CWI, Google announce first collision for Industry Security Standard SHA-1

23 February 2017, by 'industry Deprecation Proved To Be Too Slow'

Credit: shatterered.io

Today, researchers at the Dutch research institute CWI and Google jointly announce that they have broken the SHA-1 internet security standard in practice. This industry standard is used for digital signatures and file integrity verification, which secure credit card transactions, electronic documents, GIT open-source software repositories and software distribution. CWI cryptanalyst Marc Stevens says: "Many applications still use SHA-1, although it was officially deprecated by NIST in 2011 after exposed weaknesses since 2005. Our result proves that the deprecation by a large part of the industry has been too slow and that migration to safer standards should happen as soon as possible".

The joint effort headed by Marc Stevens (CWI) and Elie Bursztein (Google) started more than two years ago to realize Stevens' advanced cryptanalytic research in practice with Google's computing infrastructure. They now successfully broke the industry standard SHA-1 using a so-called collision attack. SHA-1 is a cryptographic algorithm designed by the NSA and was standardized by NIST in 1995 to securely compute message fingerprints. These fingerprints are used in the computation of digital signatures, which are fundamental to Internet security, such as HTTPS (TLS,SSL) security, electronic banking, signing documents and software. Collisions – different messages with the same fingerprint – can lead to forgeries of digital signatures. For instance, a SHA-1 signature obtained for one file can also be misused as a valid signature for any other colliding file.

The SHA-1 collision announced today is the culmination of a research line initiated at CWI more than seven years ago to develop an optimal practical collision attack against SHA-1. This previously resulted in the currently best known theoretical attack by Stevens in 2012 on which the announced result has built further upon. Elie Bursztein says: "Finding the collision in practice took a lot of effort both in building the cryptanalytic attack and in its large scale execution. It required over 9,223,372,036,854,775,808 SHA1 computations that took 6,500 years of CPU computation and 100 years of GPU computations. Yet this is more than 100,000 times faster than a brute force attack. We used the same infrastructure that powers many Google AI projects including Alpha Go and Google Photo as well as Google Cloud".

Stevens says: "Lessons should have been learned from the warnings about similar attacks against SHA-1's predecessor MD5, such as the creation of a rogue Certification Authority in 2009 by an international team I was part of, and an attack by nation states in 2012 to craft malicious Windows updates to infect targeted machines in the Middle-East for espionage, which I showed to be a – then unknown – cryptographic attack variant." In the fall of 2015 Stevens, together with two co-authors, warned that finding a SHA-1 collision might cost around $75K-$120K by exploiting low-cost GPU resources on Amazon EC2, which was significantly cheaper than previously expected.

The team's collision is used to create two different PDF files with the same SHA-1 fingerprint but chosen distinct visible contents, for instance two contracts with substantially different financial fees. Following the responsible disclosure process, the team will wait 90 days before releasing a PDF generator that will allow anyone to create lookalike

PDF document pairs of their choice using the team's collision.

Provided by Centrum Wiskunde & Informatica

To help prevent misuse by such forged PDF documents, the team offers a free online tool to scan for SHA-1 collisions in documents, which is based on Stevens' 2013 counter-cryptanalysis technique to detect whether any given single file has been created with a cryptanalytic collision attack. It can be found on: shattered.io/ . The same protection for PDF documents is now automatic for Gmail and Google Drive users. To defend against SHA-1 collision attacks systems must migrate to SHA-2 or SHA-3. In the case of HTTPS, the effort to move from SHA-1 certificates to SHA-2 certificates began in 2015. And starting this year browsers will mark SHA-1 based certificates as insecure. Similarly, backup systems and document signatures systems should be transitioned to SHA-2.

This result is the product of a long term collaboration between the Cryptology Group at Centrum Wiskunde & Informatica – the national research institute for mathematics and computer science in the Netherlands - and the Google Research Security, Privacy and Anti-abuse Group. Two years ago Marc Stevens and Elie Bursztein, leader of Google's anti-abuse research team, began collaborating on making Marc's cryptanalytic attacks against SHA-1 practical using Google infrastructure. Since then many CWI researchers and Googlers have helped make this project possible, including Pierre Karpman (CWI) who worked on the cryptanalysis and prototype GPU implementation, and from Google Ange Albertini who developed the PDF attack, Yarik Markov who took care of the distributed GPU code and Clement Blaisse who oversaw the reliability of the computations.

More details about the SHA1 attack, how to detect it and the research paper detailing the attack is available at https://shattered.io/.

More information: For the research paper, please refer to shattered.io