One million SSL certificates still using “insecure” SHA-1 algorithm

Nearly a million SSL certificates found in Netcraft's October SSL Survey were signed with the potentially vulnerable SHA-1 hashing algorithm, and some certificate authorities are continuing to issue more. Google Chrome already regards these certificates as insecure, resulting in more warning signals than if the sites had been served over a completely unencrypted HTTP connection.

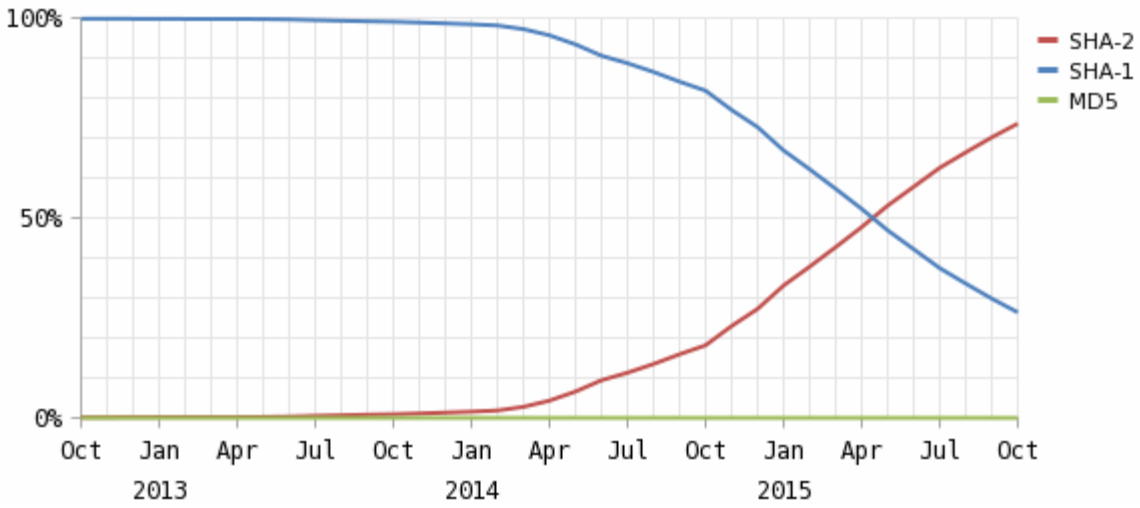
The latest research, dubbed the SHAppening, shows that these warnings are well founded, projecting that a full SHA-1 collision could be found within 49-78 days on a 512-GPU cluster. Renting the equivalent processing time on Amazon's EC2 cloud computing service would cost only $75k-$120k, which is an order of magnitude less than earlier estimates. The researchers point out that this represents an important alarm signal, and that the industry's plans to move away from SHA-1 by 2017 might not be fast enough.

The researchers consider that is now feasible [pdf] for a well funded attacker to impersonate an SSL site that uses a publicly trusted SHA-1 certificate. Worse still, while browsers still accept SHA-1 signatures, SSL sites remain at risk even after migrating to SHA-2: if an attacker were to compromise an intermediate CA certificate signed with SHA-1, he could generate valid certificates for arbitrary domains.

The SHA-2 and SHA-3 family of cryptographic hash algorithms are now the only ones approved by the National Institute of Standards and Technology (NIST) for digital signature generation. Although the SHA-2 family includes SHA-224, only the stronger SHA-256, SHA-384 and SHA-512 algorithms are allowed by the CA/Browser Forum's Baseline Requirements for the issuance and management of publicly-trusted certificates.

These newer algorithms do not exhibit the mathematical weaknesses of SHA-1, and also generate longer digests than the 160-bits computed by SHA-1. Almost all new SHA-2 subscriber certificates use SHA-256 (99.99%), while only a handful use SHA-384 and SHA-512. Most of the latter are issued by DigiCert.

growth increased in the wake of the 2014 HeartBleed bug. This bug resulted in around half a million certificates being potentially compromised, requiring urgent reissuance and revocation. By this time, many certificate authorities were already using SHA-256 for new certificates, which in turn caused a significant boost in the number of SHA-2 certificates in use on the web.



SHA-1 vs SHA-2 (source: Netcraft SSL Survey October 2015)

SHA-2 eventually overtook SHA-1 in May 2015, but there are still nearly a million certificates currently using SHA-1.

The use of SHA-1 in new certificates is expected to halt by the close of this year, as from 2016, the CA/Browser Forum Baseline Requirements will forbid the issuance of any new subscriber certificates or subordinate certificates that use the SHA-1 algorithm.

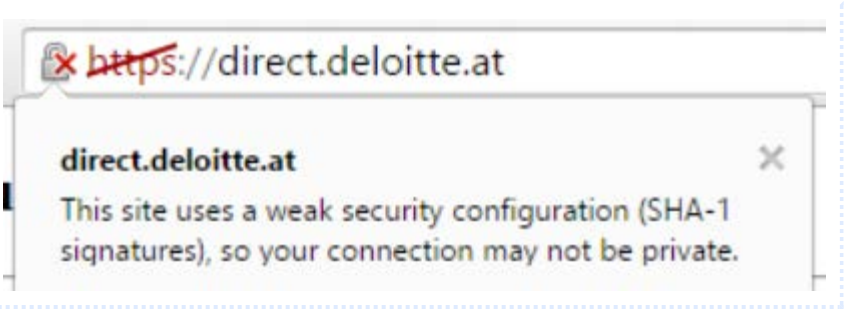
However, with less than three months to go, Symantec proposed a motion (endorsed by Entrust, Microsoft and Trend Micro) to allow the issuance of SHA-1 signed certificates throughout 2016. The proposed changes to the Baseline Requirements would have catered for "a very small number of very large enterprise customers" who are unable to migrate to SHA-2 before the end of this year. But with the new cost projections making the risk of a real-world attack higher than previously believed, Symantec and the endorsers subsequently withdrew the ballot on 12 October.

Even if this ballot were accepted, many certificate authorities have already decided to avoid using SHA-1 because of the way some browsers will treat these certificates. For example, if an existing SHA-1 certificate is due to expire during 2016, Google Chrome currently flags this up as a weak security configuration and warns the user that their connection may not be private. Certificates that are valid until 2017 or later are treated as **affirmatively insecure**, with the "https" protocol crossed out.

Weak and insecure certificates

Despite being regarded as weak or insecure by one of the most commonly used browsers, over 120,000 of the SHA-1 certificates currently in use on the web were issued during 2015, and 3,900 of these have expiry dates beyond the start of 2017. The owners of these certificates will undoubtedly need to replace them months — or in some cases, years — before they are due to expire.

For example, Deloitte is still using a SHA-1 signed certificate that was issued in February 2015 and valid until 2020. Google Chrome already regards this certificate as insecure:



This SHA-1 certificate was issued by A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, who operate the *A-Trust-nQual-03* root certificate that is trusted by all mainstream browsers.

In February 2014, when Netcraft first published a look at SHA-2 migration, more than 256,000 SHA-1 signed certificates would have been valid beyond the start of 2017. Despite the browser vendors' deprecation plans, this total is roughly the same today.

Buggy browsers treating some SHA-2 certificates as insecure

Some certificate authorities were hit by an unexpected pitfall after migrating to SHA-2, after failing to use new names for their SHA-2 signed intermediate certificates. SSLMate, an SSL certificate vendor, published two examples of how Google Chrome could erroneously suggest that a site was affirmatively insecure for serving a SHA-1 certificate, even when the full certificate chain actually used the SHA-2 hashing algorithm. This undesirable behaviour was caused by caching in the cryptographic libraries used by Chrome (CryptoAPI on Windows, and NSS on Linux).

When a CA migrates to SHA-2, it can either reuse an existing intermediate certificate by re-signing the existing public key with SHA-2, or it can generate a new one with a new public key and subject name. If the existing certificate is reused, some Windows browsers will end up ignoring the chain provided by the server and instead use the old SHA-1 intermediate certificate if it has been cached previously. This will cause Chrome to believe that the connection to the site is affirmatively insecure.

SSLMate observed that StartCom was still issuing SHA-2 certificates that were signed by a SHA-1 intermediate, despite CA/Browser Forum Ballot 118 stating that CAs should not do this. Netcraft's SSL Survey also shows the same mistakes being made by other certificate authorities, including WoSign, Entrust and Unizeto amongst others. All of these certificates may be regarded as insecure by the Chrome browser.

The second example involved a bug in older versions of NSS on Linux, which could cause Chrome to use a cross-signed root even if a shorter and newer chain exists. If the cached cross-signed certificate uses SHA-1, Chrome will consider the chain to be weak, even though the server may have sent a chain that used SHA-2 throughout.

Posted by Paul Mutton on 19th October, 2015 in Security

Share:

« Previous post: October 2015 Web Server Survey

» Next post: U.S. military cyber security fails to make the grade

Most Popular