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