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.

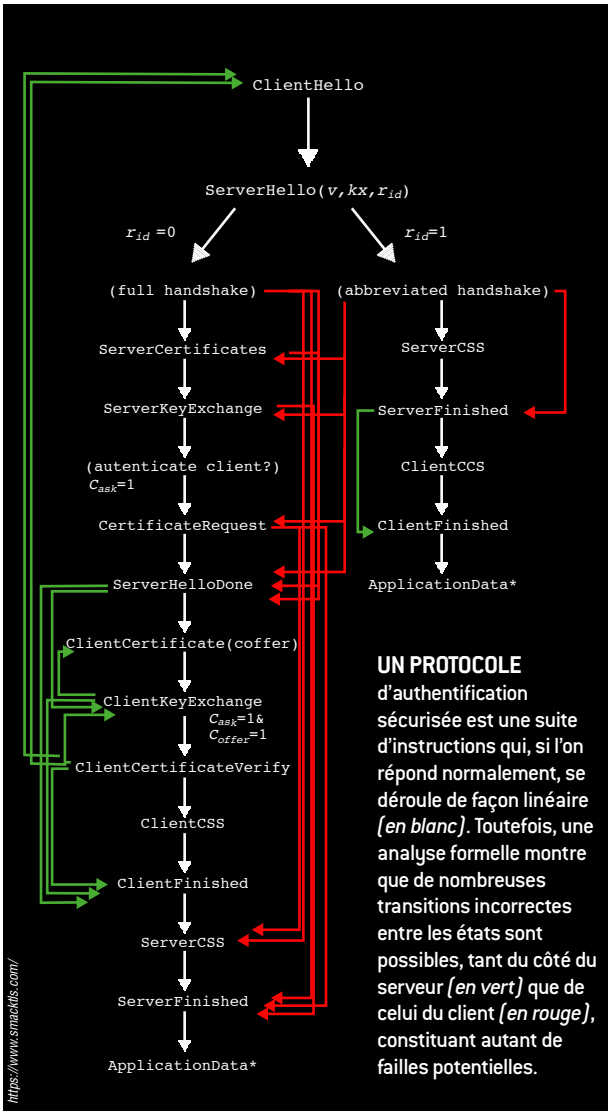
Pour déchiffrer votre message, votre correspondant a aussi besoin de la clé secrète utilisée. Il existe des moyens très malins pour fabriquer des clés secrètes communes à deux personnes et connues d'elles seules. Le protocole dit de Diffie-Hellman en est l'exemple type, mais il est coûteux en temps. 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

© Pour la Science - n° 459 - Janvier 2016

– les *bug bounty programs* ou *vulnerability reward programs*. Ces programmes offrent des primes aux chercheurs indépendants qui signalent des vulnérabilités ou des problèmes de sécurité. Netscape Communications a créé le premier programme de prime à la découverte de bugs en 1995 afin de repérer les éventuels défauts du navigateur Netscape. Aujourd'hui, vingt ans plus tard, la recherche a montré que cette stratégie est une des mesures les plus rentables que la société et sa successeure, Mozilla, aient prises pour renforcer la sécurité. Les communautés privées et publiques de professionnels de la sécurité partagent leurs informations sur les logiciels malveillants, les menaces et les vulnérabilités. Elles créent ainsi une sorte de système immunitaire distribué.

À mesure que le cyberespace s'étend, constructeurs automobiles, entreprises de matériel médical, fournisseurs d'installations de cinéma à domicile et autres vont devoir raisonner comme des sociétés de cybersécurité. Cela suppose d'intégrer la sécurité dans la recherche et le développement, d'investir dans la sécurité des produits et des services dès la phase de conception, et non en fin de développement ou en réponse à des injonctions gouvernementales. Là encore, la communauté des hackers peut apporter sa contribution. En 2013, par exemple, les experts américains en sécurité Joshua Corman et Nicholas Percoco ont lancé le mouvement « I Am The Cavalry », pressant les pirates de s'engager dans une recherche responsable des failles de sécurité, notamment dans les domaines critiques tels que les infrastructures publiques, les équipements médicaux ou automobiles et les technologies domestiques connectées. Une autre initiative – BuildItSecure.ly –, à l'instigation des chercheurs en sécurité Mark Stanislav et Zach Lanier, vise à créer une plateforme pour développer des applications sécurisées de l'Internet des objets.

La bonne nouvelle est que ce système immunitaire distribué est de plus en plus solide. En janvier, Google a lancé un nouveau programme qui complète son programme de prime à la découverte de bugs, offrant des subventions pour encourager les chercheurs en sécurité à vérifier les produits de la compagnie. Cette décision montre que même des entreprises ayant recruté les meilleurs talents en technologie bénéficient du regard extérieur de pirates bien intentionnés. Certains gouvernements font de même. Ainsi, le Centre national néerlandais de cybersécurité a établi son propre programme de divulgation responsable, qui permet aux pirates de signaler des vulnérabilités sans risque de représailles juridiques.

Aux États-Unis, la mauvaise nouvelle est que certains éléments de l'approche cybersécuritaire du gouvernement pourraient *de facto* criminaliser les pratiques et les outils classiques de la recherche de vulnérabilités, ce qui affaiblirait le système immunitaire. Beaucoup d'acteurs de la sécurité craignent que la version actuelle de la loi *Computer Fraud and Abuse* (Fraude et malveillance informatiques) et les modifications proposées donnent une définition si large du piratage que le simple fait de cliquer sur un lien vers un site web contenant des fuites ou des informations volées soit considéré comme du trafic de biens volés. Cette criminalisation du travail des chercheurs indépendants nous ferait du tort à tous et aurait peu d'effet sur les criminels mus par le profit ou l'idéologie.

Quelques règles de cyberhygiène

Les prochaines années pourraient être critiques. Le nombre de violations de données va augmenter et un ardent débat aura certainement lieu pour savoir quel pouvoir sur le monde numérique céder aux gouvernements en échange de sécurité. En fait, on ne pourra sécuriser le cyberespace sans combiner des solutions de diverses natures : techniques, légales, économiques et politiques. Et cela dépend aussi de nous, le grand public. En tant que consommateurs, nous devrions exiger que les entreprises rendent leurs produits plus sûrs. En tant que citoyens, nous devrions tenir nos gouvernements pour responsables quand ils affaiblissent volontairement la sécurité. Et en tant que points individuels de failles potentielles, nous avons la responsabilité de sécuriser nos installations.

Pour se défendre, il existe des mesures simples, telles que mettre à jour nos logiciels, utiliser des sites Web sécurisés et activer l'authentification à deux facteurs sur nos comptes de courriel et de réseaux sociaux. Mais cela suppose aussi d'être conscient que chacun de nos appareils est un nœud d'un vaste système et que les choix que nous faisons à notre petite échelle peuvent avoir des effets bien plus importants. La cybersécurité est comme la santé publique. Lavez-vous les mains, vaccinez-vous, et vous ne transmettrez pas les infections. ■

Le bug Heartbleed

Le 7 avril 2014, l'annonce de la faille Heartbleed dans la bibliothèque de cryptographie OpenSSL a soufflé un vent de panique chez les administrateurs systèmes. Durant deux ans, OpenSSL a présenté une vulnérabilité, introduite lors d'une amélioration. Il s'agit d'un bug d'implémentation. Heartbeat, une extension du protocole au cœur d'OpenSSL (SSL), récupère chez le client un message qui sert juste à vérifier que la connexion est active : il envoie un message basique au terminal client, qui lui répond. En utilisation normale, le message a deux parties : une suite d'octets et deux octets indiquant sa longueur. Mais dans Heartbleed, la longueur indiquée était bien plus grande que celle de la suite. En retour, le terminal client répondait un message de même longueur contenant la suite d'octets, comme en temps normal, mais aussi les octets suivants dans la mémoire, jusqu'à la longueur indiquée : avec de la chance, les identifiants utilisés…

BIBLIOGRAPHIE

K. Zetter, **Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon**, Crown, 2014.

J. Healey (éd.), **A Fierce Domain : Conflict in Cyberspace, 1986 to 2012**, Cyber Conflict Studies Association, 2013.

L'ère d'Internet, *Dossier Pour la Science*, n° 66, janvier-mars 2010.