As devastating as KRACK: New vulnerability undermines RSA encryption keys

A new security flaw has placed the security of RSA encryption in jeopardy.

By Charlie Osborne for Zero Day | October 17, 2017 -- 08:57 GMT (09:57 BST) |

Topic: Security

http://www.zdnet.com/article/as-devastating-as-krack-new-vulnerability-undermines-rsa-encryption-keys/

(Image: File Photo)

Flawed chipsets used by PCs to generate RSA encryption keys have a vulnerability that has weakened the security of stored passwords, encrypted disks, documents, and more.

MORE SECURITY NEWS

- **Android security: Google cracks down on apps that want to use accessibility services**
- **Resilience to phishing attacks is failing to improve**
- **Google: Our hunt for hackers reveals phishing is far deadlier than data breaches**
- **Equifax spends $87.5 million on data breach, more expenses on deck**

This week, researchers from the Centre for Research on Cryptography and Security at Masaryk University, Czech Republic; Enigma Bridge Ltd, Cambridge, UK; and Ca' Foscari University of Venice, Italy, revealed the flaw in cryptographic smartcards, security tokens, chipsets and secure hardware manufactured by German semiconductor firm Infineon Technologies.

The ROCA vulnerability, CVE-2017-15361, relates to the Trusted Platform Module (TPM) used to cryptographically sign and protect computer systems and services. The bug was discovered within the implementation

of RSA keypair generation in a cryptographic library used by Infineon TPM products, allowing what is called a "practical factorization attack."

This attack type permits a threat actor to use a target's public key to generate a private key with some time and power. The attack is possible for common key lengths, including 1024 and 2048 bits.

Any RSA keys generated by the firm's flawed products are not truly randomized, leaving them weak and therefore crackable, and as the bug-ridden product line -- including NIST FIPS 140-2 and CC EAL 5+ certified devices -- extends back to as early as 2012, these products are now commonplace -- placing countless supposedly secure files and keys at risk.

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

The attack was verified using randomly selected 1024-bit RSA keys and for several selected 2048-bit keys.

The team has provided rough estimates on how long and how much it would cost attackers to be able to crack a private key based on their knowledge of a public key based on an Intel E5-2650 v3@3GHz Q2/2014, as below:

- 512 bit RSA keys - 2 CPU hours (the cost of $0.06)
- 1024 bit RSA keys - 97 CPU days (the cost of $40-$80)
- 2048 bit RSA keys - 140.8 CPU years, (the cost of $20,000 - $40,000)

4096-bit RSA keys are not practical to crack now, but the researchers say that it could be possible "should the attack be improved."

Infineon's cryptographic chips and TPMs are also integrated within authentication, signature and encryption tokens of other vendors and chips.

With such a wide array of applications, unless patched or worked around, the bug could shatter the security of everything from disk encryption to account security, secure browsing, software signing and authentication tokens.

"The actual impact of the vulnerability depends on the usage scenario, availability of the public keys and the lengths of keys used," the team said. "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 currently confirmed number of vulnerable keys found is about 760,000 but possibly up to two to three magnitudes more are vulnerable."

Google Chromebooks, HP, Lenovo and Fujitsu PCs and laptops, alongside routers and other devices are all affected.

It is important to note that RSA algorithms are not at fault here, but rather buggy products that mean the implementation of the security algorithm does not happen correctly and are not truly randomized.

The researchers have provided offline and online detection tools for users to check to see whether or not they are affected.

Vendors have not been left flat-footed. They may already be dealing with the aftermath of the KRACKA Wi-Fi WPA2 attack, but tech giants including Microsoft, Google, HP, Lenovo and Fujitsu have already posted security advisories, patch updates and guidelines to mitigate the problem.

The researchers discovered the bug in January, but now that Infineon and affected vendors have been given the best part of a year to develop fixes, they plan to reveal the full scale of the vulnerability in two weeks at the ACM Computer and Communications Security (CCS) conference.