussi une autre chose : en dépit de l'existence de standards ouverts en matière de DRM, les formats de fichiers gérés par les composants « agréés » sont propriétaires et fermés. En admettant que les éditeurs réussiront à imposer leurs propres standards aux fournisseurs de contenus, ils obligeront les utilisateurs à opter pour les « bons » lecteurs.

Le processus est d'ailleurs en marche. On ne peut que constater la mainmise grandissante de Microsoft sur le contrôle d'accès aux contenus : il fournit tous les composants de la chaîne de gestion des DRM, des lecteurs multimédia aux serveurs de DRM chez le fournisseur, en passant par le format du fichier. Si l'utilisateur dispose de Windows, il sera tiré d'affaire. En revanche, s'il est sur Linux, il est coincé : il n'y a pas de lecteur Open Source interopérable avec les lecteurs « agréés ». Belle perspective !

Au bout du compte, le noble sentiment d'une informatique mieux sécurisée semble bien loin ; les DRM ne font qu'entériner la légalisation du verrouillage des contenus. C'est comme s'il s'agissait de trouver un prétexte pour imposer un contrôle absolu sur des processus destinés à conserver un marché captif pour des éditeurs de plus en plus menacés par la montée du logiciel libre, ou à des maisons de disques qui, pour survivre, tentent de substituer au disque le concept de droit d'écoute (donc le DRM).

TCPA, Palladium et NGSCB

La TCPA (Trusted Computing Platform Alliance, Alliance pour une informatique de confiance) désigne un groupe de travail créé par Intel en 1999, et qui réunit aujourd'hui la fine fleur de l'industrie informatique américaine, soit plus de 200 industriels. L'objectif de la TCPA est de définitir une nouvelle architecture matérielle, qui intègre la sécurité dès le départ. Le but affiché est clairement de s'armer contre le fléau des attaques sur Internet, et de rendre l'ordinateur plus sûr.

Les travaux du groupe débouchent aujourd'hui sur la réalisation d'une plate-forme de nouvelle génération, dite « TCPA » : s'appuyant sur la collaboration des principaux fondeurs (AMD, Intel), les plates-formes TCPA intègrent désormais une puce spéciale, à l'intérieur de laquelle plusieurs briques de sécurité sont implémentées, dont un ensemble complet de mécanismes cryptologiques. Ces mécanismes, bâtis sur des algorithmes fiables par nature, font maintenant partie intégrante du matériel et sont capables d'offrir des services de sécurité de haut niveau, très difficilement contournables. De la cryptologie forte en natif dans le cœur du matériel, c'est déjà une petite révolution.

En soi, l'initiative de la TCPA est tout à fait recevable : combattre les piratages en tous genres, à commencer par les attaques à répétition tirant parti des multiples vulnérabilités du système d'exploitation, tout le monde le réclamait.

Cependant, les possibilités techniques offertes par ces nouveaux et puissants mécanismes ouvrent la voie à des dérives qui, cette fois, sont loin d'emporter l'adhésion des utilisateurs. Microsoft fait partie de cette alliance. Compte tenu de sa position dominante, son pouvoir d'influence sur la finalité de TCPA est immense. En s'appuyant sur l'infrastructure sécurisée de TCPA, Microsoft a bâti sa propre architecture logicielle de sécurité, Palladium, rebaptisée pudiquement NGSCB (Next-Generation Secure Computing Base), en raison d'une violente polémique qui secoua la communauté des utilisateurs, et de la mauvaise réputation acquise in fine par Palladium. Aujourd'hui, NGSCB-Palladium constitue l'un des fondements de la sécurité de Vista.

Faisant abstraction de la méfiance suscitée par le déploiement prochain de Palladium, il faut reconnaître que les mécanismes de cet édifice contribueront incontestablement à améliorer la sécurité des ordinateurs. Citons quelques exemples :

- Palladium est conçu pour qu'il y ait authentification des logiciels et des matériels au sein de la machine. Traditionnellement, la notion d'authentification sous Windows nous laisse comme un sentiment de légèreté (hormis peut-être avec XP ou Server 2003). Avec Palladium, l'authentification s'appuie sur des mécanismes cryptologiques implémentés dans le matériel ; très sincèrement, réussir une attaque demandera une bonne dose de talent ! Corrolaire, Palladium est censé garantir que seuls les logiciels autorisés pourront s'exécuter sur la machine ; difficile, dans ce cas, d'insérer un cheval de Troie.
- Les données sensibles sont écrites dans la mémoire vive spéciale située à l'intérieur de la puce cryptologique, accessible uniquement par des moyens sécurisés ou des logiciels autorisés ; les attaques basées actuellement sur l'interception d'une clé de déchiffrement – ou de toute information sensible – présente dans la mémoire vive risquent de devenir un tantinet plus compliquées.
- Avec Palladium, le dialogue entre certains composants de la machine se fait au travers de canaux chiffrés (les claviers pourront par exemple être dotés d'une puce cryptologique) ; là aussi, le piratage devient plus complexe.

Il ne s'agit là que de quelques exemples parmi d'autres, mais il faut honnêtement remarquer qu'en ce qui concerne l'attaque des machines TCPA/Vista, les pirates du monde entier risquent d'avoir du fil à retordre.

Cependant, tout n'est pas rose, loin de là. Nous savons de longue date que les éditeurs cherchent à renforcer le contrôle sur les activités de leurs clients ; les plates-formes TCPA, combinées aux riches mécanismes contenus dans la technologie Palladium–NGSBP, risquent fort de leur en donner les moyens, réduisant d'autant l'espace de liberté de chacun.

Il est difficile de prévoir les impacts sur le modèle économique à terme, d'autant que Microsoft fait tout ce qu'il peut pour afficher un discours rassurant – tout au moins tant que TCPA, NGSBP et les DRM ne seront pas suffisamment déployés et adoptés par les fournisseurs de contenus. Sachons toutefois qu'il est désormais techniquement possible de :

- rendre inaccessibles les programmes estampillés NGSCB si celui-ci est désactivé ;
- empêcher l'installation de logiciels non dotés d'une signature valide (la signature est attribuée par Microsoft ou les éditeurs sous l'œil de Microsoft) ;
- maintenir le contact permanent avec l'éditeur au travers de flux chiffrés, le tout en dehors du contrôle de l'utilisateur ;
- informer l'éditeur des applications présentes sur la machine de l'utilisateur ;
- ordonner au poste utilisateur d'effacer à distance des fichiers sur sa machine ;
- invalider le fonctionnement de logiciels et verrouiller l'accès aux données qu'ils avaient créées, etc.

Au bout du compte, la dérive principale de la TCPA–Palladium–NGSBC est d'amener progressivement l'ordinateur sous le contrôle des constructeurs et des éditeurs, et de garder un œil sur le contenu hébergé par ces machines. Difficile à avaler pour l'utilisateur !

Aller plus loin **La sécurité délivrée par TCPA–Palladium**

Force est de constater que NGSBC–Palladium est omniprésent lorsqu'il s'agit de réaliser une opération sensible affectant la sécurité des données (authentification, chiffrement d'une donnée, chiffrement à la volée des disques, etc.).

Il faut savoir que toutes ces fonctionnalités, tout au moins celles qui intéressent l'utilisateur ou l'entreprise (authentification sur la machine ou sur le réseau, chiffrement des données en local, établissement de liens chiffrés à distance à travers des tunnels VPN) sont disponibles depuis belle lurette. De plus, lorsque les mécanismes cryptologiques sont implémentés au sein de dispositifs matériels externes, comme les cartes à puce ou les clés USB, le niveau de sécurité est élevé (revoir à ce sujet l'analyse conduite au chapitre 8). En outre, ce type de dispositif laisse à l'utilisateur ou à l'entreprise le choix du constructeur.

TCPA revient en fait à ramener ces mécanismes au cœur de la machine et à imposer une sécurité Microsoft. En clair, lorsque des intérêts nationaux sont en jeu, il faut considérer de que TCPA–Palladium n'offre aucune sécurité.

La sécurité, je fais tout seul

Au-delà de toutes ces constatations, une autre polémique prend actuellement de l'ampleur : accusé encore une fois d'abuser de sa position dominante, Microsoft a choisi d'intégrer ses propres solutions de sécurité dans son système d'exploitation (et pas seulement la sécurité d'ailleurs !), au détriment des produits fournis par ses traditionnels partenaires.

Décidément, Microsoft au centre de questions antitrust, ce débat nous semble déjà familier. Pourtant condamné en 2004 à la suite du conflit sur fond de concurrence déloyale qui l'avait opposé à Bruxelles, Microsoft n'hésite pas à rééditer des pratiques contraires au principe de respect de la libre concurrence. En quelques mots :

- Le Centre de sécurité de Vista s'étoffe et intègre de plus en plus de solutions Microsoft :
  - fonctions anti-malware (virus, vers, logiciels espions) ;
  - pare-feu logiciel ;
  - logiciel anti-spam.
- Avec Windows XP, le Centre de sécurité était capable de s'interfacer avec les produits d'éditeurs indépendants. Sous Vista, cela devient plus difficile. À titre d'information, si Microsoft a récemment consenti à « ouvrir » la porte, c'est uniquement afin d'éviter un nouveau procès antitrust à Bruxelles.
- Habitué à coopérer avec ses partenaires, Microsoft a cette fois fermé aux éditeurs l'accès au code de Vista.
- Face à la pression grandissante des autorités de régulation et des grands groupes tels Symantec, McAfee ou Adobe, Microsoft a finalement consenti à fournir à ses concurrents une interface de programmation qui permettrait d'accéder au noyau de Vista 64-bits. Toutefois, ces éditeurs rencontrent des problèmes techniques, notamment à cause du logiciel PatchGuard (voir plus loin) qui interdit l'écriture dans le noyau en mode protégé.

Au delà des problèmes de stratégie industrielle que l'on comprend parfaitement, il est profondément gênant de constater que cette démarche est en totale contradiction avec un principe dont la pertinence a été maintes fois démontrée au cours de ce livre : la sécurité est une affaire de spécialistes.

Comment imaginer que Microsoft, qui a fait des efforts certes, mais qui est encore loin d'être reconnu dans le domaine de la sécurité, sache atteindre subitement le niveau de performances d'éditeurs de pare-feu comme CheckPoint, ou d'antivirus comme F-Secure ou Kaspersky, dont le métier consiste exclusivement à lutter contre une forme de menaces spécifique ?

Comment comprendre que Microsoft tienne à distance les éditeurs d'antivirus comme F-Secure, Kaspersky, McAfee, Symantec ou Panda (pour ne citer que ceux-là), alors qu'un antivirus est fortement couplé au système d'exploitation ?

Comment penser que Microsoft offrira une meilleure sécurité alors que les spécialistes, sur leurs terrains respectifs, sont parfois tenus en echec ?

Il est clair que Microsoft cherche à dominer sans partage sur tous les marchés du logiciel, à faire de Vista une arme anti-concurrentielle. Malheureusement, cela ne peut avoir lieu qu'au détriment de la sécurité de l'utilisateur.

Améliorations de la sécurité du système

Malgré toutes ces réserves, il y a tout de même un domaine où seul Microsoft a la capacité d'apporter une vraie valeur ajoutée : la sécurité du système d'exploitation, l'environnement qu'il maîtrise.

Si l'on fait abstraction du reste, il convient en effet de noter une amélioration générale des fonctions de sécurité, qui rendront Vista plus sûr que ses prédécesseurs. On peut citer notamment :

- **Protection renforcée des comptes d'utilisateurs** – Afin de limiter notamment la portée des intrusions ou des erreurs de manipulation, le système n'accorde plus par défaut les droits administrateur. Avec Windows XP, cela finit toujours par poser problème lorsqu'un utilisateur travaille avec des droits restreints (il peut avoir du mal à exécuter certaines applications, à définir une nouvelle imprimante, etc.). Vista résout ce problème.
- **Authentification** – Vista simplifie l'intégration de nouvelles méthodes d'authentification, comme la biométrie.
- **Protection de l'accès au réseau** – Il est possible d'empêcher un utilisateur de se connecter au réseau tant que ses mises à jour de sécurité et ses fichiers de définition de virus ne sont pas actualisés.
- **Renforcement de la sécurité d'Internet Explorer** – IE restreint maintenant ses actions en fonction des droits alloués à l'utilisateur. Ce principe tend à diminuer la marge de manœuvre d'un code malveillant exploitant une faille potentielle d'IE, qui tenterait d'éditer le Registre, d'installer des logiciels, ou de copier des fichiers dans le dossier de démarrage de l'utilisateur. Cependant, cet avantage reste mineur si l'utilisateur utilise un autre navigateur.

- **Chiffrement des données** – Vista offre la possibilité de chiffrer ponctuellement les données spécifiques ou de chiffrer à la volée des volumes entiers, et permet de stocker les clés de chiffrement sur un *token* (une carte à puce par exemple).

  Ces mécanismes ne résisteront pas à certaines attaques gouvernementales, mais un tel service réduit malgré tout les risques de compromission de données en cas de perte ou de vol de la machine.
- **Contrôle parental** – Vista fournit un système de contrôle parental permettrant de limiter les accès à la machine, aux logiciels installés sur la machine, en fonction de tranches horaires. Il est aussi possible d'activer un filtrage des pages affichées.
- **Pare-feu et protection anti-malware (vers, virus, anti-spyware)** – Ces fonctions sont citées parmi les fonctions de sécurité de Vista, mais ne font pas partie du système d'exploitation.

  Avec Vista, le pare-feu devient bidirectionnel et l'anti-spyware Windows Defender est présent en natif (Microsoft commercialise son antivirus séparément).

S'il y a un terrain sur lequel Microsoft est absolument irréprochable, c'est lorsqu'il tente de renforcer la sécurité du cœur de son système d'exploitation et de l'accès aux ressources Utilisateur (gestion des droits d'accès) ou Système (pilotes de périphériques). Il est impératif, pour améliorer la confiance des utilisateurs, que le système d'exploitation se montre moins vulnérable aux attaques extérieures. En cela, Vista apporte des réponses. Par exemple, afin de protéger le système contre l'exploitation de failles et les actes de piratage, Microsoft a développé une technologie intéressante, PatchGuard, destinée à préserver la stabilité du noyau. PatchGuard interdit les accès en écriture au noyau, bloque l'accès aux pilotes, aux logiciels et aux correctifs qui tenteraient de modifier cet espace noyau (selon Microsoft, un grand nombre des « plantages » provient d'un pilote mal programmé).

Intéressante sur le fond, cette nouvelle technologie met toutfois des bâtons dans les roues de nombreux éditeurs de sécurité (antivirus pour ne citer que ceux-là).

Vista, forteresse imprenable ?

En dépit de la position dure adoptée par Microsoft, le noyau de Windows Vista sera-t-il cette fois réellement à l'abri des attaques ?

Bien entendu, il est difficile de répondre à cette question tant que le système n'est pas déployé et n'a pas encore essuyé les coups de boutoir des pirates du monde entier.

Il semble cependant que des chercheurs et experts aient déjà démontré la possibilité de contourner les protections.

AVANCÉ **Blue Pill**

Pour en connaître davantage sur les failles de Windows Vista, vous pouvez consulter le blog de Joanna Rutkowska :

- http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html

Faut-il migrer ?

Cette courte analyse a été menée en toute indépendance et sans aucun parti pris. Force est de constater qu'elle n'est toutefois pas très favorable à Vista !

En ce qui concerne les DRM, on ne peut certes pas reprocher à un industriel d'innover, d'autant que, sur le plan technique, Microsoft a réalisé une performance. Cependant, les utilisateurs ne sont pas non plus obligés d'accepter des technologies qu'ils ne souhaitent pas, ni un modèle auquel ils n'adhèrent pas.

Les utilisateurs auraient certainement bien mieux accueilli une action de Microsoft essentiellement orientée vers le renforcement de la sécurité de son système d'exploitation, afin de le rendre plus imperméable aux attaques incessantes des pirates. Néanmoins, cela n'est qu'un avis d'utilisateur, qui ne pèse pas bien lourd à côté des intérêts financiers des éditeurs, des maisons de disques et des fournisseurs de contenus multimédia.

De toutes manières, il est encore trop tôt pour formuler un avis. L'année 2007 sera riche en enseignements et en retours sur expérience. Par ailleurs, les interfaces de programmation permettant aux éditeurs d'accéder au noyau Vista 64-bits sera livrée avec le Service Pack 1 de Vista. Selon le cabinet d'études Gartner, la première mise à jour de Vista ne serait pas publiée avant le début de 2008.

Rien ne presse donc. Il existe des systèmes alternatifs et Windows XP fonctionne encore très bien.

ALTERNATIVE **Autres systèmes**

Si Vista vous fait peur, c'est peut-être l'occasion pour vous de découvrir Linux. Ce système extraordinaire est doté d'une riche diversité de logiciels adaptés à toutes les tâches de l'utilisateur, aussi bien à domicile que dans l'entreprise. En outre, Linux affiche des performances étonnantes, et fonctionne à merveille sur les vieilles machines (justement celles pour lesquelles Palladium, TCPA et consorts sont des notions absolument étrangères !).

- 🕮 *Ubuntu efficace*, Lionel Dricot, Éditions Eyrolles, 2006.

Notions de cryptologie A

Connaissez-vous l'expression $a \equiv b \pmod{n}$?

Si cela ne vous dit rien, c'est normal ! À moins d'être plongé toute la journée dans des problèmes de cryptologie, il est rare d'avoir à affronter une telle expression.

En revanche, il est possible que, pendant vos cours de mathématiques, vous ayez eu l'occasion d'aborder l'arithmétique modulaire. Hélas, l'expérience montre que le calcul des congruences laisse généralement de mauvais souvenirs, et que les étudiants s'empressent bien vite d'oublier les délices de cette branche mystérieuse de la théorie des nombres.

Néanmoins, la cryptologie fait un usage intensif de l'arithmétique modulaire… et pour bien comprendre le fonctionnement d'algorithmes à clés publiques tels que RSA, il n'est pas inutile d'acquérir quelques rudiments dans ce domaine.

DÉFINITION **$a \equiv b \pmod{n}$**

Que signifie donc $a \equiv b \pmod{n}$? En fait, il s'agit d'une chose très simple : lorsque vous divisez un entier a par un entier n, vous obtenez un reste dont la valeur est b. On dit alors que a est congru à b modulo n. L'entier n est appelé module ou modulus.

Quand on divise 21 par 8, l'école nous a appris : « il y va 2 fois et il reste 5 ». Pour reprendre l'expression énoncée dans la définition précédente, on peut donc affirmer que 21 est congru à 5 modulo 8. Vous conviendrez que jusque là, il n'y a rien de bien compliqué.

Nous constatons déjà que tous les nombres inférieurs à 8 sont congrus à eux-mêmes modulo 8 ; par exemple, 3 est égal à 0 fois 8 et il reste 3. Nous pourrions faire le même calcul avec 0, 1, 2... jusqu'à 7, et nous obtiendrions :

$0 \equiv 0 \pmod 8$	$4 \equiv 4 \pmod 8$
$1 \equiv 1 \pmod 8$	$5 \equiv 5 \pmod 8$
$2 \equiv 2 \pmod 8$	$6 \equiv 6 \pmod 8$
$3 \equiv 3 \pmod 8$	$7 \equiv 7 \pmod 8$

Que se passe-t-il pour 8 ? 8 est tout simplement égal à 1 fois 8 et il reste 0. Donc $8 \equiv 0 \pmod 8$. Et pour 9 ? $9 \equiv 1 \pmod 8$. Et ainsi de suite. Si l'on dressait la même séquence que précédemment avec les nombres compris entre 8 et 15, nous obtiendrions :

$8 \equiv 0 \pmod 8$	$12 \equiv 4 \pmod 8$
$9 \equiv 1 \pmod 8$	$13 \equiv 5 \pmod 8$
$10 \equiv 2 \pmod 8$	$17 \equiv 6 \pmod 8$
$11 \equiv 3 \pmod 8$	$15 \equiv 7 \pmod 8$

Vous aurez sans doute remarqué le caractère assez répétitif de cette arithmétique. Abordons maintenant quelques opérations plus complexes, ces dernières étant toujours effectuées modulo 8 ; par exemple :

$6 + 7 \equiv \mathbf{5} \pmod 8$
$7 \times 9 \equiv \mathbf{7} \pmod 8$
$43 \times 257 \equiv \mathbf{2} \pmod 8$ car $43 \times 257 = 10\,794 = 1\,349 \times 8 + \mathbf{2}$
$13^7 \equiv \mathbf{5} \pmod 8$ car $13^7 = 62\,748\,517 = 7\,843\,564 \times 8 + \mathbf{5}$

Vous constaterez facilement que, quelles que soient la taille des nombres et la nature de l'opération effectuée modulo 8, le résultat est toujours compris entre 0 et 7. De la même façon, si la valeur du module était de 587, le résultat de toutes les opérations effectuées modulo 587 serait compris entre 0 et 586.

L'arithmétique modulaire définit donc un espace fini, à l'intérieur duquel nous sommes condamnés à évoluer… impossible de s'échapper. Quels que soient les stratagèmes compliqués, les calculs savants, les nombres importants, point de salut : le module nous ramènera brutalement, quoi qu'il arrive, à l'intérieur de notre espace fini…

À partir de maintenant, nous allons « oublier » la plus grande part de chaque nombre mis en jeu dans nos opérations, pour nous intéresser à une toute petite valeur, celle qui se situe à l'intérieur de notre espace fini : le résidu.

Définition **Résidu et espace fini**

Dans l'expression $a \equiv b \pmod{n}$, le résidu est le nombre b, reste de la division de a par n. Le résidu prend ses valeurs dans un espace fini compris entre 0 et n-1.

Il s'agit peut-être de l'aspect le plus déroutant de l'arithmétique modulaire. Certes, il y a bien cette petite gymnastique intellectuelle de la division et du reste, mais nous allons très vite l'oublier pour nous concentrer sur la notion de résidu. Ainsi, à partir de 62 748 517, nous ne conservons qu'un résidu d'information, le 5 !

Vous vous demandez certainement quel est l'intérêt de perdre une telle quantité de données, sachant de surcroît qu'il existe une infinité d'entiers congrus à b modulo n. La section qui suit vous donnera un début de réponse.

Exemple **Modulo, l'opérateur d'un perpétuel recommencement**

Dans la vie courante, chacun pratique quotidiennement cette notion de congruence sans s'en apercevoir. Imaginez par exemple que vous décollez à 22 heures pour un vol long-courrier en direction du grand Sud. Si la durée du vol est de 9 h 30, vous vous dites en toute logique que, vers 7 h 30 le lendemain matin, vous avez de bonnes chances de contempler les magnifiques paysages de l'Afrique. Jamais vous n'auriez eu l'idée d'évoquer un atterrissage aux alentours de 31 h 30. Vous vous êtes dit : « il est 22 h, pour aller à 24 h il y a 2 h, que je retire à 9 h 30, ce qui fait 7 h 30 demain matin ». Ou alors, vous avez réellement calculé 31 h 30, auxquels vous avez retranché 24 h. Vous avez intuitivement effectué une réduction de 31 h 30 modulo 24 et retenu le résidu, seule information dont vous ayez réellement besoin.

Un rendez-vous secret

Imaginons une horloge munie d'une unique aiguille qui donne à la fois l'heure, les minutes et les secondes. Supposons en outre que l'aiguille ne puisse se déplacer que dans un sens (disons le sens des aiguilles d'une montre) et uniquement sous l'impulsion d'une force extérieure. Enfin, admettons qu'un mécanisme extrêmement fiable l'empêche de rebrousser chemin, rendant définitif tout déplacement : il s'agit d'une aiguille « à sens unique ». Nous évoluons donc à l'intérieur d'un espace fini compris entre 0 et 23 h 59 min et 59 s.

Actuellement, notre aiguille marque 16 h 43 min et 22 s. C'est l'heure du rendez-vous qu'Alice souhaite fixer à Bernard pour échanger les informations secrètes, qui, réunies, leur permettront de trouver le trésor. Or, il ne faut surtout pas que l'équipe adverse sache à quelle heure ils vont se rencontrer, car elle chercherait certainement à leur dérober les documents pour accéder au trésor avant eux : cette information doit absolument rester secrète.

Aussi, comment Alice procède-t-elle pour faire parvenir cette information à Bernard ? Elle recourt à un artifice très simple : elle communique une impulsion à notre aiguille à sens unique, avec une force dont la

valeur a été choisie par Bernard. À l'issue de sa course folle, l'aiguille s'arrête en face d'un point marquant 4 h 32 min et 17 s. Elle peut avoir fait plusieurs centaines de tours, et pourtant, elle vient s'arrêter en face d'une valeur tout aussi banale que la précédente, une simple valeur située dans notre espace fini. Et c'est ce résultat qui importe à Alice, le tout petit résidu insignifiant de la valeur immense qu'à dû atteindre l'aiguille, réduite à néant par cet intransigeant « modulo 24 » : le précieux 4 h 32 min et 17 s.

Cette valeur est tellement précieuse qu'Alice va s'empresser de la faire parvenir à Bernard. Peu importe comment : elle peut l'écrire sur un bout de papier et la confier à un messager, elle peut faire des signaux de fumée sur la colline ou alors, si elle veut, la crier très fort pour que Bernard arrive à l'entendre de l'autre côté du village.

Bien sûr, Estelle, un redoutable agent de renseignement de l'équipe adverse, a réussi à capter cette information ; il est même probable qu'elle soit parvenue à construire exactement la même horloge. Elle connaît la valeur 4 h 32 min et 17 s, elle connaît la force précise avec laquelle Alice a lancé son aiguille (car elle entend toutes les informations véhiculées par les merveilleux moyens de communication de l'époque moderne) ; il lui suffit donc d'effectuer l'opération inverse pour découvrir l'heure exacte du rendez-vous. Seulement voilà : elle ne le peut pas, car l'aiguille est incapable de tourner dans le sens contraire. C'est une aiguille **à sens unique** et personne, pas même Bernard, ne peut effectuer cette opération.

Clés privée/publique

La force utilisée par Alice peut être divulguée à tout le monde : il s'agit de la « clé publique » de Bernard.
Celle utilisée par Bernard doit absolument rester secrète : c'est sa « clé privée ».

Alors que peut faire Bernard de ce 4 h 32 min et 17 s ? En fait, Alice n'a pas employé n'importe quelle force pour lancer son aiguille. Pourquoi ? parce que Bernard dispose d'une autre force de lancement, que l'on pourrait qualifier de « complémentaire ». Autant la force utilisée par Alice pour chiffrer son message peut être connue de tous, autant la valeur de cette deuxième force est gardée secrète !

Que fait donc Bernard ? Exactement comme Alice mais avec sa force privée, il lance l'aiguille initialement positionnée sur 4 h 32 min et 17 s. Au bout de quelques centaines de tours, toujours dans le sens des aiguilles d'une montre, elle vient tranquillement s'arrêter sur 16 h 43 min et 22 s, l'heure exacte du rendez-vous.

Magique ? Non, mais indéniablement astucieux, car il est évident qu'il existe une relation étroite entre la « force publique », ou « clé publique » utilisée par Alice et la « force privée », ou « clé privée » de Bernard. La connaissance de cette clé publique ne permet absolument pas de deviner la valeur de la clé privée. Même si tout le monde construit la même horloge, connaît la clé publique et le texte chiffré, seule la connaissance de la clé privée permet d'accéder au message clair original.

Tous ces éléments illustrent presque exactement les principes et le fonctionnement de l'algorithme à clés publiques RSA. La seule différence se situe au niveau de l'horloge et des actions entreprises pour l'élaboration des messages chiffrés. Avec RSA, ces mécanismes sont réalisés par des fonctions mathématiques.

Algorithme de chiffrement RSA

RSA est le plus célèbre et le plus répandu des algorithmes de chiffrement à clés publiques. Il a été inventé en 1977 par les mathématiciens et cryptologues Ron Rivest, Adi Shamir et Leonard Adleman.

À RETENIR

RSA est une « horloge à sens unique »

RSA fonctionne comme l'horloge à sens unique dont nous venons de décrire le comportement : il repose sur la mise en œuvre d'une fonction mathématique à sens unique, « à brèche secrète ».

Équation de base de RSA

Avant d'entrer dans un discours plus formel, prenons le temps d'examiner l'équation employée par RSA, de la forme :

$$\texttt{Message Transformé} = (\texttt{Message})^{K} \bmod n$$

`Message` est le message à chiffrer ou à déchiffrer, `n` le module, `K` un nombre entier formant, lorsqu'il est associé au module `n`, la clé de chiffrement ou la clé de déchiffrement.

Prenons tout de suite un exemple simple afin d'expérimenter concrètement cette formule : choisissons un module n égal à 15 et un exposant de chiffrement égal à 3. La fonction RSA s'exprime alors de la façon suivante :

$$\texttt{Message chiffré} = (\texttt{Message})^{3} \bmod 15$$

Imaginons que nous souhaitions chiffrer le message « 7 ». Le calcul de cette valeur chiffrée s'obtient très simplement en appliquant la formule :

$$(7)^{3} \bmod 15$$

Calculons :

$$(7)^{3} \text{ est égal à } 7 \times 7 \times 7 = 343$$
$$343 = 22 \times 15 + \mathbf{13}$$
$$\text{donc } : (7)^{3} \equiv \mathbf{13} \pmod{15}$$

La valeur chiffrée de 7 est donc 13, lorsque la clé de chiffrement est égale à (3,15). Ce n'est pas plus difficile que cela, tout au moins dans le principe.

Cependant, la réalité est un peu plus complexe. En effet, si 13 est la valeur chiffrée d'un message satisfaisant à la relation $(message)^3 \equiv 13 \pmod{15}$, Estelle a-t-elle vraiment du mal à retrouver la valeur de `message` ? Évidemment non : Estelle avait de très bon résultats en arithmétique modulaire à l'école et il est probable que cette équation ne va pas lui résister bien longtemps. Vous aussi êtes en mesure de trouver le nombre inférieur à 15 qui, élevé au cube et diminué de 13, donne un multiple de 15 : ce n'est pas 0, ce n'est pas 1, ni 2, ni 3 non plus... mais on s'aperçoit rapidement que 7 convient très bien. Connaissant la fonction RSA utilisée ainsi que la valeur chiffrée du message, il est donc parfaitement aisé pour un adversaire de recalculer le message clair original et d'accéder à vos secrets.

En fait, ce n'est pas la fonction RSA qui est en cause, mais uniquement ses paramètres qu'il faut modifier : ils sont beaucoup trop petits. Essayons l'équation suivante :

$$\text{Message chiffré} = (\text{Message})^{13} \bmod 85$$

Sauriez-vous retrouver le message clair sachant que le message chiffré est 28 ? Cette équation est déjà plus compliquée à résoudre, mais avec une bonne calculatrice, un peu de courage et quelques crampes aux doigts, on découvre assez vite que 78 est la bonne réponse. Que diriez-vous maintenant de l'équation :

$$\text{Message chiffré} = (\text{Message})^{28\,477} \bmod 77\,837$$

Si vous interceptez le message chiffré `56 846`, trouver la valeur claire correspondante devient cette fois plus pénible et vous devrez avoir recours à des moyens de calcul sophistiqués. Toutefois, ici encore, un bon tableur et quelques procédures Visual Basic en viennent à bout.

Que faire alors ? Pour empêcher de façon définitive la résolution de cette équation, il va falloir utiliser des modules et des exposants de taille suffisamment importante pour défier la puissance des calculateurs du monde entier. Dans l'état actuel des technologies, les nombres utilisés dans les calculs RSA sont composés de plusieurs centaines de chiffres, de l'ordre de trois cents à six cents chiffres, voire plus. Autrement dit, ils reposent sur des modules de 1 024 à 2 048 bits, voire plus.

Fontionnement de RSA

Où sont donc passés l'horloge, l'aiguille et le sens unique de notre exemple précédent ?

Le sens unique, non seulement nous venons de l'évoquer, mais nous venons de montrer que, sous certaines conditions, le sens interdit s'avérait difficile, voire impossible à prendre. En effet, nous avons vu qu'il était relativement aisé de calculer une valeur `C` telle que $C = (Message)^K \pmod n$, mais que la résolution en « message » de cette même équation mettait en échec tous les ordinateurs actuels. C'est la raison pour laquelle la fonction RSA est, tout comme l'aiguille de notre horloge, qualifiée de fonction à sens unique.

Quelle analogie existe-t-il ensuite entre un tour de cadran et la fonction RSA ? Pour comprendre cette analogie, nous allons brièvement parler des aspects pratiques du calcul du nombre $(Message)^K \pmod n$.

Que dire de la valeur d'un nombre de 300 chiffres ? au moins une chose : qu'elle dépasse notre entendement. A fortiori, que dire de la valeur d'un nombre de 300 chiffres élevé à la puissance d'un autre nombre de 300 chiffres ? Non seulement cette valeur nous dépasse, mais elle dépasse aussi largement les capacités de calcul des plus grands ordinateurs au monde. Comment calculer alors ce nombre immense $(Message)^K \pmod n$?

Nous allons pour cela nous appuyer sur les propriétés de ce que l'on notera désormais ZZn, l'ensemble des entiers {0...n-1}. Pour raviver les mauvais souvenirs de la théorie des ensembles, rappelons que l'arithmétique `modulo n`, munie des deux opérateurs + et ×, est dotée d'une structure algébrique d'anneau.

Supposons que nous souhaitions calculer $a^3 \bmod n$. Lorsque nous avons calculé $7^3 \bmod 15$ dans l'exemple précédent, nous avons d'abord cherché la valeur de 7^3, c'est-à-dire 343, et effectué ensuite une réduction `modulo 15` de 343.

Élever un nombre de 300 chiffres au cube oblige à travailler sur 900 chiffres, ce qui est encore envisageable en informatique. Cependant, il ne serait nullement question d'élever ce nombre à la puissance 100, nombre pourtant bien infime dans le contexte d'un calcul RSA...

C'est ici que les propriétés d'anneau de notre espace fini viennent à notre secours :

$$a^3 \bmod n = (((a \times a) \bmod n) \times a) \bmod n$$

En dépit des apparences, nous venons de réaliser un progrès considérable. Imaginons le cheminement du programme informatique effectuant ce calcul :

CONCRÈTEMENT Ordres de grandeur

Avons-nous une idée de la valeur d'un nombre de 300 chiffres ? Imaginons au hasard un nombre « très grand » : un milliard de milliards de milliards. De combien de chiffres un tel nombre est-il constitué ? Un milliard de milliards de milliards ne comporte que 28 chiffres ! Quelle est la masse d'un électron, cette particule infiniment microscopique ? Elle est de l'ordre de 10^{-31} grammes, c'est-à-dire un nombre constitué d'un un placé après 30 zéros derrière la virgule ! De combien d'atomes l'univers est-il constitué ? environ 10^{84}, un nombre de « seulement » 85 chiffres.

Structure algébrique d'anneau

Ce terme exprime de façon générique un ensemble de propriétés qui vont considérablement nous simplifier la vie : l'addition et la multiplication en arithmétique modulaire fonctionnent exactement comme l'addition et la multiplication que nous utilisons tous les jours pour jouer au Monopoly, à la différence toutefois que les résultats sont réduits `modulo n`.

ZZn

On note ZZn l'ensemble des entiers {0...n-1}.

1. L'ordinateur calcule d'abord `a` × `a`. Faisons l'hypothèse que l'entier `a` comporte effectivement plus de trois cents chiffres (1 024 bits). Cette opération a toutes les chances de nous faire bondir en dehors des frontières de l'espace ZZn. En effet, le résultat de l'opération `a` × `a` compte plus de 600 chiffres, ce qui donne nécessairement une valeur bien supérieure au module `n`.
2. L'ordinateur effectue alors une réduction `modulo n` de `a` × `a`, ce qui a pour effet de nous faire revenir instantanément à l'intérieur de ZZn. Le résidu peut prendre n'importe quelle valeur à l'intérieur de l'espace {0...n-1}, il peut très bien être constitué de 1, 178 ou 300 chiffres, peu importe.
3. Ce résidu est maintenant à nouveau multiplié par `a`. Là encore, nous avons de bonnes chances de sortir de l'espace ZZn.
4. Enfin, la valeur obtenue est réduite `modulo n` et nous obtenons ainsi le résidu que nous cherchons.

Vérifions rapidement le fonctionnement de cette technique sur notre exemple précédent 7^3 `mod 15` :

```
7 × 7 = 49
49 mod 15 = 4
4 × 7 = 28
28 mod 15 = 13
```

Donc, lorsque vous calculez $(Message)^K$ `mod n`, même lorsque vous employez des puissances très élevées (l'entier `K` est généralement immense), jamais l'ordinateur ne devra manipuler des nombres de taille supérieure à deux fois celle du module. Dès qu'il y a multiplication, une réduction modulaire intervient immédiatement après.

ANALOGIE **Horloge à sens unique**

Cela ne vous rappelle-t-il pas notre horloge ? Lorsque vous effectuez une multiplication, il se peut que sortiez de l'espace fini ; si c'est le cas, la réduction `modulo n` vous y ramène et vient pointer sur un nouveau résidu de cet espace ; si ce n'est pas le cas, la réduction `modulo n` ne changera pas votre valeur, elle-même résidu de cet espace.
C'est un peu comme si vous lanciez l'aiguille autour du cadran : si elle a suffisamment d'énergie pour dépasser la limite de l'espace fini 23 h 59 min et 59 s, elle entame un nouveau tour et vient pointer sur une autre valeur, un autre « résidu » de ce même espace, grâce à la réduction `modulo 24 h`. Le calcul de $(Message)^K$ `mod n` peut donc s'interpréter comme la succession de très nombreux tours de cadran avec, au passage, un pointage successif sur différents résidus de l'espace. Cette opération est en quelque sorte un beau voyage de résidu en résidu au sein de ZZn, et la valeur chiffrée du message n'est autre que le résidu final obtenu au terme de ce voyage.

Vous devinez maintenant sans peine que la force de lancement de l'aiguille utilisée par Alice est symbolisée par l'exposant `K` de notre équation. Plus il est élevé, plus l'aiguille a des chances de faire plusieurs tours de cadran. Les valeurs de `K` et du module `n` peuvent être connus de tout le monde, car, à l'image de notre horloge à sens unique, aucun ordinateur au monde n'a la puissance suffisante pour retrouver `Message` à partir de sa valeur chiffrée.

Pour retrouver le texte clair à partir du message chiffré, Bernard va procéder comme avec l'horloge : continuer à faire des tours de cadran, c'est-à-dire continuer à élever à la puissance le message chiffré. En d'autres termes, il va continuer à voyager de résidu en résidu à l'intérieur de ZZn, jusqu'à retomber sur un résidu particulier qui, justement, s'avère être le message clair lui même. C'est une des propriétés intéressantes de la fonction RSA, la fameuse brèche secrète évoquée plus haut.

Mise en œuvre concrète

Élaboration du module

Pour mettre en œuvre RSA, la première opération consiste à déterminer une valeur pour le module `n` : il suffit d'engendrer de façon aléatoire deux nombres premiers, `p` et `q` et de les multiplier : `n = p × q`. Nous verrons plus loin pourquoi `p` et `q` doivent être premiers et aléatoires.

Lorsqu'on parle d'une clé RSA de 1 024 bits, cela veut dire que le module `n` est un nombre de 1 024 bits, c'est-à-dire qu'il a été élaboré à partir de deux nombres `p` et `q` de 512 bits.

Élaboration des clés de chiffrement et de déchiffrement

φ(n)

Les calculs de clés de chiffrement et de déchiffrement RSA font intervenir un nombre noté `φ(n)`. Il s'agit du cardinal de l'ensemble restreint des résidus `modulo n`, c'est-à-dire de l'ensemble des résidus premiers par rapport à `n`.

Prenons un exemple pour mieux comprendre. Dans une arithmétique `modulo 8`, l'ensemble des résidus est {0, 1, 2, 3, 4, 5, 6, 7}. Dans cet ensemble, 2, 4 et 6 ne sont manifestement pas premiers avec 8 ; l'ensemble restreint des résidus `modulo 8` est donc {1, 3, 5, 7}, le nombre 0 ne faisant jamais partie de cet ensemble. φ(8) est donc égal à 4.

Plus généralement, dans une arithmétique `modulo p`, si `p` est un nombre premier, `φ(p)` est égal à `p-1` : tous les élément de ZZp, à l'exception de 0, sont premiers avec `p`. Lorsque `n` est le produit de deux nombres premiers `p` et `q`, on démontre aisément que `φ(n)` est égal à `(p-1)(q-1)`.

COMPRENDRE Quantité de nombres premiers de 512 bits

Vous pensez peut-être que le fait de se cantonner à des nombres premiers limite considérablement les possibilités. Avez-vous une idée de la quantité de nombres premiers de 512 bits ? Bruce Schneier, dans son remarquable ouvrage intitulé *Cryptographie Appliquée*, apporte une réponse très éloquente : « Le Père Noël ne tombera jamais à court de nombres premiers pour tous les petits garçons et toutes les petites filles sages. En fait, il y a plus de 10^{151} nombres premiers de 512 bits de long ou moins. Il y a 10^{84} atomes dans l'univers. Si chaque atome de l'univers avait besoin d'un milliard de nombres premiers chaque micro-seconde depuis l'origine des temps jusqu'à maintenant, il faudrait 10^{116} nombre premiers ; il en resterait encore approximativement 10^{151}. »

φ(n)

Il s'agit du cardinal de l'ensemble restreint des résidus modulo n, c'est-à-dire de l'ensemble des résidus premiers par rapport à n.
Lorsque n est le produit de deux nombres premiers p et q, φ(n) = (p-1)(q-1).

EN PRATIQUE Tests de primalité

Le théorème de Fermat est notamment utilisé pour effectuer des tests de primalité sur les grands nombres : on choisit quelques valeurs au nombre x et si les opérations $x^{p-1} \bmod p$ sont égales à 1, cela veut dire que le nombre p est probablement premier.

$\varphi(n)$ est dotée de propriétés intéressantes qui vont nous être très précieuses dans les calculs RSA. Si par exemple n est premier et a n'est pas un multiple de n, alors le petit théorème de Fermat indique que $a^{n-1} \equiv 1 \bmod n$.

Enfin, le petit théorème de Fermat généralisé par Euler montre que $a^{\varphi(n)} \equiv 1 \bmod n$. Dans le cas où $n = p \times q$, cette formule revient à : $a^{(p-1)(q-1)} \equiv 1 \bmod n$.

Exposant de chiffrement

Ceci étant brièvement rappelé, nous pouvons maintenant aborder le choix de l'exposant de chiffrement, noté e par convention. Il s'agit d'un élément de ZZn choisi au hasard, qui doit satisfaire à une seule condition : les nombres e et $\varphi(n)$ dont la valeur est égale à (p-1)(q-1) doivent être premiers entre eux. Cette condition est impérative afin de pouvoir calculer la clé de déchiffrement.

Il existe donc un très grand nombre de possibilités pour e. Une manière de déterminer une valeur de e consiste à engendrer un nombre aléatoire inférieur à n et à tester si ce nombre et (p-1)(q-1) sont premiers entre eux. Cette vérification s'effectue simplement en très peu d'opérations grâce à l'algorithme d'Euclide : leur plus grand commun diviseur (PGCD) est égal à 1. Si ce n'est pas le cas, il suffit d'incrémenter ce nombre aléatoire jusqu'à ce que le PGCD de ce nombre et de $\varphi(n)$ soit égal à 1. La valeur ainsi obtenue est un candidat probable pour e. Vous avez généralement une grande latitude pour choisir e.

Exposant de déchiffrement

Lorsque la valeur de e est fixée, l'exposant de déchiffrement, noté d, est calculé de manière à ce que : $e \times d \equiv 1 \pmod{(p-1)(q-1)}$.

d représente donc l'inverse de e modulo $\varphi(n)$. On démontre que cette équation admet une solution unique si et seulement si e est premier avec $\varphi(n)$. La valeur de d s'obtient très facilement en appliquant le théorème de Bezout.

Clé publique, clé privée

Nous venons donc de calculer deux exposants. Chaque exposant associé au module va devenir une clé : e servira à chiffrer et d à déchiffrer l'information. Le fait de ne pas utiliser la même clé pour chiffrer et déchiffrer est une propriété très intéressante. Lorsque vous souhaitez utiliser la fonction RSA pour garantir la confidentialité d'un secret, vous avez tout le loisir de publier la clé de chiffrement : tout le monde pourra effectuer cette opération de chiffrement. En revanche, la clé de déchiffrement ne doit être connue que du destinataire.

EN RÉSUMÉ **Nombres constituant les clés**

Le couple de nombres `e` et `n` constitue ce que l'on appelle la clé publique.
Le nombre `d` constitue ce que l'on appelle la clé privée.

Chiffrement et déchiffrement RSA

EN COULISSES **Chiffrer et déchiffrer un message**

Pour chiffrer un message, il suffit de l'élever à la puissance de la clé de chiffrement, cette opération étant effectuée `modulo n` :
$c = m^e \bmod n$
Pour déchiffrer le message, il suffit d'élever le message chiffré à la puissance de la clé de déchiffrement, cette opération étant effectuée `modulo n` :
$m = c^d \bmod n$

Pour les courageux, en voici une petite démonstration.

Toutes les opérations sont effectuées `modulo n`. Vous déchiffrez, donc vous élevez le message chiffré à la puissance `d` :

$$c^d = m^{ed}$$

Par définition, `d` est calculé de manière à ce que `e` × `d` soit congru à 1 `modulo (p-1)(q-1)`. Exprimé en français, cela revient à dire que `e` × `d` est un multiple de `(p-1)(q-1)`, plus 1. Sous une forme mathématique, cela devient : `e` × `d` = `k (p-1)(q-1) + 1`. Nous pouvons donc écrire :

$$m^{ed} = m^{k(p-1)(q-1)+1} = m \times m^{k(p-1)(q-1)}$$

C'est ici que le petit théorème de Fermat généralisé par Euler vient à la rescousse : lorsque `p` et `q` sont des nombres premiers, cette expression $m^{k(p-1)(q-1)}$ si compliquée est tout simplement congrue à 1 `modulo n`, ce qui nous permet de déduire :

$$m \times m^{k(p-1)(q-1)} = m \times 1 = m$$

Grâce à notre brèche secrète, nous venons de retrouver notre message clair.

COMPRENDRE **Fiabilité des clés**

Pourquoi utiliser des nombres si grands ? Vous connaissez les valeurs de `n` et de `e`, la clé publique. Supposez que vous réussissiez à factoriser `n`, c'est-à-dire à retrouver ses facteurs premiers, les valeurs de `p` et `q` : vous savez donc calculer `φ(n)`, vous en déduisez immédiatement la valeur de `d`, la clé secrète, et vous avez cassé le chiffre ! La sécurité de RSA est donc basée sur la difficulté à factoriser `n`. Aujourd'hui, les techniques de factorisation les plus performantes parviennent à traiter des nombres d'une taille supérieure à 512 bits, et les développements en théorie des nombres, hélas pour les concepteurs d'algorithmes, rendent la factorisation plus facile. Dans l'état actuel des technologies, l'utilisation d'une clé de 1 024 bits peut préserver la confidentialité de vos secrets pour encore une certaine durée... disons d'ores et déjà qu'il est préférable d'utiliser une clé de 2 048 bits pour sécuriser des informations vraiment sensibles pour les 10 années à venir.

Exemple

Chiffrons le message suivant : « Code : J&B007 ».

En code ASCII avec l'en-tête, on obtient le message suivant :

```
m = 21045644444432673111310031012322582322742382662482482 55
```

Calculons tout d'abord nos clés :

1. Choisissons aléatoirement deux nombres premiers, par exemple :
   `p = 83, q = 191`
2. Calculons le module `n` :
   `n = p × q = 15 853`
3. Calculons `φ(n) = (p-1)(q-1)` :
   `φ(n) = 82 × 190 = 15 580`
4. Choisissons `e` tel qu'il soit premier avec `φ(n)`, par exemple :
   `e = 771`
5. Calculons la clé privée `d` :
   `d = 1 071`

Pour chiffrer le message, il convient d'abord de le décomposer en blocs dont la taille est inférieure à `n = 15 853`. On chiffre ensuite chaque bloc avec la formule m^{771} `mod 15 853` (deuxième colonne du tableau).

m	$c = m^{771} \bmod 15\,853$	$m = c^{1\,071} \bmod 15\,853$
2104	8876	2104
5644	7470	5644
4444	15726	4444

m	$c = m^{771} \bmod 15\,853$	$m = c^{1\,071} \bmod 15\,853$
3	10977	3
2673	2482	2673
11131	3761	11131
003101	14977	003101
2322	9391	2322
5823	5271	5823
2274	6999	2274
2382	6700	2382
6624	12049	6624
8248	5240	8248
255	1823	255

On obtient ainsi le message chiffré suivant :

```
c = 8876 7470 15726 10977 2482 3761 14977 9391 5271 6999 6700 1
2049 5240 1823
```

Pour déchiffrer ce message, on procède au même type de calcul avec la clé privée `d` (dernière colonne du tableau).

Notion de signature électronique

À l'heure de la dématérialisation des procédures administratives et du développement de l'échange par voie électronique, il est capital de disposer d'un moyen d'établir la confiance et, notamment, de garantir l'authenticité d'un document. Ce moyen se nomme signature électronique.

La signature électronique est un élément fondamental sans lequel l'acte officiel sur Internet n'existerait pas. Au même titre que la signature manuscrite, la signature électronique garantit :

- l'**authentification** de l'origine d'un document ;
- l'**intégrité** du document ;
- la **validité** d'informations importantes comme l'horodatage ;
- l'**impossibilité de répudier** un acte.

Le site de la DCSSI (www.ssi.gouv.fr/fr/dcssi) traite de façon très complète la problématique de la signature électronique, et des aspects politiques, juridiques et organisationnels qui s'y rapportent.

Nous nous contenterons ici de présenter les principes d'élaboration d'une signature électronique, l'objectif étant de fournir les bases techni-

ques nécessaires à la compréhension des mécanismes de gestion des certificats, de sécurisation de la messagerie et des transactions électroniques (chapitres 6 à 9).

Sur le plan technique, une signature électronique, tout au moins celle que nous rencontrerons dans les certificats sur Internet, repose sur deux opérations mathématiques :

- l'élaboration d'un condensé cryptologique (aussi appelé empreinte numérique ou code de hachage) ;
- une opération de chiffrement à l'aide d'un algorithme à clés publiques, tel que RSA.

Fonctions de hachage et empreinte numérique

Une fonction de hachage est une fonction mathématique dont nous n'allons pas détailler ici les mécanismes, car ils n'aident pas spécialement à la compréhension du service offert et sortent largement du cadre de ce livre.

En revanche, il est important de retenir ceci : une fonction de hachage a pour objet de convertir une chaîne de caractères d'une longueur arbitraire (texte, exécutable de plusieurs méga-octets, fichier musical...) en une chaîne de taille fixe, qui s'étend le plus souvent sur 128, 160, 256, voire 512 bits.

Cette chaîne de caractères, ou empreinte numérique, possède des propriétés tout à fait remarquables :

- On part du principe qu'à une empreinte numérique donnée correspond un document unique. L'empreinte numérique d'un document est en quelque sorte équivalente à l'empreinte génétique d'un individu (attention toutefois, si elle est communément admise sur Internet, cette affirmation est mathématiquement fausse ; voir l'encadré).
- Une modification à l'intérieur d'un document, même infinitésimale, provoque un changement radical de son empreinte : toute modification devient ainsi immédiatement détectable.
- Les fonctions de hachage sont à sens unique : il est aisé de calculer l'empreinte numérique d'un document, mais il est très difficile de retrouver le document initial à partir de son empreinte. Lorsqu'une empreinte numérique est publiée, il est fait l'hypothèse qu'aucune information relative au contenu du document associé n'est divulguée.

Les principaux algorithmes de hachage utilisés actuellement sont :

- **MD5** (MD pour *Message Digest*) : MD5 crée une empreinte de 128 bits. C'est à la base un très bon algorithme. Cependant, une faille importante a été découverte il y a quelques mois et, bien qu'il ne

Référence Cryptologie

Le lecteur désireux d'approfondir ses connaissances en cryptologie pourra se référer à l'excellent ouvrage de Bruce Schneier :

📖 *Cryptographie Appliquée*, publié aux éditions International Thomson Publishing.

semble pas possible de forger une collision sur une signature donnée, la sécurité de MD5 n'est plus garantie.

- **SHA-1** (*Secure Hash Algorithm*) : SHA-1 crée des empreintes de 160 bits. Il est beaucoup plus fiable que MD5, bien que des attaques cryptologiques récentes tendent à réduire sensiblement sa robustesse.
- **SHA-256/SHA-512** : beaucoup plus sûrs mais moins répandus, ces algorithmes créent respectivement des empreintes de 256 et de 512 bits. SHA-256 est actuellement recommandé par les spécialistes.

ALLER PLUS LOIN **L'attaque des anniversaires**

L'hypothèse selon laquelle une empreinte numérique correspond à un document unique n'est pas tout à fait vraie. Même si l'ensemble formé par les nombres de n bits représente un espace colossal, surtout si n est égal à 512 (revoir à ce sujet la discussion consacrée à RSA), cet espace est fini. Il en résulte fatalement que deux, voire plusieurs messages, pourront inévitablement correspondre à une même empreinte numérique. Ce phénomène s'appelle une « collision ».

Bien entendu, lorsque l'algorithme cryptologique est fiable et, surtout, lorsqu'il est bien utilisé, la probabilité d'occurrence d'une collision est extrêmement faible. Cependant, il existe une attaque qui, sous certaines conditions, élève cette probabilité dans des proportions vertigineuses.

L'attaque classique contre les fonctions de hachage s'appuie sur ce que l'on appelle le « paradoxe des anniversaires » : combien faut-il réunir de personnes dans une assemblée pour que vous ayez une bonne chance de rencontrer une personne née le même jour que vous ? Une année comportant 365 jours (faisons abstraction des années bisextiles), on pourrait s'attendre à un nombre conséquent. Effectivement, on montre mathématiquement que si 253 personnes sont présentes, vous avez plus d'une chance sur deux que l'événement se réalise. Maintenant examinons ceci : combien de personnes doivent être réunies dans une pièce pour que deux d'entre elles aient de bonnes chances d'être nées le même jour ? Cette fois, la réponse est tout à fait différente : seulement 23 ! Dans le premier problème, vous fixez deux conditions : la date d'anniversaire (la vôtre en l'occurrence), et le fait que deux personnes soient nées le même jour. Dans le second problème, une seule condition est posée : deux personnes doivent être nées le même jour, peu importe la date.

L'exemple ci-après illustre bien la fameuse attaque des anniversaires dirigée à l'encontre des fonctions de hachage. Imaginons le protocole suivant :

- Alice souhaite établir un contrat avec Bernard. Elle prépare donc un document que Bernard jugera tout à fait honnête. Alice calcule l'empreinte numérique du document et l'enregistre dans une table.
- En secret, Alice rédige une autre version de ce contrat, cette fois beaucoup plus favorable à elle qu'à Bernard. Pareillement, elle calcule l'empreinte numérique de ce « faux » document et l'enregistre dans une table différente.
- Alice apporte au contrat « honnête » une modification mineure et indécelable (par exemple l'insertion d'un espace à la fin d'une ligne), calcule l'empreinte numérique du document modifié et l'enregistre dans la première table. Elle réitère ce même processus des dizaines de millions de fois, en prenant bien soin d'enregistrer chaque nouvelle empreinte dans la table (notons qu'avec le simple fait d'insérer ou de ne pas insérer un espace en fin de ligne, avec seulement 32 lignes Alice crée 2^{32} versions différentes du même document !).
- Alice procède de la même manière avec le faux contrat et la deuxième table.
- Elle compare ensuite les deux tables à la recherche de deux valeurs de hachage identiques.

Nous nous trouvons exactement dans le cas du deuxième problème « d'anniversaire » : Alice ne s'impose aucune valeur de hachage au départ, elle espère seulement trouver un couple de valeurs égales parmi une infinité de valeurs. S'il existe effectivement une collision, Alice retiendra bien évidemment les versions des documents qui correspondent. Elle pourra alors prétendre que Bernard a signé le faux contrat et, par la suite, l'attaquer en justice.

Plus généralement, si l'empeinte numérique comporte n bits, on démontre mathématiquement qu'en calculant $2^{n/2}$ empreintes numériques, la recherche de collisions a plus d'une chance sur deux d'aboutir. Pour fixer les idées, MD5 sort une empreinte sur 128 bits. En théorie, il faudrait donc pouvoir calculer et stocker 2^{64} empreintes numériques, ce qui nécessiterait environ un million de fois 300 To d'espace mémoire, le tout pour avoir une chance sur deux de réussir ! Lancer une recherche exhaustive implique donc des moyens importants et une certaine motivation. Toutefois, n'oublions pas que les cryptanalystes mettent constamment au point des techniques plus subtiles et plus rapides que la traditionnelle « force brute ». Pour prendre un exemple, une attaque actuelle dirigée contre SHA-1 demande « seulement » 2^{63} opérations, au lieu des 2^{80} théoriques.

Notez qu'un tel stratagème peut fonctionner uniquement si le code de hachage du document initial n'est pas fixé à l'avance. Pour éviter les écueils :

- Établissez vous-même cette valeur : créez vous-même la version électronique du document qui vous engage ou, au besoin, imposez une modification mineure sur la version finalisée du document qu'on vous soumet.
- Veillez à ce que l'empreinte numérique soit élaborée avec un bon algorithme de hachage (ex. SHA-256). De tels algorithmes offrent des propriétés de résistance à la collision (il est difficile de trouver deux messages correspondant à la même empreinte numérique).

À titre indicatif, on rencontre dans la littérature de nombreuses dénominations pour désigner la valeur produite par un algorithme de hachage : empreinte numérique, condensé cryptologique, *checksum* cryptologique, résumé, code de hachage, valeur de hachage, *digest*, etc. Toutes ces dénominations veulent sensiblement dire la même chose.

Exemples d'utilisation

Examinons de plus près l'utilisation des empreintes numériques en se basant sur des exemples concrets.

Calculer une empreinte numérique est extrêmement simple. Commencez d'abord par créer un petit fichier texte (vous pouvez notamment vous servir du Bloc-notes) :

```
« C'est un plaisir de faire sauter l'ingénieur avec son propre
pétard.
  HAMLET »
```

Sauvegardez ce fichier sous un nom quelconque, par exemple `essaiEmpreinte.txt` et calculez son condensé cryptologique SHA-1. Vous réaliserez très facilement cette opération à l'aide du petit utilitaire `sha1sum.exe`, téléchargeable gratuitement sur Internet. Vous obtenez la valeur suivante :

```
BFCD:5B5B:E4E2:FC43:D56A:6B56:7031:A316:DBE5:5991
```

Cette notion de « résumé », d'« empreinte » ou de « condensé » prend ici tout son sens : une telle valeur ne vous dit absolument rien à propos du contenu du fichier, mais elle vous indique en un clin d'œil si celui-ci a été modifié par rapport à une version précédente. Essayez de changer très légèrement le contenu du fichier texte créé il y a quelques instants, en supprimant par exemple le point à la fin de la phrase. Calculez à nouveau l'empreinte cryptologique du fichier :

```
032B:B5A2:16C9:15DC:CF07:9E2A:11A4:27A0:48ED:057F
```

Constatez l'énorme différence entre les deux valeurs obtenues ! Bien sûr, l'œil perspicace aurait peut-être détecté l'absence du point dans le fichier modifié. Imaginez toutefois l'ajout d'une phrase sibylline à l'intérieur d'un contrat de trois cents pages, que vous avez déjà relu et dont vous vous apprêtez à signer une version modifiée !

Dans le cadre de l'échange de documents électroniques sur Internet, une empreinte numérique revêt donc de multiples intérêts. Supposons par

À RETENIR Empreinte de longueur fixe

De même, amusez-vous à calculer l'empreinte SHA-1 d'un fichier plus volumineux, comme une vidéo. Vous constaterez que vous obtenez toujours une valeur de 160 bits.

exemple que vous souhaitiez envoyer un message chiffré à un correspondant ; vous lui demandez sa clé publique, il vous l'envoie par courriel, ou, plus simplement, vous la récupérez à partir d'un annuaire. Si l'on s'appuie sur l'implémentation artisanale de RSA évoquée précédemment, supposons que la valeur de cette clé publique soit : `e=771`, `n=15853`. Dans ce cas précis, il est facile de vérifier via une autre source (le téléphone, un autre annuaire, le site web de votre correspondant...) que ces valeurs constituent bien la clé publique de votre interlocuteur.

Qu'en est-il dans la réalité, lorsque ces nombres atteignent des valeurs astronomiques ? Voici l'exemple d'une « vraie » clé publique RSA :

```
« 30818902818100a32d946ea519646f84109e62548bfa7050c5ab378fbfd4a
c099815c1edb2e4530f1de18033ea79c4f371f0784f248286684220b240a9fc
2fc17879d28bbe916518292db70b62c5e0aaea56fa32a534ec5162706b2b63d
79d222167c549e0546a0194384c685e566191690ff7baa1f867d5983c7b78b5
73dcee4b51a29f72c0070203010001 »
```

Allez-vous passer du temps à téléphoner à votre correspondant pour vérifier bit à bit que cette valeur est exacte ? Évidemment non ! Le plus simple consiste alors pour le correspondant à publier dans un annuaire l'empreinte numérique de sa clé :

```
Empreinte MD5:
A031:51E1:D1CD:DE6D:3C06:5185:C6FA:F80A
Empreinte SHA-1:
FE50:98DD:C8EC:2E6B:EE74:77CF:DDAC:0196:FD3B:D8DD
```

De votre côté, vous téléchargez cette clé, puis vous recalculez son empreinte numérique à l'aide de `md5sum.exe` ou de `sha1sum.exe` (ce dernier est préférable) ; vous effectuez ensuite la comparaison. En quelques secondes, vous saurez si vous avez téléchargé la bonne clé.

De même, vous téléchargez un logiciel. Comment savoir si vous rapatriez le bon logiciel, ou une version dans laquelle un pirate a inséré un code suspect ? Vous n'allez certainement pas inspecter le code avant de l'utiliser. Un moyen simple consiste encore à s'appuyer sur les empreintes numériques. Aujourd'hui, tous les éditeurs publient sur leurs sites au minimum les condensés MD5 et SHA-1 de leurs logiciels ; il vous appartient de faire le nécessaire pour vérifier si la version chargée sur votre poste correspond bien à celle de l'éditeur.

Certes, de telles informations ne sont pas passionnantes à manipuler, mais elles représentent un moyen simple et efficace pour éviter de télécharger bon nombre d'objets corrompus !

Bien entendu, le modèle que nous venons de décrire est incomplet : dans le cas où vous rapatriez un objet émis par une source extérieure (un éditeur, un client, un site web, etc.), comment garantir que l'objet, associé à

En coulisses Aucun secret dans les fonctions de hachage

Aucun secret n'est mis en œuvre au cours de l'opération de hachage. Les algorithmes de hachage sont publics, aucune clé n'est requise. Les codes de hachage sont publics, tout le monde peut calculer l'empreinte numérique d'un fichier, tout le monde peut vérifier une empreinte et détecter une éventuelle compromission.

une vraie empreinte numérique, n'est pas en réalité un faux émis par un pirate se faisant passer pour l'entité émettrice (nous avons fait jusqu'ici l'hypothèse que l'empreinte numérique avait été calculée par l'émetteur de cet objet) ? La réponse est simple : il faut faire appel à la signature électronique.

Signature électronique

Pour simplifier, raisonnons sur un exemple concret. Supposons qu'Alice lance un ordre d'achat sur Internet (cet ordre d'achat est matérialisé ici par un petit fichier texte édité à l'aide du Bloc-notes) :

```
« Achetez les 6 Vermeer à n'importe quel prix »
```

Toutefois, avant d'adresser ce message à Bernard, la personne qui va réaliser l'achat propremement dit, Alice veut être sûre que cet ordre sera bien compris. Elle effectue alors quelques opérations préliminaires :

1. Elle calcule l'empeinte numérique SHA-1 de ce fichier.
2. Elle chiffre cette valeur *avec sa clé privée*.
3. Elle prépare ensuite un message constitué du fichier texte initial, de la valeur chiffrée qu'elle vient de calculer et de sa clé publique :

```
« Achetez les 6 Vermeer à n'importe quel prix »
« 1949 38750 41029 11039 26928 22558 45045 25432 46635 15171
43797 34568 30566 42513 33950 8337 45045 30182 18020 40340 8822
44994 40340 30705 19988 33950 27196 33368 18992 45045 39714
34958 21506 »
« Clé publique Alice: e = 15709, n = 48689 ».
```

4. Elle envoie le tout à Bernard.

Dès à présent, notons que seule Alice a pu calculer cette valeur chiffrée. Personne d'autre n'a été en mesure de le faire car elle seule est en possession de sa clé privée.

Bernard reçoit donc le message et déchiffre la succession de nombres à l'aide de RSA et de la clé publique d'Alice : $1\,949^{15\,709} \bmod 48\,689$, $38\,750^{15\,709} \bmod 48\,689$, etc. Bernard finit par retrouver le texte clair qu'Alice avait chiffré (le lecteur courageux saura aussi retrouver ce message) :

```
« F966:D09E:AB27:A868:447E:BACB:1258:EBE4:CD1D:C701 »
```

Il s'agit de toute évidence d'un code de hachage SHA-1, vraisemblablement l'empreinte numérique du texte du message. À l'aide de

`sha1sum.exe`, Bernard recalcule donc l'empreinte numérique du fichier texte reçu et trouve la valeur suivante :

> « `F966:D09E:AB27:A868:447E:BACB:1258:EBE4:CD1D:C701` »

La comparaison est évidente : les deux valeurs sont identiques.

Nous pouvons donc déduire de ce résultat deux conclusions :

- Le fichier texte émis par Alice n'a subi aucune modification au cours de son transfert sur le réseau, il est intègre. Si un pirate avait modifié le contenu du message, par exemple « `Achetez les 2 Vermeer à n'importe quel prix` », Bernard l'aurait détecté en recalculant l'empreinte SHA-1 de ce message.
- Bernard a été capable de déchiffrer une information correcte avec la clé publique d'Alice. Cela prouve qu'Alice a obligatoirement chiffré l'empreinte, et personne d'autre : Alice est donc authentifiée avec certitude en tant qu'émetteur de ce message.

Cette valeur chiffrée est ce que l'on appelle une *signature électronique*, elle garantit :

- **l'intégrité** du document signé ;
- **l'authentification** de l'émetteur du document ;
- **la non répudiation** de l'acte (Alice ne pourra plus nier avoir émis ce message).

Signature électronique

Une signature électronique n'est autre que le chiffrement de l'empreinte numérique d'un document avec la clé privée de l'émetteur. Seul l'émetteur peut réaliser cette opération, en revanche tout le monde peut vérifier cette signature, en se servant de la clé publique de l'émetteur.

Récapitulatif des principaux risques encourus

B

Cette annexe présente un bilan des risques que nous avons identifiés tout au long de l'ouvrage. Elle ne prétend pas à l'exhaustivité. Son principal objectif consiste à :

- donner un aperçu rapide des principales menaces qui pèsent directement sur un poste de travail ou un réseau informatique de taille modeste (pour plus de détails, nous vous renverrons aux chapitres concernés) ;
- identifier les conséquences potentielles sur le système si la menace se réalise ;
- proposer des mesures simples qui permettent de réduire significativement le risque.

Il convient de remarquer que cette annexe est adaptée à la problématique du poste de travail de l'utilisateur individuel et du petit réseau domestique ou d'entreprise. De nombreux aspects concernant les grands systèmes informatiques ne sont pas abordés ici. Si le lecteur souhaite se faire une vision plus complète, il peut se référer à la méthode EBIOS, disponible gratuitement à partir du site de la DCSSI.

Toutefois, le simple suivi des recommandations listées ci-après évitera bon nombre de catastrophes.

Erreurs d'utilisation

Voir le chapitre 1.

Comportement à risque	Conséquences	Mesures
L'utilisateur divulgue son mot de passe à un tiers.	Un inconnu peut alors usurper l'identité de l'utilisateur et s'introduire au cœur du système. * Divulgation, altération et/ou destruction d'informations sensibles (par exemple base des clients). * Ouverture possible de trappes cachées pour que l'attaquant puisse revenir ultérieurement.	Ne jamais donner son mot de passe à quelqu'un, même s'il s'agit en apparence d'un officiel (représentant de la banque, administrateur informatique...).
L'utilisateur choisit un mot de passe faible : « 12345678 », « azertyui », « password », « nathalie »...	Un pirate peut très facilement trouver la valeur du mot de passe et se connecter au système.	Dans tous les cas, choisir un mot de passe robuste (ex. « Fz5#Bs15 »).
Arrêt brutal du système d'exploitation ou d'une application. Interruption brutale d'un processus.	Altération de fichiers système : * Le système entre dans un état incohérent. * Certains fichiers sont corrompus. * Le système d'exploitation est détérioré ou ne démarre plus.	Ne jamais interrompre un processus en cours d'exécution. Ne jamais éteindre brutalement son poste. Quitter les applications proprement.
Suppression involontaire de fichiers situés sur un répertoire réseau.	Suppression définitive : les fichiers ne sont pas envoyés dans la corbeille. Ils ne peuvent être restaurés.	Toujours conserver une copie des données importantes en local. Sauvegarder les lecteurs réseau. Maîtriser les procédures de restauration.
Arrachage intempestif d'une clé USB au cours de l'édition d'un fichier stocké sur cette clé.	Fichier corrompu. Au pire, disparition du fichier.	Ne jamais travailler sur une clé USB.
L'utilisateur ne pense jamais à faire le ménage sur sa machine.	Les fichiers grossissent, finissent par « planter » l'application qui les gère et deviennent inaccessibles (c'est le cas notamment des messageries). Trop d'applications installées sur un poste peuvent entrer en conflit.	Penser à faire le ménage (au moins une fois l'an). Archiver les données anciennes sur supports externes (CD-Rom non réinscriptibles). Archiver la messagerie. Stocker les archives en lieu sûr. Désinstaller les applications dont on ne se sert plus.
Fichiers dotés de noms « à rallonge ».	Ils sont mal gérés par Windows : * mal copiés * pas toujours sauvegardés.	Toujours affecter un nom raisonnable à un fichier (moins de 30 caractères).
Le système affiche régulièrement un message d'erreur et l'utilisateur ne réagit pas.	Certains fichiers système sont peut-être corrompus, exposant l'utilisateur à une interruption de services et/ou à la perte d'informations. Une attaque est possible (un message d'erreur persistant est le symptôme de la présence possible d'un cheval de Troie).	Ne jamais traiter un message d'erreur par le mépris. Il faut résoudre le problème : * Contacter un administrateur. À défaut, se renseigner auprès d'une personne compétente de son entourage. * Faire appel au service d'assistance.
« Plantage » du système d'exploitation ou d'une application en cours d'utilisation.	Perte des données saisies depuis le dernier enregistrement.	Activer les fonctions d'enregistrement automatique.

Comportement à risque	Conséquences	Mesures
Incident logiciel : découverte en fin de journée que la fonction d'enregistrement ne fonctionne pas.	Perte d'une journée de travail.	Enregistrer le document dès son ouverture, avant de commencer l'édition. Effectuer des enregistrements fréquents.
Incidents réseau survenant lors de transferts massifs de données entre plusieurs machines (serveurs/serveurs, serveurs/clients).	Certains fichiers ne sont pas copiés. D'autres fichiers sont transférés mais restent illisibles. Interruption prématurée du processus de transfert.	Le câblage du réseau doit respecter les normes et les caractéristiques des constructeurs (câbles de bonne qualité, architecture, environnement...). Éviter les perturbations électromagnétiques (chemins de câbles près des néons...) Vérifier systématiquement le déroulement des transferts (comparaison nombre/volume fichiers et répertoires entre source et destination). En cas de rénovation du parc, conserver les anciens serveurs, au moins pendant une période transitoire.
Forcer une application à exécuter des tâches « tordues » augmente le risque de la faire « planter ».	Les fichiers en cours d'édition peuvent être endommagés ou perdus. L'application entre dans un état incontrôlé et peut « planter « le système.	Ne jamais forcer une application à exécuter des tâches pour lesquelles elle n'est pas prévue.
Perte d'un périphérique de stockage amovible (CD-Rom, clé USB, balladeur MP3...).	Perte de données précieuses. Divulgation externe de données confidentielles.	Plusieurs copies de sauvegardes des données stockées sur la clé USB (CD-Rom, disque réseau, disque dur externe, bande...). Chiffrement des fichiers sensibles stockés sur le support (ex. GnuPG).

Sauvegardes

Voir le chapitre 1.

Comportements à risque	Conséquences	Mesures
L'utilisateur ne sauvegarde pas ses données.	Une donnée non sauvegardée finit par disparaître tôt ou tard.	S'assurer que des procédures de sauvegarde ont été définies et sont claires pour les acteurs concernés. Toujours disposer de plusieurs sauvegardes : * bande magnétique (plutôt entreprises) ; * CD-Rom réinscriptible (données récentes) ou non réinscriptible (archives); * disque réseau et disque local ; * disque externe ; * clés USB (uniquement les sauvegardes temporaires avant la sauvegarde sur disque).

Comportements à risque	Conséquences	Mesures
L'utilisateur ne sait pas toujours où sont rangées certaines données importantes : * la messagerie ; * les données gérées par les applications (photos, morceaux de musique...) ; * le bureau ; * les favoris.	Ces données.ne sont pas toujours correctement sauvegardées et finissent par se perdre.	Bien penser la stratégie de sauvegarde. Apprendre où sont rangées ces données précieuses sur le disque. Savoir éventuellement mettre en œuvre les fonctions de sauvegarde proposées par les applications. Si utilisation d'un système de sauvegarde spécifique, définir une politique de sauvegarde prenant en compte les répertoires hébergeant ces données.
Perte/oubli des paramètres vitaux ouvrant l'accès à l'espace de travail (ces paramètres sont souvent mémorisés par le système) : * mots de passe du compte sur la machine ; * paramètres système ; * mots de passe d'accès aux ressources du réseau ; * paramètres d'accès à la messagerie ; * hébergeur...	L'espace de travail de l'utilisateur est inaccessible tant qu'il n'a pas retrouvé ces informations. Perte définitive de l'accès si l'utilisateur travaille sur le seul compte de la machine (compte administrateur) et que le mot de passe n'a été noté nulle part.	Conserver soigneusement dans un lieu sûr les éléments utiles et toutes les données importantes sans lesquels il n'est plus possible de travailler normalement.
L'obésité du système est un facteur de « plantage » et de perte d'information.	Perte de temps. Perte de données vitales.	Définir et mettre en œuvre une procédure d'archivage adaptée. Prévoir des mesures de conservation des archives adaptées aux délais de rétention.

Restauration

Voir le chapitre 1.

Comportement à risque	Conséquences	Mesures
Ignorance du mode opératoire des procédures de restauration.	En cas de perte d'information, les sauvegardes ne sont d'aucun secours.	Définir clairement les procédures de restauration. Se familiariser avec les procédures de restauration. Apprendre à restaurer complètement des données (par exemple une messagerie).
Les données sauvegardées sont inexploitables.	En cas de perte d'information, celles-ci seront irrécupérables.	Toujours vérifier et valider la procédure de sauvegarde.

Pannes

Voir le chapitre 1.

Problème	Conséquences	Mesures
« Plantage » inopiné de la machine en cours de travail. Panne secteur ou extinction intempestive de la machine pour quelque raison que ce soit.	Perte des données saisies depuis le dernier enregistrement. Fichiers en cours d'édition/fichiers système endommagés.	Réseau d'entreprise : alimentation de secours obligatoire sur les serveurs (onduleurs).
Le système ne démarre plus.	Indisponibilité momentanée ou définitive du système et des données qu'il renferme.	Savoir identifier l'origine d'une panne. Se familiariser avec les procédures de récupération du système. Se préparer à réparer un système endommagé : * Savoir activer la dernière bonne configuration connue. * Se familiariser avec le mode sans échec. * Connaître l'existence des plans de récupération offerts par les systèmes d'exploitation et savoir les exploiter.

Configuration du poste de travail

Voir le chapitre 2.

Attaque risquée	Conséquences	Mesures
Accès non contrôlé à la machine de l'utilisateur (par exemple machine libre service ou sans mot de passe).	Accès illicites : * aux données contenues sur la machine ; * au réseau et aux serveurs de l'infrastructure (intranet). Atteinte possible à la confidentialité, l'intégrité et la disponibilité des données et des services. Modification illicite de la configuration du système (par exemple ouverture de trappes cachées pour accroître les possibilités d'accès non autorisés).	Créer des comptes d'utilisateurs et leur affecter des mots de passe robustes. Activer l'écran de veille et protéger la sortie de veille avec un mot de passe robuste. En entreprise : * proscrire toute forme de naïveté ; l'espionnage économique peut venir de l'intérieur (par exemple stagiaire, consultant extérieur, sous-traitant) ; * allouer des droits d'accès aux utilisateurs ; * supprimer les comptes d'utilisateurs ayant quitté la société ; * activer la journalisation des événements ; * auditer l'activité des systèmes et du réseau.

Attaque risquée	Conséquences	Mesures
Connexion non autorisée sur une machine en usurpant l'identité d'un utilisateur reconnu.	Accès illicite à l'espace de travail de l'utilisateur et aux ressouces du réseau. Divulgation externe d'informations sensibles. Altération, modification frauduleuse d'informations utilisateur et système. Atteintes possibles à la disponibilité des données, des services et du système.	Définir des mots de passe robustes : * protéger l'accès aux comptes d'utilisateurs ; * protéger l'accès aux ressources partagées et au réseau. Saisir le mot de passe à l'abri des regards indiscrets. Définir une procédure de changement régulier des mots de passe. En entreprise, auditer l'activité des systèmes et du réseau.
Volumes non formatés NTFS.	De nombreuses fonctions de sécurité ne peuvent être activées, dont : * fonctions plus élaborées d'affectation de droits et de contrôle d'accès aux données ; * fonctions natives de chiffrement EFS.	Penser à formater les volumes en NTFS, si cette opération n'a pas déjà été effectuée en usine.
Exploitation frauduleuse des partages ouverts sur un ordinateur.	Recenser les ressources actives, les réseaux, obtenir une liste valide d'utilisateurs autorisés. Accéder sans autorisation à des ressources partagées. Divulgation externe, modification et/ou destruction de données accessibles sur les partages. Pénétrer une organisation en profondeur.	Définir des mots de passe robustes pour protéger l'accès aux ressources partagées. Inspecter régulièrement les partages actifs et fermer ceux qui ne sont pas nécessaires. Réduire au strict minimum les permissions associées à un partage. Désactiver impérativement les services SMB sur les interfaces avec les réseaux non sûrs (Internet).
Manipulation frauduleuse du registre par un exécutable malveillant.	Contamination de la machine par un virus, un cheval de Troie ou un logiciel espion. Ouverture de canaux cachés. Prise de contrôle de l'ordinateur à distance. Atteinte au bon fonctionnement de l'ordinateur.	Vérifier, maîtriser les permissions associées aux objets du Registre. Ne jamais travailler sous un compte doté des droits administrateur. Vigilance : veiller à installer sur son poste des exécutables de provenance fiable. Un pare-feu logiciel sachant détecter les applications qui tentent de modifier le registre. Un antivirus à jour.
Éplucher l'historique des actions réalisées par un utilisateur sur son poste.	Espionner l'activité de l'utilisateur	Vider les historiques et désactiver les mouchards.
Exploitation malveillante d'une vulnérabilité logicielle.	Système d'exploitation soumis à des requêtes mal formées : * exécution/installation à distance de codes arbitraires ; * prise de contrôle à distance de l'ordinateur.	Procéder à la mise à jour permanente du système d'exploitation et des logiciels installés sur le poste. Un antivirus/antispyware à jour. Réseau d'infrastructure : pare-feu matériel doté de fonctions d'analyse des contenus véhiculés par les protocoles Internet (HTTP, SMTP, DNS...).

Attaque risquée	Conséquences	Mesures
Exploitation malveillante de protocoles peu sécurisés, ou pas sécurisés du tout.	Interception d'informations sensibles (mots de passe) transitant via des flux non chiffrés. Accès non autorisé au poste et à l'infrastructure informatique. Intrusion du réseau.	Désactiver tous les services réputés dangereux ou inutilisés (SNMP, Telnet, TFTP, ICMP...). Opter pour l'utilisation de protocoles sécurisés (par exemple SSH au lieu de Telnet).
Vol de l'ordinateur (menace élevée dans le cas des postes nomades)	Atteinte à la confidentialité de données sensibles. Risque de chantage, d'extorsion de fonds à l'encontre de l'entreprise. Perte de données précieuses.	Ne pas attirer l'attention, transporter l'ordinateur dans une serviette banalisée. Chiffrer les fichiers et/ou les dossiers sensibles : * système natif Windows (EFS) pour un chiffrement de premier niveau ; * utilisation de GnuPG (sécurité forte si gestion rigoureuse) ; * pour les fichiers très sensibles, envisager un produit de sécurité spécialisé avec chiffrement du disque à la volée. Authentification forte de l'utilisateur au démarrage de la machine, avec dispositif matériel externe (cartes à puce, clé USB).

Virus, vers, Troyens et logiciels espions

Voir les chapitres 3 et 4.

Attaque risquée	Conséquences	Mesures
Installation non contrôlée d'un code malveillant au cœur de l'ordinateur (message électronique infecté, exécutable de provenance douteuse...). Lancement automatique de ce code malveillant à chaque démarrage de la machine (par exemple suite à une modification non autorisée du registre).	Le virus est résident. Son pouvoir de nuisance est multiple : * interception des appels système ; * altération, destruction partielle ou totale du système de fichiers ; * transformer la machine en un relais pour lancer des attaques ultérieures (par exemple DDoS-Distributed Deny of Service).	Adopter avant tout un comportement prudent. Ne jamais travailler sous le compte Administrateur. S'assurer que les utilisateurs de la machine disposent d'un accès limité au registre. Pare-feu logiciel capable de détecter les modifications du registre. Un antivirus/antispyware à jour.
Le code malveillant active le téléchargement et l'installation de codes arbitraires à travers des canaux cachés.	Machine sous le contrôle d'une entité distante.	Pare-feu logiciel capable de : * détecter la modification d'exécutables (applications, commandes système) ; * signaler les processus qui tentent de réaliser des actions suspectes (ouvertures de connexions Internet, manipulation d'applications). Un antivirus/antispyware à jour.

Attaque risquée	Conséquences	Mesures
Modification par le code malveillant de certains exécutables présents sur la machine.	Pervertir le fonctionnement de l'ordinateur, servir les intérêts du virus (par exemple désactiver l'antivirus ou son système de mise à jour, intercepter les appels système, modifier les fonctions d'affichage pour camoufler sa présence).	Pare-feu logiciel capable de détecter la modification d'exécutables (applications, commandes système). Un antivirus/antispyware à jour.
Ouverture illicite de ports sur la machine pour recevoir et traiter des commandes lancées par l'attaquant à distance.	Prise de contrôle partiel ou total de la machine à distance. Divulgation externe, altération, destruction d'informations sensibles. Transformation du poste de travail en une base avancée pour lancer une attaque au cœur du réseau (infiltration, saturation des ressources).	Sauvegarde régulière des données. Pare-feu logiciel apte à détecter les comportements suspects des processus. Vigilance de l'utilisateur : inspection régulière de la configuration du pare-feu. Un antivirus/antispyware à jour.
Envoi en masse de messages à tous les utilisateurs répertoriés dans le carnet d'adresses.	Propagation du ver. Contamination possible d'autres utilisateurs. Pollution de la messagerie.	Un antivirus à jour, configuré pour détecter les tentatives d'envoi massif de courriers électroniques.
Observation du comportement de l'utilisateur. Envoi de rapports détaillés à des inconnus. Divulgation des informations sensibles à l'extérieur.	Espionnage.	Toutes les mesures citées précédemment. Un antispyware à jour.

Installation hasardeuse de logiciels « attractifs »

Voir les chapitres 3 et 4.

Attaque risquée	Conséquences	Mesures
Infection de la machine par de multiples chevaux de Troie.	Le PC devient partiellement ou totalement sous contrôle d'une entité extérieure. Le réseau local (domestique ou d'entreprise) est menacé. Divulgation à l'extérieur d'informations sensibles.	Ne jamais installer de logiciels issus d'une source non digne de confiance. Un antivirus/antispyware à jour.

Attaques réseau

Voir les chapitres 5 et 6.

Attaque risquée	Conséquences	Mesures
Un protocole de communication, quel qu'il soit, peut être détourné pour véhiculer un flux malveillant.	Attaques en tous genres du poste utilisateur. Attaques en tous genres du réseau informatique (domestique ou entreprise).	Fermer systématiquement sur la machine tous les services inutiles. Désactiver systématiquement les services dangereux sur toutes les interfaces avec les réseaux non sûrs (NetBIOS, SNMP, ICMP, Telnet, TFTP). Pare-feu indispensable dès que le poste ou le réseau est relié à un réseau non sûr : * pare-feu logiciel sur chaque poste (contrôle des flux entrants et sortants, de l'intégrité et du comportement des applications) ; * pare-feu matériel en entrée de site doté de fonctions d'analyse de contenus. Un antivirus/antispyware à jour.
Présence d'un accès à distance aux systèmes et réseaux locaux (ressources partagées, accès non protégés, télé-maintenance, externalisation des sauvegardes).	Risque accu de pénétration extérieure du réseau et des systèmes informatiques. Vol, modification et/ou destruction de données. Saturation des ressources système et réseau (déni de service).	Désactiver tout lien « remote » permanent. Tout échange entre un poste extérieur (nomade, sauvegarde externe, télé-maintenance) doit impérativement : * emprunter un canal établi à la demande ; * passer par un tunnel chiffré (lien de type VPN) ; * s'effectuer au sein d'une communauté d'utilisateurs clairement identifiés ; * débuter par une authentification forte de l'utilisateur distant, basée sur des moyens cryptologiques implémentés dans un dispositif matériel (carte à puce, clé USB).
Poste nomade plus exposé en dehors du périmètre de l'entreprise.		Être sensibilisé aux attaques informatiques et aux comportements dangereux qu'il faut éviter. Pare-feu logiciel indispensable (contrôle étroit des flux échangés et des applications demandant l'accès à Internet). Un antivirus/antispyware à jour.

Menaces liées aux codes mobiles

Voir le chapitre 7.

Attaque risquée	Conséquences	Mesures
Installation non contrôlée de codes mobiles malveillants sur le poste (par exemple via la consultation de pages HTML à partir de sites peu dignes de confiance).	Rapatriement/installation non contrôlée de codes mobiles sur le poste (ActiveX, applets Java, Javascript), en provenance d'horizons multiples sur Internet. Ouverture de trappes cachées. Accès illicite au système de fichiers (divulgation externe, altération et/ou destruction de données). Accroissement de la vulnérabilité du poste face aux attaques. À terme, contamination assurée du poste par une multitude de codes furtifs, Troyens ou logiciels espions.	Vigilance de l'utilisateur. Configurer le navigateur pour désactiver systématiquement tous les codes mobiles, Java et JavaScript, à l'exception des sites identifiés nominativement par l'utilisateur. Sur ces sites, autoriser uniquement les composants qui représentent potentiellement le moins de risques pour l'ordinateur : * composants authentifiés avec « Authenticode ». * composants reconnus « Sûrs pour l'écriture de scripts ». Refuser tous les autres.
Le code mobile établit et entretient des communications illicites avec des sites dangereux via les protocoles autorisés du pare-feu. Il établit des de tunnels chiffrés (non contrôlables par un pare-feu) entre le poste utilisateur situé au cœur du réseau et un site distant arbitraire.	Le pare-feu devient inopérant face aux protocoles de haut niveau encapsulés à l'intérieur de protocoles standards (HTTP, SMTP, DNS). Le pare-feu ne sait pas filtrer les protocoles chiffrés. Intrusion sur poste à travers le pare-feu. Toutes les opérations sont envisageables : * rapatriement d'autres codes malveillants ; * accès au système de fichiers (divulgation externe, altération, destruction de données) ; * contrôle à distance des actions de l'utilisateur...	Un pare-feu logiciel sachant détecter les comportements suspects des applications et les tentaives d'ouvertures de ports. Inspection régulière de la configuration du pare-feu (vérification des communications sortantes autorisés). Interdire a priori toutes les communications entrantes, en particulier la messagerie instantanée. Un antivirus/antispyware à jour.
Exécution en local de commandes lancées à distance par un site pirate (protocole spécifique transitant via les flux non filtrés par le pare-feu).	Exécution à la demande d'opérations voulues par le pirate : * divulgation externe de fichiers confidentiels ; * saturation du réseau local (domestique ou d'entreprise) ; * téléchargement à distance d'autres exécutables...	Vigilance de l'utilisateur : * éviter à tout prix de se retrouver dans cette situation (appliquer les mesures précédentes) ; * inspection de la configuration du pare-feu ; * suivi des processus ; * exploitation des journaux du pare-feu. Pare-feu logiciel capable de détecter et de contrôler : * l'installation de nouvelles applications ; * les modifications du registre ; * les actions suspectes.

Menaces directement liées aux problèmes de la navigation sur le Web

Voir le chapitre 7.

Attaque risquée ou comportement dangereux	Conséquences	Mesures
Consultation de pages HTML dynamiques.	Rapatriement possibles de codes mobiles en provenace d'horizons très différents.	Voir section « Menaces liées aux codes mobiles ».
Téléchargement/installation/utilisation par l'internaute d'exécutables et applications d'origines les plus diverses (utilitaires, jeux).	L'ordinateur devient un cheval de Troie au cœur du réseau informatique (domestique ou entreprise). Infiltration du réseau informatique. Attaque par saturation des ressources (Déni de service).	Vigilance accrue de l'utilisateur : * sensibilisation de l'utilisateur aux risques pesant sur le système d'information, aux méthodes d'attaque, aux problèmes de sécurité potentiels ; * définition et suivi de la charte pour une utilisation sûre de l'outil informatique. Pare-feu logiciel et/ou matériel en entrée de site : * règles de filtrage adaptées ; * détection des tentatives de connexion suspectes vers Internet. Suivi de l'activité du réseau (volume des flux, origine).
Attaque par langage de script d'un site distant (Cross Site Scripting) : visitant un site de confiance, l'utilisateur est redirigé à son insu vers un site pirate au moment de livrer des informations sensibles.	Divulgation d'informations sensibles.	Vigilance de l'utilisateur : toujours vérifier l'authenticité d'un site avant de livrer des information sensibles.
Exploitation malveillante des vulnérabilités du navigateur (débordements de tampons).	Prise à distance du contrôle de l'ordinateur. Installation à distance de codes arbitraires sur le poste de l'utilisateur.	Maintenir systématiquement à jour les système d'exploitation et applications. Un antivirus/antispyware à jour.
Phishing : stratagème bien huilé conçu pour piéger l'utilisateur trop crédule.	L'utilisateur trop confiant dévoile ses codes secrets à un tiers.	Sensibilisation de l'utilisateur aux problèmes classiques de « social engineering » (baratinage). Ne jamais répondre à un message où l'on demande à l'utilisateur d'entrer ses codes secrets (même si le message semble provenir d'une source de confiance). C'est un faux dans tous les cas.
Détournement des protocoles mal gérés par les pare-feux.	Infiltration du réseau local. Injection à distance de codes malveillants. Chantage, racket.	En milieu professionnel, éviter systématiquement les sites peer-to-peer et les messageries instantanées. Éviter systématiquement tous les sites mafieux (pornographie, pédophilie).

Cookies

Voir le chapitre 7.

Attaque risquée	Conséquences	Mesures
Vol des cookies sur la machine de l'internaute.	Les informations personnelles de l'internaute sont connues du pirate. Usurpation de l'identitité de l'internaute par le pirate. Rejeu par le pirate d'une session de navigation de l'internaute (sur un site bancaire par exemple).	Configurer le navigateur pour désactiver systématiquement tous les cookies, à l'exception des sites identifiés nominativement par l'utilisateur. Refuser les cookies permanents. Effacer tous les cookies de l'ordinateur.

Messagerie

Voir le chapitre 8.

Attaque risquée	Conséquences	Mesures
Réception d'un message porteur de virus en pièce jointe. L'utilisateur effectue un clic malheureux sur la pièce jointe.	La machine est infectée par le virus.	Ne jamais ouvrir la pièce jointe d'un message, à moins d'être absolument sûr de sa provenance (attention à l'usurpation d'identité !). Un antivirus/antispyware à jour. Filtrage de contenus actifs sur le pare-feu logiciel ou le pare-feu matériel en entrée de site (blocage des fichiers .zip, .exe, .com, .src, .lnk, .bat, .vbe, .js, .vbs, .cmd, ou .cpl).
Réception d'un message porteur d'un virus sachant exploiter une vulnérabilité du client de messagerie ou du navigateur.	La machine est infectée par le virus, sans qu'il y ait forcément intervention de l'utilisateur.	Tenir son client de messagerie et son navigateur à jour. Suppression immédiate des messages de provenance inconnue, sans les ouvrir. Un antivirus/antispyware à jour.
Réception d'un message émanant d'une « source officielle », demandant à l'utilisateur de saisir des informations personnelles.	Divulgation de codes secrets à des inconnus. Ce type de message est un faux (phishing).	Ne jamais répondre à un message demandant à l'utilisateur de saisir des informations personnelles.
Flux de messagerie non chiffrés (courrier électronique et messageries instantanées).	Divulgation d'informations confidentielles à des tiers.	Chiffrer la messagerie avec des mécanismes fiables (GnuPG, utilisation des certificats...). Si la messagerie ne peut être chiffrée, s'abstenir d'échanger des informations confidentielles par ce canal.
Messagerie chiffrée par le fournisseur.	Divulgation d'informations confidentielles : le niveau de sécurité dépend du niveau de confiance accordé au fournisseur.	Si les messages sont potentiellement sensibles (cadre dirigeant d'une entreprise), opter pour un fournisseur de confiance (un fournisseur national traitant les messages sur le territoire national).

Spams

Voir le chapitre 8.

Attaque risquée	Conséquences	Mesures
Découverte d'adresses valides de messagerie, stockage de ces adresses dans des listes de spam.	L'internaute est bombardé de spams.	Ne jamais publier, telle quelle, son adresse de messagerie sur une page web. La publier sous forme d'image. Ne pas affecter à cette image de lien de type « mailto:monAdresse » ! Se faire attribuer des adresses « jetables » pour réaliser les opérations qui nécessitent une adresse électronique. Se faire attribuer des addresses difficiles à deviner (comme ast_784@barycentre.fr).
Bombardement de l'internaute.	Encombrement de la messagerie, gêne à l'utilisation. Risque accru de contamination du poste par un code malveillant (virus, ver, cheval de Troie, logiciel espion). Exposition plus élevée au phishing.	Ne jamais ouvrir un message non sollicité. Utilisation de clients de messagerie dotés de filtres antispam performants (Thunderbird). Lorsque le problème devient incontrôlable : * changer d'adresse de messagerie et repartir sur un bon pied (suivre les mesures ci-dessus). Envisager à l'extrême limite l'acquisition d'un produit spécialisé antispam. Un antivirus/antispyware à jour.

Menaces liées au Wi-Fi

Voir le chapitre 4.

Attaque risquée	Conséquences	Mesures
Écoute du trafic échangé par voie radio entre le poste utilisateur et le point d'accès.	Atteinte à la confidentialité des données échangées.	Sécurisation SSL/HTTPS entre le poste et le site distant. Activation du chiffre WPA2 (à la rigueur WPA) entre le poste et le point d'accès.
Accès illicite au poste utilisateur par la voie radio.	Accès au système de fichiers de l'utilisateur avec toutes les conséquences qui en découlent (divulgation externe, altération et/ou destruction de données). Infiltration du réseau informatique « par la voie des airs », en dépit des éventuelles protections du réseau filaire (pare-feu, DMZ, etc.).	Désactiver l'accès Wi-Fi tant que l'on ne s'en sert pas. Pare-feu logiciel indispensable sur le poste, avec contrôle de l'activité des applications. Activation du chiffre WPA2 (à la rigueur WPA)) entre le poste et le point d'accès. Un antivirus/antispyware à jour.

Glossaire

Il est important de bien connaître les différents types d'attaques qu'un pirate est susceptible de lancer à l'encontre de votre machine. Ainsi vous sera-t-il plus facile de mettre en place les solutions adéquates pour protéger vos données.

- **Attaque de l'homme du milieu**

  Man in the middle, attaque du singe intercepteur

  Lorsque deux machines échangent des informations via un réseau de télécommunication, le pirate s'insère entre elles à leur insu et réussit à intercepter, voire modifier leur messages. Se faisant passer pour l'une des parties, il peut obtenir de précieux renseignements.

- **Attaque cryptologique par force brute**

  En possession d'un morceau du message chiffré, le pirate essaie toutes les clés possibles jusqu'à tomber sur le message en clair correspondant. Si votre clé a une longueur de 40 bits, le pirate devra effectuer 2^{40} opérations pour essayer toutes les clés (en moyenne, la moitié suffira). Avec la technologie actuelle, casser une clé de 40 bits est très faisable. En revanche, si vous utilisez une clé de 128 bits, il faudrait en théorie « mouliner » pendant une durée supérieure à la durée de vie de l'Univers.

- **Balayage de ports**

  Connaissant l'adresse IP d'une machine, l'attaquant essaye d'entamer une session TCP sur chacun de ses 65 535 ports. Les réponses obtenues le renseignent sur les applications de communication qui « tournent » sur cette machine. Un balayage est souvent suivi d'une attaque plus précise visant un service actif spécifique.

- **Commande NBNS pour connaître des noms valides de domaines et d'utilisateurs**

  ```
  net view /domain:NomDeDomaine
  ```

- **Commandes SMB pour établir une connexion nulle avec un partage masqué**

  ```
  net use \\NomDeMachine\IPC$ "" /u:""
  net use \\NomDeMachine\C$ "" /u:""
  net use \\NomDeMachine\Admin$ "" /u:""
  ```

- **Commande telnet pour connaître une version de logiciel**

  En lançant la commande `telnet www.votreSiteWeb.com 80`, le pirate reçoit un message d'erreur mentionnant le nom et la version du logiciel de votre serveur web.

- **Commande TFTP pour accéder à des informations sensibles**

  ```
  get configFichier.cfg
  ```

RÉFÉRENCES Attaques

Le lecteur désireux d'en savoir-plus sur les attaque pourra se référer à l'ouvrage suivante :

📖 *Halte aux Hackers 4éme édition*, Éditions Eyrolles, 2003.

- **Cross Site Scripting (XSS)**

  Attaque d'un site distant via un langage de script : l'utilisateur charge la page web d'un site de confiance, au sein de laquelle un pirate est parvenu – de diverses manières, les moyens ne manquent pas ! – à injecter un script malveillant. Ce script est alors exécuté par le navigateur de l'utilisateur. Généralement conçu pour rediriger vers le site du pirate, l'utilisateur est invité à saisir des informations confidentielles (son nom, son mot de passe, etc.), qui tombent désormais en possession du pirate.
- **Débordement de tampon**

  Le pirate provoque l'exécution d'un code malveillant en envoyant à un programme légitime une commande contenant trop de données. S'il provoque un débordement de tampon, le pirate peut accéder au répertoire racine de la machine avec des droits administrateur.
- **Déni de service distribué**

  Distributed Deny of Service (DDoS)

  Attaque par inondation dirigée contre un ordinateur ou un réseau d'ordinateurs (par exemple les serveurs d'une entreprise). Réalisée par des milliers d'ordinateurs agissant de concert (généralement par l'intermédiaire d'Internet), cette attaque vise à saturer les ressources des serveurs de la victime afin de les rendre indisponibles.
- **Détournement des protocoles chiffrés**

  Un cheval de Troie préalablement installé établit une communication chiffrée avec le pirate, grâce à laquelle ce dernier peut prendre possession de la machine distante à l'insu du pare-feu.
- **Écoute Wi-Fi**

  Grâce au Wi-Fi, le pirate peut écouter tout ce que vous échangez, pénétrer sur votre machine, et même infiltrer votre réseau si votre machine y est branchée.
- **Encapsulation de protocole**

  Le pirate utilise un protocole autorisé par le pare-feu (HTTP, DNS, FTP, SMTP...) pour transporter un autre protocole aux fins moins avouables, qu'un cheval de Troie préalablement infiltré saura exploiter.
- **Exploitation du TTL (Time To Live)**

  Le pirate envoie un message constitué de plusieurs paquets. Le premier paquet a un TTL de 1, le deuxième de 2, le troisième de 3, etc. Chacun des routeurs situés sur la route du message vers son destinataire renvoie alors un message ICMP `TIME EXPIRED`, informant ainsi le pirate à la fois de son existence et de son adresse IP. Comme il y a de grandes chances pour que le dernier routeur sur le chemin soit

celui d'entrée du réseau abritant le destinataire, le pirate sait maintenant vers quelle machine tourner son attaque.

- **Injection SQL**

  Un site s'appuyant sur une base de données relationnelle reçoit comme commandes des requêtes SQL. Si les paramètres de ces requêtes ne sont pas correctement contrôlés, le pirate peut les modifier pour s'octroyer le contrôle total sur la base.

- **IP spoofing**

  Usurpation d'adresse IP.

  Le pirate utilise frauduleusement l'adresse IP d'une machine « autorisée » et se fait passer pour elle pour obtenir des informations confidentielles.

- **Phishing**

  Le terme « phishing », ou « hameçonnage » en français, est issu de la contraction de deux termes : « phreaking », le piratage des centraux téléphoniques, et « fishing », aller à la pêche. « En informatique, l'hameçonnage, ou phishing en anglais, est un terme désignant l'obtention d'informations confidentielles (comme les mots de passe ou d'autres informations privées), en se faisant passer auprès des victimes pour quelqu'un digne de confiance ayant un besoin légitime de l'information demandée. »

  http://fr.wikipedia.org/wiki/Phishing

- **PHF**

  Attaque aujourd'hui dépassée, lorsque le serveur web recevait la commande suivante :

  ```
  /cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
  ```

  il renvoyait tout bonnement au pirate le fichier contenant la liste des identifiants utilisateurs et des mots de passe chiffrés (pour le pirate averti, retrouver ensuite les mots de passe en clair n'était pas très compliqué).

- **Ping de la mort**

  Cette attaque consistait à envoyer des paquets IP trop grands (plus de 65 536 octets) pour faire « planter » une machine distante. Avec les systèmes actuels, elle est désormais obsolète.

- **Téléchargement de codes mobiles**

  Le pirate télécharge télécharge sur votre poste, en même temps que les pages web, de façon transparente et totalement à votre insu, des codes exécutables de toutes sortes, dont des codes malveillants.

- **Violation de répertoires**

Directory traversal

Lorsqu'un programme s'exécute sur un serveur, il le fait avec des droits restreints à certains répertoires seulement. Par diverses ruses, le pirate réussit à en « sortir » et à obtenir l'accès à des répertoires sensibles de la machine, d'où il peut provoquer de gros dégâts.

- **Vol de session**

  TCP hijacking.

  Lorsque deux machines initient une session TCP, le contrôle d'authentification n'est effectué qu'à l'ouverture de la session. En jouant habilement sur les numeros de séquence, le pirate peut détourner la session et prendre le contrôle de la connexion.

- **Wardriving**

  Écoute Wi-Fi

  Le pirate se déplace en voiture avec un matériel spécial pour tâcher de capter les réseaux Wi-Fi qu'il pourrait infiltrer.

Index

A

adressage IP 125
adresse électronique
  créer 273
  divulgation 272
  domaine peu usité 274
  en image 274
  et certificat 292
  liste 272
  privée/publique 272
  protéger contre le spam 272
  résistant au spam 274
  source 272
adresse IP non routable 181
adware *voir* logiciel espion
algorithme
  MD5 370
  RSA 361, 363
  SHA-1 371
  SHA-256 371
  SHA-512 371
algorithme cryptologique
  WEP (Wired Equivalent Privacy) 152
  WPA (Wi-Fi Protected Access) 153
algorithme de chiffrement
  3DES 327
  asymétrique 327
  DES 327
  MD5 327
  RC2 327
  RC4 327
  RSA 327
  SHA-1 327
  symétrique 327
antispam 164, 193
antivirus 164, 193
  analyse complète 110
  analyse de la messagerie 88
  analyse sur demande 87
  blocage de scripts 88
  capacité de nettoyage 90
  choisir 89
  configurer 107
  critère de choix 90, 101
  démarrage à partir du support d'installation 113
  désinstaller 101
  détection de menace 85
  disquettes d'urgence 116
  efficacité 90
  fichier de définitions 84
  fichier des définitions de virus 85
  filtrer les courriers électroniques 285
  fonctionnalité importante 87, 90
  fonctionnement 84
  installer 101
  méthode heuristique 86
  mise à jour 82, 87, 102, 110, 114
  mise à jour via un réseau 88
  mise en quarantaine 88
  offre du marché 88
  optimiser 109
  optimiser pour la messagerie 285
  planification 111
  protection en temps réel 87
  rapport d'analyse 88
  reconnaissance de signature 85
  réparation des fichiers 87
  réponse aux urgences 87
  restriction d'accès 88
  surveillance des processus 86
  vérification de l'intégrité des fichiers 85
application
  mise à jour 117
attaque 75
  balayage d'adresses 161
  balayage de ports 136, 162, 193, 390
  code mobile 386
  connexion nulle SMB 390
  contre les applications 224
  Cross Site Scripting 249
  cryptologique par force brute 390
  DDoS 72
  DDoS (Distributed Deny of Service) 391
  débordement de tampon 160, 163, 193, 387, 391
  débordement de tampon sur SNMP 391
  deni de service 387
  déni de service 160, 161, 193, 385
  déni de service distribué 72, 76, 391
  des anniversaires 371
  détournement de flux chiffrés 145
  détournement de protocole 391
  Directory traversal 392
  directory traversal 163, 193
  du dictionnaire 42
  écoute Wi-Fi 391
  encapsulation de protocole 144, 391
  exploitation du TTL 138, 391
  faiblesse des contenus 160
  hameçonnage 392

homme du milieu 326, 390
injection SQL 163, 392
insertion de scripts 193
IP spoofing 392
IP spoofing 162
liée aux contenus applicatifs 161
localisation des points d'accès Wi–Fi 152
MITM (Man in The Middle) 390
navigateur Internet 387
NBNS 390
orientée communication 160, 161
ouverture de session à distance 161
ouverture de session TCP 136
par courrier électronique 145
PHF 148, 392
phishing 147, 276, 330, 387, 392
phreaking 392
ping de la mort 162, 392
réseau 160, 161, 385
singe intercepteur 390
TCP hijacking 162, 393
téléchargement de code mobile 144
téléchargement de codes mobiles 392
telnet 390
TFTP 390
usurpation d'adresse IP 162
usurpation d'identité 161
usurpation d'adresse IP 392
via HTTP 143
via ICMP 135
via Telnet 139
via un protocole applicatif 143
via un protocole réseau 134
via une application Internet 147
violation de répertoire 163
violation de répertoires 392
virus 160
vol de session 161, 162, 393
wardriving 152, 393
WI-FI 389
XSS (Cross Site Scripting) 163
XSS (Cross-Site Scripting) 387, 391
autorité de certification 210, 218
chaîne de certification 216
intermédiaire 217
principale 216
principe de confiance 214
racine 215, 216
réseau de confiance 214
subordonnée 217

C

certificat 194, 210, 290, 292, 327
authenticité 213
authentification de l'expéditeur 302
autorité de certification 260
Autorité de Certification (AC) 291, 327
autorité de certification française 255
autorité de certification racine 216, 217
autorités de certification réputées 255
chaîne de certification 216
changement de navigateur 336
chercher 296
déchiffrer 211
diffuser 295
empreinte numérique 328
frauduleux 262
gérer 254
intégrité 213
liste de révocation 220, 262
liste du navigateur 219
non vérifiable 258
non-répudiation 213
organisme qualifié 307
valeur juridique 303
vérifier 300
X.509 215
cheval de Troie 72, 383, 384
chiffrage des données
VPN (Virtual Private Network) 154
WEP (Wired Equivalent Privacy) 152
WPA (Wi-Fi Protected Access) 153
chiffrement
algorithme de hachage 210
avec EFS (Encryption File System) 58
chiffrer un fichier 56
clé de chiffrement 55
clé privée 366
clé publique 366
créer une paire de clés 64
cryptologie (histoire) 55
fiabilité des clés 368
GnuPGP 61
identité 63
OpenPGP 61
PGP 61
signature électronique 369
WinPT 63
chiffrer une information 54
clé de chiffrement
de session 328
privée 328
publique 327
clé privée 328, 366
clé publique
authentifier 209, 212
certifier 209
code
exécutable 224
source 224
code mobile 225, 386
applet Java 231
Authenticode 228, 230
bloquer dans les courriers 285
contrôle ActiveX 226
contrôle ActiveX reconnu sûr pour l'écriture de script 231
module externe 234
plug-in 234
script 234
code mobile malveillant 161
compression des données 327
configurer le poste de travail 381
connexion nulle 142
connexion sécurisée 208
contrôle d'accès aux contenus 346
contrôle de contenu 193
cookie 235, 388
durée de vie 246
emplacement 236
tiers 244, 245
types 245
cookie traceur 76
cookies 161
cryptologie 194, 357, 370
3DES 287, 288, 289
algorithme asymétrique 289
algorithme MD5 370
algorithme RSA 361, 363
algorithme SHA-1 371
algorithme SHA-256 371
algorithme SHA-512 371
algorithme symétrique 289
checksum cryptologique 372
chiffrement RSA 367
clé de chiffrement 361, 365, 366
clé de déchiffrement 361, 365, 366
clé privée 289, 291, 292, 367
clé publique 289, 291, 292, 367

clé secrète 289
code de hachage 372
condensé cryptologique 372
congruence 357
déchiffrement RSA 367
DES 287, 288, 289
digest 372
empreinte 290
empreinte électronique 370
empreinte numérique 372
estampille temporelle 288
fiabilité des clés 305
fonction à sens unique 359, 360, 361, 364
fonction de hachage 370
MD5 290, 291
module 357, 361, 365
modulo 357, 359, 363
RC2 287, 288, 289
résidu 359
résumé 372
RSA 288, 289, 291
SHA-1 290, 291
signature électronique 289, 374
structure algébrique d'anneau 363
valeur de hachage 372
valeur juridique de la signature électronique 308
cryptologie et gouvernements 215

D

DADVSI (Droits d'auteurs et droits voisins dans la société de l'information) 346
DCSSI (Direction centrale de la sécurité des systèmes d'information) 307
DCSSI (Direction centrale de la sécurité des systèmes d'information) 308
DDoS (Distributed Deny of Service) 385, 387
deni de service 387
détournement de flux chiffrés 145
disquettes d'urgence 116
DMZ (DeMilitarized Zone) 166
dossier partagé 45
DRM (Digital Rights Management) 346
durée de vie d'un paquet IP *voir* TTL

E

EFS (Encryption File System) 58
encapsulation de protocole 144, 145, 163
Enigmail
configurer 314
enregistreur de frappe clavier 77
Excel
restaurer des données 21
sauvegarder des donnéees 7

F

FAI (Fournisseur d'accès Internet) 168
faille logicielle 79
fichier de définitions de virus 84, 85
Firefox
sauvegarder les favoris 14
fonction de hachage cryptographique 86
format de fichiers
FAT (File Allocation Table) 35
FAT32 (File Allocation Table - 32 bits) 35
NTFS (New Technology File System) 35
freeware *voir* logiciel gratuit

G

GnuPG 313

H

hameçonnage *voir* phishing

I

IGC (infrastructure à gestion de clés) 194
image piégée 80
informations confidentielles 277
infrastructure X.509 215, 218
Internet
informations confidentielles 277
Internet Explorer
afficher les certificats 255
liste de révocation 262
paramètre de sécurité 241
sauvegarder les favoris 14
zone de sécurité 238
zone Internet 239
zone Intranet local 239
zone Sites de confiance 239
zone Sites Sensibles 239

K

keylogger *voir* logiciel espion

L

logiciel espion 73, 161, 383
adware 76
agissement 75
commercial 76
cookie traceur 76
enregistreur de frappe clavier 76
expulser 118
numéroteur 76
spybot 76
logiciel gratuit 75
lois sur la vie privée 76

M

machine virtuelle Java 232
macro infectée 80
messagerie électronique 81, 388
authenticité 286
authentifier l'expéditeur 302
chercher un certificat 296
chiffrer un message 287, 298
confidentialité 286
configurer un filtre antispam 281
constituer une liste noire 282
déchiffrer un message 300
diffuser un certificat 295
échanges sécurisés 287
filtre antispam 278
installer un filtre antispam additionnel 281
lire en format texte 285
messages signés/chiffrés avec OpenPGP 318
messages signés/chiffrés avec un certificat 291
obtenir un certificat 292
renforcer la sécurité des échanges 307
signer un message 289, 298
Thunderbird 308
vérifier un certificat 300
vérifier une signature 300
modèle OSI
appliqué au monde IP 132
couche 1 (physique) 130
couche 2 (liaison) 130
couche 3 (réseau) 130
couche 4 (transport) 131
couche 7 (application) 131
modèle TCP/IP 131, 132
Mozilla Firefox
gérer les certificats 256
liste de révocation 266
paramètres de sécurité 250

N

NAT (Network Address Translation) 154,

181
navigateur
afficher les certificats 255
effacer les mots de passe 52
fonction de sécurité 236
gérer les certificats 254
gérer les listes de révocation 262
Internet Explorer 237
modifier la liste des certificats 257
Mozilla Firefox 250
Netscape Navigator 246
niveau de confidentialité 245
paramètre de confidentialité 244
paramètre de sécurité 240, 246
vider les historiques 51
navigateur Internet 387
Netscape Navigator
cookies 246
gérer les certificats 255
interprétation des pages web 248
liste de révocation 262
paramètre de sécurité 246
plug-ins 248
scripts 248, 249
NGSCB (Next Generation Secure Computing Base) 350
numéroteur 76

O

OpenPGP 308
adresse électronique 317
chiffrer un message 318
diffuser la clé publique 317
nouvelle paire de clés 315
obtenir une clé 318
signer un message 318
outil logiciel
antivirus
Antivir Personal Edition Classic 99
BitDefender 93
F-Secure Antivirus 90
Kaspersky Antivirus 92
McAfee VirusScan 94
Norton Antivirus 97
Panda Titanium Antivirus 95
PC-cillin Internet Security 95
Sophos antivirus 100
tueur de logiciel espion
Ad-aware 120
Spybot - Search & Destroy 118
Outlook
restaurer la messagerie 23
sauvegarder la messagerie 11
sauvegarder le carnet d'adresses 13
Outlook Express
paramètres de courrier 9
restaurer la messagerie 22
sauvegarder la messagerie 12
sauvegarder le carnet d'adresses 13

P

Palladium 350
pare-feu 117
accéder à Internet via un programme tiers 178
applicatif 140, 149, 163
choisir 168, 197
choisir un type 165
cible 161
configurer 170
définir la politique de filtrage 170
détecter une tentative d'intrusion 199
différents types 161
DMZ (DeMilitarized Zone) 166, 175
écrire une règle de détection d'intrusion 202
erreur de configuration 159
et antivirus 160
filtrage du trafic ICMP 174
filtrer les applications 176
fonctionnement 163
IDPS (Intrusion Detection and Prevention System) 166, 200
journaux d'activité 188
limites 165
logiciel 167, 192
logiciel, installer 170
matériel 140, 191, 194
mesures de sécurité 205
NAT (Network Address Translation) *voir* traduction d'adresse
ports ouverts implicitement 171
principales règles de filtrage protocolaire 172
protéger l'accès aux fonctions d'administration 191
réagir aux alertes 187
recommandations pour la configuration 190
règle de filtrage 166
règles natives des IDPS 201
rôle 159
sonde de détection et de prévention d'intrusion 164, 166
stateful inspection 162
tester 168
traduction d'adresse 181
vérifier la configuration 180
VPN (Virtual Private Network) 166
zone Internet 172
zone sûre 172
PatchGuard 353, 355
payer sur Internet 325
peer-to-peer 75, 272
perte de données
arrêt brutal du système 3
bogues des logiciels 6
causes 3
éviter 7
noms de fichiers à rallonge 5
profils itinérants 4
système corrompu 5
système de fichiers 4
phishing 387
éviter 277
pièce jointe infectée 79
ping 133, 135
PKI (Public Key Infrastructure) 194
politique de confidentialité d'un site 246
port
autoriser en sortie 175
TCP 110 (POP3) 148, 175
TCP 139 (NBSS) 173
TCP 139 (SMB) 47
TCP 20 (FTP) 185
TCP 21 (FTP) 185
TCP 25 (SMTP) 131, 137, 149, 175
TCP 443 (HTTPS) 148, 175
TCP 445 (SMB) 47, 173
TCP 445 (SMB) 143
TCP 80 (HTTP) 144, 148, 175
TCP 110 (POP3) 149
TCP 139 (SMB) 142
TCP 139 (NBSS) 143
TCP 25 (SMTP) 148
TCP 445 (SMB) 142
TCP 53 (DNS) 133
TCP 80 (HTTP) 131, 136, 137
UDP 137 (NBNS) 173
UDP 53 (DNS) 173
UDP 137 (NBNS) 47, 142

UDP 137 (NBNS) 143
UDP 53 (DNS) 133
porte dérobée 74, 161
pourriel *voir* spam
Powerpoint
restaurer des données 21
sauvegarder des donnéees 7
protocole
applicatif 145
contrôle du transport des données 128
de transmission 125
DHCP (Dynamic Host Configuration Protocol) 133, 173
DNS (Domain Name Service) 133, 173
encapsulation 163
encapsulation de protocole 144
FTP (File Transfer Protocol) 137, 164, 185
HTTP (HyperText Transfer Protocol) 131, 143, 164
HTTPS (HTTP sécurisé) 131, 145, 208, 325, 326
ICMP (Internet Control Message Protocol) 132, 133, 173
IGMP (Internet Group Management Protocol) 173
IMAP4 (Internet Message Access Protocol) 131, 146
IP (Internet Protocol) 125, 130
modèle OSI 129, 132
modèle TCP/IP 131, 132
NBNS (NetBIOS Name Service) 47, 142
NBSS (NetBIOS Session Service) 47
NetBIOS 47, 173
OCSP (Online Certificate Status Protocol) 265
POP3 (Post Office Protocol) 131, 146, 164
rôle 173
SET (Secure Electronic Transaction) 333
SMB (Server Message Block) 47, 142
SMTP (Simple Mail Transfer Protocol) 131, 146, 164
SNMP (Simple Network Management Protocol) 133, 141
SSL (Secure Socket Layer) 325, 333
TCP (Transport Control Protocol) 128, 131, 173
TCP/IP 134
TFTP (Trivial File Transfer Protocol) 140
TLS (Transport Layer Security) 325
transmission par IP 126
UDP (User Datagram Protocol) 132, 173
VPN-SSL (Virtual Private Network-Secure Sockets Layer) 145
proxy 176

R

refuser des connexions entrantes 175
règle de filtrage 166
créer 184
ports TCP et UDP 176
protocoles de la messagerie 175
protocoles du Web 175
relais (proxy) 193
relais *voir* proxy
réparer le système 381
réseau de confiance
IGC (Infrastructure à gestion de clés) 308
OpenPGP 308
PKI (Public Key Infrastructure) 308
réseau de confiance mutuelle 310
réseau de confiance X.509 214
réseau IP 127
restaurer des données 21, 380
document Office 21
document supprimé 21
messagerie 21
utilitaire de sauvegarde 23
restreindre l'accès aux applications 39
routage dynamique 196

S

sauvegarde
virus 114
sauvegarder des données 7, 379
bureau et favoris 14
carnet d'adresses 13
ce qu'il faut sauvegarder 8
enregistrer automatiquement 7
graver sur CD-Rom 11
messagerie 11
planifier une sauvegarde 17
sauvegarde automatique 14
sauvegarde différentielle 16
sauvegarde incrémentielle 16
sauvegarde manuelle 11
sauvegarde normale 16
sauvegarde quotidienne 16
support de sauvegarde 10
vérifier la sauvegarde 19
Scriptlet 231
sécuriser NetBIOS 143
sécurité assurée par les fournisseurs d'accès 168
sécurité informatique 158
shareware 82
signature 210
signature électronique
authentification 369, 375
intégrité 369, 375
non répudiation 369, 375
validité 369
Signtool 233
spam 73, 75, 270, 389
algorithme à apprentissage 277
définition 271
filtre antispam 277
liste noire 278
ne pas répondre 272
pièges à éviter 275
pop-up 271
règle de filtrage 279
supprimer 279
spybot 76
spyware *voir* logiciel espion
SSL (Secure Socket Layer)
fonctions de sécurité 325
système d'exploitation
afficher le Bureau 43
Centre de sécurité 33
chiffrer avec EFS (Encryption File System) 58
chiffrer un dossier ou un fichier 54
commande convert 36
compte restreint 38
configurer 33
convertir une partition en NTFS 35
créer un compte restreint 39
définir un mot de passe utilisateur 41
dossier partagé 45
fichier caché 53
format de fichiers 35
formater en NTFS 34
formater une partition en NTFS 36
mettre en veille 43
modifier les permissions du Registre 37

mot de passe robuste 43
mot de passe sur les documents 45
mot de passe Windows 42
nom de fichier long 46
partager des informations en réseau 45
partages fantômes 47
personnaliser le menu Démarrer 40
programme cmd 35
programme regedit 38
régler les autorisations d'un partage 46
sécuriser le Registre 37
sécurité de Windows 33
supprimer un partage 47
Vides la liste Mes documents récents 49
visualiser les partages 45
Windows Server 2003 33
Windows XP Pro 33
XP édition familiale 33

T

TCPA (Trusted Computer Platform Alliance) 346, 350
téléchargement de code mobile 144
terminal de paiement électronique (TPE) 329
Thunderbird
extensions de sécurité 313
paramètres de courrier 9
restaurer la messagerie 22
sauvegarder la messagerie 12
sauvegarder le carnet d'adresses 13
traduction d'adresse 181
traduction d'adresse (NAT) 154
transaction sécurisée
certificats des AC signataires 338
clé de session 328
déclaration des revenus sur Internet 334
déroulement 326
législation favorable 331
niveau de sécurité 329
obtenir votre certificat auprès d'une administration 335
principes 325
protéger son certificat 342
renforcer la sécurité 331
transaction avec tiers 332
trojan *voir* cheval de Troie
troyen 72
TTL (Time To Live) 133
type MIME 80

V

ver 72, 383
virus 383
agissement 73
Anna Kournikova 79
auteur 82
Bagle.BJ 84, 178
charge utile 73
cheval de Troie 72
d'application 72
de macro 72
de secteur d'amorce 72
définition 71
disquettes d'urgence 116
eicar.com 81
éradiquer 106, 112
éviter l'infection 117
exploitation d'une faille logicielle 79
fichier de définitions 84
fichier des définitions 85
I Love You 81
image piégée 80
infection de la machine 79
infection par la messagerie 284
installation 73
Internet Exploder 230
macro infectée 80
Melissa 80
messagerie électronique 81
MyDoom 83
Mydoom 73
Netsky.P 112, 149
nettoyer une machine contaminée 113
Nimda 80
nouveau 114
ouverture des ports 74
perversion du système 74
pièce jointe 79
porte dérobée 74
propagation 81
Sasser 83
sauvegarde 114
signature 85
Sober.Q 74
troyen 72
types 71
ver 72, 161
VPN (Virtual Private Network) 166, 194

W

WI-FI 389
Wi-Fi
SSID (Service Set IDentifier) 152
SSID (Service Set Identifier) 154
WEP (Wired Equivalent Privacy) 152
WPA (Wi-Fi Protected Access) 153
Windows
démarrage 24
dernière bonne configuration connue 26
fermeture incomplète 4
gestion de l'ordinateur 19
gestionnaire des sauvegardes 14
journalisation de la sauvegarde 20
mise à jour 117
mode sans échec 27
options de démarrage 27
planifier une sauvegarde 17
réparer après un virus 26
réparer l'installation 28
système de fichiers 4
utilitaire de sauvegarde 23
Windows Messenger 179
Word
restaurer des données 21
sauvegarder des données 7
worm *voir* ver

X

XSS (Cross-Site Scripting) 387

Z

zone Internet 172
zone sûre 172