# Concealing for freedom

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 mai 2022

https://www.bortzmeyer.org/concealing-for-freedom.html

Auteur(s) : Ksenia Ermoshina, Francesca Musiani
ISBN n°
Éditeur : Mattering Press
Publié en 2022

---

Le chiffrement est depuis longtemps un sujet de controverses. Indispensable pour assurer la sécurité des communications sur les réseaux informatiques (donc, tous les réseaux, y compris le téléphone), il est régulièrement attaqué par des politiciens qui l'accusent de permettre aux délinquants et aux criminels de dissimuler leurs communications. Mais il n'y a pas que ces attaques grossières, il y a aussi beaucoup de débats autour du chiffrement et de la meilleure façon de protéger les communications de M. et Mme Toutlemonde. Ce livre <https://www.matteringpress.org/books/concealing-for-freedom> de deux chercheuses en sociologie explore de manière très claire mais aussi très approfondie ces débats. En bref, le chiffrement est nécessaire mais pas forcément suffisant. Ce livre est très recommandé à toutes les personnes qui veulent comprendre ce difficile problème.

Notez tout de suite avant d'acheter la version papier du livre qu'il est également gratuitement disponible en ligne <https://www.matteringpress.org/books/concealing-for-freedom>. Même si vous achetez la version papier, la version numérique vous intéressera peut-être, par exemple pour rechercher un mot, ou pour copier-coller une citation.

Les informaticien[Caractère Unicode non montré [1] ]nes ont parfois tendance à avoir une approche strictement technique du chiffrement. On chiffre, et on est protégé, et les seuls débats concernent des points tels que « dois-je utiliser ECDSA ou EdDSA ? ». Mais les auteures montrent bien que bien d'autres questions se posent, et peuvent affecter la sécurité des communications. Par exemple, le livre contient une analyse du modèle de menaces. On veut se cacher de qui ? Le problème d'une militante féministe en Russie n'est pas forcément le même que celui d'un journaliste qui couvre des manifestations aux États-Unis <https://www.bortzmeyer.org/info-sec-essentials.html> ou que celui d'une femme qui veut se protéger d'un mari violent. L'adversaire n'a pas les mêmes moyens, et le niveau de risque est différent à chaque fois. Ainsi, de manière peut-être contre-intuitive, il peut être plus prudent

1. Car trop difficile à faire afficher par LaTeX

d'utiliser un logiciel moins sûr, mais plus répandu, pour ne pas attirer l'attention. (Ce chapitre, comme d'autres dans le livre, est repris d'un précédent article des auteures <https://www.bortzmeyer.org/hiding-from-whom.html>.)

Le livre s'appuie sur beaucoup d'ateliers et de formations où les auteures ont participé. Ici, un dessin du modèle de menaces par une militante russe lors d'un de ces ateliers, montrant les différents ennemis :

Dans bien des cas, le choix du système le plus sûr n'a pas de solution évidente, d'autant plus que bien des critères de choix se bousculent. Un chapitre est ainsi consacré au débat centralisation/décentralisation. Un système de communication centralisé est-il plus sûr ? La réponse n'est pas simple. Un système décentralisé a l'avantage de ne pas avoir de point de contrôle unique, susceptible d'être piraté, corrompu, ou soumis à des pressions financières ou juridiques. Utilisant des techniques standardisées, il est indépendant de tout fournisseur. Il règle de manière élégante la question du pouvoir et de ses abus en limitant la quantité de pouvoir dont dispose chaque acteur. Mais il a aussi des inconvénients : difficulté à faire évoluer techniquement (exemple du courrier électronique, réseau social décentralisé bien antérieur aux réseaux centralisés des GAFA, mais qui a du mal à déployer massivement des techniques de sécurité nouvelles), difficulté pour les utilisateurs à comprendre à qui il faut faire confiance (l'administrateur d'un serveur décentralisé n'est pas forcément « meilleur » que Gmail), risque d'invasion par des parasites contre lesquels il sera difficile de lutter (pensez au spam). Les auteures ne disent évidemment pas qu'il faut préférer les systèmes centralisés, simplement que le choix de la sécurité n'est pas toujours simple. (Une bonne partie du chapitre est consacrée aux controverses autour de Signal et du discours très pro-centralisation de son créateur, mais il parle aussi de systèmes moins connus comme Briar.) Et les arguments techniques cachent souvent des volontés de contrôle. Et parfois c'est la technique qui rend certaines solutions difficiles (faire du chiffrement de bout en bout est plus difficile si on veut des communications de groupe, faire de la distribution de message sans serveur est plus difficile si on veut épargner les batteries, etc).

La fédération (telle qu'utilisée par le fédivers) est souvent présentée comme la solution au problème du contrôle de la communication par quelques géants. Mais elle aussi pose ses propres problèmes, comme l'ont montré les difficultés de XMPP et Matrix à vaincre les messageries instantanées privatrices.

En parlant de messageries instantanées, un des chapitres les plus intéressants concerne l'analyse qu'avait publiée l'EFF pour aider les utilisateurices à choisir une messagerie instantanée sûre. La première version avait suscité de nombreuses critiques (pas toutes innocentes, et pas toutes intelligentes), portant par exemple sur la prépondérance excessive de critères purement techniques, ou s'inquiétant du fait de résumer un choix aussi complexe à un simple tableau de critères. Les auteurs détaillent longuement ces débats, et comment ils ont mené à une sérieuse réflexion sur la meilleure manière d'informer les utilisateurices.

Le livre est clairement écrit, et les auteures connaissent leur sujet (j'ai apprécié que le fédivers ne soit pas juste appelé Mastodon et que Pleroma soit aussi cité). Si vous croyez que le problème est simple, et que vous vous exprimez sèchement à ce sujet sur les réseaux sociaux, c'est le livre à lire d'abord.

---

https://www.bortzmeyer.org/concealing-for-freedom.html