

Edward Snowden et les portes dérobées

Gâce aux révélations d'Edward Snowden, on a su que la NSA tentait et réussissait parfois à introduire des portes dérobées dans certains programmes de cryptographie (comme celui d'un générateur pseudoaléatoire du NIST), se donnant ainsi la possibilité de déchiffrer facilement les communications de ceux qui les utilisaient : la NSA espionnait ainsi des citoyens américains, ce que les lois des États-Unis interdisent pourtant.



Le film *Snowden* du réalisateur Oliver Stone est sorti en 2016. Il retrace les péripéties de ce lanceur d'alerte toujours recherché par la police des États-Unis et aujourd'hui réfugié en Russie.

Récemment encore, une vieille idée pourtant combattue par tous les spécialistes de sécurité informatique a resurgi. Deux sénateurs américains, Richard Burr et Dianne Feinstein, ont déposé un projet de loi qui forcerait tous les acteurs des technologies de l'information à truffer de portes dérobées leurs matériels et logiciels. Le projet voulait accorder aux tribunaux américains le pouvoir d'exiger des entreprises telles que Microsoft, Apple, Google, Facebook, etc. qu'elles donnent accès à toutes les données des appareils qu'elles vendent et des services qu'elles offrent.

Comme c'est le cas depuis longtemps maintenant, un grand nombre d'experts se sont élevés contre cette idée qui, si elle était

adoptée, reviendrait à affaiblir gravement tous les systèmes de sécurité pourtant de plus en plus nécessaires qui protègent les informations des particuliers et des entreprises. Comme l'écrivaient Pauline Glikman et Nicolas Gladys de l'Essec (École supérieure des sciences économiques et commerciales) le 27 mai 2016 dans une tribune sur www.silicon.fr : « Si ce projet de loi américain était voté, les entreprises européennes se verraient donc dans l'obligation d'abandonner l'usage des appareils et services informatiques des fournisseurs américains. Ce serait un coup majeur porté à la compétitivité des États-Unis, qui verraient leurs clients se tourner vers les services chiffrés offerts par des entreprises non soumises à ces contraintes... »

Même aux États-Unis, où l'on sait que les révélations d'Edward Snowden ont déjà affaibli la confiance dans les entreprises et produits nationaux, le projet de loi fait l'objet de très vives critiques. Reste qu'il n'y a aujourd'hui aucun doute que les systèmes d'écoute et d'espionnage massifs mis en place par la NSA au niveau mondial sont un problème pour la souveraineté de tous les États, en même temps qu'un danger économique majeur... et que ces systèmes n'ont pas été désactivés.

la destruction simultanée de tous les gants. Certes, les autorités ne devraient utiliser ce message radio secret que dans des enceintes fermées ne laissant pas échapper le signal destructeur, et uniquement dans le but de s'attaquer à des gants mêlés à des affaires de banditisme ou de terrorisme, mais comment ne pas craindre un accident ou un détournement ?

Le FBI contre Apple

Ces questions ont récemment défrayé la chronique à propos des téléphones d'Apple. En février 2016, le FBI (*Federal Bureau of Investigation*, la police judiciaire américaine) demanda à Apple de l'aider à rendre accessibles les données du téléphone d'un des auteurs de la tuerie de décembre 2015 à

San Bernardino, où 14 personnes périrent. Le problème n'était pas directement celui d'une porte dérobée, mais il se fondait sur l'idée très proche que le système de protection des téléphones d'Apple pouvait être contourné avec l'aide des ingénieurs d'Apple. En clair, le FBI ne doutait pas qu'une sorte de porte dérobée existait et demandait à Apple de la faire fonctionner pour lui livrer le contenu du téléphone.

Apple répondit qu'il ne voulait pas collaborer, non pas que cela fût pour lui impossible, mais parce que cela aurait été contraire à l'intérêt de ses clients. Plus précisément, le FBI demandait à Apple de lui donner un moyen d'éviter que ne fonctionne le système d'effacement automatique qui s'enclenche en cas de tentatives répétées d'accès aux données de l'appareil.

Tim Cook, le président d'Apple, a expliqué : « Le gouvernement des États-Unis a exigé qu'Apple prenne une mesure sans précédent qui menace la sécurité de nos clients. Nous ne voulons pas nous soumettre à sa demande, car cela aurait des conséquences bien au-delà du cas particulier concerné. La situation exige un débat public ; nous voulons que nos clients et tous les gens à travers le pays comprennent ce qui est en jeu. »

Quelques jours plus tard, l'affaire trouva un épilogue décevant et inquiétant pour les clients d'Apple : le FBI, avec une aide dont l'identité est restée cachée, réussit à accéder aux données du téléphone. Ce dénouement signifie tout simplement que les protections prétendues inviolables des téléphones d'Apple ne le sont pas, soit parce qu'un tiers sait les contourner, soit parce

L'AUTEUR



J.-P. DELAHAYE est professeur émérite à l'université de Lille et chercheur

au Centre de recherche en informatique, signal et automatique de Lille (CRISTAL).

BIBLIOGRAPHIE

Computerworld UK staff, *The eight security backdoors that helped kill faith in security*, 2017 : www.computerworlduk.com/security/7-security-backdoors-that-helped-kill-faith-in-security-3634220/

Absolute poker and UltimateBet cheating scandals, World Casino Index, 2016 : www.worldcasinoindex.com/guide/absolute-poker-and-ultimatebet-cheating-scandals/

Safest poker sites, Ultimate Bet Review, 2016 : www.safestpokersites.com/ultimate-bet/

P. Bellanger, *La Souveraineté numérique*, Stock, 2014.

N. Perlroth et al., *NSA able to foil basic safeguards of privacy on Web*, *The New York Times*, 5 septembre 2013.

F. Daignière, *F5 BIG-IP remote root authentication bypass vulnerability*, 2012 : www.trustmatta.com/advisories/MATTA-2012-002.txt

qu'Apple, sans l'avouer, a cédé aux injonctions du FBI et qu'il sait les contourner ! Il y a bien une porte dérobée ou un équivalent dans les téléphones d'Apple.

Les grandes firmes informatiques prétendent défendre la sécurité des systèmes et appareils qu'elles vendent et affirment refuser de placer des portes dérobées dans leurs machines et logiciels. Il serait naïf de les croire : il est certain que cela n'a pas toujours été le cas, et la collaboration entre les géants d'Internet et les autorités américaines a été prouvée à maintes reprises, en particulier à la suite des révélations du lanceur d'alerte Edward Snowden. La NSA (*National Security Agency*), grâce au programme de surveillance PRISM, a eu un accès direct aux données d'Apple, de Facebook, de Microsoft, de Google, d'AOL et de Skype, et il est vraisemblable que c'est encore le cas aujourd'hui.

Le temps des illusions est fini

Quand vous utilisez ces services, soyez certains que vos informations seront soigneusement rangées dans les immenses entrepôts de données de la NSA, dont la capacité de stockage est colossale. Le centre de la NSA récemment construit dans l'Utah aurait des capacités se comptant en centaines d'exaoctets (1 exaoctet = 10^{18} caractères). Certains médias évoquent même des yottaoctets (10^{24} octets), même si cela semble peu vraisemblable, du moins dans un avenir proche.

Une autre histoire un peu plus ancienne que celle des téléphones d'Apple montre que les autorités américaines (mais elles ne sont sans doute pas les seules), ne se contentent pas de demander publiquement qu'on leur communique les clés d'accès des portes dérobées concernant des appareils dont on prétend qu'ils n'en ont pas, mais qu'elles en insèrent secrètement !

En cryptographie, disposer de programmes qui engendrent rapidement des suites pseudoaléatoires est important, car ces méthodes servent comme composants de base à de nombreux algorithmes de chiffrement de données. Le NIST (*National*

Institute of Standards and Technology, l'institut américain des normes et de la technologie) publie des conseils et des normes sur le sujet. Ces normes étaient largement suivies. Or la norme du *Dual Elliptic Curve Deterministic Random Bit Generator* (Dual-EC-DRBG) a été, sans qu'il ne subsiste aucun doute, manipulée par la NSA. Ce générateur contient une porte dérobée qui permet aux détenteurs de clés appropriées de contrôler la production des bits censés être pseudoaléatoires et donc de casser les méthodes de chiffrement qui les utiliseraient.

Dès 2007 paraissaient des études suspectant l'existence d'une porte dérobée dans le Dual-EC-DRBG. Pourtant, le NIST l'indiquait parmi quatre méthodes recommandées pour des usages cryptographiques, ce qu'il a cessé de faire seulement en 2014. À nouveau, ce sont les révélations d'Edward Snowden qui ont permis de connaître le fin mot de l'histoire. Elles indiquent que la NSA avait travaillé sur la normalisation du Dual-EC-DRBG, jusqu'à devenir le responsable unique de sa formulation.

Le *New York Times*, qui a analysé les documents d'Edward Snowden, affirme même que la NSA dépense 250 millions de dollars par an (parfois en payant simplement les entreprises concernées) pour insérer dans les produits cryptographiques des portes dérobées ou des faiblesses lui permettant de casser les chiffrements. On comprend bien que la réputation du NIST en a pâti et que, dorénavant, ses normes sont considérées avec méfiance. C'est plus généralement le cas de nombreux produits et matériels américains, dont on sait qu'ils sont souvent conçus pour faciliter les tâches d'espionnage généralisé de la NSA.

La situation de domination et d'intrusion généralisée de systèmes étrangers (notamment américains) dans le monde numérique est un danger non seulement pour la vie privée de tous, mais aussi pour les entreprises dont les secrets techniques et commerciaux risquent de tomber dans des mains concurrentes ou adverses. Pierre Bellanger, dans un excellent livre sur le sujet (*voir la bibliographie*), évoque avec raison un grave problème de « souveraineté numérique ».



Retrouvez la rubrique
Logique & calcul sur
www.pourlascience.fr