© 360b / Shutterstock.com

© Jstone / Shutterstock.com

en sécurité (l'une dirigée par Neel Mehta, expert en sécurité chez Google, et l'autre de Codenomicon, dont le siège est en Finlande) ne découvrent le bug. Quelques jours plus tard, le magazine *Bloomberg Businessweek* citait des sources anonymes affirmant que la NSA utilisait cette faille depuis des années pour le cyberespionnage.

Nombre d'États puissants ont affecté leurs meilleurs techniciens et des millions d'euros à la découverte et à l'exploitation de vulnérabilités telles que Heartbleed. Les gouvernements achètent aussi des bugs sur le marché libre, contribuant à soutenir l'industrie des failles de sécurité. Un nombre croissant d'entreprises, telles que Vupen Security, à Montpellier, et Exodus Intelligence, à Austin, se spécialisent dans la découverte et la commercialisation de ces précieux bugs. Certains gouvernements dépensent même plus pour la recherche et le développement de capacités offensives que pour la défense contre les cyberattaques. Le Pentagone emploie nombre de chercheurs en vulnérabilités, et le budget de la NSA pour la cyberrecherche offensive est plus du double de celui consacré à la défense.

Cela ne signifie pas que les gouvernements ont des intentions malfaisantes ou qu'ils sont des ennemis de la cybersécurité. Les agences telles que la NSA recueillent des renseignements afin d'empêcher des actes abominables et il est logique qu'elles utilisent tout outil à leur disposition pour y parvenir. Toutefois, une étape importante de la sécurisation du cyberespace consistera à soupeser avec honnêteté les coûts et avantages de l'entretien des vulnérabilités par les agences gouvernementales. Une autre clé de la réussite sera de tirer le plein parti du pouvoir des gouvernements, qui peuvent par exemple obliger des entreprises et autres organismes à partager leurs informations sur les cyberattaques.

Les banques, en particulier, auraient tout intérêt à le faire, car les attaques sur les institutions financières suivent d'ordinaire un schéma prévisible : quand les criminels trouvent un angle d'attaque qui fonctionne avec une banque, ils l'essaient sur une autre, puis une autre… Toutefois, les banques évitent de divulguer des informations sur les attaques subies, car cela soulève des questions sur leur propre sécurité. Elles évitent aussi de communiquer avec leurs concurrentes ; dans certains cas même, les lois antitrust l'interdisent. Les gouvernements, en revanche, peuvent faciliter le partage d'informations entre banques. Ce partage est déjà mis en place aux États-Unis sous la forme du Centre de partage et d'analyse d'informations pour les services financiers (FS-ISAC), qui sert aussi les organismes financiers mondiaux. Et en février, Barack Obama a signé un décret présidentiel qui enjoint d'autres entreprises à partager leurs renseignements entre elles et avec le gouvernement.

DEUX CYBERATTAQUES qui ont marqué les esprits : le 24 novembre 2014, Sony Pictures Entertainment, filiale américaine du groupe japonais Sony, est piratée. De nombreuses données sont détruites, d'autres sont divulguées, notamment des films en postproduction. Quelques mois plus tôt, durant l'été 2014, des pirates ont volé les données personnelles de milliers de clients de la société américaine de portefeuille JP Morgan Chase.

Les pirates à la rescousse

Tant que les hommes écriront des programmes, des vulnérabilités existeront. Sous la pression concurrentielle, les entreprises du secteur des technologies introduisent leurs produits sur le marché plus vite que jamais. Ces entreprises seraient bien avisées d'exploiter l'énorme ressource humaine que constitue la communauté mondiale des hackers. Au cours de l'année passée, catalysées par des événements tels que les révélations d'Edward Snowden sur la NSA, l'industrie technologique et la communauté des hackers ont commencé à accepter l'idée de travailler ensemble. À présent, des centaines d'entreprises voient l'intérêt d'embaucher des hackers en les attirant au moyen de programmes qui récompensent la découverte de bugs ou de vulnérabilités

Aussi efficace soit-il, l'emploi de hackers n'est pas la seule façon d'éprouver la sécurité d'un système informatique. De plus en plus d'entreprises et d'institutions utilisent les méthodes formelles, et pour de bonnes raisons. La meilleure est sans doute que, le plus souvent, les hackers ne peuvent trouver des vulnérabilités que parmi un catalogue d'attaques connues, certes vaste, mais fini.

Les méthodes formelles visent davantage. Issues de la recherche en informatique, elles consistent à modéliser tout ou partie d'un système informatique et à appliquer des algorithmes de vérification. Un tel algorithme prend en entrée le modèle conçu et une propriété de sécurité à vérifier, par exemple la confidentialité d'un message, et retourne une réponse oui (la propriété est vérifiée sur le modèle) ou non (une attaque est possible). La recherche d'une attaque est exhaustive : si une seule attaque existe contre la propriété dans le modèle, l'algorithme la trouvera.

Longtemps, les méthodes formelles ont semblé l'apanage de quelques chercheurs. Les industriels considéraient que les attaques trouvées étaient théoriques, c'est-à-dire inapplicables. C'est en train de changer, notamment pour la vérification des jetons de sécurité. Un jeton de sécurité est, typiquement, une clé USB qui fonctionne comme un coffre-fort pour vos clés secrètes. Vous la branchez dans votre ordinateur et, avec elle, vous pouvez vous authentifier et vous connecter à un site, chiffrer des documents confidentiels, déchiffrer ceux que l'on vous envoie. Vos clés secrètes ne sortent jamais du jeton : pour chiffrer un document, votre ordinateur l'envoie au jeton, qui le chiffre et le renvoie à l'ordinateur.

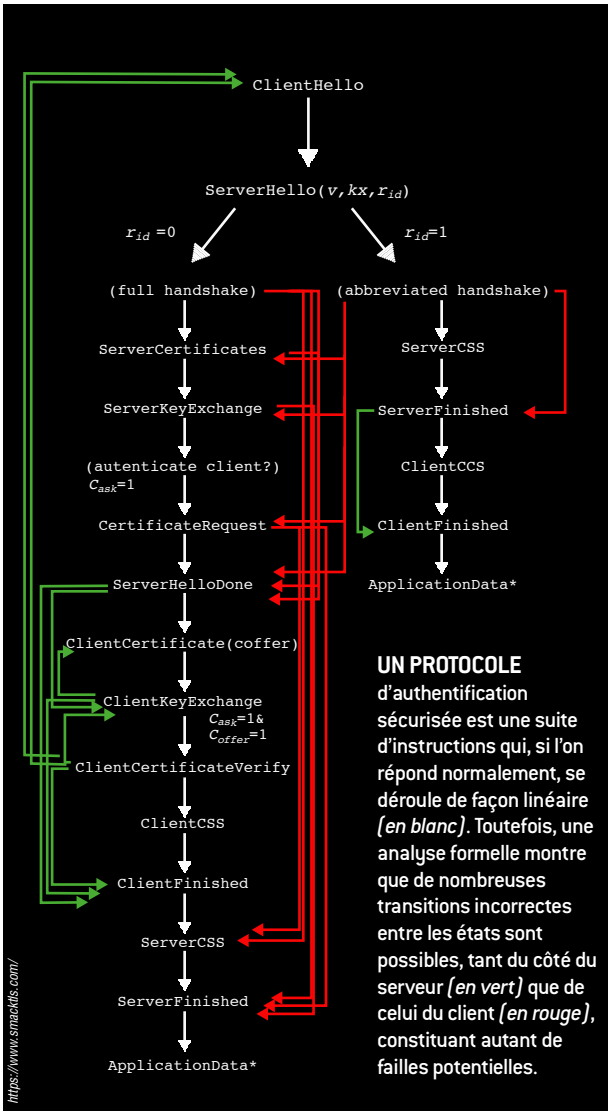
Pour déchiffrer votre message, votre correspondant a aussi besoin de la clé secrète utilisée. Il existe des moyens très malins pour fabriquer des clés secrètes communes à deux personnes et connues d'elles seules. Le protocole dit de Diffie-Hellman en est l'exemple type, mais il est coûteux en temps. En pratique, on obtient une fois pour toutes une clé K' par ce moyen et, pour toutes les autres clés K à partager, on demande au jeton d'encapsuler K en la chiffrant avec K'. Le jeton de votre correspondant déchiffre alors le message encapsulé à l'aide de K' et obtient K. Ainsi, votre clé K est certes sortie de votre jeton de sécurité, mais elle n'a circulé que sous forme chiffrée. De nouveau, la sécurité est assurée… Du moins, c'est ce que l'on pourrait croire.

En 2003, un jeune chercheur de Cambridge, Jolyon Clulow, a découvert une attaque théorique contre les jetons de sécurité. Elle fonctionne en deux étapes. On demande d'abord au jeton d'encapsuler la clé K avec la clé K'. On obtient, hors du jeton, une suite de bits M qui est le résultat du chiffrement de K avec K'. Jusque-là, rien d'utilisable. Mais si l'on demande au jeton de déchiffrer le message M avec la clé K', comme si M était un message chiffré que l'on venait de recevoir d'un correspondant, le jeton renvoie le message déchiffré : la clé K, lisible en clair…

De nombreuses précautions sont prises aujourd'hui pour éviter cette attaque, mais il y en a d'autres. Aussi, la jeune société française Cryptosense a développé un outil qui teste automatiquement votre jeton de sécurité *via* une méthode formelle, puis envoie un rapport de sécurité : pas de pirate à embaucher et une exhaustivité exceptionnelle dans la recherche d'attaques.

Autre exemple : la découverte en mars 2015 de l'attaque FREAK sur les protocoles sécurisés SSL/TLS. FREAK vous fait croire que vous disposez d'une connexion sécurisée avec des sites tels que Amazon ou PayPal, alors même que vous êtes connecté à un autre site, pirate. Même la NSA était vulnérable ! FREAK est une des attaques découvertes par des équipes communes à Inria et Microsoft, à l'aide de modèles fondés sur des machines à états *(des graphes tel celui ci-contre)*. Elles ont montré que les réalisations des protocoles faisaient bien davantage que ce qu'ils spécifiaient, et que ces possibilités supplémentaires étaient à l'avantage d'un attaquant.

Les méthodes formelles permettent d'assurer, sous certaines hypothèses, que votre système est sûr (s'il l'est). Notamment, la société française Prove&Run propose des solutions de sécurisation pour l'Internet des objets, les smartphones et tablettes, à destination des décideurs gouvernementaux ou des grandes entreprises qui ne peuvent se permettre d'être piratés. Ces solutions sont fondées sur des logiciels prouvés. Il faudrait un pirate bien malin pour les contourner.



UN PROTOCOLE d'authentification sécurisée est une suite d'instructions qui, si l'on répond normalement, se déroule de façon linéaire *(en blanc)*. Toutefois, une analyse formelle montre que de nombreuses transitions incorrectes entre les états sont possibles, tant du côté du serveur *(en vert)* que de celui du client *(en rouge)*, constituant autant de failles potentielles.

– Jean Goubault-Larrecq
LSV, CNRS, ENS, Cachan