The Sunsetting of SHA-1

Finnbarr P. Murphy

(fpm@fpmurphy.com)

SHA-1 (Secure hash algorithm) is a 160-bit hash algorithm that is at the heart of many web security protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) since shortly after it was developed by the NSA (National Security Agency) in 1995.

In 2005, a professor in China demonstrated an attack that could be successfully launched against the SHA-1 function, suggesting that the algorithm might not be secure enough for ongoing use. Because of this, NIST immediately recommended federal agencies begin moving away from SHA-1 toward stronger algorithms. In 2011, NIST mandated that many applications in federal agencies move away from SHA-1 by December 31, 2013. Other attacks have been found on SHA-1, and NIST estimated in 2013 that SHA-1 provides only 69 bits of security in digital signature applications.

A recent survey by Netcraft found that 98 percent of all the SSL certificates used on the web still use SHA-1 signatures, and less than 2 percent use SHA-256 signatures.

Last year Microsoft announced that Windows will stop accepting SHA-1 certificates in SSL by 2017, and code signing certificates with SHA-1 hashes will no longer be accepted by Windows on January 1, 2016. Recently Google announced Chrome will stop accepting SHA-1 certificates in SSL in a phased way by 2017. Similarly, Mozilla Firefox is also planning to stop accepting SHA-1-based SSL certificates by 2017.

So it looks like SHA-1 certificates will sunset by the end of 2017 in most major applications.

