THE NATIONAL TRIBUNE

Critical flaw demonstrated in common digital security algorithm

Science | 24 Jan 2020 12:28 pm AEST   Share

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 theorised 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 customised 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