https://www.forbes.com/sites/thomasbrewster/2017/10/16/worse-than-krack-google-and-microsoft-patch-massive-5-year-old-encryption-hole/#5d9544ed47c3

OCT 16, 2017 @ 10:41 AM

'Worse Than KRACK' -- Google And Microsoft Hit By Massive 5-Year-Old Encryption Hole

Thomas Fox-Brewster , FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

infineon
Production Villach
Innovative semiconductor solutions for energy efficiency, mobility and security

Widespread vulnerability in Infineon chips gives people another reason to update their devices. (Photographer: Krisztian Bocsi/Bloomberg).

It's just another manic Monday in the cybersecurity world. First there was KRACK, a vulnerability that allowed for snooping on almost anyone's Wi-Fi. Now there's the plainer-named ROCA -- another complex but dangerous weakness in widely used cryptography found in chips made by German company Infineon Technologies AG. Fujitsu, Google, HP, Lenovo and Microsoft have all pushed out fixes for their relevant hardware and software, so users should update where they can. Again.

The problem in the Infineon chips is to do with the vendor's implementation of the encryption, based in this case on the widely-used RSA standard. Thanks to the bugs, it's possible to calculate someone's private key by just having the public key. A large number of Google Chromebook and Windows devices created by Fujitsu, HP and Lenovo are amongst those affected. "The currently confirmed number of vulnerable keys found is about 760,000 but possibly up to two to three magnitudes more are vulnerable," the researchers warned. They'll present their full findings at the ACM Conference on Computer and Communications Security later this month.

So what?

To understand the seriousness of the academics' findings, a quick recap on the basics of public key encryption is required. To start, a private and a public key are derived from two large prime numbers being multiplied together. Those prime numbers must be kept secret and should be incredibly difficult for an outside party to determine, due to the fact that it's very hard to deduce the factors of the large sum, even if one of the numbers is already known. But anyone who can get hold of both those original prime numbers can create a key pair and read messages.

In the ROCA hack, the researchers (from the Centre for Research on Cryptography and Security, Masaryk University, Enigma Bridge and Ca' Foscari University) crafted a version of an old technique called the Coppersmith's attack -- ROCA stands for the Return of Coppersmith's Attack. It relies on the fact that the publicly-shared number (called, by crypto experts, as the modulus) can be factored to reveal the crucial primes. Infineon didn't check that its moduli weren't factorable and so millions of devices are now thought to be vulnerable. Ultimately, the company's pseudorandom number generator didn't generate truly random numbers, said University of Surrey cryptography specialist Professor Alan Woodward.

There are limitations to the attacks. As noted by Woodward: "It probably is only practical against 1024-bit keys. 2048 is pushing it and higher forget it." (The higher the bits, mean the bigger the number, which would be harder to factor and therefore get those prime figures). The researchers noted differences in the energy it would take to derive private keys too, saying that running an attack via Amazon cloud servers, it'd cost just $76 for the 1024-bit key and about $40,000 for the 2048-bit version.

Making KRACK look like a baby

But to former NSA staffer and chief of cybersecurity company RenditionSec, Jake Williams, the ROCA issue is more severe than KRACK. The latter was only executable within Wi-Fi range, while it's uncertain as to whether patches will be rolled out widely for ROCA, given it's a more esoteric issue, he added. The vulnerability has also been present in affected devices since at least 2012.

Williams theorized two attacks over ROCA. First, by abusing code signing certificates, used to validate software is coming from a legitimate, trusted source. "Given a code signing certificate's public key (which an organization has to publish), an attacker could derive the private key allowing them to sign software impersonating the victim," Williams said. Given the kinds of attacks that have recently relied on fake software updates (remember the NotPetya ransomware and the CCleaner infection), this could be a serious threat.

An attacker could also potentially fool a Trusted Platform Module (TPM) -- a specialized chip on a computer or smartphone that stores RSA encryption keys - to run malicious, untrusted code, Williams added. "The TPM is used to ensure the code used to boot the kernel is valid. Bypassing a TPM could allow the attacker to perform an inception style attack where they virtualize the host operating system. There are dozens of other variations of attacks, but these Infineon chips are huge in hardware security modules (HSMs) and TPMs," he warned.

With patches available, users' and IT teams' first recourse should be vendor updates. Infineon, Google and Microsoft all put out notices last week ahead of today's reveal, which all include advice for concerned users. Estonia's national ID card system was also affected, with 750,000 affected by the weakness, opening up the threat of identity theft, according to local media.

Second, it's possible to check whether keys are vulnerable by visiting https://keychest.net/roca and entering the public key there. And there's more advice on the researchers' advisory.

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.