Never mind the WPA2 drama... Details emerge of TPM key cockup that hits tonnes of devices

About a third of all crypto modules globally generate weak, crackable RSA pairs

By John Leyden 16 Oct 2017 at 22:14
https://www.theregister.co.uk/2017/10/16/roca_crypto_vuln_infineon_chips/

RSA keys produced by smartcards, security tokens, laptops, and other devices using cryptography chips made by Infineon Technologies are weak and crackable – and should be regenerated with stronger algorithms.

In short, Infineon TPMs – aka trusted platform modules – are used in countless computers and gadgets to generate RSA key pairs for securing VPNs, implementing trusted boot sequences, performing whole disk encryption, granting access to cloud accounts, producing encryption certificates, and more. The secrets at the heart of these systems can be mathematically cracked by determined adversaries, allowing them to potentially gain control of computers and decipher data secured by the TPM-built RSA keys.

We've previously covered the firmware bug on these pages. Now, while everyone's distracted by the WPA2 KRACK flaw, a few more details of the Infineon screwup have emerged, and you should check them out to make sure you're not affected or take action if so. For example, the bug

causes some Yubikey 4 gadgets to generate weak authentication keys, and should be replaced as soon as possible.

Essentially, you should upgrade your TPM's firmware, via updates from your device's manufacturer or operating system's maker, as soon as possible, and refresh your weak keys using the new code on the hardware or using a stronger implementation.

Crypto expert Thomas Ptáček had this to say:


Thomas H. Ptáček @tqbf
The Infineon bug is a bigger deal than the WiFi bug.
3:32 PM - Oct 16, 2017 · Austin, Chicago

- 17 Replies

- 180 Retweets

- 362 likes

Twitter Ads info and privacy


Thomas H. Ptáček @tqbf
Replying to @tqbf
Meanwhile: we'll be checking RSA keys for this stupid Infineon prime search bug for the next 10 years.
7:23 PM - Oct 16, 2017 · West Town, Chicago

- 2 Replies

The TPM vulnerability can be exploited to compute, by factorization, the private keys from public keys in TPM-generated RSA private-public key pairs. Suffice to say, this shouldn't be possible, and the private component is supposed to remain secret.

The bug lies in the chipset's firmware code that generates key pairs, and was discovered by a team of researchers at Masaryk University in Brno, Czech Republic; UK security firm Enigma Bridge; and Ca' Foscari University of Venice, Italy. Infineon security chips manufactured from 2012 onwards, including the latest versions, are all vulnerable.

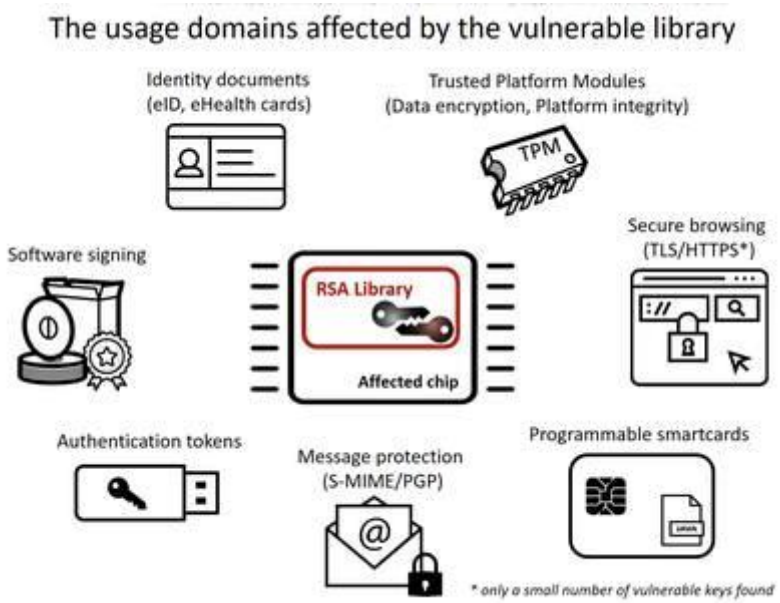
We're told you'll need somewhere in the region of $30,000 in cloud computing power to crack a 2,048-bit RSA key pair generated by the dodgy Infineon hardware. For 1,024-bit keys, which are generally crap anyway, it is trivial to factorize a vulnerable private key.

“The attack is practical, although it’s unlikely to be cost-effective for large-scale attacks,” Dan Cvrcek of Enigma Bridge told *El Reg* on Monday. “The current indicative processor times for 1,024 and 2,048 bit keys are 97 vCPU days ($40 to $80) and 51,400 vCPU days ($20,000 to $40,000), respectively.

“Worst hit, at the moment, seems to be ... whole-disk encryption, as well as for securing access to some cloud platforms, but it extends to non-repudiation signatures, email signing, access to VPN and buildings, e-Health cards, and e-IDs."

Cvrcek estimated that Infineon's TPMs are "25 to 30 per cent of TPMs used globally." The flawed Infineon chipset has been integrated into motherboards, laptops including Chromebooks, authentication systems, trusted boot mechanisms, and cryptographic tokens sold by computer and device makers worldwide.

Major vendors including HP, Lenovo and Fujitsu have released software updates and mitigation guidelines.



An idea of the stuff affected by the TPM bug ... From the bug's researchers

The vulnerability has been dubbed ROCA, aka Return of Coppersmith's Attack aka CVE-2017-15361, and is believed to be behind recent security problems with Estonian ID cards. The code flaw was documented by Google and Microsoft last week.

Full details of the research, including the factorisation method, will be released at the ACM's Computer and Communications Security (CCS) conference. A paper, "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli," will be unveiled at the confab in Dallas, Texas, on November 2.

Ahead of the talk, the researchers have produced offline and online detection tools that will allow folks to figure out whether or not their keys are affected by the issue. ®