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.

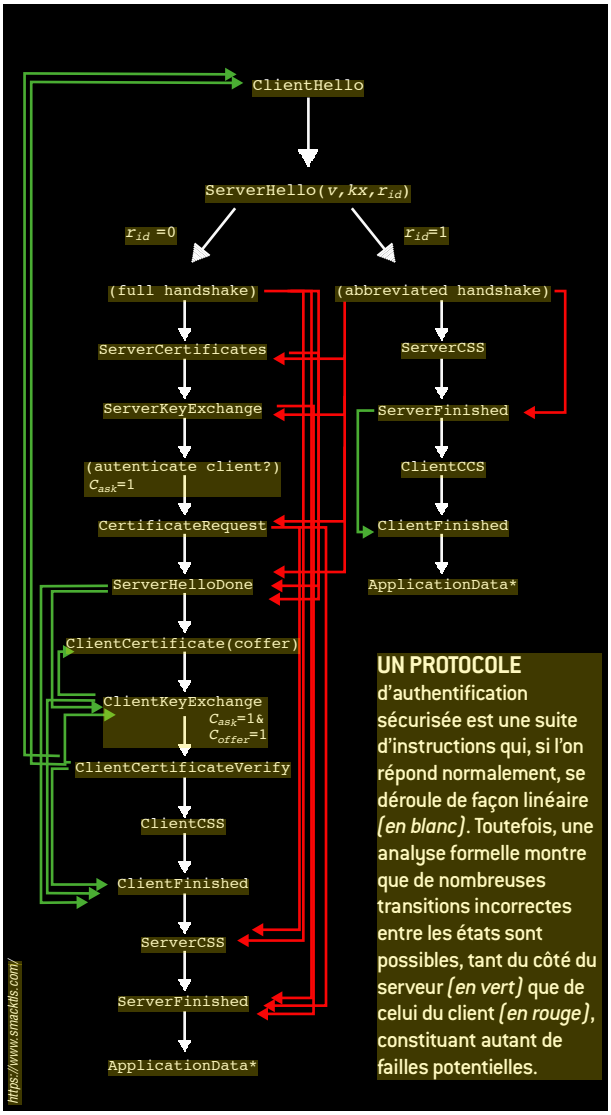
Pour déchiffrer votre message, votre correspondant a aussi besoin de la clé secrète utilisée. Il existe des moyens très malins pour fabriquer des clés secrètes communes à deux personnes et connues d'elles seules. Le protocole dit de Diffie-Hellman en est l'exemple type, mais il est coûteux en temps.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