Une deuxième attaque par collision encore plus puissante que la première fait tomber

Les chercheurs demandent d'arrêter l'utilisation de l'algorithme de hachage

Le 8 janvier 2020 à 19:50, par Stéphane le calme (https://www.developpez.com/user/profil/616766/Stephane-le-calme)

35 commentaires (https://www.developpez.net/forums/d1652514-2/webmasters-developpement-web/general-conception-tomber-sha-1/#post11313394)

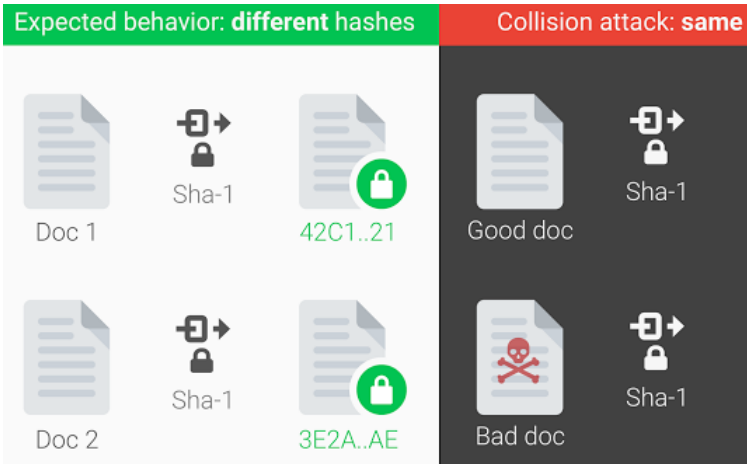
En 1995, SHA-1 (Secure Hash Algorithm), l'algorithme de hachage cryptographique conçu par la NSA, a été publié par le gouverne SHA-1 venait remplacer SHA-0 qui a été rapidement mis de côté par le NIST (Institut national des normes et de la technologie, ur sécurité insuffisante.

Néanmoins, avec les années, SHA-1 n'a plus été considéré comme sûr face à des adversaires disposant de moyens importants, c'est ce théoriques. Aussi, l'institut américain des standards avait déclaré SHA-1 obsolète en 2011. Il n'en a pas fallu beaucoup plus aux principaux r Mozilla ont annoncé la fin du support de SHA-1 sur leurs produits respectifs.

En 2017 (https://www.developpez.com/actu/119391/Arretez-d-utiliser-SHA-1-Des-chercheurs-affirment-etre-parvenus-a-casser-l-algorithme composée de chercheurs issus du Centrum Wiskunde et Informatica (CWI, Pays-Bas) et de Google a annoncé avoir mis au point une méth l'authenticité des documents numériques. Dans le cadre de la rédaction détaillée de leur réalisation, les chercheurs ont également publié de des hachages SHA-1 identiques, mais affichant des contenus différents.

L'une des propriétés des fonctions cryptographiques est le fait qu'elles sont unidirectionnelles ; en clair, il n'est pas possible de retrouver la c chaînes de caractères différentes donneront systématiquement deux hash différents. C'est cette théorie que les chercheurs sont parvenus à d

Google explique qu'une collision se produit lorsque deux morceaux de données distinctes (un document, un binaire ou un certificat de site expliqué plus haut, les collisions ne devraient jamais se produire pour des fonctions de hachage sécurisées. Cependant, si l'algorithme de hac une collision. L'attaquant pourrait alors utiliser cette collision pour tromper les systèmes qui s'appuient sur les hachages et leur faire accepte contrats d'assurance avec des termes radicalement différents. Les attaquants pourraient également créer une mise à jour logicielle fraudul valide les mises à jour en vérifiant les signatures numériques.



Trois ans plus tard, une équipe de chercheurs a révélé une attaque encore plus forte que la première. La nouvelle collision offre aux attaq précédente. Elle permet de créer des clés de chiffrement PGP qui, lorsqu'elles sont signées numériquement à l'aide de l'algorithme SHA-1, us hachage pour deux ou plusieurs entrées choisies par l'attaquant en ajoutant des données à chacune d'entre elles. L'attaque dévoilée mardi ne 2017, en revanche, n'a pas permis de falsifier des préfixes prédéterminés de documents spécifiques et a été évaluée à un coût de 110 000 avec laquelle les adversaires voulaient l'exécuter.

La nouvelle attaque est importante. Bien que SHA-1 ait été progressivement abandonné au cours des cinq dernières années, il est loin d'être pour certifier les clés PGP dans la branche héritée de la version 1.4 de GnuPG, le successeur open source de l'application PGP pour chiffrer les par la branche GnuPG moderne jusqu'à récemment, et n'ont été rejetées qu'après que les chercheurs à l'origine de la nouvelle collision eurent

Et l'équipe d'expliquer que : « Nous avons calculé la toute première collision avec préfixe choisi pour SHA-1. En résumé, cela signifie une i implications pratiques dangereuses si vous utilisez toujours cette fonction de hachage. Pour le dire autrement: toutes les attaques considérablement amélioré la complexité des attaques SHA-1, avec un facteur d'accélération d'environ 10 ».

Qu'est-ce qu'une collision à préfixe choisi ?

Une collision classique (ou collision à préfixe identique) pour une fonction de hachage H est simplement deux messages M et M' qui conduis sécurité est fondamentale en cryptographie, l'exploitation d'une collision classique pour les attaques est difficile en pratique.

Une collision à préfixe choisi est un type de collision plus contraint (et beaucoup plus difficile à obtenir), où deux préfixes de message P et P calculer deux messages M et M' tel que H (P || M) = H (P' || M'), où || désigne la concaténation.

Avec une telle capacité, l'attaquant peut obtenir une collision même si les préfixes peuvent être choisis arbitrairement (et donc contenir important lorsque la fonction de hachage est utilisée dans un schéma de signature numérique, l'une des utilisations les plus courantes d'une fo

Dans un article présenté au Real World Crypto Symposium de cette semaine à New York, les chercheurs ont averti que même si l'utilisation d cela va laisser les utilisateurs vulnérables aux attaques potentielles. Les chercheurs ont déclaré que leurs résultats soulignaient l'importance d

« Ce travail montre définitivement que SHA-1 ne doit pas être utilisé dans un protocole de sécurité où une sorte de résistance aux collisio « L'utilisation continue de SHA1 pour les certificats ou pour l'authentification des messages de négociation en TLS ou SSH est dangereuse et cassé depuis 2004, mais il est toujours utilisé dans de nombreux systèmes de sécurité ; nous conseillons vivement aux utilisateurs de supprim

Source : équipe de chercheurs (https://sha-mbles.github.io/), article technique (https://eprint.iacr.org/2020/014.pdf)

Voir aussi :

➔ Les mises à jour de Windows 7 et Server 2008 vont nécessiter le support de SHA-2 à partir de juillet 2019, l'algorithme SHA-1 étant devenu de-Windows-7-et-Server-2008-vont-necessiter-le-support-de-SHA-2-a-partir-de-juillet-2019-l-algorithme-SHA-1-etant-devenu-moins-sur/)
➔ Intel obtient un brevet pour un procédé de minage plus économe en énergie basé sur des ASIC écoénergétiques et l'algorithme de hac brevet-pour-un-procede-de-minage-plus-econome-en-energie-base-sur-des-ASIC-ecoenergetiques-et-l-algorithme-de-hachage-SHA-256/)
➔ Adam Langley : « SHA-3 n'apporte pas grand-chose par rapport à SHA-2, on pourrait s'en passer », la team Keccak répond à l'ingénieur d n-apporte-pas-grand-chose-par-rapport-a-SHA-2-on-pourrait-s-en-passer-la-team-Keccak-repond-a-l-ingenieur-de-Google/)

35 COMMENTAIRES (HTTPS://WWW.DEVELOPPEZ.NET/FORUMS/D1652514-2/WEBMASTERS-DEVELOPPEMENT-WEB/GENERAL-CONCEPT