Sériousse Cryptographie

Avant-Propos

Sériousse Cryptographie est une traduction de l'ouvrage **Serious Cryptography**, de Jean-Philippe Aumasson, publié en 2017 par No Starch Press, voir https://nostarch.com/seriouscrypto.

L'extrait ci-dessous est publié sur le site de l'auteur : https://www.aumasson.jp/.

Si vous trouvez des erreurs dans le livre, merci de les reporter à jeanphilippe.aumasson@gmail.com.

v20220910

Avant-Propos

Si vous avez déjà lu un livre ou deux sur la sécurité informatique, vous aurez sûrement rencontré un jugement récurrent sur le domaine de la cryptographie. La « cryptographie », disent-ils, est « le plus fort maillon de la chaîne ». Élogieux, certes, mais quelque peu simpliste. Si la cryptographie était en réalité le composant le plus fiable d'un système, pourquoi investir autant de temps à l'améliorer alors que tant d'autres parties du système pourraient bénéficier de notre attention ?

S'il y a une chose que j'espère que vous retiendrez de cet ouvrage, c'est que cette vision de la cryptographie est idéalisée ; c'est en grande partie un mythe. La cryptographie est solide *en théorie*, mais en pratique elle est aussi fragile que toute autre partie du système. C'est particulièrement vrai quand les implémentations sont développées sans l'expertise, l'expérience, et l'attention adéquate, comme c'est le cas de nombreux systèmes cryptographiques déployés aujourd'hui. Et le plus grave : quand des implémentations cryptographiques ont des problèmes, les conséquences sont souvent remarquablement impressionnantes.

Mais pourquoi s'en inquiéter, et pourquoi ce livre ?

Quand j'ai commencé à travailler dans le domaine de la cryptographie appliquée il y a une vingtaine d'années, l'information disponible aux développeurs de logiciels était souvent parcellaire et dépassée. Les cryptographes développaient des algorithmes et protocoles, les ingénieurs cryptographiques les implémentaient pour créer des librairies impénétrables et mal documentées destinées principalement à d'autres experts. Il y avait—et il y a toujours—un grand clivage entre ceux qui connaissent et comprennent la cryptographie, et ceux qui les utilisent (ou les ignorent, à leurs risques et périls). Il y a peu de livres décents disponibles, et encore moins offrent des outils utiles aux professionnels.

Les résultats n'étaient pas beaux à voir. Je parle de problèmes impliquant les termes « CVE » et « Severity : High », et dans certains cas alarmants, des slides classés « TOP SECRET ». Vous connaissez peut-être certains des exemples les plus célèbres, ne serait-ce que parce qu'ils ont affecté des systèmes dont vous dépendez. Nombre de ces problèmes sont dus au fait que la cryptographie est subtile et mathématiquement élégante, et que les experts en cryptographie n'ont pas partagé leurs connaissances avec les ingénieurs qui écrivent les logiciels.

Heureusement, cela a commencé à changer et ce livre est un symptôme de ce changement.

Serious Crypto a été écrit par l'un des plus grands experts en cryptographie appliquée, mais il ne s'adresse pas aux experts. Il ne se limite toutefois pas à un aperçu superficiel du domaine. Au contraire, il offre une discussion approfondie et actualisée de l'ingénierie cryptographique, écrite pour aider les praticiens du domaine à mieux faire. Dans ces pages, vous apprendrez non seulement comment fonctionnent les algorithmes cryptographiques, mais aussi comment les utiliser dans des vrais systèmes.

Le livre commence par une exploration des principales primitives cryptographiques, dont les algorithmes de base tels que les chiffrements par bloc, schémas à clé publique, fonctions de hachage, ou générateurs de nombres aléatoires. Chaque chapitre présente des exemples concrets du fonctionnement des algorithmes, et ce que vous devez ou ne devez *pas* faire. Les derniers chapitres couvrent des sujets plus avancés, comme TLS, ainsi que l'avenir de la cryptographie—que faire lorsque des ordinateurs quantiques viendront nous compliquer la vie.

Bien qu'aucun livre ne puisse résoudre tous nos problèmes, un minimum de connaissances peut tout changer. Ce livre offre beaucoup de connaissances. Peut-être assez pour que la cryptographie réelle et déployée soit à la hauteur des grandes attentes qu'elle suscite chez beaucoup d'entre nous.

Bonne lecture.

Matthew D. Green
Professeur
Information Security Institute
Johns Hopkins University, USA