

Sécurité informatique

Principes et méthode

**Laurent Bloch
Christoph Wolfhugel**

**Préfaces de
Christian Queinnec et Hervé Schauer**

**Avec la contribution de Solveig,
Florence Henry et Nat Makarévitch**

© Groupe Eyrolles, 2007,
ISBN : 2-212-12021-4
ISBN 13 : 978-2-212-12021-9

EYROLLES



Préface I

L'internet, on le lit souvent, est une jungle, un lieu plein de dangers sournois, tapis et prêts à frapper fort, péniblement et durablement. On aura intérêt à ne pas s'attarder sur cette banalité car la jungle est l'endroit où l'on doit obligatoirement vivre. En revanche, tout comme pour les MST (maladies sexuellement transmissibles), être ignare, ne pas vouloir apprécier les dangers, persister à les ignorer sont des attitudes blâmables.

Ce qui est moins évident est qu'un ordinateur est un assemblage hétéroclite, historiquement enchevêtré, de matériels et de logiciels dont les innombrables interactions sont au-delà de l'humainement appréhendable. Un ordinateur est tout autant une jungle et cette jungle s'étend au fil de ses expositions successives à Internet.

Comme dans tant d'autres domaines sociétaux, la « sécurité » est réputée être la solution à ces problèmes !

Mais au-delà de bonnement nommer cette solution, d'espérer un monde meilleur où l'on pourrait enfin jouir de cette fameuse sécurité, il faut s'interroger sur son existence, sa nature, ses constituants, ses conditions d'apparition ou de disparition, son développement, etc. C'est précisément à ces interrogations que répond l'ouvrage de Laurent Bloch et Christophe Wolfhugel.

Un tel état de grâce ne s'obtient ni par décret, ni par hasard. C'est le résultat d'une confluence opiniâtre de comportements et de solutions techniques. Ces dernières sont présentes depuis l'article séminal de Diffie et Hellman [40] en 1976 qui a permis de résoudre le problème, ouvert depuis des millénaires : comment

deux personnes, ne se connaissant au préalable pas, peuvent-elles élaborer un secret commun à elles seules en n'ayant échangé que des messages publics ? Clés publiques/privées, certificat, signature électronique sont les plus connues des innovations qui en découlent. Notariat électronique, respect de l'anonymat (réseau TOR), crypto-virus blindés en sont d'autres plus confidentielles aujourd'hui.

Si, dès maintenant, des solutions techniques existent pour un monde meilleur, c'est sur le plan humain que peine le salut à s'instaurer. On ne peut souhaiter un monde sûr que si l'on prend la mesure de l'actuelle insécurité. On ne peut espérer un monde plus sûr que si l'on sait qu'il est réalisable, que si l'on est prêt à tolérer des changements personnels importants de comportement, que si l'entière société humaine stimule l'adoption de ces nouvelles règles et veille à les adapter au rythme des inéluctables évolutions.

La sécurité n'est qu'un sentiment dont l'éclosion est due à la conjonction de facteurs techniques et sociétaux. La mise en place d'un contexte favorable à ce sentiment est complexe, tant sont grandes les difficultés de réalisation et les oppositions entre les différentes inclinations libertaires, dirigistes ou *Big Brother*iennes. L'anonymat est-il autorisé sur Internet ? Puis-je mettre mon ordinateur en conformité avec mes désirs sécuritaires ? Comment rétribuer une création intellectuelle incarnée numériquement (*sic*) et dont la duplication est quasiment gratuite ? Devons-nous laisser l'offre des industriels diriger notre morale et notre liberté ?

L'excellent livre de Laurent Bloch et Christophe Wolfhugel a pour thème la sécurité. Loin de s'appesantir sur les seuls aspects techniques ou de broder autour de banalités comme « la sécurité parfaite n'existe pas » ou encore « avoir listé les menaces garantit une éternelle quiétude », ce livre est à lire et à méditer pour tous ceux qui y croient et tous ceux qui n'y croient pas afin que tous puissent participer intelligemment à l'avènement de l'ère numérique. Cet espace incommensurablement démocratique (les internautes votent avec leur souris) que réalise l'interconnexion de toutes les puces calculantes, nous avons une chance de modeler son avenir tout autant que de le transformer en le plus effroyablement fliqué lieu communautaire. À nous de choisir à la lueur de ce que nous en dit cet ouvrage.

Christian Queinnec
Professeur à l'Université
Pierre et Marie Curie