La cryptographie nous protège t-elle vraiment de l'espionnage par la NSA ou la DGSE ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 septembre 2013

https://www.bortzmeyer.org/crypto-protection.html

Cet article est une exploration, essentiellement théorique, d'un problème technique intéressant : l'utilisation de la cryptographie est-elle utile lorsqu'on veut protéger sa vie privée contre l'espionnage massif auquel se livrent des agences gouvernementales comme la NSA ou la DGSE ? Je vous le dis tout de suite, il n'y a pas de réponse simple.

Notez bien la définition du problème : je ne parle pas des attaques par le pirate du coin (celui qui "*sniffe*" votre réseau Wi-fi au cyber-café), car la cryptographie est certainement indispensable contre lui, contre cet attaquant ordinaire. Et je ne parle pas non plus du cas où l'agence d'espionnage vous cible **individuellement**. Si la NSA a décidé que vous êtes un objectif intéressant et met tous ses moyens à **vous** espionner, il n'y a pas grand'chose à faire (le plus probable est qu'ils utilisent un "*spyware*" dans votre ordinateur, ou bien une écoute électromagnétique, à moins qu'ils ne préfèrent la méthode bien décrite dans xkcd <http://xkcd.com/538/>). Dans ce cas, on fait de la gestion de risque, mais on n'espère pas être invulnérable.

Non, je me focalise sur l'espionnage de masse, passant à l'échelle, et visant des tas de gens dont la NSA ou la DGSE ne savent pas a priori s'ils sont une cible intéressante ou pas. C'est cet espionnage qui a fait l'objet récemment d'une prise de conscience, suite aux révélations d'Edward Snowden. Il a parlé de la NSA (et du GCHQ) mais il n'y a aucun doute que d'autres agences font pareil. En France, en raison d'une tradition d'obéissance au monarque qui remonte à longtemps, on n'a pas encore vu de « lanceur d'alerte » héroïque et désobéissant comme Snowden mais cela ne veut pas dire qu'un tel espionnage n'a pas lieu.

Mais comment savoir exactement les capacités de la NSA ? L'adage classique de la sécurité s'applique tout à fait ici : « Ceux qui savent ne parlent pas, ceux qui parlent ne savent pas ». Comme j'écris beaucoup sur ce blog, vous pouvez en déduire que je ne sais pas grand'chose. Il faut donc commencer par un sérieux avertissement : comme les agences secrètes sont... secrètes, on ne peut pas savoir exactement à quoi s'attendre. Cela n'empêche pas les Jean-Kevin <https://twitter.com/jeank3vin> de toute

sorte d'affirmer bien haut « la crypto, c'est nul, on sait bien que la NSA peut tout casser et tout lire, lol, mdr ». Il faut juste se rappeler que ce genre d'affirmations ne vaut rien.

Est-ce que seuls les Jean-Kevin disent n'importe quoi ? Évidemment non. Les chercheurs en sécurité sont connus pour leur goût pour le sensationnalisme et les annonces spectaculaires, qui seront oubliés trois mois après. Chaque année, à Blackhat ou Defcon, il y a une annonce comme quoi la cryptographie est fichue, l'Internet à poil, et que nous allons tous mourir. En 2011, c'était BEAST <https://www.bortzmeyer.org/beast-tls.html>, qui devait mettre fin à TLS. En 2013, on a eu la prédiction comme quoi RSA serait cassé dans cinq ans (un article particulièrement grotesque dans le sensationnalisme fut celui de Technology Review <http://www.technologyreview.com/news/517781/math-advances-raise-the-prospect-of-an-internet-security-crisis/>).

Bon, maintenant que j'ai critiqué ceux qui disaient n'importe quoi, que peut-on dire de sérieux ? Revenons un peu sur la cryptographie dans son service de confidentialité. Alice et Bob veulent communiquer secrètement. Ils chiffrent leurs communications, empêchant un tiers naïf de comprendre ce qu'ils se disent. Mais pour un tiers plus motivé et ayant davantage de moyens ? Il peut utiliser plusieurs méthodes anti-crypto (je ne cite que celles qui passent à l'échelle par automatisation, sans nécessiter de kidnapper Bob et de le faire parler) :

— L'espion peut installer du "*spyware*" dans les logiciels de tout le monde (le nom de code « GENIE <http://www.lemonde.fr/ameriques/article/2013/09/01/la-nsa-a-aussi-espionne-la-di 3469495_3222.html> » à la NSA concerne apparemment un tel programme). C'est d'autant plus facile pour la NSA que la majorité des logiciels sont produits par des entreprises états-uniennes. La cryptographie ne protège qu'en transit, pas si une des machines terminales <https://www.bortzmeyer.org/terminal-host.html> trahit.
— Puisque, dans mon hypothèse de départ, l'attaquant est un État doté d'importants moyens matériels, il peut aussi utiliser la force brute. Si la clé de chiffrement fait 256 bits, on peut (en théorie) essayer systématiquement les $2\hat{\{\}}256$ valeurs. Aucun algorithme (à part le "*one-time pad*") ne résiste aux attaques par force brute. Mais, avec les tailles de clé utilisées dans les systèmes cryptographiques sérieux, c'est probablement irréaliste en pratique.
— Il peut trouver une faille dans les logiciels de cryptographie. S'il casse GnuPG et la mise en œuvre de TLS utilisée dans Firefox, il aura déjà accès à bien des choses. Les logiciels de cryptographie sont des logiciels comme les autres et ont des bogues.
— Il peut casser les protocoles de cryptographie. Il est étonnamment difficile de réaliser un protocole sûr, même quand les algorithmes sous-jacents sont corrects, comme le montrent les différentes failles de TLS (comme celle de renégociation <https://www.bortzmeyer.org/tls-renego.html>). Sans compter **la** faille récurrente par laquelle trébuchent tant de mises en œuvre de la cryptographie : le générateur de nombres aléatoires (RFC 4086 [1]).
— Il peut enfin casser les algorithmes de cryptographie eux-mêmes. C'est le plus spectaculaire (et c'est pour cela que les Jean-Kevin du monde entier aiment bien affirmer des choses comme « on sait bien que la NSA a cassé RSA depuis des années - sans doute dans son centre de recherches de la zone 51 ») mais pas le plus facile, loin de là. Les mathématiques résistent longtemps et, surtout, leurs progrès sont imprévisibles (comme le note à juste titre Schneier <http://www.schneier.com/blog/archives/2013/08/the_cryptopocal.html>). Peut-être que, dans cinq ans, un étudiant dans sa chambre va subitement trouver un moyen simple de décomposer en facteurs premiers, cassant ainsi RSA. Peut-être. Et peut-être pas. Les affirmations comme quoi « RSA sera cassé dans cinq ans » sont ridicules : on ne prévoit pas les percées en maths comme les progrès de l'ingénierie (cf. la loi de Moore).
— L'attaquant peut aussi contourner la cryptographie en se faisant passer pour le correspondant. C'est ce qu'on nomme une attaque de l'homme du milieu et cela a par exemple été utilisé par le gouvernement iranien en 2011. Leur méthode était de détourner le trafic HTTPS vers une machine

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4086.txt

gouvernementale **et** de présenter un « vrai/faux » certificat obtenu auprès d'une AC piratée, comme Diginotar. Ainsi, Alice croyait parler avec Bob alors qu'elle parlait à un espion... Le fait que la communication soit chiffrée n'aide pas si on parle au méchant.

— L'attaquant peut aussi, s'il a l'autorité d'un État derrière lui, ne pas s'embêter et aller prendre les données où elles sont, chez le fournisseur de service. C'est ce que fait le programme PRISM, révélé par Snowden, avec la complicité des gros silos de données comme Facebook ou Gmail. (Dans certains États - mais pas les États-Unis depuis le "*Patriot Act*" - il faut normalement l'autorisation d'un juge. Mais il existe des écoutes illégales comme dans l'affaire des gendarmes de l'Élysée.)

— Une faiblesse souvent oubliée est celle des **métadonnées** : même quand on n'a pas accès aux communications elles-mêmes, les seules métadonnées peuvent être une mine de renseignements (ce qu'on nomme l'analyse de trafic). Les métadonnées peuvent être le qui (Alice écrit à Bob), le quand et le combien (pour une session HTTP, la taille des données transférées indique si on a lu un fichier ou si on en a envoyé un). C'est d'autant plus vrai que les métadonnées, contrairement à la plupart des contenus, sont **structurées**, conçues pour être analysées par des programmes informatiques (car elles servent à la facturation ou au routage).

À noter que certaines de ces attaques peuvent se faire dans le temps : la NSA enregistre la conversation à tout hasard... et la lira dans dix ou vingt ans, quand les progrès de la technique ou de la science le lui permettront. Pensez donc aussi à cela : cette conversation sera t-elle toujours « sensible » dans dix ans ?

Maintenant, quelles protections peut fournir la crypto contre ces attaques ? Attention, cela va être plus laborieux que la description des attaques.

— Contre le "*malware*" installé sur la machine de l'utilisateur, rien à faire. La crypto suppose une plate-forme sûre. Il est possible que des machines construites à partir de composants sécurisés (TPM) résolvent le problème mais je ne suis pas optimiste, notamment parce que ces composants sont plus souvent utilisés pour contrôler l'utilisateur que pour l'aider à se protéger.

— Contre les attaques par force brute, il faut des clés suffisamment longues. Rappelez-vous du pouvoir de l'exponentielle. 2 puissance 256, par exemple, est un nombre qui défie l'imagination humaine. Il ne suffit pas de dépenser beaucoup d'argent et d'acheter des grosses machines pour tester 2{}256 possibilités... (Attention, avec certains algorithmes, il existe des attaques appelées « force brute » mais qui intègrent en fait plusieurs astuces pour ne pas tout essayer. C'est ce qui explique que la longueur de la clé ne soit pas le seul paramètre à prendre en compte.) On entend souvent dire que le calcul quantique va tout changer en permettant des bonds colossaux de performance. Mais, malgré les prétentions des commerciaux qui vendent des « ordinateurs quantiques », on en est **très** loin. Les résultats concrets avec ces ordinateurs restent du domaine du laboratoire. Et, comme le note Schneier <http://www.schneier.com/blog/archives/2008/10/quantum_cryptog.html>, les systèmes cryptographiques ont bien d'autres failles, plus faciles à exploiter que le cassage de la clé par le mythique ordinateur quantique.

— Et contre les failles dans les logiciels ? Code source disponible, bonnes pratiques de programmation, examen par les pairs... Aucune de ces techniques ne fait de miracle mais, ensemble, elles aident à avoir une assez bonne sécurité. (J'ai lu sur un forum un texte d'un Jean-Kevin proclamant avec assurance que « la NSA a une porte dérobée dans PGP ». Inutile de dire qu'il ne fournissait aucune preuve.)

— Pour les failles dans les protocoles de cryptographie, c'est à peu près la même approche : protocoles publiés, examinés publiquement par de nombreux experts. Il restera forcément des failles (on en découvre de nouvelles de temps en temps, dont certaines étaient peut-être déjà connues de la NSA) mais c'est mieux que rien. Notez que les protocoles non publiés utilisés dans les produits commerciaux fermés ne valent pas grand'chose. À chaque conférence de sécurité, un chercheur explique comment il en a rétro-ingénieré un. Parfois, un protocole secret chanceux tient le coup plus longtemps (RC4...) mais c'est rare.

— Pour les algorithmes de cryptographie, c'est un pari sur l'avenir : on espère que l'algorithme ne sera pas cassé. À part l'espérance, la contre-attaque est la même que pour les programmes et les protocoles, à savoir la publication et l'analyse de sécurité au grand jour. On ne sait bien sûr pas où en est la NSA (on dit parfois qu'ils ont dix ou vingt ans d'avance sur la recherche publiée <http://www.wired.com/opinion/2013/09/black-budget-what-exactly-are-the-nsas-cryptanalytic
mais l'ensemble des chercheurs qui travaillent et publient fait néanmoins un bon travail. Si RSA

faiblit et devient vraiment trop incertain, on pourra passer aux courbes elliptiques (RFC 6090). Notez quand même qu'une bonne partie des chercheurs compétents ne publie pas, parce qu'ils travaillent pour la NSA, ou parce qu'ils préfèrent vendre leurs découvertes plutôt que d'aider l'humanité (si vous arrivez à trouver une décomposition en facteurs premiers facile, et que vous publiez, vous gagnez les 10 000 euros de la médaille Fields, soit bien moins que si vous vendez l'information à la NSA ou un de ses équivalents en Russie ou en Chine).

— Contre l'attaque de l'homme du milieu, les solutions envisagées (encore largement expérimentales) tournent autour d'ajouts ou de remplacement du système des AC, comme le système DANE du RFC 6698 ou comme Perspectives <https://www.bortzmeyer.org/perspectives-ssh.html>.
— Par contre, contre l'utilisation d'un gros silo de données comme Gmail ou Facebook, qui donne accès à toutes ses données à la NSA, la crypto ne peut rien. Elle ne protège que le voyage des données, mais tout est stocké en clair chez les fournisseurs de PRISM.
— Enfin, pour la protection des métadonnées, le problème est compliqué <https://www.bortzmeyer.org/metadonnees.html>. Les intermédiaires ont besoin des métadonnées pour acheminer le trafic et il n'est donc pas évident de les dissimuler (il existe des pistes de recherche mais pas encore de solution applicable). C'est pour cela que PGP ne chiffre pas les en-têtes. Pour sécuriser le courrier électronique, par exemple, il faudrait combiner PGP et SMTP sur TLS (RFC 3207 et attention : en pratique, SMTP sur TLS a des tas de limites, question sécurité).

Tout cela n'était que des solutions techniques car cet article se focalise sur l'aspect technique des choses. Mais, évidemment, le problème de fond est politique et c'est dans des changements politiques profonds qu'il faut chercher les vraies solutions. Il n'est pas normal qu'il faille être expert en crypto pour avoir une vie privée !

Autres bonnes lectures après cet article : l'interview d'un des développeurs de GnuPG <https://www.april.org/vie-privee-en-2013-pourquoi-quand-comment-par-werner-koch> ou bien un très bon article de Dan Goodin <http://arstechnica.com/security/2013/09/spooks-break-most-in> expliquant comment contourner (et non pas casser) la crypto ou encore celui de Peter Bright <http://arstechnica.com/security/2013/09/of-course-nsa-can-crack-crypto-anyone-can-the-ques> sur les vraies capacités de la NSA. Voir aussi l'article de Matthew Green <http://blog.cryptographyengineer.com/2013/12/how-does-nsa-break-ssl.html> qui fait le tour des techniques connues et inconnues pour déchiffrer le trafic TLS.

Conclusion ? Il faut évidemment de la cryptographie, ne serait-ce que « dans le doute », et à cause des nombreux attaquants moins équipés que la NSA. Snowden lui-même note que cela gêne l'attaquant <http://www.businessinsider.com/edward-snowden-email-encryption-works-against-the-nsa> Mais ce n'est pas une solution magique et, dans son analyse de sécurité, il faut se demander « et si elle était cassée, quelles seraient les conséquences pour moi ? ».

Merci aux twittériens entre autres (hélas, je n'ai pas pensé à noter tout le monde) Nicolas Caproni <https://twitter.com/ncaproni>, Ollivier Robert <https://twitter.com/Keltounet> (également relecteur de cet article), Marc Levy <https://twitter.com/marc99>, Geoffroy Couprie <https://twitter.com/gcouprie>, Gildas Ribot <https://twitter.com/Giribot>, Damien Clauzel <https://twitter.com/dclauzel>, et les autres. Merci à Gérard Fadrelle pour m'avoir rappelé l'attaque de l'homme du milieu que j'avais bêtement oubliée. Merci surtout au relecteur anonyme qui a fait l'essentiel de la relecture mais ne souhaite pas que son nom apparaisse.