Se cacher de qui ? Chiffrement, sécurité informatique et modèle de menace

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 mars 2020

https://www.bortzmeyer.org/hiding-from-whom.html

Depuis les révélations d'Edward Snowden, il est difficile d'ignorer le fait que des méchants nous espionnent via les outils numériques. Les solutions proposées se limitent fréquemment à la technique : chiffrement de bout en bout et vous êtes en sécurité. Mais c'est évidemment plus compliqué que cela, comme l'analysent bien Ksenia Ermoshina et Francesca Musiani dans leur article « Hiding from Whom ? Threat-models and in-the-making encryption technologies <https://halshs.archives-ouvertes.fr/halshs-02320706> ».

L'article repose sur beaucoup de travail de terrain, auprès de dissidents, lanceurs d'alerte et défenseurs des droits humains un peu partout dans le monde. Ils et elles ne sont pas en général informaticiens et ne maitrisent pas tous les détails techniques. Mais elles ou ils comprennent souvent le modèle de menace : on veut se protéger contre qui ? Ce n'est pas la même chose d'être un employé qui ne veut pas être surveillé par son patron, et d'être un agent secret infiltré dans un pays ennemi disposant de puissants moyens de surveillance. C'est en effet le point crucial souvent oublié des discours sur la sécurité informatique : qui est l'ennemi ?

Évidemment, s'il existait un outil de communication idéal, simple à utiliser, parfaitement sécurisé, ne nécessitant pas de faire confiance à tel ou tel acteur, et largement déployé, le problème serait simple. Il suffirait de dire « utilisez cet outil ». Mais comme il n'existe pas, il faut s'adapter. Et cela nécessite de bien comprendre les menaces. Par exemple, les interviews par les auteures de femmes au Moyen-Orient montrent une claire prise de conscience du fait que le risque, pour la femme, est à la maison (ce qui n'est évidemment pas limité au monde musulman.)

Comprendre les menaces est évidemment plus facile à dire qu'à faire. Les auteures dégagent deux axes de classification des utilisateurs, l'axe du risque (haut risque vs. faible risque) et l'axe compétences techniques (connaissances étendues vs. faibles connaissances.) Il y a des gens à faible risque et compétences élevées (l'informaticien spécialiste des questions de sécurité et vivant dans un pays calme et démocratique) et, malheureusement pour eux, des gens à risque élevé et compétences limitées (la militante écologiste dans un pays autoritaire.) Et il faut aussi compter avec le graphe social : dans beaucoup de circonstances, si on est à faible risque mais qu'on fréquente des gens à haut risque, on devient une cible.

Ah, et vous voulez encore compliquer les choses ? Notez alors que l'utilisation de l'application la plus efficace n'est pas forcément une bonne idée, si elle est peu répandue : l'ennemi peut considérer que la seule utilisation de cette application indique que vous êtes dangereux. Être trop différent peut être un délit et en rester à WhatsApp, malgré toutes ses faiblesses, peut être plus sûr…

Bref, la sécurité, c'est compliqué, vous vous en doutiez, il n'y a pas de solution magique. L'intérêt de cet article est d'élargir la perspective, surtout celle des informaticiens, et de comprendre la variété et la complexité des problèmes de sécurité.

Un résumé de l'étude avec interview des auteures a été publié sur le journal du CNRS <https://lejournal.cnrs.fr/articles/le-chiffrement-des-messageries-passe-au-crible-des-sciences

---

https://www.bortzmeyer.org/hiding-from-whom.html