ANDREA DANTI - FOTOLIA

Appel à un abandon plus rapide de SHA-1

par
Valéry Marchive
Rédacteur en chef adjoint

Publié le 12 oct. 2015

Des chercheurs appellent à un abandon accéléré de l'algorithme de chiffrement SHA-1 au profit de son successeur. Selon eux, la barrière à l'entrée pour le casser n'est plus dissuasive.

Des chercheurs du Centrum Wiskunde & Informatica (CWI) d'Amsterdam, d'Inria en France, et l'université technique de Nanyang à Singapour, viennent de publier une lettre ouverte appelant l'industrie IT à agir rapidement : « le standard de sécurité Internet SHA-1 devrait être retiré plus tôt, parce que le coût pour le casser est significativement plus bas qu'imaginé précédemment ».

Comme ils le rappellent, l'algorithme de chiffrement SHA-1 est utilisé pour « les signatures électroniques, qui sécurisent les transactions par cartes de crédit, la banque en ligne et la distribution de logiciels ».

Mais celui-ci n'est pas parfait et commence à montrer ses limites, notamment du fait de son âge. Publié en 1995, SHA-1 a d'ailleurs fait l'objet d'un avertissement du Nist américain, début 2014 : selon l'institut de standardisation américain, l'algorithme ne devrait déjà plus être utilisé pour la signature électronique. Pourquoi ? Parce que sa résistance aux attaques par collision atteint ses limites. Ce type d'attaque consiste à chercher deux messages en entrée produisant la même valeur de hash.

Mais jusqu'ici, le coût nécessaire pour conduire ce type d'attaque avec succès sur SHA-1 était considéré comme suffisamment élevé pour être rédhibitoire. Les signataires de l'appel rappellent ainsi que, en 2012, Bruce Schneier estimait qu'il faudrait investir 700 000 $, cette année, pour réussir à casser SHA-1. Un coût dont l'expert s'attendait à ce qu'il chute à 173 000 $ en 2018.

Mais pour les chercheurs, la technologie a progressé et baissé de prix bien plus rapidement : « nous estimons désormais qu'une collision SHA-1 complète coûtera entre 75 000 et 120 000 $ en louant Amazon EC2 sur plusieurs mois, à ce jour, au début de l'automne 2015 ». Et de retirer une conclusion simple : « les collisions sont déjà accessibles aux syndicats criminels, près de deux ans avant ce qui était précédemment anticipé ».

Initialement, les navigateurs Web devaient faire l'impasse sur SHA-1 au profit de son successeur, SHA-2, en janvier 2017. Une demande vient d'être formulée pour que l'émission de certificats SHA-1 puisse se faire jusqu'à la fin 2016. Les trois chercheurs à l'origine de la lettre ouverte s'y opposent.