RISK ASSESSMENT / SECURITY & HACKTIVISM

SHA1 algorithm securing e-commerce and software could break by year’s end

Researchers warn widely used algorithm should be retired sooner.

by **Dan Goodin** - Oct 8, 2015 11:02am CEST

SHA1, one of the Internet's most crucial cryptographic algorithms, is so weak to a newly refined attack that it may be broken by real-world hackers in the next three months, an international team of researchers warned Thursday.

SHA1 has long been considered theoretically broken, and all major browsers had already planned to stop accepting SHA1-based signatures starting in January 2017. Now, researchers with Centrum Wiskunde & Informatica in the Netherlands, Inria in France, and Nanyang Technological University in Singapore have released a paper that argues real-world attacks that compromise the algorithm will be possible well before the cut-off date. The results of real-world forgeries could be catastrophic since the researchers estimate SHA1 now underpins more than 28 percent of existing digital certificates.

Hashing it out

SHA1 is what's known as a cryptographic hash function. Like all hash functions, it takes a collection of text, computer code, or other message input and generates a long string of letters and numbers that serve as a cryptographic fingerprint for that message. Even a tiny change, such as the addition or deletion of a single comma in a 5,000-word e-mail, will cause a vastly different hash to be produced. Like all fingerprints, the resulting hash is useful only as long as it's unique. The moment two different

LATEST FROM ARS TECHNICA/UK

EVEN MURDOCH'S MAD

EU antitrust chief wades into Google UK tax row

First-person drone racing is much harder than I expected

SCAM CRACKDOWN

TalkTalk call centre staff manacled over security breach

Dutch researchers have created flexiramics—flexible ceramics for circuit boards

BAHFest London: Hard science collides with fake theories and SMBC

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Why the calorie is broken

“I’m kind of pissed at the scientific community for not coming up with something better."

WATCH ARS VIDEO

message inputs produce the same hash, the so-called collision can open the door to signature forgeries that can be disastrous for the security of banking transactions, software downloads, and website communications.

A series of attacks on MD5, a hashing algorithm that's much more collision-prone than SHA1, provides a glimpse at the dire results of collision attacks. The Flame espionage malware, which the US and Israel are reported to have unleashed to spy on sensitive Iranian networks, wielded such a collision attack to hijack Microsoft's Windows Update mechanism so the malicious program could spread from computer to computer inside an infected network. Separately, in 2008, a team of computer scientists and security researchers used the technique to forge a master secure sockets layer certificate that could authenticate virtually any website of their choosing.

FURTHER READING

FLAME MALWARE WIELDED RARE “COLLISION” CRYPTO ATTACK AGAINST MICROSOFT

Such real-world exploits are almost unheard of, underscoring Flame's ingenuity.

MD5 has since been largely abandoned for use in generating digital signatures, although it still remains viable in other cases. (Notably, MD5 is also unsuitable for cryptographically protecting passwords, but this has nothing to do with its susceptibility to collision attacks.) SHA1, by contrast, is considerably more resistant than MD5 to collisions, although it too has long been considered vulnerable. In 2012, cryptographers warned that the growing advances in computing made real-world collision attacks against SHA1 viable by 2018.

The 2012 warning was based on contemporaneous estimates from Bruce Schneier that it would cost $700,000 to perform a full-on collision attack on SHA1 by 2015 and, thanks to the ever-advancing speed of computers, just $173,000 by 2018. That latter amount, Schneier reasoned, was well within the budget of a well-financed criminal hacking group. Now, based on research completed last month, the international team of researchers believe that such an attack could be carried out this year for $75,000 to $120,000. The much lower cost is the result of efficiencies the researchers discovered in the way graphics cards can use a technique known as "boomeranging" to find SHA1 collisions.

FURTHER READING

SHA1 CRYPTO ALGORITHM UNDERPINNING INTERNET SECURITY COULD FALL BY 2018

Attacks on weaker MD5 algorithm show how devastating a crack could be.

The estimate was based on the researchers' ability to carry out a successful collision attack on the SHA1 compression function. While not a collision on the actual SHA1 algorithm itself, the feat nonetheless invalidates the security proof upholding the algorithm and demonstrated the soundness of the new graphics-card technique.

"Our new GPU-based projections are now more accurate and they are significantly below Schneier’s estimations," the researchers wrote in their paper. "More worrying, they are theoretically already within Schneier’s estimated resources of criminal syndicates as of today, almost two years earlier than previously expected, and one year before SHA-1 being marked as unsafe in modern Internet browsers. Therefore, we believe that migration from SHA-1 to the secure SHA-2 or SHA-3 hash algorithms should be done sooner than previously planned."

The paper noted that the collisions involved in the research are known as identical-prefix collisions, as opposed to the significantly more severe and costly chosen-prefix collisions at the heart of Flame's attack on Windows Update or the 2008 certificate authority impersonation. Identical-prefix collisions still allow signature forgeries, but their capabilities are far less flexible than chosen-prefix collisions.

CES 2016: Ars walks the length and breadth of CES so you don't have to

Ars Technica Automotive Editor Jonathan M. Gitlin walked the length and breadth of the Consumer Technology Association conference (CES) in Las Vegas, Nevada.

STAY IN THE KNOW WITH

LATEST NEWS

Apollo 1, *Challenger*, and *Columbia*: Remembering NASA’s lost astronauts

GOOD RIDDANCE

Oracle deprecates the Java browser plugin, prepares for its demise

HTC Vive Pre impressions: A great VR system has only gotten better

Aereo founder’s next business: Wireless gigabit home Internet

RELEASED INTO WILD

VMware Fusion, Workstation team culled in company restructure

Wikimedia’s newest board appointment steps down amid editor hostility

Identical-prefix collisions, for example, allow for two different executable files that nonetheless generate the same digital signature. They also allow for colliding PDF documents that show different content. They also make it possible to generate colliding certificates, but those are only different in the public key, and not different in, say, the identities' name, so they can't be easily abused.

Kicking the can

Thursday's research showing SHA1 is weaker than previously thought comes as browser developers and certificate authorities are considering a proposal that would extend the permitted issuance of the SHA1-based HTTPS certificates by 12 months, that is through the end of 2016 rather than no later than January of that year. The proposal argued that some large organizations currently find it hard to move to a more secure hashing algorithm for their digital certificates and need the additional year to make the transition.

The paper was written by Marc Stevens, Pierre Karpman, and Thomas Peyrin. The new calculations, should they be confirmed by the researchers' peers, are likely to provide a strong argument for voting no and instead quickly migrating to use of SHA2, which is much more resistant to collisions.

PROMOTED COMMENTS

zepi | Smack-Fu Master, in training — jump to post

> Vincent294 wrote:
> Why are people still using SHA1? (rhetorical question)

Legacy systems that just don't have support for SHA-2. Bazillion of embedded / industrial things run on OS'es that don't handle anything never and programming such functionality to the application layer is a huge undertaking, not to mention prone to even bigger errors.

edit: And when you have a million euro machine that doesn't get OS updates anymore and your options are either "running it as it is" or buying a huge project from your system provider, many choose not to do anything while still connecting this machine to their corporate network.

Or if you have 10 000 boxes (electricity network control, weather stations, whatnot) distributed around a country that run on something like Windows CE or some other ancient OS, you are easily in trouble because upgrades are far from easy.

51 posts | registered Jun 18, 2010

---

blingting | Wise, Aged Ars Veteran — jump to post

Seems to me that based on Bruce Schneier's cost-to-crack estimate, SHA1 should already have been considered broken since at least 2012. $700k might have priced criminals out of the market, but it must be well within the budgets of state-funded operations in Russia, China and pretty much every developed nation on Earth.

125 posts | registered Feb 22, 2012

Madlyb | Ars Praetorian — jump to post

> Vincent294 wrote:
> Why are people still using SHA1? (rhetorical question)

Well, the short answer is exactly what @tmt stated, but there are other non-lazy decisions with the biggest being infrastructure costs. Typically, the more resistant a crypto function is, the more compute needed per use and this can quickly become a non-trivial amount.

In 2001, we *had* to use SHA1 with our VPN because the mobile devices of the day would literally overheat maintaining the tunnel. The interesting thing is that as we roll compute out to more and more things, many of these systems are incredibly small and possibly running on very limited power, so using strong crypto is again challenging.

This challenge also impacts the backend, when we moved to stronger crypto on our data center hosts in 2006, it took about 30% more hardware to process the same number of transactions. In our case, 30% actually cascaded into facility costs because we blew through our planned growth projections and had to invest in building, power and cooling to normalize the curve...it was a 7 figure impact...just changing the crypto function.

Finally, there is a User Experience issue with cryptographically secured files. Files just keep getting bigger and the overhead of encrypting and decrypting them can soar with multi-gig files and once again mobile comes into the equation because of the high compute cost. For our less sensitive but not public materials, we returned to SHA1 because mobile devices and use the SHA2 family for only the most sensitive material.

One last note, we did some testing last year with the SHA3 family versus SHA2 and it will be the same ballgame all over again and with the move to encryption everywhere, the costs are just going to continue to grow.

452 posts | registered Mar 4, 2009

---

daneren2005 | **Ars Scholae Palatinae** **jump to post**

> Vincent294 wrote:
> Why are people still using SHA1? (rhetorical question)

To add to what others said, CloudFlare has a good detailed analysis on the situation as it pertains to certificates: https://blog.cloudflare.com/cloudflare- ... tificates/

A little snippet of interest:

> **Quote:**
> Sites that have tried to upgrade to SHA-2 have seen a backlash due to browser incompatibility. In July, mozilla.org upgraded their site to use a SHA-2 certificate. In doing so they lost around 145,000 Firefox downloads per week due to browser incompatibility. Even google.com (as of November 10, 2014) continues to use SHA-1 for compatibility reasons, despite the company’s push to deprecate SHA-1 in Chrome.

1168 posts | registered Sep 21, 2012

READER COMMENTS

- - -

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY | NEWER STORY →

YOU MAY ALSO LIKE