Secure Hashing Algorithm

Author
Pål Tømte Karlsen

Supervisor
Sigurd Kristian Brinch

Essay i IKT207

Faculty of Engineering and Science
University of Agder
Grimstad, Autumn 2020

Status
Final

Keywords
cryptographic, hash function

Hashing Algorithm or Hash function is a mathematical function which convert numerical value into another compressed numerical value. A hash function take some string or number and turns it to a fixed length bit string for how many bits the hash function is. Values return by the hash function are called message digest or hash values. There exist several ways to hash a value one of them is SHA or Secure Hashing Algorithm.

SHA is a sudo random. This mean it has the appearance of randomness but in reality it is not. Because it has the appearance of randomness SHA can and is wildly used to authenticate files, signatures and verify if a message have not been changed[1].

SHA-1 was founded in 1995 by the NSA. It is a 160-bit hash value which is render in a 40-digit-long hexadecimal form[2]. Even though SHA-1 is so old, it is still used alot. This is a major concern. As of 2010 many organizations have recommended replacing it. As of 23rd of February 2017 there have been found a weaknesses and a SHA-1 collision have been accomplished[3]. This effectively make SHA-1 obsolete. A collision means that they have been able to create 2 different documents with the same hash.

Within the SHA family there exit 4 types: SHA-0, SHA-1, SHA-2 and SHA-3
Today SHA-0, and SHA-1 is obsolete and is not recommended to use.
SHA-2 have become more and more used. When someone say they are using SHA-2 one can not be sure which one they are refering to. This is because SHA-2 have a small family tree of its own. This include SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256[4].
SHA-3 or Keccak is actually developed from a crowed sourcing contest to see who could design a new algorithm for cybersecurity[5].

The move from SHA-1 to SHA-2 is still ongoing, in the mean time SHA-2 should still be viable for a time. Even though there are many that do not recommend SHA-1 it is still in us, and alot of organizations refuse to take the move to SHA-2. The reason for this is because the move to SHA-2 is a one-way operation. Once you move your web server from SHA-1 to SHA-2, clients that does not understand SHA-2 will see error or fail. The move to SHA-2 will be a risky leap to take for unsupported devices and application[4]. The biggest problem with SHA-2 is that it is not identical to SHA-1 but they share the same underlying math, which contains the same security flaws. The only reason they decided not to just move directly to SHA-3 is because it was created by an independent contest and then released as public-use patent[4].

Secure Hashing Algorithm was developed in order to vertify files, communication, signature, and more. Even if SHA-0, and SHA-1 have been cracked the SHA family is still in development and the newest family is SHA-3. There are still alot of organization that still uses SHA-1. One of them is GIT. Everything from authentication, to committing is done through SHA-1. This is a major security concern. This because someone can intercept a massage and send a custom made massage with the same hash value and no one would know.

References

[1] Dr Mike Pound, *Sha: Secure hashing algorithm - computerphile*, [Accessed 02/11/2020]. [Online]. Available: https://www.youtube.com/watch?v=DMtFhACPnTY&ab_channel=Computerphile.

[2] Jaimin Patel, "Secure hashing algorithm and advance encryption algorithm in cloud computing," 2017. [Online]. Available: https://search.datacite.org/works/10.5281/zenodo.1340245.

[3] Google Security Blog, *Announcing the first sha1 collision*, [Accessed 02/11/2020]. [Online]. Available: https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html.

[4] Roger A. Grimes, *All you need to know about the move from sha-1 to sha-2 encryption*, [Accessed 02/11/2020]. [Online]. Available: https://www.csoonline.com/article/2879073/all-you-need-to-know-about-the-move-from-sha1-to-sha2-encryption.html.

[5] techopedia.com, *Secure hash algorithm (sha)*, [Accessed 02/11/2020]. [Online]. Available: https://www.techopedia.com/definition/10328/secure-hash-algorithm-sha.