SHA-1 : un algorithme clef du chiffrement HTTPS n'est plus sécurisé

SHA-1, un des principaux algorithmes de cryptage employé sur Internet – notamment pour les connexions HTTPS -, est trop friable à un nouveau type d'attaques et doit être remplacé. C'est en tout cas ce qu'affirme une équipe de chercheurs réunissant **Pierre Karpman de l'Inria** (qui, pour ces travaux, a reçu l'appui financier de la Direction Générale de l'Armement), **Thomas Peyrin** (NTU, Singapour) et **Marc Stevens** (CWI, Pays-Bas).

En réalité, la faiblesse de SHA-1 était déjà connue des spécialistes, les principaux navigateurs Internet ayant d'ailleurs prévu de ne plus accepter de signatures basées sur cet algorithme à partir de janvier 2017. Une échéance trop lointaine, assurent aujourd'hui les chercheurs qui expliquent qu'une attaque à des coûts accessibles par une organisation cybercriminelle est possible bien avant cette date. La découverte est d'importance car les chercheurs estiment qu'environ 28 % des certificats en circulation s'appuient sur SHA-1, un algorithme de hachage conçu par la NSA américaine en 1995.

Ces fonctions dites de hachage prennent des données en entrée et les injectent dans une empreinte, servant de signature cryptographique au message de départ. Une fonction de hachage n'est utile que si deux messages en entrée, même très proches, aboutissent à des empreintes très différentes. Si tel n'est pas le cas, on parle alors d'un phénomène dit de collision, ce qui compromet la sécurité de l'algorithme tout entier. Un assaillant étant alors en mesure de créer une signature (une empreinte), autrement dit de se faire passer pour ce qu'il n'est pas, mettant en péril les communications chiffrées (e-commerce, banque en ligne…).

100 000 dollars seulement au tarif AWS

La puissance de ce type d'attaque a été démontrée dans le passé par le malware Flame, à l'origine conçu probablement par les Etats-Unis et Israël pour espionner l'Iran. Cette menace utilisait une attaque par collision contre un autre algorithme de hachage, MD5, pour compromettre le mécanisme de mise à jour de Windows Update. Imparable pour signer du code malicieux avec un certificat semblant émaner de Microsoft ! Depuis, MD5 a depuis été largement abandonné pour la création de signatures.

Si SHA-1 est considéré comme bien plus résistant aux collisions que MD5, la communauté scientifique jugeait, jusqu'à présent, qu'il n'était certes pas immunisé contre ce type d'attaques, mais que ces dernières restaient coûteuses à mettre en œuvre. A l'époque, en se basant sur des estimations fournies par l'expert en sécurité Bruce Schneier, les chercheurs avaient évalué qu'une attaque par collision coûterait 700 000 dollars en 2015 et 173 000 en 2018, en raison de la puissance de calcul grandissante accessible. Schneier avait alors jugé que mettre 173 000 dollars sur la table était à la portée des organisations cybercriminelles (sans même parler des services d'espionnage étatiques). D'où la date de retrait de SHA-1.

C'est ce calendrier que vient bousculer la recherche menée par le CWI (Centrum Wiskunde &

Informatica), l'Inria et le NTU (Nanyang Technological University). Cette étude montre en effet que, dès à présent, une attaque par collision contre SHA-1 ne coûterait qu'entre 75 000 et 120 000 dollars (en se basant sur les coûts de location d'instances Amazon EC2 sur quelques mois). Une enveloppe à la portée d'une organisation mafieuse bien financée. Pour abaisser le coût de leur attaque par force brute, Pierre Karpman, Marc Stevens et Thomas Peyrin exploitent la puissance des cartes graphiques pour mettre en place une technique dite « du boomerang » afin d'identifier des collisions dans SHA-1. « *Nous avons montré comment les cartes graphiques peuvent être exploitées très efficacement dans ce type d'attaques* », explique Pierre Karpman.

SHA-1 : un Titanic qui a heurté l'iceberg

Cette nouvelle estimation des coûts s'appuie sur une attaque réussie contre la fonction de compression de SHA-1, menée avec un cluster de 16 noeuds basé sur du« *matériel bon marché et largement disponible* » (photo ci-contre). Si l'algorithme lui-même n'a pas été compromis, c'est une entaille sévère dans sa sécurité et une démonstration de la puissance des techniques d'attaque par force brute reposant sur des cartes graphiques (GPU). Un des chercheurs compare ainsi les résultats de cette étude sur SHA-1 à la collision d'un bateau avec un iceberg : « *nous savons que la voie d'eau est importante, que les flots s'engouffrent rapidement à l'intérieur du navire et que ce dernier va couler, tout prochainement* », dit Ronald Cramer, qui dirige le groupe spécialisé en cryptographie du CWI.

« *Nos nouvelles projections à base de GPU sont aujourd'hui plus sûres et significativement en dessous des estimations de Bruce Schneier*, écrivent les chercheurs. *Plus inquiétant, elles sont théoriquement déjà à la portée des ressources estimées d'un syndicat du crime, environ deux ans avant la date anticipée, et un an avant que SHA-1 ne soit identifié comme non sécurisé par les navigateurs Internet modernes. C'est pourquoi nous pensons que la migration de SHA-1 aux algorithmes de hachage sécurisés SHA-2 et SHA-3 doit être anticipée.* »

SHA-1 : durée de vie prolongée… malgré tout ?

La publication de cette étude, la semaine dernière, intervient au moment où les autorités de certification et les éditeurs de navigateurs étudient, au sein du CA/Browser Forum, une proposition visant à étendre la permission d'émettre des certificats HTTPS basés sur SHA-1. Celle-ci pourrait alors courir jusqu'à la fin de l'année prochaine plutôt que jusqu'en janvier 2016. La migration vers SHA-2 est complexe (il faut réémettre les certificats), avancent les promoteurs de cette proposition pour justifier leur projet. La publication de Pierre Karpman, Marc Stevens et Thomas Peyrin met la pression sur le vote de cette extension, vote qui se termine demain, le 16 octobre.

Marc Stevens, du CWI néerlandais, est un pionnier des attaques par collision. Il était membre de

l’équipe de 7 chercheurs qui, en 2008, a mis en œuvre la première démonstration pratique de ce qui était connu depuis longtemps sur le plan théorique. Avec 200 Playstation 3, cette équipe était parvenue à construire une autorité certificatrice pirate, reconnue par les navigateurs et systèmes d’exploitation, en s’attaquant à MD5.

A lire aussi :

Chiffrement : tous les navigateurs vont abandonner l’algorithme RC4

Le chiffrement source de multiples failles de sécurité

E. Thomé, Inria : « Les clefs de chiffrement de 768 bits ne suffisent plus »

LogJam : nouvelle faille dans le chiffrement des sites Web

Crédit photo : Maksim Kabakou / Shutterstock