Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

SHA-1 Collision

First successful practical collision attack on SHA-1 Hashing Algorithm.

Manas Marawaha [1533734]
marawahm@tcd.ie

Introduction

- SHA-1 is a widely used 1995 NIST cryptographic hash function standard.
- SHA-1 produces a 160-bit (20-byte) hash value known as a message digest.
- Due to fundamental security weaknesses demonstrated in various analyses and theoretical attacks, SHA-1 is not considered secured and officially deprecated by NIST in 2011

SHA-1 Depreciation

- Despite its depreciation SHA-1 remains widely used in 2017 for Digital Certificate signatures, Backup systems, Deduplication systems , GIT …
- Impracticality in finding an actual collision from long time caused the industries reluctance to replace SHA-1 with a safer alternative.
- On February 23, 2017 first practical collision attack against SHA-1 was announced by CWI Amsterdam and Google[3].

SHA-1 Collision Attack

- A collision occurs when two distinct pieces of data a document, a binary, or a website's certificate hash to the same digest.

- As a proof of concept two dissimilar PDF files which produce the same SHA-1 hash were published [1].

```
manas@OptimusPrime:SHA1_Collison$ sha1sum PDF1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  PDF1.pdf
manas@OptimusPrime:SHA1_Collison$ sha1sum PDF2.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  PDF2.pdf
manas@OptimusPrime:SHA1_Collison$ sha256sum PDF1.pdf
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0  PDF1.pdf
manas@OptimusPrime:SHA1_Collison$ sha256sum PDF2.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff  PDF2.pdf
manas@OptimusPrime:SHA1_Collison$
```

SAME SHA-1 HASH

SHA-1 Collision Computation

- Collision computation:
  - Nine quintillion (9,223,372,036,854,775,808) SHA1 computations in total.
  - 6,500 years of CPU computation to complete the attack first phase.
  - 110 years of GPU computation to complete the second phase.

- SHA-1 shattered attack is still more than 100,000 times faster than a brute force attack which remains impractical.

Risk Mitigation

- Majority of industry player have already announced that their respective browsers will stop accepting SHA-1 SSL certificates by 2017.

- It's more urgent than ever for security practitioners to migrate to safer cryptographic hashes such as SHA-256 and SHA-3

References

[1] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, “The first collision for full SHA-1”, https://shattered.io, Feb 2017.

[2] https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html.

[3] https://en.wikipedia.org/wiki/SHA-1.

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Thank You