Article
David Shambroom · Feb 24, 2017 1m read

Collision for SHA-1 hash algorithm

The recent announcement of a collision for the SHA-1 hash algorithm has caused some consternation:

https://shattered.io/

Here is some background to help put this in perspective.

Cryptographic hash functions can have a variety of properties. The property at issue here is:

"Collision resistance - it is computationally infeasible to find any two distinct inputs x, x' which hash to the same output, i.e., such that h(x) = h(x')."

(Menezes, van Oorchot, and Vanstone, "Handbook of Applied Cryptography", section 9.2.2)

What properties are required depends on the application for which the hash function is used. Secure digital signature generation does require collision resistance. This is why vendors are discontinuing support for X.509 TLS and code-signing certificates signed using SHA-1. Other uses of hash functions, such as hashed passwords, or hash-based message authentication codes (HMAC) for data integrity protection, do not require collision resistance.

The U.S. government still permits the use of SHA-1 for certain applications, as specified in NIST Special Publication 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", section 9:

SHA-1 for Digital signature generation is "Disallowed except where specifically allowed by NIST protocol-specific guidance".
SHA-1 for Digital signature verification is "Legacy-use".
SHA-1 for Non-digital signature applications" is "Acceptable".

Hope this helps,

--David

#Security #Encryption #Caché