SoylentNews

SoylentNews is people

Factorization Flaw in TPM Chips Makes Attacks on RSA Private Keys Feasible

posted by takyon on Wednesday October 18, @12:00PM
from the really-secure-amirite? dept.

Fnord666 writes:

> A flawed Infineon Technology chipset used on PC motherboards to securely store passwords, certificates and encryption keys risks undermining the security of government and corporate computers protected by RSA encryption keys. In a nutshell, the bug makes it possible for an attacker to calculate a private key just by having a target's public key.
>
> Security experts say the bug has been present since 2012 and found specifically in the Infineon's Trusted Platform Module used on a large number of business-class HP, Lenovo and Fijitsu computers, Google Chromebooks as well as routers and IoT devices.
>
> The vulnerability allows for a remote attacker to compute an RSA private key from the value of a public key. The private key can then be misused for purposes of impersonation of a legitimate owner, decryption of sensitive messages, forgery of signatures (such as for software releases) and other related attacks, according to researchers.
>
> The Infineon flaw is tied to a faulty design of Infineon's Trusted Platform Module (TPM), a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices and used for secured crypto processes.

Source: https://threatpost.com/factorization-flaw-in-tpm-chips-makes-attacks-on-rsa-private-keys-feasible/128474/

Original Submission

(1)

- **honest mistake (Score: 2) by crafoo on Wednesday October 18, @12:44PM (2 children)**

  by crafoo (6639) on Wednesday October 18, @12:44PM (#583903)

  Even the name should make you immediately skeptical: "Trusted Platform Module". Really? Trusted by whom, exactly? Certainly not me because I cannot verify what is inside.

  - **Re:honest mistake (Score: 2) by KiloByte on Wednesday October 18, @12:59PM**

    by KiloByte (375) on Wednesday October 18, @12:59PM (#583908)

    This is correct, but not in the common sense of the word. In security speak, "trusted" means "authorized to break your security".

    The word you're looking for is "trustworthy". Which also tends to be abused in marketing materials these days.

    --
    Ceterum censeo systemd esse delendam.

  - **Re:honest mistake (Score: 2) by DannyB on Wednesday October 18, @01:26PM**

    by DannyB (5839) on Wednesday October 18, @01:26PM (#583921)

    > Even the name should make you immediately skeptical: "Trusted Platform Module". Really?

    The name does make me immediately skeptical: "Trump Platform Module" Really?

    > Trusted by whom, exactly?

    How can I expect a TPM to be working in my best interest?

    It does things I neither wanted nor asked for. While I cannot verify what is on the inside of a TPM, I can see the results of having it installed and operational, without a means of overriding it or shutting it down in the BIOS.

- **security vs cost savings (Score: 3, Interesting) by bzipitidoo on Wednesday October 18, @12:58PM**

  by bzipitidoo (4388) ★ on Wednesday October 18, @12:58PM (#583907) Journal

  We know how to formally verify systems, and also when it is impractical to do so. This subsystem seems one in which thorough formal verification was possible, and that it would have caught the problem.

  However, formal verification can be a long, slow, and costly process. I can see them using formal verification on a few parts of a system, to say they did it, then skipping the rest, to save money and time, rush the good to market faster. To skip it on a security feature seems particularly stupid. Way to turn real security into more security theater.

  It may all be academic, when practical quantum computers with sufficient numbers of qbits are built. That will break RSA, and may even break all known methods of public key cryptography. That may only be a few years away, hard to say.

- **CVE (Score: 1, Insightful) by Anonymous Coward on Wednesday October 18, @01:02PM (2 children)**

  by Anonymous Coward on Wednesday October 18, @01:02PM (#583911)

  > CVE-2017-15361

  Ok, let's take a look. I don't look at those things as often as I should, so I'll go to NIST [nist.gov]:

  > The Infineon RSA library 1.02.013 in Infineon Trusted Platform Module (TPM) firmware, such as versions before 0000000000000422 - 4.34, before 000000000000062b - 6.43, and before 0000000000008521 - 133.33, mishandles RSA key generation, which makes it easier for attackers to defeat various cryptographic protection mechanisms via targeted attacks, aka ROCA. Examples of affected technologies include BitLocker with TPM 1.2, YubiKey 4 PGP key generation, and the Cached User Data encryption feature in Chrome OS.

  I guess I'll keep using free software to generate my keypairs. It's easier to `emerge -1av gnupg gnutls openssl` if there's a fix needed than to flash TPM firmware.

  - **CVSSv2 Scores (Score: 2) by AssCork on Wednesday October 18, @01:48PM**

    by AssCork (6255) ★ on Wednesday October 18, @01:48PM (#583941) Journal

    Just to put it in perspective, this has a higher 'base' score than KRACKATTACK, but the 'Overall' score is middle-of-the-pack.

    CVE-2017-15361 as scored by CERT [cert.org] (CVSSv2 for some reason)

    - **Base:** 8.8
    - **Temporal:** 6.9
    - **Environmental:** 6.9

    The 'overall' CVSSv2 score can be calculated by punching in the metrics CERT provides into the NVD CVSSv2 Score Calculator [nist.gov].

    - **Overall:** 6.9

    ProTIP: The 'Environmental' section is where an organization would make adjustments to a score. That's a Good Thing(tm), because some people implement technologies using a different strategy (though in this particular case, I don't know how you could mess with this)

  - **Bitlocker (Score: 2) by nobu_the_bard on Wednesday October 18, @01:50PM**

    by nobu_the_bard (6373) on Wednesday October 18, @01:50PM (#583944)

    I thought I recognized that term from something I read lately. I was looking into different Bitlocker configurations recently. Thank you for saving me the effort double checking it :)

    I'm surprised that didn't make it into the linked article, it is a popular feature on newer Microsoft Windows machines in some industries.

- **affects ID cards issued by Estonian government (Score: 0) by Anonymous Coward on Wednesday October 18, @01:38PM**

  by Anonymous Coward on Wednesday October 18, @01:38PM (#583932)

  https://www.reuters.com/article/us-infineon-cyber/infineon-says-has-fixed-encryption-flaw-found-by-researchers-idUSKBN1CL2KC [reuters.com]

- **Also Yubikey 4 (Score: 3, Informative) by Knowledge Troll on Wednesday October 18, @01:42PM**

  by Knowledge Troll (5948) on Wednesday October 18, @01:42PM (#583936) Journal

  See https://www.yubico.com/support/security-advisories/ysa-2017-01/ [yubico.com]

(1)

These screamingly hilarious gogs ensure owners of X Ray Gogs to be the life of any party. -- X-Ray Gogs Instructions