Forbes / Security / #CyberSecurity
FEB 23, 2017 @ 11:09 AM 15,232

Google Just 'Shattered' An Old Crypto Algorithm -- Here's Why That's Big For Web Security

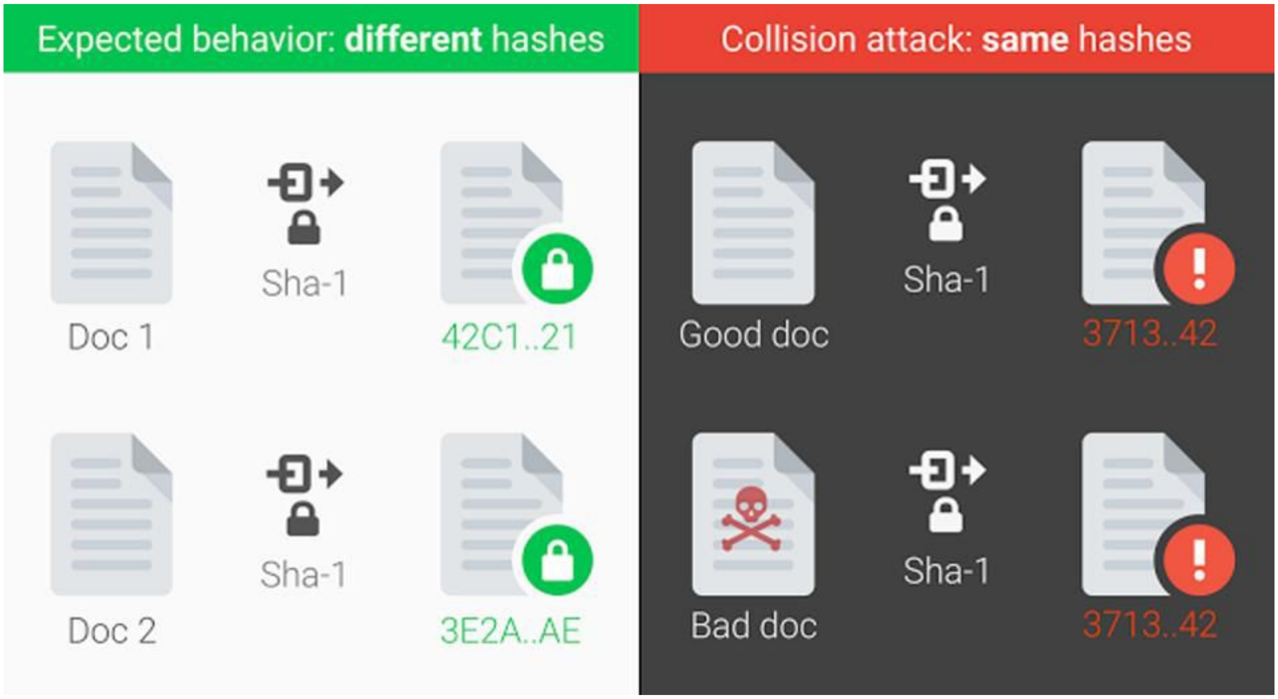
Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. **FULL BIO**

It might not sound like the most important milestone in cybersecurity, but today Google cracked an old cryptographic algorithm called SHA-1. It's significant because SHA-1 has been in use across the web for some time, largely to check the authenticity of digital artefacts flying around the internet.

To understand what Google did, we have to understand what SHA-1 is. It's known as a "cryptographic hash function." That is, a mathematical algorithm that takes a digital object and turns it into a "digest", or hash, which is simply a representation of that object, which could be a file or a message. The hash is just a string of characters, and in the case of SHA-1, it's 40 characters. It'll look something like this: 988881adc9fc3655077dc2d4d757d480b5ea0e11. (Thanks to security researcher Andreas Lindh for giving me this simplified explanation and that hash example, which is the hash of a test file he created).

Now, that hash should be unique and only represent that single file. Identical files will have the same hash. But it shouldn't be possible for someone to create an entirely different file and have SHA-1 give it the same hash. But using some extreme maths and computing power, that's what Google did, alongside researchers from the CWI Institute in Amsterdam, with two distinct PDFs. This is known as a "collision" and such attacks are very rare indeed.

How does the math translate into an attack? Imagine that second file is malware or a forged document, like a certificate designed to guarantee the authenticity of a website, such as Google.com. An attacker could have their malware or their fake website trusted by any system that checks SHA-1 hashes to verify. "Another use case could be if you are using application whitelisting on your computer, which uses hashes to verify that the files are what they claim to be, it could be possible for a malware file to have the same hash as for example Word or some other trusted application," noted Lindh.



Google's illustration of how a collision attack occurs.

No need for panic

Because this old and widely-deployed algorithm is broken doesn't mean people need to panic. For some time now, major web companies have downgraded SHA-1 and won't use it to carry out those verification processes. For instance, the Chrome browser will automatically mark any SSL certificate signed using SHA-1 as insecure.

The Shattered attack, as named by Google, could work in select scenarios where SHA-1 is still trusted. GnuPG e-mail encryption, for instance, deems it safe. Meanwhile, as noted by security expert Kevin Beaumont, Microsoft still relies on SHA-1, even if it's phasing the algorithm out.

> Fun fact - SHA-1 deprecation patches for Windows were due earlier this month, but held back for quality reasons.
>
> — Kevin Beaumont (@GossiTheDog) February 23, 2017

Microsoft previously announced plans to deprecate SHA-1 by the middle of this year. When that happens, it'll follow in Google's footsteps so that its Internet Explorer and Edge browsers will prevent sites protected with a SHA-1 certificate from loading and will display a warning. The next release of Windows 10 will also block SHA-1 by default in the browser. Firefox is planning to do the same this year too.

A Microsoft spokesperson said: "Today's report is further evidence that SHA-1's useful lifetime has ended as part of the normal lifecycle of encryption technologies. Microsoft has worked with the industry since 2012 to phase out the use of SHA-1. Microsoft Edge and IE 11 do not consider websites using SHA-1 certificates secure, so do not show the lock icon that’s used to indicate a secure site in the browser’s address bar."

Google still thinks its research should spur on all companies still using the algorithm to move away from SHA-1, which has long been deemed vulnerable. "We hope that our practical attack against SHA-1 will finally convince the industry that it is urgent to move to safer alternatives such as SHA-256," read a company blog post.

To be clear, anyone wanting to carry out the attack for real would require astonishing computing power. The researchers had to use the equivalent of 6,500 years of CPU computation and 110 years of GPU computation to complete the two phases of the technique, and an astonishing 9,223,372,036,854,775,808 SHA-1 computations. But Google will soon tell people just how they carried out the research, making attacks a little likelier. "We will wait 90 days before releasing code that allows anyone to create a pair of PDFs that hash to the same SHA-1," the company added.

But in the future, expect other similar hashing algorithms to fall, said Alan Woodward, a cryptography expert from the UK's University of Surrey. "In essence, what this shows is that some of the older hashes are subject to this kind of attack as computing power has moved on enormously since their introduction: just think how much more computing power we all have available than was available ten years ago when SHA1 came on the scene," he said. "We knew it was coming and now it has."

Got a tip? Email at TFox-Brewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail. Get me on Signal on +447837496820 or use SecureDrop to tip anyone at Forbes.