Sécurité informatique

3e édition

Principes et méthodes

Laurent Bloch

Christophe Wolfhugel

Préfaces de Christian Queinnec et d'Hervé Schauer

Avec la contribution de Nat Makarévitch

 ISBN : 978-2-212-13233-5

EYROLLES

Avant-propos

Ce livre procurera au lecteur les connaissances de base en sécurité informatique dont aucun utilisateur d'ordinateur ni aucun internaute ne devrait être dépourvu, qu'il agisse dans le cadre professionnel ou à titre privé. Pour cela nous lui proposerons quelques pistes qui devraient l'aider à trouver son chemin dans un domaine en évolution rapide où l'information de qualité est parfois difficile à distinguer du vacarme médiatique et des rumeurs sans fondement.

Plutôt que de proposer des recettes à appliquer telles quelles, et qui dans un domaine en évolution rapide seraient de toute façon vouées à une prompte péremption, nous présenterons des axes de réflexion accompagnés d'exemples techniques.

L'Internet est au cœur des questions de sécurité informatique : nous rappellerons brièvement ses principes de fonctionnement, placés sous un éclairage qui fera apparaître les risques qui en découlent. Pas de sûreté de fonctionnement sans un bon système d'exploitation : nous passerons en revue les qualités que nous sommes en droit d'en attendre. Nous examinerons les différentes formes de malfaisance informatique, sans oublier les aspects organisationnels et sociaux de la sécurité. Pour les entreprises, nous proposerons quelques modèles de documents utiles à l'encadrement des activités informatiques de leur personnel.

La protection des systèmes d'information repose aujourd'hui sur la cryptographie : nous donnerons un exposé aussi simple que possible des principes de cette science, qui permettra au lecteur qui le souhaite d'en comprendre les bases mathématiques. Celui qui serait rebuté par ces aspects pourra en première lecture sauter sans trop de dommages ces développements.

Nous terminerons par un tour d'horizon des possibilités récentes de l'Internet, qui engendrent autant de nouveaux risques : échange de fichiers *peer to peer*, téléphonie sur IP avec des systèmes tels que Skype.

Les lignes qui suivent sont avant tout le fruit de nos expériences professionnelles respectives, notamment dans les fonctions de responsable de la sécurité des systèmes d'information de l'Institut national de la santé et de la recherche médicale (INSERM) pour l'un, d'expert des protocoles de l'Internet au sein de la division Orange Business Services de France Télécom pour l'autre.

L'informatique en général, ses domaines techniques plus que les autres, et celui de la sécurité tout particulièrement, sont envahis de « solutions » que des entreprises s'efforcent de vendre à des clients qui pourraient être tentés de les acheter avant d'avoir identifié les problèmes qu'elles sont censées résoudre. Il est vrai que la démarche inductive est souvent fructueuse dans les domaines techniques, et que la démonstration d'une solution ingénieuse peut faire prendre conscience d'un problème, et du coup aider à sa solution. Mais l'induction ne peut trouver son chemin que dans un esprit déjà fécondé par quelques interrogations : le but des lignes qui suivent est de contribuer à cet effort de réflexion.

L'axe de ce livre, on l'aura compris, n'est pas dirigé vers les modes d'emploi de logiciels ou de matériels de sécurité, mais plutôt vers la position et l'explication des problèmes de sécurité, insérés dans un contexte technique dont il faut comprendre les tenants et les aboutissants si l'on veut adopter des solutions raisonnables. Et donner dans un livre des solutions techniques ou, pire, des recettes toutes faites, nous semblerait futile à une heure où le contexte technique évolue si vite que le Web et la presse spécialisée (qui se développe, y compris en langue française, cf. par exemple la revue MISC [93]) nous semblent bien mieux placés pour répondre à ce type d'attente. Il nous a paru plus judicieux de proposer au lecteur un tour d'horizon des problèmes afin qu'il puisse plus facilement, le moment venu, choisir entre plusieurs solutions techniques qui pourraient s'offrir à lui face à un problème concret.

Mode d'emploi du livre

Comment aborder la lecture de ce livre ? Il propose une progression des explications. Pour le chiffrement, qui est le point le plus difficile parce que assez technique mais à la base de tout le reste, il y a d'abord une évocation informelle et succincte

(chapitre 1), ensuite une présentation générale de la fonction de chiffrement, sans préjuger de ce qu'elle est (chapitre 2), puis l'explication précise avec exposé mathématique (chapitre 4). Il semble difficile de faire autrement, parce que certains lecteurs ont le droit de ne pas lire les mathématiques du chapitre 4, mais ils ont le droit de comprendre le reste quand même. Mettre l'explication complète au début risquerait de décourager le lecteur, supprimer l'explication préalable du chapitre 2 est logiquement impossible parce que ce serait saper les développements qui suivent. Le prix de cette progression est qu'il y a des *flashbacks* : nous pensons qu'il vaut mieux revenir sur un sujet que d'égarer le lecteur par une attaque trop abrupte.

Conventions typographiques

Les textes encadrés ainsi sont destinés à des explications plus techniques que les autres passages, à des exemples pratiques ou à des apartés.

Les nombres entre crochets comme ceci [24] renvoient aux entrées de la bibliographie, en fin de volume.

Le livre comporte quatre parties, qui nous semblent correspondre aux quatre axes selon lesquels un responsable de sécurité doit déployer ses compétences et son activité :

- la première partie expose les principes généraux de sécurité, de façon aussi peu technique que possible ; vous devriez pouvoir la faire lire à votre directeur du système d'information ;
- la seconde partie, consacrée à la *science de la sécurité informatique*, présente les bases scientifiques sur lesquelles reposent les techniques pratiques ; elle est plus exigeante pour le lecteur en termes de difficulté conceptuelle ;
- la troisième partie aborde les aspects politiques, sociaux et psychologiques de la sécurité ; vous devriez pouvoir la placer sous les yeux de votre directeur juridique et de votre DRH ;
- la quatrième partie, qui envisage les évolutions récentes des menaces et de la sécurité, devrait intéresser quiconque navigue régulièrement sur l'Internet.

Remerciements

La liste de tous ceux à qui ce livre doit quelque chose serait trop longue pour que nous prenions le risque, en la dressant, d'en oublier trop. Nous citerons Dominique Sabrier, pour ses relectures toujours précises et d'une exigence judicieuse. L'idée de ce livre naquit d'un enseignement de master organisé à l'université Paris 12 par Alexis Bes. Christian Queinnec (outre sa préface), Michel Gaudet, Bernard Perrot, Patrick Lerouge, Nat Makarévitch et Solveig ont relu, utilement commenté, conseillé et encouragé. Nos collègues de l'Inserm et de France Télécom, sans en avoir forcément eu conscience, ont aussi contribué tant par les échanges d'expériences et d'avis que par les situations concrètes soumises à notre examen. Muriel Shan Sei Fan fut une éditrice à l'exigence stimulante. Florence Henry et Sébastien Mengin ont mis à la composition la touche finale qui fait l'esthétique de l'ouvrage. Les activités et réunions organisées par l'Observatoire de la sécurité des systèmes d'information et des réseaux (OSSIR), par le Symposium sur la sécurité des technologies de l'information et de la communication (SSTIC) et par les Journées réseau de l'enseignement supérieur (JRES) furent des sources d'inspiration permanentes : parmi les intervenants, nous citerons notamment Éric Filiol, Nicolas Ruff, Hervé Schauer. Je remercie François Bayen pour ses suggestions qui ont amélioré notablement les exposés cryptographiques du chapitre 4. La responsabilité des erreurs qui subsistent néanmoins dans ce texte ne peut être imputée qu'aux auteurs.

Ce livre a été écrit, composé et mis en page au moyen de logiciels libres, notamment GNU/Linux, GNU/Emacs, TEX, LATEX, BIBTEX et `xfig` : il convient d'en remercier ici les auteurs et contributeurs, dont le travail désintéressé élargit le champ de la liberté d'expression.