CSCI 531 Spring 2019

Mukesh Dangi

-

What is SHA-1 ?

- A cryptographic hash function(**Secure Hash Algorithm**) which takes an input and produces a 160-bit (20-byte) hash value or a message digest.
- SHA-1 was a widely used 1995 NIST cryptographic hash function standard.
- Widely used for document and TLS certificate, signatures, software updates, versioning system(git/svn) for integrity and backup purposes.

- Officially deprecated by NIST in 2011 due to fundamental security weaknesses. Despite its deprecation, SHA-1 remained widely used.

- Why ?

Companies were reluctant, and assumed that finding an actual collision is impractical by brute force attack.

What is SHATTERED

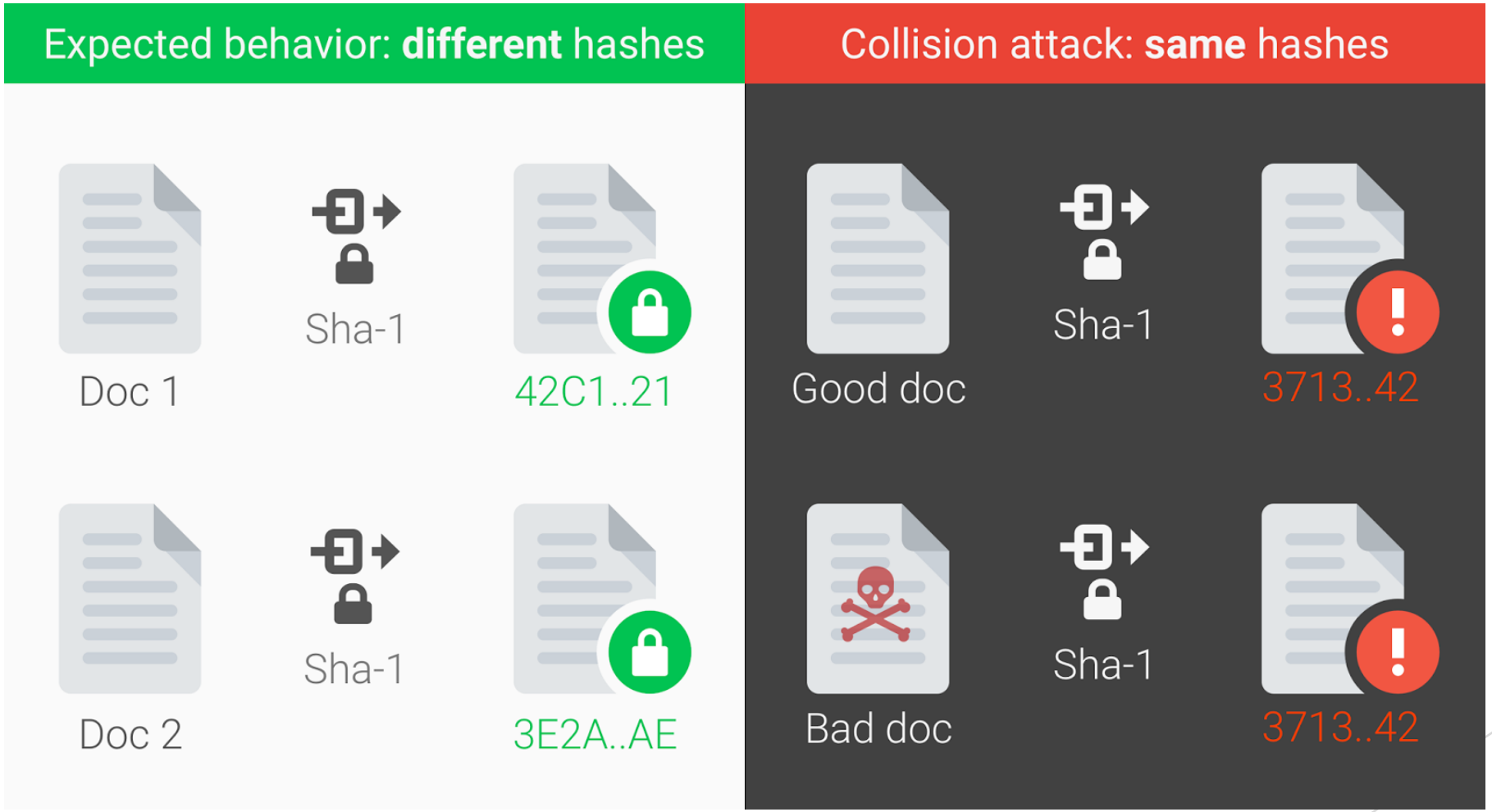
On 23 February 2017, the CWI and Google announced the SHAttered attack, in which they generated two different PDF files with the same SHA-1 hash in roughly $2^{63.1}$ SHA-1 evaluations.

This attack is about 100,000 times faster than brute forcing a SHA-1 collision with a birthday attack, which was estimated to take 280 SHA-1 evaluations

Birthday paradox is a inherent weakness in all hashes, including SHA-1.

Obtain a SHA-1 digital signature on the first PDF file which can also be abused as a valid signature on the second PDF file.

What is SHATTERED



Computing power to break ?

- Generate two documents with arbitrary distinct visual contents, but that would hash to the same SHA-1 digest.
- Here are some numbers that give a sense of how large scale this computation was:

a) Nine quintillion (9,223,372,036,854,775,808) SHA1 computations in total.

b) This attack required "the equivalent processing power as 6,500 years of single-CPU computations and 110 years of single-GPU computations

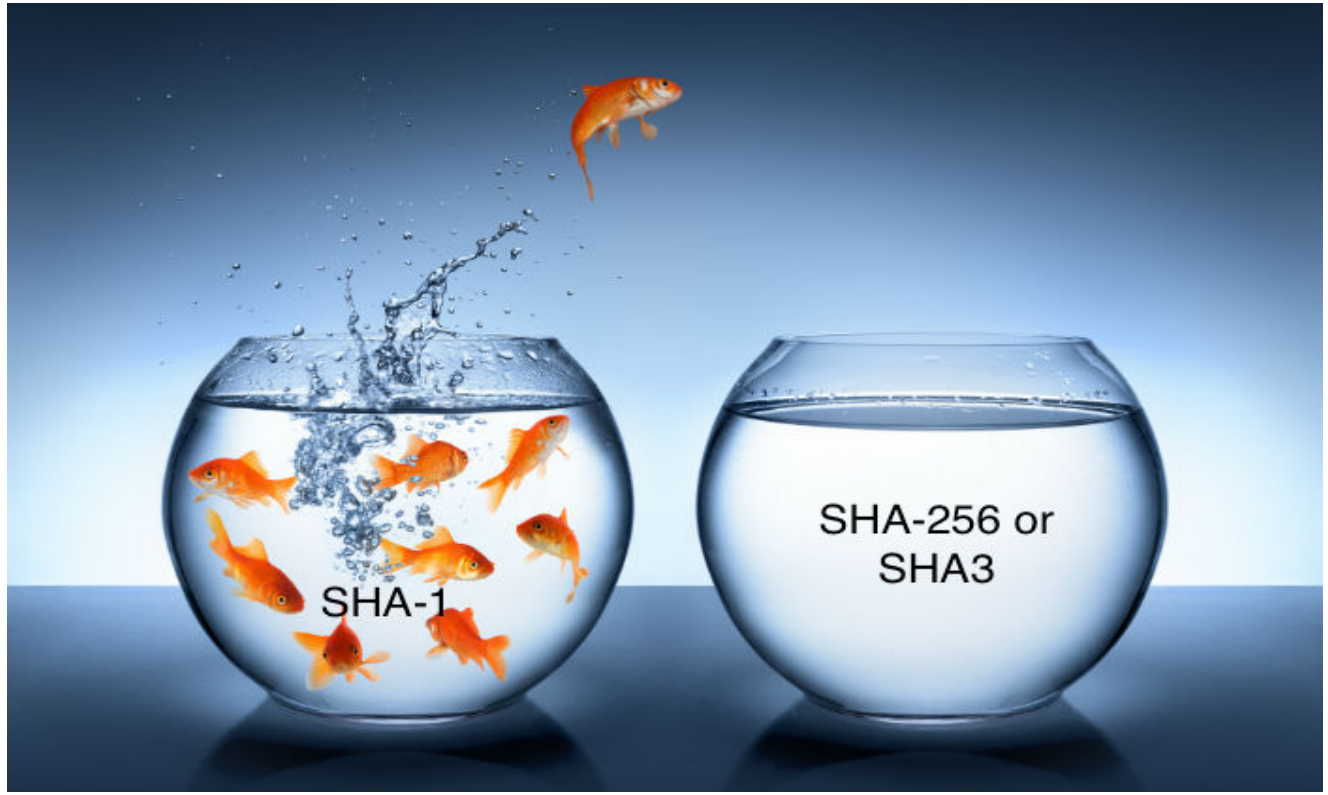
Google leveraged its technical expertise and cloud infrastructure to compute the collision which is one of the largest computations ever completed.

While those numbers seem very large, the SHA-1 shattered attack is still more than 100,000 times faster than a brute force attack which remains impractical.

Potentially impacted systems

- Applications which rely on SHA-1 for digital signatures, file integrity, or file identification, software updates/downloads are potentially vulnerable.
- Digital Certificate signatures
- Email PGP/GPG signatures
- Software vendor signatures
- Software updates
- ISO checksums
- Backup systems
- Deduplication systems
- GIT/SVN

Escape



- Consider using safer alternatives, such as SHA-256, or SHA-3.

Reference

- https://shattered.io/ and https://shattered.it/
- https://en.wikipedia.org/wiki/SHA-1
- https://www.howtogeek.com/238705/what-is-sha-1-and-why-will-retiring-it-kick-thousands-off-the-internet/
- https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html
- Code to check escape
- https://github.com/cr-marcstevens/sha1collisiondetection