by **Michael Mimoso** Follow @mike_mimoso October 9, 2015 , 10:00 am

When Bruce Schneier made his oft-cited and mathematically sound projections about the life expectancy of the SHA-1 cryptographic algorithm, he didn't think he was being conservative.

"I thought I was being accurate given the information I had at the time," Schneier said on Thursday.

Schneier in 2012, projected that a practical collision attack (where two inputs produce the same hash) against SHA-1 would cost $700,000 by 2015, and $143,000 by 2018, numbers—especially the 2018 total—that are certainly within reach of a well-funded government or criminal organization.

New research released this week, however, has reeled in the 2018 projection, postulating that a practical collision could be three months, and not three years away.

Researchers Marc Stevens, Pierre Karpman and Thomas Peyrin, respectively of the Centrum Wiskunde & Informatica of the Netherlands, Inria of France, and the Nanyang Technological University of Singapore, published a paper called "Freestart collision for full SHA-1" that describes tweaks to existing attacks and advances in analyzing of the algorithm that drastically reduce the cost and potential time to generate a collision. Those factors in combination with the relative continued health of Moore's law, which states the computer processing power doubles every two years, significantly reduce the time to create a collision attack.

Related Posts

Jon Callas on Securing Our Private Data
January 28, 2016 , 10:00 am

Government Agencies Audit for Juniper Backdoor
January 26, 2016 , 9:59 am

OpenSSL to Patch Two Vulnerabilities This Week
January 25, 2016 , 12:59 pm

From the paper:

> "Our freestart collision attack can be done in about 9 to 10 days on a cluster with 64 GPUs, or by renting GPU time on Amazon EC2 for about 2K US$. Based on experimental data obtained in this new work and the 2013 state-of-the-art collision attack, we can project that a real SHA-1 collision will take between 49 and 78 days on a 512 GPU cluster. Renting the equivalent GPU time on EC2 will cost between 75K US$ and 120K US$ and will plausibly take at most a few months."

"Moore's law is taken into account in the old estimate. Tweaks to attacks explained in the new paper were not taken into account, and there have been major advances in the algorithm that were not taken into account," Schneier said. "The problem is that the last two things are not predictable."

The paper explains that the freestart collisions are collisions against SHA-1's compression function, and not the algorithm itself, but still undermine its security.

"They represent an important alarm signal that warns users to quickly move away from using this hash function," the researchers wrote. "In particular, we believe that our work shows that industry's plan to move away from SHA-1 in 2017 might not be soon enough."

All of the major browser vendors have announced their intention to stop supporting SHA-1, especially in new development projects. Microsoft was among the first, recommending to developers in November 2013 they begin deprecating not only SHA-1, but also RC4. Google and Mozilla followed suit within weeks of each other in September 2014.

A wrinkle, however, was introduced Oct. 2 by the CA/Browser Forum which proposed a motion to allow the issuance of SHA-1 certificates through Dec. 31, 2016. The reasoning behind the motion is that a number of large enterprises don't believe they will be able to fully transition to SHA-2 certificates by the current termination date at the end of this year.

"This is attributed to the sheer volume of certificates that they need to migrate (numbering in the thousands), and their end-of-year blackout period," the motion reads. "These customers accept the risk of continuing to use new SHA-1 certificates, and assert that if they can continue to enroll for and receive SHA-1 certificates through 2016 (all with an expiration date of 31 December 2016 or earlier), they will be able to complete the transition by the end of 2016."

The review period for the motion ends on Monday with a vote taking place Oct. 16.

"The answer should have been 'no' then," Schneier said. "Now, it's 'hell no.'"

SHA-1 has been theoretically broken for more than a decade, Schneier said, and wrote in a blogpost on Thursday. While SHA-1 collisions have been more theory than practice, collisions against MD5, for example, have been achieved. The most notorious MD5 collision was pulled off by the attackers behind the Flame malware. Like a state-sponsored attack, Flame used a MD5 collision to sign malware as if it were coming from Microsoft, and as a result, would be trusted. The Flame attackers used the forged Microsoft digital certificate to perform a man-in-the-middle attack against victims, impersonating the Windows Update mechanism and installing malicious code instead.

The new SHA-1 research significantly reduces the amount of work to create a collision, making it feasible for the NSA, for example, or well-funded criminal syndicates.

"There's a saying inside the NSA: 'Attacks always get better; they never get worse,'" Schneier said, adding some advice: "Don't panic, but prepare for a future panic."

Categories: **Cryptography**, **Government**, **Hacks**, **Privacy**

Comments (2)