# SHA1 Algorithm Could Become Useless by the End of the Year



*The Shappening project just broke SHA1 encryption*

*Oct 8, 2015 14:49 GMT · By Catalin Cimpanu*

**SHA1, a cryptographic hash function developed by the NSA in 1995, is taking its last breaths, according to a team of security researchers which claim that the monetary costs and time needed to break the algorithm have gone down much faster than previously expected, and that by the end of the year security experts should not be surprised if the algorithm has been broken and compromised.**

Researchers break SHA1 algorithm

If you're unfamiliar with cryptography terms or the InfoSec domain, SHA1 is computational algorithm which takes an input string (email, password, email, or any other text) and scrambles it, generating a completely, unreadable string of text, known as a fingerprint.

Like MD5, another hashing algorithm, SHA1 is vulnerable to collision attacks. These appear when two different input strings generate the same output (fingerprint), even if they don't have anything in common. This is possible due to some mathematical probabilities and is how attackers can break communications encoded with SHA1 (and MD5).



## SHA1 is still widely used, even today

While MD5 has been abandoned for securing communications a long, long time ago, SHA1 is still used in even today for securing some HTTPS connections and for signing digital certificates, used by software makers to authenticate legitimate software.

According to a project called The Shappening, three researchers from universities in France, Holland, and Singapore, have adapted the collision attack into a new method which they've dubbed freestart collision.

Using this new method, the three researchers managed to break the full SHA-1 algorithm (all 80 out of 80 steps), only in 10 days of continuous computation on a cluster of 64 GPU cards.

## Breaking SHA1 now costs between $75,000 and $120,000 in server bills

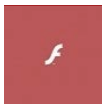
Security experts around the world were expecting this moment to come up, but not now. According to previous research from 2012, cryptography experts were warning that the cost to break down SHA1 would plummet significantly by 2018, when the computational servers needed to run the attack would go down to a value of $173,000 / €153,000, an acceptable sum of money for both cyber-criminal groups and nations involved in cyber-espionage.

Using the freestart collision method, researchers claim that this could be done **right now** with costs between $75,000 and $120,000 (€67,000 and €107,000).

Alternatives to SHA1 exist in the form of SHA2 (developed by the NSA) and SHA3 (developed by a group of independent researchers). Google and Mozilla have announced that they would be moving away from SHA1 certificates starting with January 1, 2017. Microsoft has already moved to SHA2 starting with 2013 and Windows 8.

Acting on their findings, researchers have already submitted a recommendation to the regulatory body responsible for Certificate Authorities, urging it to speed up the process of implementing SHA2-based certificates.

Mozilla Outlines Plan to Phase Out SHA-1 Certificates, As 1 Million



Insecure Flash Cross-Domain Policies Expose Users to Abuse on One in

President Obama Believes in Strong Encryption

Google Adds HTTPS

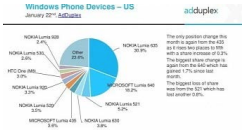
#SHA1, #encryption, #algorithm, #collision attack, #SHA2



## Hot right now · Latest news

**iPhone 5se to Launch Alongside iPad Air 3, New Apple Watch Models in March**

**More Bloatware in Windows 10: Microsoft to Pre-Install Another App**




**Even with Windows 10 Mobile Flagships Out, the US Oblivious to Windows Phones**


**Oracle Will Kill Java Browser Plugin with JDK 9 in 2017**

## Comments

Share your thoughts on this story!