CERT-EU

SHA1 collision attacks shown to be practical

Threat Memo - TM 20-007 - Date: 17/01/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Vulnerability	Collision attack	World	IT, digital services, digital infrastructure	A1

Key Points

- A new research demonstrates the practicality and affordability of attacks against the SHA1 hash[1] function.
- SHA1 has been considered unsafe since 2005.
- The new findings are relevant because SHA1 is still used in multiple applications.

Summary

SHA1, or Secure Hash Algorithm 1, is a cryptographic hash function that is part of several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It is also used in revision control systems such as Git, Mercurial, and Monotone to verify data integrity. The integrity of a legitimate document or any other file is guaranteed by the unique result of the hash function of the document. An attack against a hashing algorithm aims to produce a counterfeit document or file with the same hash value as the legitimate one.

Conducting a collision attack on the SHA1 cryptographic hash function has been considered theoretically feasible since 2005. Multiple papers[2] have been published over the last decade theorising on how the hash function could be abused to produce a collision[3]. In 2017, the first actual collision was demonstrated in the SHAttered[4] attack, when two distinct pdf files with the same SHA1 were generated. However, the SHAttered attack provides very little control over the content of the hashed file and therefore is of limited practical value.

In April 2019 a chosen-prefix attack against the SHA1 algorithm was proposed[5]. In this, the attacker appends special values to the counterfeit document in order to produce the desired SHA1 result. On January 5, the first practical implementation of this attack was described[6]. In practice, this permits attackers to create two or more visually different documents that yield the same SHA1 hash value. This means that any cryptographic applications or integrity checking mechanisms that use SHA1 are now vulnerable. Reportedly, it currently costs about $45.000 to produce a SHA1 collision. Accordingly, the attack is well within the means of criminal organisations and state actors.

Comments

SHA1 is slowly being phased out. Major web browsers do not accept SHA1 SSL certificates since 2017. Microsoft no longer signs their code with SHA1, having moved to SHA2 in July 2019. However, SHA1 is still the default hash function for some PGP (Pretty Good Privacy) communication security applications. It is also the default data integrity check mechanism for some revision control systems, used in software development and other collaboration platforms.

One imaginary collision attack scenario is impersonating someone by creating a new PGP key and through a SHA1 chosen-prefix attack, giving it the same identity certificate as that of the legitimate key.

In revision control systems, a SHA1 collision attack could theoretically be used to introduce altered or malicious software packages into a software development workflow, causing integrity checks to miss the doctored code. This is likely a very attractive prospect for entities looking to conduct supply chain attacks by introducing malicious code to legitimate software.

[1] A one-way mathematical function that takes an arbitrarily sized value as an input and creates a standard-sized sequence of characters as an output. A unique input should always create a mathematically unique output.

[2] https://eprint.iacr.org/2005/010, https://sites.google.com/site/itstheshappening/

[3] A collision occurs when two distinct pieces of data produce the same hash value.

[4] https://shattered.io/static/shattered.pdf

[5] https://link.springer.com/chapter/10.1007%2F978-3-030-17659-4_18

[6] https://eprint.iacr.org/2020/014.pdf