

# Exploits en cascade sur la sécurité informatique

LE MONDE SCIENCE ET TECHNO | 26.10.2015 à 16h06 • Mis à jour le 27.10.2015 à 06h39 | Par David Larousserie

(/journaliste/david-larousserie/)



KACPER PEMPEL /REUTERS

Coup sur coup, la sécurité d'Internet a tremblé sur ses bases. Plusieurs systèmes garantissant la sûreté des échanges entre machines ont été attaqués. Non par des pirates, mais par des chercheurs tout ce qu'il y a de plus académiques. Ces derniers ont trouvé et exploité des failles dans les protocoles utilisés sur le réseau des réseaux quand les communications à un site Web sont chiffrées, comme l'internaute le constate par exemple en se connectant à des adresses commençant par « https » plutôt que par « http ».

Plus précisément, la première attaque, baptisée Logjam, concerne une phase de dialogue entre ordinateurs en vue de chiffrer des messages. La seconde porte sur la signature de ces messages à des fins d'authentification.

L'étude sur Logjam, présentée le 13 octobre à Denver (Colorado) par une équipe américano-française associant l'Inria, le CNRS, Microsoft, les universités du Michigan et de Pennsylvanie, a reçu le Prix du meilleur article de cette conférence.

## Logarithme discret

Les chercheurs s'en sont pris à un protocole incontournable appelé Diffie-Hellman, qui permet à deux personnes de partager un nombre secret en échangeant publiquement d'autres nombres. Magique ? Non. Cela fonctionne grâce à une fonction mathématique, qu'il est plus facile d'effectuer dans un sens plutôt que dans l'autre. Il est ainsi « aisé » d'élever un nombre entier à une certaine puissance, mais difficile de retrouver l'exposant en ne connaissant que le résultat. Ce problème est connu sous le nom de logarithme discret.

Première étape, les chercheurs ont « inversé » la fonction mathématique difficile et trouvé les nombres secrets, les « clés », permettant de leurrer n'importe quel interlocuteur. Ils l'ont fait avec des clés de 512 bits (environ 150 chiffres). Le deuxième exploit a été de trouver une faille qui force les deux parties à utiliser une clé de plus petite taille que celle recommandée. Internet, pour rester

accessible y compris par de vieilles machines, tolère d'abaisser les garde-fous de sécurité...

## La même clé pour 70 000 sites

Troisième étape qui peut surprendre : beaucoup de serveurs utilisent les mêmes grands nombres dans ces procédures mathématiques. Dès lors, casser une clé ouvre la porte à beaucoup de machines ! 70 000 sites parmi les plus visités utilisent la même clé, estiment les chercheurs. Cela facilite la tâche des attaquants. Pour résoudre le problème du logarithme discret, une lourde étape de calculs en amont est nécessaire sur la clé visée. Cette phase prend une semaine, alors que le casse final de la clé de 512 bits ne prend que quelques minutes de calcul. « *C'est peut-être comme cela que l'agence américaine NSA a pu déchiffrer des échanges* », estime Emmanuel Thomé, coauteur de l'étude à l'Inria-Nancy. Les chercheurs ont même estimé que, pour des clés deux fois plus grandes que celles qu'ils ont cassées, il en coûterait de l'ordre de quelques centaines de millions de dollars « *seulement* ».

Deuxième pilier à être secoué par la recherche académique : le « hachage ». Derrière ce nom barbare se cachent là aussi des fonctions mathématiques qui transforment un fichier fait de longues séries de 0 et de 1 en de plus petites suites faciles à manipuler. Elles sont comme des empreintes digitales du fichier initial. Par exemple, les mots de passe ne sont pas stockés en clair dans les serveurs, mais sous forme de « hachés ». Et les connexions sont ainsi « signées » entre ordinateurs.

## Correctifs

Créer une fausse signature ayant le même « haché » que la vraie serait catastrophique pour la sécurité. Le 8 octobre Marc Stevens (CWI, Pays-Bas), Pierre Karpman (Inria-Rennes) et Thomas Peyrin (NTU-Singapour) y sont arrivés. Plus exactement, ils ont franchi une étape importante dans cette direction, en s'en prenant au cœur d'une des fonctions de hachage encore très utilisée, SHA-1. Il existait depuis dix ans des attaques théoriques sur celle-ci, mais elles semblaient irréalisables. Les chercheurs l'ont fait pour moins de 120 000 dollars (106 000 euros)... « *Nous voulions alerter sur cette faille pour éviter que se reproduise l'histoire de la fonction de hachage précédente, MD5 : son remplacement a pris plus de dix ans, alors que des vulnérabilités avaient été démontrées* », explique Pierre Karpman.

SHA-1 devrait disparaître au 1<sup>er</sup> janvier 2016 pour certaines procédures, mais son successeur, SHA-2, s'est déjà répandu. Quant à Logjam, des correctifs ont été apportés sur les navigateurs pour que des clés de niveaux plus faibles que ceux recommandés ne soient pas autorisées. Pour cette fois, les protocoles d'Internet semblent sauvés.