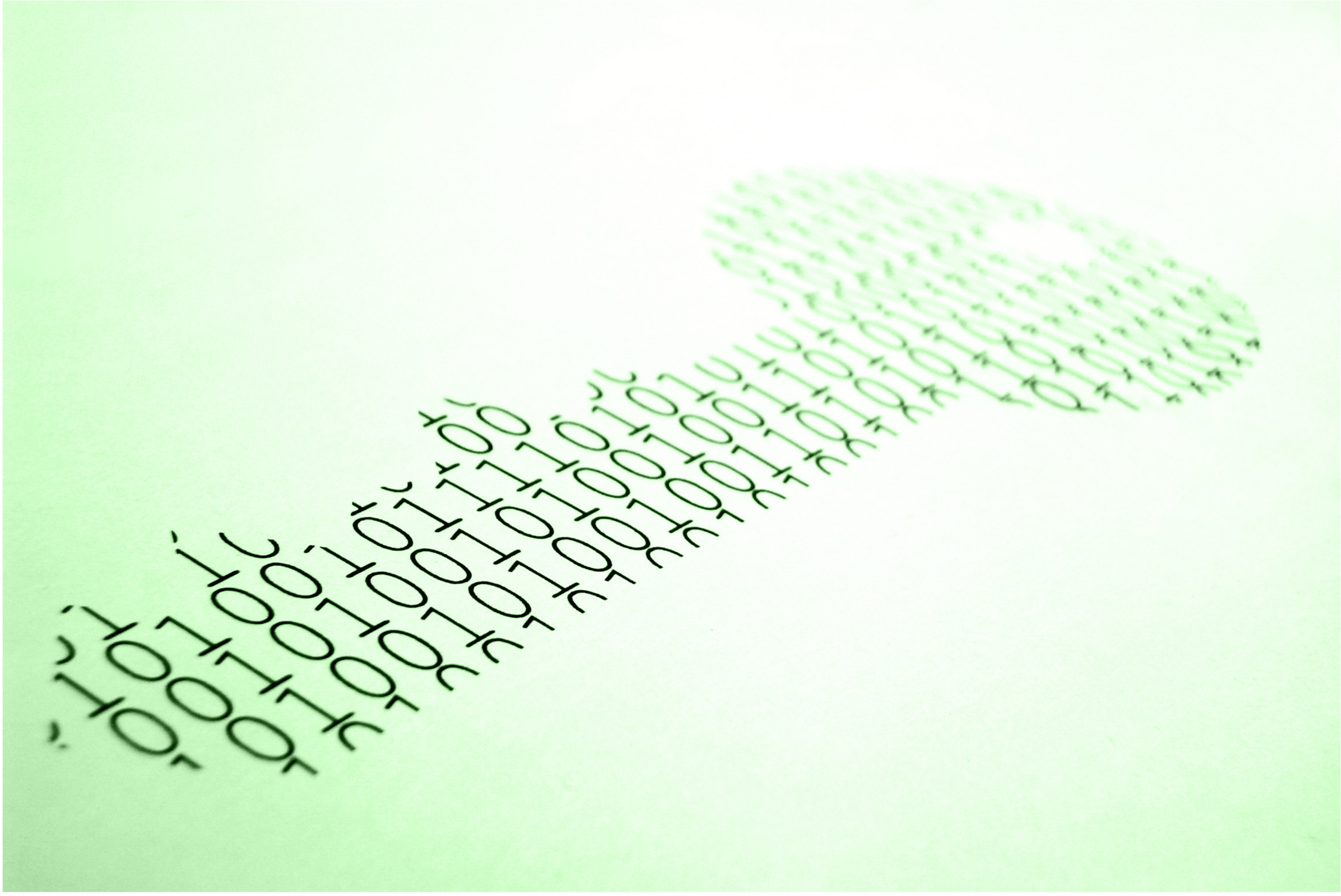
# Mozilla mulls early cutoff for SHA-1 digital certificates



*Digital key Credit: IDGNS*

The browser maker might decide to ban SHA-1 digital certificates in July 2016

MORE

By Lucian Constantin FOLLOW

IDG News Service | Oct 21, 2015 12:11 PM PT

In light of recent advances in attacks against the SHA-1 cryptographic function, Mozilla is considering banning digital certificates signed with the algorithm sooner than expected.

The CA/Browser Forum, a group of certificate authorities and browser makers that sets guidelines for the issuance and use of digital certificates, had previously decided that new SHA-1-signed certificates should not be issued after Jan. 1, 2016.

Browser makers have also decided that existing SHA-1 certificates will no longer be trusted in their software starting Jan. 1, 2017, even if they're technically set to expire after that date.

On Tuesday, Mozilla announced that it's re-evaluating the cutoff date and is considering the feasibility of pushing it forward by six months, on July 1, 2016. The decision is guided by recent research that improves the practicality of attacks against SHA-1.

Earlier this month Thomas Peyrin of Nanyang Technological University (NTU) in Singapore, Marc Stevens of the Centrum Wiskunde and Informatica in the Netherlands and Pierre Karpman of both NTU and Inria in France, published a research paper that describes a new way to break SHA-1.

The researchers estimate that pulling off their attack, which breaks the full 80 rounds of SHA-1, would cost between $75,000 and $120,000 using commercial cloud-computing resources, a price that many cybercriminal groups can afford. While their particular attack can not be used to forge SSL certificates, it clearly shows that the practicability of breaking SHA-1 signatures is increasing at a much faster pace than previously anticipated.

"We advise the industry to not play with fire, and accelerate the migration process toward SHA2 and SHA3, before such dramatic attacks become feasible," Thomas Peyrin told the IDG News Service earlier this month.

It seems that the industry is listening. Following the research's publication, the CA/Browser Forum withdrew a motion put forward by Symantec and endorsed by Entrust, Microsoft and Trend Micro to allow the issuance of SHA-1 certificates throughout 2016 in order to accommodate "a very small number of very large enterprise customers" who cannot complete the transition to SHA-2 certificates by the end of this year.

According to Internet services company Netcraft, almost one million SHA-1 SSL certificates are still in use on the Internet, 120,000 of which were issued in 2015 and 3,900 having expiry dates past Jan. 1, 2017. According to statistics from the SSL Pulse project, 24% of the world's top 143,000 HTTPS websites by traffic use SHA-1 certificates.

Google Chrome is already displaying different connection security indicators for HTTPS websites that use SHA-1 certificates than for those that use SHA-2 certificates in order to encourage migration away from the aging hash function.

Webmasters who are concerned about the cost of replacing their certificates will soon have a free alternative. A non-profit certificate authority called Let's Encrypt will launch in November and announced Monday that its root certificates have been cross-signed by IdenTrust and are now trusted by all major browsers.

RELATED TOPICS

Encryption | Data Security | Network Security | Security

Lucian Constantin — *Romania Correspondent*

**Windows 10 cheat sheet (with video)**

View Comments

## YOU MIGHT LIKE