The Register®
Biting the hand that feeds IT

Security

Crypto cadre cloud-cracks SHA-1 with just $75k of compute cost

Plans to retire cipher in 2017 may need to be brought forward

9 Oct 2015 at 05:02, Darren Pauli

39 185

A crypto cadre has busted the SHA-1 security standard after using $US75,000 of cloud computing resources, handily undercutting conservative crypto cracking estimates and putting such an attack within reach of well-resourced groups.

The work brings forward the beginnings of the death knell for the widely-used hash function by two years. Security minds estimated SHA-1 should be retired in 2017 in-line with then estimated advances in compute capacity.

It was estimated in 2012 that such attacks would cost $173,000 to pull off by 2017.

The work paves the way for SHA-1 collision attacks and while impressive ought not to spark panic.

Crypto mind Bruce Schneier says SHA-1 is known to be theoretically broken and the research merely adds weight to the argument that support for it among browser barons should not be extended.

"This is not that unexpected," Schneier says .

"All the major browsers are planning to stop accepting SHA-1 signatures by 2017 [and] Microsoft is retiring it on that same schedule.

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

Faster compute power, tweaked attacks, and new attack vectors all add up to circumstances in which it is hard to predict the end of life for crypto standards.

The cracking work was performed by researchers Marc Stevens of the Dutch research institute Centrum Wiskunde and Informatica with Pierre Karpman and Thomas Peyrin from Singapore’s Nanyang Technological University.

More like this

Encryption Cryptography Security Research

Most read

GitHub falls offline, devs worldwide declare today a snow day

Cops hate encryption but the NSA loves it when you use PGP

NSA’s top hacking boss explains how to protect your network from his attack squads

The trio describes their work in in the paper *Freestart collision for full SHA-1* [PDF] and in a dedicated website bearing the tongue-in-cheek title *The SHAppening*.

The team writes that the freestart collision targeting the SHA-1 internal compression function is "the first practical break of the full SHA-1, reaching all 80 out of 80 steps".

It took 10 days for the researchers' Amazon-powered 64-GPU cluster, dubbed The Kraken, to pull off the attack. Here's how the researchers explain their efforts:

> **"Freestart collisions, like the one presented here, do not directly imply a collision for SHA-1. However, this work is an important milestone towards an actual SHA-1 collision and it further shows how graphics cards can be used very efficiently for these kind of attacks.**
> **We therefore recommend the industry, in particular internet browser vendors and Certification Authorities, to retract SHA-1 soon. We hope the industry has learned from the events surrounding the cryptanalytic breaks of MD5 and will retract SHA-1 before example signature forgeries appear in the near future."**

The researchers call on the tech industry to reject a proposal to extend the issuance of SHA-1 certificates by a year due to alleged difficulties in switch over to SHA-3.

The work, like most research, builds on the shoulders of others; the team credits its work as an extension of the recent freestart collision work on reduced-round SHA-1 from CRYPTO 2015 [PDF and EUROCRYPT 2013 PDF.] ®

Tips and corrections

29 Comments

More from The Register

Oracle hardwires encryption and SQL hastening algorithms into Sparc M7 silicon

OPENWORLD Claims world-record breaking performance

9 Comments

DNS chief and wannabe master-of-the-internet ICANN pwned… again

Hashed passwords, email addresses and more exposed

10 Comments

French say 'Non, merci' to encryption backdoors

Minister brands crypto skeleton keys 'vulnerability by design' – is the US listening?

44 Comments

GCHQ spies quashed this phone encryption because it was too good against snoopers

MIKEY-IBAKE could alert people to fact they're being monitored

56 Comments

ICANN speak clearly now .gay has gone – Council of Europe

And could you sort out the Whois database while you're at it?

10 Comments

Oh UK.gov. Say you're not for weakened encryption – Google and Facebook

IPB Companies weigh in on Investigatory Powers Bill

44 Comments

Whitepapers

Behind the mask: The changing face of hacking

Helping you learn more about hackers and how they work. And that can help you better plan

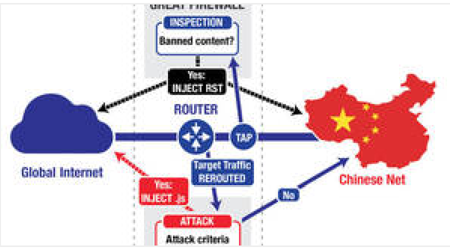
You've seen things people wouldn't believe – so tell us your programming horrors

Oracle to kill off Java browser plugins with JDK 9

Spotlight

Techie on the ground disputes BlackEnergy Ukraine power outage story

Asda slammed for letting vulns fester on its cyber shelves



What if China went all GitHub on your website? Grab this coding tool

Invite-only bug bounty criticised for turning up the heat on Tor

Law enforcement versus Silicon Valley's idle problem children