



LANDS'END
SHOP AT LANDSEND.COM



EVERNOTE
CLEARLY

Get more from online reading, with Clearly

With just one click, strip any article of all distractions.
With one more click, save any article in Evernote, forever.
Try it now!

Read with Clearly

RISK ASSESSMENT / SECURITY & HACKTI

SHA1 sunset will block millions from encrypted net, Facebook warns

Companies unveil controversial fallback plan for tens of millions of browsers.

by Dan Goodin - Dec 10, 2015 1:46pm EST

Share Tweet Email 171



Michael Rivera

Tens of millions of Internet users will be cut off from encrypted webpages in the coming months unless sites are permitted to continue using SHA1, a cryptographic hashing function that's being retired because it's **increasingly vulnerable to real-world forgery attacks**, Facebook and Web security company CloudFlare have warned.

Facebook said as many as seven percent of the world's browsers are unable to support the SHA256 function that serves as the new minimum requirement starting at the beginning of 2016. That translates into tens of millions of end users, and a disproportionate number of them are from developing countries still struggling to get online or protect themselves against repressive governments. CloudFlare, meanwhile, estimated that more than 37 million people won't be able to access encrypted sites that rely on certificates signed with the new algorithm.

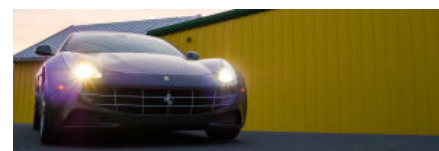
Both companies went on to unveil a controversial fallback mechanism that uses SHA1-based certificates to deliver HTTPS-encrypted webpages to people who still rely on outdated browsers. The remaining, much larger percentage of end users with modern browsers would be served HTTPS pages secured with SHA256 or an even stronger function. The mechanisms, which both companies are making available as open-source software, will allow websites to provide weaker HTTPS protection to older browsers while giving newer ones the added benefits of SHA256. Facebook is deploying the plan on most or all of the sites it operates, while CloudFlare will enable it by default for all of its customers. CloudFlare said other sites, including those run by Chinese portal Alibaba, are also implementing it.

In a **blog post published Wednesday**, Facebook Chief Security Officer Alex Stamos wrote:

We don't think it's right to cut tens of millions of people off from the benefits of the encrypted Internet, particularly because of the continued usage of devices that are known to be incompatible with SHA-256. Many of these older devices are being used in developing countries by people who are new to the Internet, as we learned recently when **we rolled out TLS encryption** to people using our Free Basics Platform. We should be investing in privacy



LATEST FEATURE STORY



FEATURE STORY (3 PAGES)

Getting to know the FF, a Ferrari you can drive every day

Stratospheric price, morally questionable fuel thirst, amazing noise, and... practicality?

WATCH ARS VIDEO

and security solutions for these people, not making it harder for them to use the Internet safely.


Both he and CloudFlare officials also called for changes in the [official baseline requirements](#) mandated by the CA/Browser forum, the industry group that sets encryption policy for certificate authorities and browsers to follow. Under the proposal, the forum would adopt a new class of certificate known as the LV, short for legacy validated. It would be issued to organizations that have demonstrated they offer SHA256 certificates to modern browsers. Current requirements call for SHA1 to be retired on the first of the year with no exceptions.

Becoming Facebook

Like all hash functions, SHA1 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. Hashes are useful only when they're unique. The moment two different 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.

SHA1 has long been considered theoretically broken because it was known to be susceptible to collision attacks. The ever-increasing speed of computer chips have gradually made such attacks within the reach of nation states and even criminal enterprises. In October, an international team of researchers warned that it might cost from \$70,000 to \$120,000 to carry out a limited collision attack on SHA1. At the time, the function was used to digitally sign an estimated 28 percent of the Internet's digital certificates. As a result, Internet companies put SHA1 on an accelerated retirement path, lest the weakness be exploited to generate certificates that cryptographically impersonate Google, Facebook, or other websites. All major browsers support SHA256, but that support isn't available for some people, most notably those using Windows XP prior to Service Pack 3 or devices running Android prior to the Gingerbread version.


The proposal by Facebook and CloudFlare to roll back some of those changes touched off howls of dissent from some security experts, including Ryan Sleevi, a Google employee who is a member of the Chromium cross-platform crypto team. In the hours after the proposals were announced on Wednesday morning, [Sleevi's Twitter stream lit up with criticisms](#). "There's just perverse economies at play; need CAs to stop selling X in order to browser to block X," he wrote in one, referring to the browser-trusted certificate authorities.



Ryan Sleevi
 @sleeви_

9 Dec

[@alexstamos](#) And that's something that can be done quickly, achieves same results, and doesn't get conflated with SHA-1 :)



Ryan Sleevi
 @sleeви_

Follow

[@alexstamos](#) There's just perverse economies at play; need CAs to stop selling X in order to browser to block X

1:42 PM - 9 Dec 2015

↩ ↺ 1 ❤ 2

For his part, Stamos seemed to anticipate the controversy. "This is not an easy issue, and there are well-meaning people with good intentions who will disagree," he wrote in his blog post. "We hope that we can find a way forward that promotes the strongest encryption technologies without leaving behind those who are unable to afford the latest and greatest devices."

PROMOTED COMMENTS

dfjde julio | Ars Scholae Palatinae

[jump to post](#)




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

 **Clever bank hack allowed crooks to make unlimited ATM withdrawals**

MOVE ALONG, FOLKS, NO INFRINGEMENT HERE


Samsung patent counterstrike against Nvidia falls flat


GOOGLE PLASTIC?

Report: Google to launch a Gear VR competitor, build VR into Android OS

TAKE IT TO THE LIMIT

UK, Dutch police may use attack eagles to take down drones

 **Firewatch review: Getting lost in the remote wilderness and loving it**

 **Winners act as thick as thieves**

DanNeely wrote:

The problem is that, like with most hard problems, there are *NO* good solutions. We could:

- 1) Yank the plug before a disaster happens; don't have any fallback mechanisms in place. This is the current plan. It will have the unfortunate effect of cutting off millions of people whose \$10 featurephone with a minimalistic web browser is the only way they can get online, and which they can't afford to replace because \$10 is a weeks total income/a years disposable income making it unaffordable.
- 2) Maintain the status quo. Allow SHA1 to continue to be used. This keeps poor people who can't afford to replace their very low end hardware able to access the internet. Eventually, we'll discover that someone, either an entity that owns super computers; or that runs botnets with supercomputer scale compute capacity is breaking SHA1 for malicious purposes. In this case, the abrupt, disorderly shutdown that occurs when the major players all pull the plug in SHA1 immediately after the disclosure will be messy and spread the harm across most than just people who'd lose any secure internet access.
- 3) Pull the plug for most people but offer a fallback for when they encounter people who can't do SHA256. This is Facebook's proposal. The problem is that the same entities who'd break SHA1 and abuse it in scenario 2 would still be able to do so by conducting a man in the middle downgrade attack.

Pick your poison. These choices all suck.

I think what I'd like Facebook to do is make this a setting I can configure for my own account/data.

"This account should never be permitted to access anything via SHA1, and none of the data I share with any privacy controls turned on should be viewable via SHA1."

Then I wouldn't be subject to MITM attacks. Folks who need SHA1 would have their accounts configured accordingly, but the rest of us would be able to ignore many of the security issues that creates.

2935 posts | registered May 7, 2011

vcsjones | Smack-Fu Master, in training | **et Subscriptor**

[jump to post](#)

dfjde julio wrote:

 [show nested quotes](#)

I think what I'd like Facebook to do is make this a setting I can configure for my own account/data.

"This account should never be permitted to access anything via SHA1, and none of the data I share with any privacy controls turned on should be viewable via SHA1."

Then I wouldn't be subject to MITM attacks. Folks who need SHA1 would have their accounts configured accordingly, but the rest of us would be able to ignore many of the security issues that creates.

It's not something Facebook can do, it's something your browser would have to do because the TLS handshake comes before anything else. By the time Facebook's application layer knows it's you and SHA1 should be blocked, you've already transmitted your authentication cookie, request body, etc.

What Facebook could do is provide a completely separate domain that uses SHA1, like "sha1.facebook.com" that uses a SHA1 certificate, but that's incredibly user unfriendly and would require an update to apps, and updates (whether it's the operating system or an app) are part of the problem in the first place.

61 posts | registered Dec 4, 2013

SmokeTest | Wise, Aged Ars Veteran

[jump to post](#)

I'm a little surprised to see security professionals (Cloudflare) calling for a fallback mechanism. I haven't read the details of their proposal, but fallback mechanisms in security are *extremely* dangerous. There is the potential for an attacker to simply downgrade you to the less secure standard, which they can then attack. It's a common attack on SSL for misconfigured servers.

That said, I'm sensitive to the problem at hand. HTTPS everywhere is going to happen sooner or later, and if 7% of the world can't use the accepted cipher, then this is a big problem. So it seems that allowing SHA-1 in some form or another is unavoidable.

The downgrade problem could be mitigated somewhat by communication. If users hitting the less secure certificate got redirected to insecure.foo.com, then it would make it obvious if your session had been downgraded, and provide a nice, strong motivation to get secured. But good luck getting Facebook et. al. to put the word "insecure" in anything. Your average know-nothing computer user posting cat pics would lose their mind.

I mean, we are talking about a website where tens of thousands of users misidentified a blog post about Facebook as the Facebook login page and posted their account name and password as comments on the blog (along with complaints that they don't like the new design) because it was the top Google result for "facebook login".

528 posts | registered Feb 19, 2015

Kayling | Smack-Fu Master, in training

[jump to post](#)

toast0 wrote:

 [show nested quotes](#)

How does serving SHA1 certificates to shitty clients hobble the web for clients that indicate support for SHA2 and receive a SHA2 certificate? Would you rather have the shitty clients get their traffic via https with a certificate you wouldn't trust but they do, or http?

The potential problem is that on sites which still support sha1, a man-in-the-middle attacker can downgrade /anyone/ to sha1. So it wouldn't matter if your browser said it supported something stronger.

3 posts | registered May 19, 2014

READER COMMENTS 171



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 →](#)

SPONSORED STORIES POWERED BY OUTBRAIN



SCIENTIFIC AMERICAN

Reversing Mitochondrial Decay With Supplements That Increase Cellular Levels of NAD



TRUTHFINDER

New Website Reveals All the Dirt Google Can't Find



KELLEY BLUE BOOK

The 10 Most Awesome Cars That Cost Under \$18,000



VIRAL IMPLOSION

This Is Why You Don't Mess With The US! Watch What Happens!



INSTANT CHECKMATE

Forget Googling them, this site reveals all. Simply enter a name and state of anyone you know, what will you learn today?



THE MODERN MAN TODAY

How Older Men Tighten Their Skin

YOU MAY ALSO LIKE 

SITE LINKS

[About Us](#)

[Advertise with us](#)

[Contact Us](#)

[Reprints](#)

SUBSCRIPTIONS

[Subscribe to Ars](#)

MORE READING

[RSS Feeds](#)

[Newsletters](#)

[Visit Ars Technica UK](#)

CONDE NAST SITES

[Reddit](#)

[Wired](#)


[Vanity Fair](#)

[Style](#)

[Details](#)

Visit our sister sites

Subscribe to a magazine



VIEW MOBILE SITE

CONDÉ NAST

© 2016 Condé Nast. All rights reserved

Use of this Site constitutes acceptance of our [User Agreement](#) (effective 1/2/14) and [Privacy Policy](#) (effective 1/2/14), and [Ars Technica Addendum](#) (effective 5/17/2012)

[Your California Privacy Rights](#)

The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.

[Ad Choices](#)