10/8/2015
04:35 PM

Jai Vijayan
News

Researchers Warn Against Continuing Use Of SHA-1 Crypto Standard

New attack methods have made it economically feasible to crack SHA-1 much sooner than expected.

The SHA-1 security standard, widely used in digital certificates, electronic banking, browsers, and other applications is weaker than previously thought and susceptible to attacks that are now well within the resources of criminal groups, an international team of cryptanalysts warned Thursday.

Security researchers had previously estimated that it would take at least another two years for so-called collision attacks against SHA-1 to become economically feasible for threat actors.

But a new method, developed by researchers Marc Stevens from CWI -- The Netherlands' national research institute for math and computer science -- Pierre Karpman from French counterpart Inria, and Thomas Peyrin from Singapore's Nayang Technological University, shows the estimates were too conservative.

"We now think that the state-of-the-art attack on full SHA-1 as described in 2013 may cost around $100,000 renting graphics cards in the cloud," the researchers said in a technical paper describing their attack.

The finding is important because browser makers and certificate authorities (CA) are currently scheduled to stop accepting SHA-1 signatures only in January 2017. Members of the CA/Browser forum are in fact currently considering a proposal that would extend the issuance of SHA-1 certificates through the end of 2016.

Approving that proposal would be dangerous, the cyrptanlaysts said, while strongly recommending that SHA-1 based signatures should be marked as unsafe "much sooner" than that.

Cryptographic hash functions like SHA-1 basically encrypt data—or "messages" in cryptospeak--in a fashion where it is considered practically impossible to reconstruct the original input message from just the hash value.

In theory at least, it should be highly difficult for anyone to find two messages with the same hash value. A collision attack is an attempt to do just that so as to enable malicious actions like creating forgeries of digital signatures.

As far back as 2005, security analysts expressed concern about SHA-1 being susceptible to collision attacks. But many believed that the computational and financial requirements to pull off such an attack would be too prohibitive for anyone to want to try it.

In 2012, noted cryptographer and security researcher Bruce Schneier estimated that it would cost attackers about $700,000 to pull off a successful collision attack on SHA-1 in 2015. He estimated that cost would drop to $173,000 in 2018; a figure that he felt would be within the reach of criminals.

But in a technical paper released Sep. 22, the three researchers presented what they described as an example of a freestart collision attack against SHA-1. The example showed how attackers could use modern graphic cards to achieve full SHA-1 collision for as little as $100,000 by renting space on Amazon's EC2 cloud. According to the researchers, it took just 10 days of computing with a 64 GPU cluster on Amazon's cloud to successfully break the full inner layer of SHA-1

"The current policy of the retraction of SHA-1 has been strongly guided by Bruce Schneier's estimates of the attack costs," Stevens says. "What has changed today is that we have shown … these kind of attacks can be done very efficiently and is in fact more cost-efficient," using graphics cards. "This means that in principle, SHA-1 collisions are within the resources of criminal syndicates two years earlier than previously expected."

In their paper, Stevens and the other researchers noted that SHA-2 and SHA-3, the successors of SHA-1, are unaffected by the attack method and remain secure. They urged websites, browser makers, and others to move to SHA-2 as soon as possible.

In a blog post, Schneier concurred with the researchers in recommending that SHA-1 should be retired before 2017. Given the continuing advances in computing technologies and efforts by researchers to improve on existing methods, it's not surprising that a new technique is available that dramatically lowers the cost of launching a collision-attack on SHA-1, Schneier said.

"What's news," he wrote, "is that our previous estimates may be too conservative."