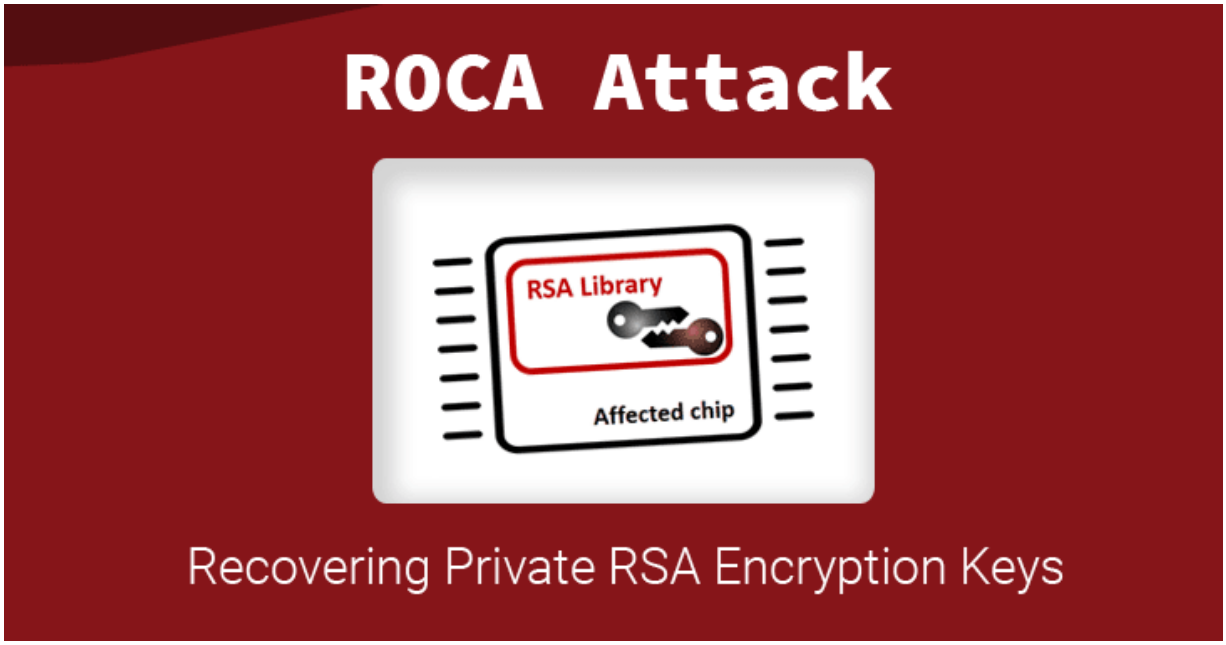
Serious Crypto-Flaw Lets Hackers Recover Private RSA Keys Used in Billions of Devices

Monday, October 16, 2017 Swati Khandelwal
https://thehackernews.com/2017/10/rsa-encryption-keys.html



If you think KRACK attack for WiFi is the worst vulnerability of this year, then hold on…

...we have got another one for you which is even worse.

Microsoft, Google, Lenovo, HP and Fujitsu are warning their customers of a potentially serious vulnerability in widely used RSA cryptographic library produced by German semiconductor manufacturer Infineon Technologies.

It's noteworthy that this crypto-related vulnerability (CVE-2017-15361) doesn't affect elliptic-curve cryptography and the encryption standard itself, rather it resides in the implementation of RSA key pair generation by Infineon's Trusted Platform Module (TPM).

Infineon's Trusted Platform Module (TPM) is a widely-used, dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices and is used for secured crypto processes.

This 5-year-old algorithmic vulnerability was discovered by security researchers at Masaryk University in the Czech Republic, who have released a blog post with more details about the weakness as well as an online toolto test if RSA keys are vulnerable to this dangerous flaw.

ROCA: Factorization Attack to Recover Private RSA Keys

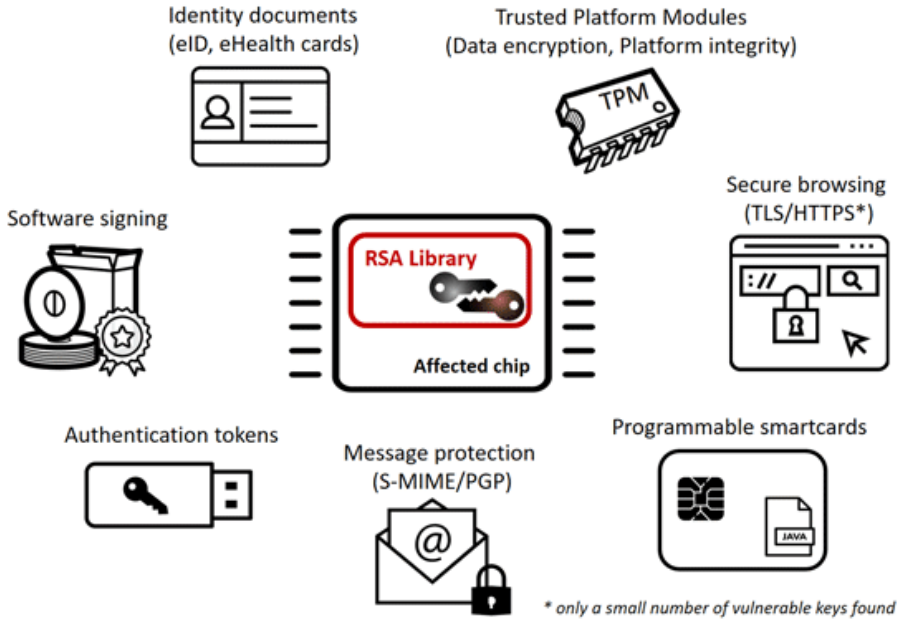
Dubbed **ROCA** (**Return of Coppersmith's Attack**), the factorization attack introduced by the researchers could potentially allow a remote attacker to reverse-calculate a private

encryption key just by having a target's public key—thanks to this bug.

"Only the knowledge of a public key is necessary and no physical access to the vulnerable device is required," the researchers said. "The vulnerability does NOT depend on a weak or a faulty random number generator—all RSA keys generated by a vulnerable chip are impacted."

This could eventually allow the attacker to impersonate key owner, decrypt victim's sensitive data, inject malicious code into digitally signed software, and bypass protections that prevent accessing or tampering with the targeted computer.

ROCA Attack Exposes Billions of Devices to Attack



The ROCA attack affects chips manufactured by Infineon as early as 2012 and is feasible for key lengths, including 1024 and 2048 bits, which is most commonly used in the national identity cards, on PC motherboards to securely store passwords, in authentication tokens, during secure browsing, during software and application signing, and with message protection like PGP.

The flaw also weakens the security of government and corporate computers protected using Infineon's cryptographic library and chips.

Majority of Windows and Google Chromebook devices developed by HP, Lenovo and Fujitsu are amongst those affected by the ROCA attack.

"We found and analyzed vulnerable keys in various domains including electronic citizen documents, authentication tokens, trusted boot devices, software package signing, TLS/HTTPS keys and PGP," the researchers said.

"The currently confirmed number of vulnerable keys found is about 760,000 but possibly up to two to three magnitudes more are vulnerable."

More Details, Testing Tool, and Patches

The security researchers have released a brief blog post about the flaw, which includes a number of tools for detection, mitigation and workarounds.

The vulnerability was discovered and reported to Infineon Technologies in February this year and the researchers will present their full findings, including the factorization method, on November 2nd at the ACM Conference on Computer and Communications Security.

Their research paper, titled *"The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli"* (ROCA), will also be released after their presentation.

So, companies and organisations have enough time to change affected encryption keys before the details of how this vulnerability works and could be exploited are released.

Major vendors including Infineon, Microsoft, Google, HP, Lenovo, and Fujitsu have already released the software updates for their relevant hardware and software as well as guidelines for a mitigation of this vulnerability.

"Some Windows security features and potentially third-party software rely on keys generated by the TPM (if available on the system)," according to a Microsoft advisory. "Microsoft is releasing Windows security updates to help work around the vulnerability by logging events and by allowing the generation of software based keys."

Therefore, users are strongly recommended to patch their devices as soon as possible—AGAIN!