ROCA 'round the lock: Gemalto says IDPrime .NET access cards bitten by TPM RSA key gremlin

Here's what to do if you have an affected badge

By John Leyden 23 Oct 2017 at 19:28
https://www.theregister.co.uk/2017/10/23/roca_crypto_flaw_gemalto/

Some Gemalto smartcards can be potentially cloned and used by highly skilled crooks due to a cryptography blunder dubbed ROCA.

Security researchers went public last week with research that revealed that RSA keys produced for smartcards, security tokens, and other devices by crypto-chips made by Infineon Technologies were weak and crackable.

In other words, the private half of the RSA public-private key pairs in the gadgets, which are supposed to be secret, can be calculated from the public half, allowing the access cards and tokens to be cloned by smart attackers. That means keycards and tokens used to gain entry to buildings and internal servers can be potentially copied and used to break into sensitive areas and computers.

Infineon TPMs – AKA trusted platform modules – are used by various computers and gadgets to generate RSA key pairs for numerous applications. A bug in the chipset's key-generation code makes it possible to compute private keys from public keys in TPM-generated RSA private-public key pairs. The research was put put together by a team from

Masaryk University in Brno, Czech Republic; UK security firm Enigma Bridge; and Ca' Foscari University of Venice, Italy.

Infineon TPMs manufactured from 2012 onwards, including the latest versions, are all vulnerable. Fixing the problem involves upgrading the module's TPM firmware, via updates from your device's manufacturer or operating system's maker.

Major vendors including HP, Lenovo and Fujitsu have released software updates and mitigation guides for their laptops and other computers. ROCA – short for Return of Coppersmith's Attack AKA CVE-2017-15361 – hit the Estonian ID card system, too.

Although not included in the initial casualty list, it turns out some Gemalto smartcards are also affected by the so-called ROCA vulnerability. Gemalto confirmed to *El Reg* today that some of its tech – specifically the IDPrime .NET access cards – are affected while downplaying the significance of the problem and saying remediation work was already in hand:

There has been a recent disclosure of a potential security vulnerability affecting the Infineon software cryptographic library also known as ROCA (CVE-2017-15361). The alleged issue is linked to the RSA on-board key generation function being part of a library optionally bundled with the chip by this silicon manufacturer. Infineon have stated that the chip hardware itself is not affected. As Gemalto sources certain products from Infineon, we have assessed our entire product portfolio to identify those which are based on the affected software. Our thorough product analysis has concluded that:
It is standard practice that Gemalto's products use our in-house cryptographic libraries, developed by our internal R&D teams and experts in cryptography. In the vast majority of cases, the crypto libraries developed by the chip manufacturer are not included in our products. We can confirm that products containing Gemalto's crypto libraries are immune to the attack. A very limited set of customized products (including IDPrime.NET) are affected. We have already contacted the customers using these products and are currently working with them on remedial solutions.

As of today, this theoretical vulnerability has only been demonstrated as a mathematical possibility but no real cases have been seen to date.

Gemalto takes this issue very seriously and has set up a dedicated team of security experts to work on it and we will continue to monitor any evolution to the situation.

Dan Cvrcek, of Enigma Bridge and one of the ROCA researchers, said: “Gemalto stopped selling these cards [IDPrime .NET smartcards] in September 2017, but there are large numbers of cards still in use in corporate environments. Their primary use is in enterprise PKI systems for secure email, VPN access, and so on.

“ROCA does not seem to affect Gemalto IDPrime MD cards. We have also no reason to suspect the ROCA vulnerability affects Protiva PIV smart cards, although we couldn’t test any of these."

Cvrcek has blogged about the issue here.

A paper detailing the research – titled The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli – is due to be published at the ACM’s Computer and Communications Security conference in Dallas, Texas, on November 2. There is no public exploit code for the TPM flaws that we know of. While we all wait for more technical details of the vulnerability to be released, this online checkercan be used to test RSA keys for ROCA-caused weaknesses.

Cvrcek added: "We managed to get two short RSA keys (512 bits only) from .NET cards (manufactured 2008 and 2017). The research team estimated the time needed for the attack to be up to two hours. The actual timing was 20 minutes (one CPU core) for one of the keys and three minutes (a 'normal' laptop) for the other.

"This verified that the ROCA test was accurate and also that the .NET attack was not theoretical," he added.®