JANUARY 24, 2020

Critical flaw demonstrated in common digital security algorithm

by Nanyang Technological University

Credit: CC0 Public Domain

Cryptographic experts at Nanyang Technological University, Singapore (NTU Singapore) and the French national research institute for digital sciences INRIA in Paris, have demonstrated a critical security flaw in a commonly used security algorithm, known as SHA-1, which would allow attackers to fake specific files and the information within them, and pass them off as authentic.

The researchers say it lays to rest the ongoing debate about continuing to use SHA-1 as a security algorithm, and they urge companies to quickly move on from using it.

SHA-1 is a hash function, a building block in cryptography used in almost every digital authentication process. They underpin the security of many digital applications in internet banking, web-based communications, and payment portals of online shopping sites.

The hash function takes a lengthy input message and creates a short digital fingerprint for it, called a hash value.

A hash function is considered secure if it is difficult for an attacker to find two different inputs that lead to identical hash values. When two different inputs share the same value, a "collision" is said to have occurred.

SHA-1, a hash function designed by the United States' National Security Agency (NSA) in the early 1990s has been incorporated into many pieces of software and remains in widespread use, but in recent years the security of SHA-1 had been called into question by researchers.

Since 2005, a plethora of security flaws have been theorized and discovered in SHA-1. In 2017, academics from the Dutch research institute Centrum Wiskunde & Informatica (CWI) and Google, generated the first practical SHA-1 hash collision; they showed it was possible to find two different input messages that produced the same SHA-1 hash value.

This computational feat involved using a huge Google-hosted graphics processing units (GPU) cluster, but it did not allow the input messages to be customized at will.

In May 2019, NTU's Associate Professor Thomas Peyrin, who lectures in its School of Physical and Mathematical Sciences, and INRIA's Dr. Gaëtan Leurent, used improved mathematical methods to devise the first-ever "chosen-prefix collision attack" for SHA-1.

Now, using a cluster of 900 GPUs running for two months, the pair have successfully demonstrated their way to break the SHA-1 algorithm using this attack, and have published details of it in a paper on the International Association for Cryptologic Research e-print site.

Both researchers also presented their findings at the Real World Crypto Symposium in January this year at New York City, and warned that even if the use of SHA-1 is low or used only for backward compatibility, it will still pose a high risk for users as it is vulnerable to attacks. The researchers said their results highlight the importance of fully phasing-out SHA-1 as soon as possible.

Their chosen-prefix collision targeted a type of file called a PGP/GnuPG certificate, which is a digital proof of identity that relies on SHA-1 as a hash function.

Led by NTU Assoc Prof Peyrin, the significance of this demonstration is that unlike the 2017 CWI/Google collision, a chosen-prefix collision attack shows how it would be possible to forge specific digital documents so they have a correct fingerprint and could be presented as apparently authentic using SHA-1.

Although SHA-1 is already progressively phased-out by industry, the algorithm is still used in many applications. Now it is demonstrably insecure and the researchers hope that system owners will move quickly to phase out the use of the SHA-1 algorithm.

"Chosen-prefix collision attack means that an attacker can start with any first part for both messages, and freely alter the rest, but the resulting fingerprint values will still be the same, they will still collide," says Assoc Prof Peyrin.

"This changes everything in terms of threat because meaningful data, like names or identities in a digital certificate, can now be counterfeited. We have given an example of its impact with a successful attack on a real system, the PGP (Pretty Good Privacy) Web-of-Trust, which is a well-known key-certification solution.

"As a result of our work, developers of software packages dealing with digital certificates have in the last few months already applied counter-measures in their last versions, treating SHA-1 as insecure. Our hope is that the publication of our study will further encourage industry to quickly move away from all use of such weak cryptographic functions."

Newer hash functions, such as the SHA-2 family of hash functions devised in 2001, are not affected by the attack.

Assoc Prof Peyrin and his team hope to improve digital security used in other everyday digital products and services: "Moving forward, we will continue to analyze the algorithms that keep our everyday digital applications secure as more services around the world become digitized.

"Our work illustrates the fact that keeping computers secure is not only about developing new cryptographic schemes, but also keeping up with the latest ways to break older schemes. As mathematical and computational methods improve, it is extremely important to discard methods that can no longer be relied upon."

"Cryptanalysis, the art of breaking cryptosystems, is a vital part of the security ecosystem—the more analysis you do on a cryptographic design, the more confidence you will have about deploying and using it in your products and services," added Assoc Prof Peyrin.

More information: SHA-1 is a Shambles – First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust, *International Association for Cryptologic Research*. sha-mbles.github.io/Shambles_RWC.pdf