THE VERGE

GOOGLE \ TECH \ CYBERSECURITY 17

Google just cracked one of the building blocks of web encryption (but don’t worry)

It’s all over for SHA-1

By Russell Brandom | @russellbrandom | Feb 23, 2017, 11:49am EST

SHARE MORE

Today, Google made major waves in the cryptography world, announcing a public collision in the SHA-1 algorithm. It’s a deathblow to what was once one of the most popular algorithms in cryptography, and a crisis for anyone still using the function. The good news is, almost no one is still using SHA-1, so you don’t need to rush out and install any patches. But today's announcement is still a major power play from Google, with real implications for web security overall.

Like most cryptography, it can get a little complicated, so it's probably best to start from the very beginning...

WHAT JUST HAPPENED?

Google publicly broke one of the major algorithms in web encryption, called SHA-1. The company's researchers showed that with enough computing power — roughly 110 years of computing from a single GPU for just one of the phases — you can produce a collision, effectively breaking the algorithm. We've known this was possible for a while, but nobody has done it, in part because of the possible fallout.

A DEATHBLOW TO A ONCE-POPULAR ALGORITHM

In accordance with its disclosure policy, Google is waiting 90 days to say exactly how they did it — but once the proof-of-concept is out, anyone with enough computing power will be able to produce a SHA-1 collision, rendering the algorithm both insecure and obsolete.

It's hard to say if Google's researchers are the first people to do this (<cough> NSA <cough>), but they're the first ones to talk about it, which has major implications for anyone still using SHA-1.

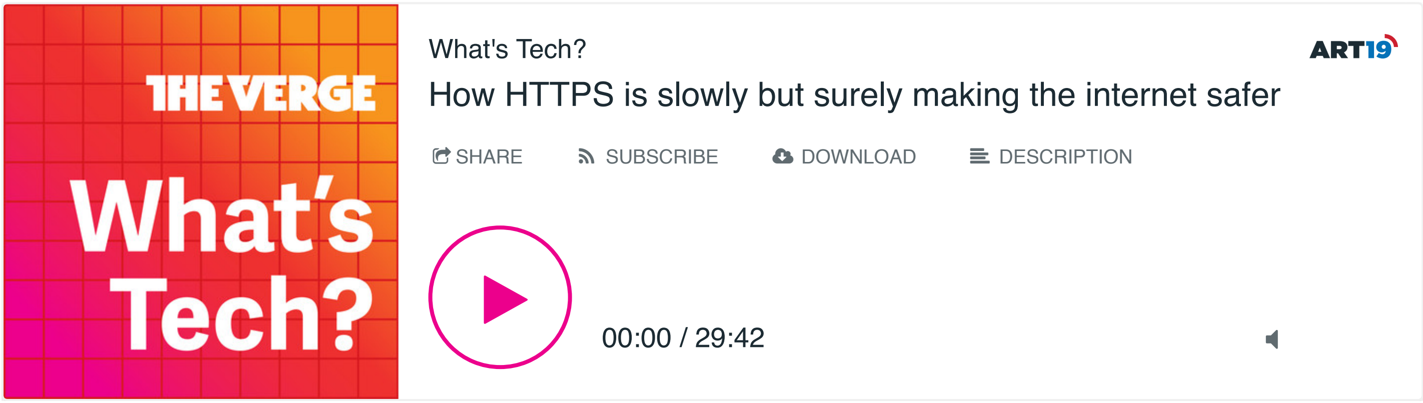
WHAT DOES SHA-1 ACTUALLY DO?

SHA-1 is a hashing function, which produces a digital fingerprint from a given file. That lets you verify a file's integrity without exposing the entire file, simply by checking the hash. If the hash function is working properly, each file will produce a unique hash — so if the hashes match, the files themselves will also match. That's particularly important for login systems, which need to verify that a password is correct without exposing the password itself.

WHAT'S A COLLISION AND WHY DOES IT MATTER?

A collision is what happens when a hashing function breaks, and two files produce the same hash. That could allow an attacker to smuggle in a malicious file because it shares its hash with a legitimate file. As proof-of-concept for today's announcement, Google published two PDF files that, run through SHA-1, produce the same hash.

In practical terms, a broken hash function could be used to break HTTPS, the encryption system that now protects more than half the web. You can learn more about that system from the podcast below (there's a whole pie-ribbon-curse metaphor; it's great), but the gist is that it guarantees that the content you see at Wikipedia.com is really coming from Wikipedia and hasn't been tampered with along the way. If that system breaks, it would be easy for criminals to insert malware into web traffic from a compromised ISP or other network provider.



What's Tech?

How HTTPS is slowly but surely making the internet safer

SHOULD I BE WORRIED?

Unless you make a habit of clicking through those scary red screens, you'll be fine. Cryptographers have been predicting a collision like this for years, making ever more specific predictions about how you'd produce one and how much computing power it would take. This is the first time anyone's burned the server time to actually do it, but we've known something like this was possible for a while.

As a result, most sites have already dropped SHA-1. As recently as 2014 it was being used for as much as 90 percent of the encryption on the web, but it's been mostly abandoned in the years since. As of January 1st, every major browser will show you a big red warning when you visit a site secured by SHA-1. It's hard to say how many of those sites are left, but anyone with a halfway decent certificate provider is already safe.

SHA-1 is still used in a couple places outside web encryption — particularly Git repositories — but given how long the algorithm has been deprecated, the broader impact shouldn’t be that widespread.

WHY DID GOOGLE DO THIS?

The short version is, they wanted to win the argument. Dropping SHA-1 took a lot of time and effort across the industry, and not everyone was eager to do it. The result has been a running fight over how fast make the switch — with Google’s Chrome Security Team providing one of the loudest voices for a faster transition. Chrome was forcing websites away from SHA-1 as early as 2014, long before other browsers started cracking down. Firefox caught on fairly quickly, too, with Microsoft’s Edge and IE bringing up the rear.

THIS IS A FIGHT ABOUT HOW SECURE THE WEB NEEDS TO BE

Chrome’s early moves caused a lot of grief among certificate providers — but now that there’s a proof-of-concept collision out there, the Chrome Security Team looks pretty smart. If we’d listened to the slowpokes, this collision could have been a major problem! Instead, the industry moved fast, everyone’s safe, and we have to write blog posts to explain why it matters at all.

In a broader sense, this is a fight about how secure the web needs to be. If you’re making smartphones or selling apps, you might not think it’s worth it to force the entire web off of a shaky algorithm. What does it matter if a few janky websites are slow to make the switch? But Google still a web advertising company, and that means any breakdown in web security is an existential threat. Whenever an algorithm like SHA-1 breaks, ad networks are among the first to be targeted, so Google’s heavily invested in making sure those encryption systems work. And since Google’s ads are served across the entire web, they need to make sure everyone’s on board. Sometimes that means cracking a few heads!

So while it might seem like a mathematical curiosity, this is really a victory lap for Google — and one that cost quite a bit of server time. People have been saying SHA-1 was shaky for years, and now we all know they were right. Luckily, we all listened to the crypto folks, and nothing too serious got broken. You’re welcome.