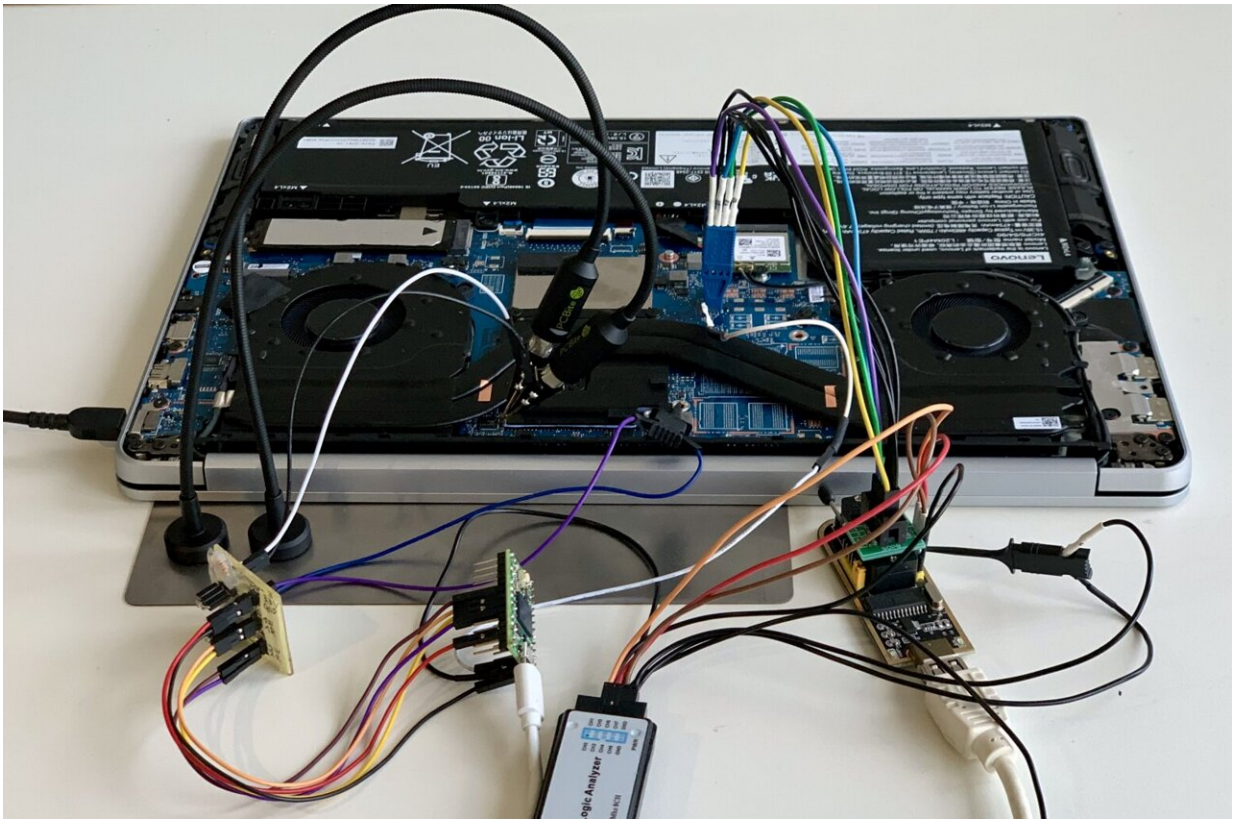
AMD fTPM vulnerability uncovered

May 3 2023, by Peter Grad



Attack setup on a Lenovo Ideapad 5 Pro-16ACH6. Credit: *arXiv* (2023). DOI: 10.48550/arxiv.2304.14717

Researchers at the Technical University of Berlin say they uncovered a new vulnerability in AMD's Trusted Platform Module (TPM). The flaw exposes firmware TPMs, or fTPMs, to attack.

This allows for extraction of cryptographic data stored in the fTPM, bypassing authentication barriers such as Platform Configuration Register validation and defenses against brute force attacks on passphrases.

Attacking a system's Trusted Execution Environment (TEE) "can lead to a full TPM state compromise," Hans Niklas Jacob warned in a paper, titled "faulTPM: Exposing AMD fTPMs' Deepest Secrets" and released last week on the *arXiv* preprint server.

One method of attack utilizes a voltage fault injection that tricks Zen 2 and Zen 3 CPUs into accepting false data that can be used to compromise any application or encryption process exclusively using TPM security.

TPMs originally were designed as discrete components physically attached to the motherboard to generate hardware-based encryption. They required an external bus to connect with the CPU. But the bus was vulnerable, providing an entryway for hackers targeting the CPU.

The fTPM was designed to incorporate encryption duties inside the chip, thus making a separate component, a potential entryway to hackers, unnecessary.

Jacob said that while discrete TPMs are still used in higher-end systems, fTPMs have proven to be convenient, more affordable alternatives for use in CPUs.

In the wake of skyrocketing firmware attacks—phishing, ransomware, supply chain—Microsoft in 2021 required users to have a PC supporting TPM in order to install Widows 11.

At that time, director of enterprise and OS security at Microsoft David

Weston explained the reason for the move was "to protect encryption keys, user credentials, and other sensitive data behind a hardware barrier so that malware and attackers can't access or tamper with that data."

As a result, many applications that underwent redesign to accommodate TPM 2.0 specifications are now vulnerable to hacking.

Jacob said his team believes their findings are "the first attack against Full Disk Encryption solutions backed by an fTPM." He said systems relying on a single defense mechanism, such as Bitlocker's TPM-only protector, can be overwhelmed by hackers who can gain access to a CPU for two or three hours.

"Applications relying exclusively on the TPM are left entirely unprotected," Jacob said, "while those employing multiple layers of defense face the loss of their TPM-based security layer." Materials used to undertake such attacks are inexpensive and easily available, he added.

An AMD spokesman, responding to an inquiry from Tom's Hardware, said, "AMD is aware of the research report attacking our firmware trusted platform module which appears to leverage related vulnerabilities previously discussed at ACM CCS 2021. This includes attacks carried out through physical means, typically outside the scope of processor architecture security mitigations."

The spokesman added, "We are continually innovating new hardware-based protections in future products to limit the efficacy of these techniques. Specific to this paper, we are working to understand potential new threats and will update our customers and end-users as needed."

More information: Hans Niklas Jacob et al, faulTPM: Exposing AMD fTPMs' Deepest Secrets, *arXiv* (2023). DOI: 10.48550/arxiv.2304.14717

Code: github.com/PSPReverse/ftpm_attack

Citation: AMD fTPM vulnerability uncovered (2023, May 3) retrieved 4 May 2024 from https://techxplore.com/news/2023-05-amd-ftpm-vulnerability-uncovered.html