Researchers discover vulnerabilities affecting billions of computer chips

November 12 2019, by Sharon Gaudin

WPI security researchers Berk Sunar (left) and Daniel Moghimi discovered security vulnerabilities in computer chips made by Intel Corp. and STMicroelectronics. Credit: Worcester Polytechnic Institute

Worcester Polytechnic Institute (WPI) security researchers Berk Sunar

and Daniel Moghimi led an international team of researchers that discovered serious security vulnerabilities in computer chips made by Intel Corp. and STMicroelectronics. The flaws affect billions of laptop, server, tablet, and desktop users around the world. The proof-of-concept attack is dubbed TPM-Fail

The two newly found vulnerabilities, which have been addressed, would have allowed hackers to employ timing side-channel attacks to steal cryptographic keys that are supposed to remain safely inside the chips. The recovered keys could be used to compromise a computer's operating system, forge digital signatures on documents, and steal or alter encrypted information.

"If hackers had taken advantage of these flaws, the most fundamental security services inside the operating system would have been compromised," said Sunar, professor of electrical and computer engineering and leader of WPI's Vernam Lab, which focuses on applied cryptography and computer security research. "This chip is meant to be the root of trust. If a hacker gains control of that, they've got the keys to the castle."

The flaws announced today are located in TPMs, or trusted platform modules, which are specialized, tamper-resistant chips that computer manufacturers have been deploying in nearly all laptops, smart phones, and tablets for the past 10 years. Following an international security standard, TPMs are used to secure encryption keys for hardware authentication and cryptographic keys, including signature keys and smart card certificates. Pushing the security down to the hardware level offers more protection than a software-only solution and is required by some core security services.

One of the flaws the WPI team discovered is in Intel's TPM firmware, or fTPM—software that runs in the Security and Management Engine in

processors the company has produced since it launched its Haswell processor microarchitecture in 2013. Haswell CPUs are used in the popular Core i3, i5, and i7 family of processors. The vulnerability is in the chip that supports trusted execution services—what should be a secure area of the processor. These small crypto chips are the basis of the root of trust for a large portion of the computers used today. The idea is that if the TPM is secure, so is the rest of the computer.

The second flaw is in STMicroelectronics' TPM. Notably, the STMicroelectronics' vulnerability is in a chip that has received a strong industry-recognized security certification from Common Criteria—a highly acknowledged security stamp of approval based on international specifications designed to ensure technology meets high security standards preferred in industrial and government deployments.

The WPI researchers worked with Thomas Eisenbarth, a professor of IT security at the University of Lübeck, and Nadia Heninger, an associate professor of computer science and engineering at the University of California, San Diego.

Once discovered, the flaws were reported to the chip makers by the WPI researchers, who also have described the flaws, how they were discovered, and how they could have been exploited in a paper that will be presented at the 29th USENIX Security Symposium in Boston next August. It also will be presented at the Real World Crypto Symposium in New York City in January.

Researchers like Sunar and Moghimi routinely search for security flaws in software, hardware, and networks, and ethically report them to the companies so the problems can be patched before malicious hackers exploit them. No technology is bug free, so researchers help companies find and fix security flaws that could otherwise lead to massive hacking attacks, malware infections and zombie systems.

"We provided our analysis tools and results to Intel and STMicroelectronics and both companies worked with us to create a patch or make sure a security patch will be provided for the next generation of these devices," said Moghimi, a Ph.D. candidate in WPI's electrical and computer engineering department.

Sunar and Moghimi were members of a multi-university research team that found the series of security flaws behind the Fallout and ZombieLoad attacks reported last spring, as well as another vulnerability known as Spoiler, which exploits side effects of speculative execution.

Broadly, these vulnerabilities are categorized as side-channel attacks, which hackers use to surreptitiously grab information about how a computer behaves while performing sensitive operations and then using that information to access internal data.

Using their own analysis tool, the researchers conducted black-box timing analysis of TPM devices to discover timing leakages that allow an attacker to apply lattice techniques to recover 256-bit private keys for and ECSchnorr cryptography signatures. The leakages make the TPMs vulnerable to remote attacks that reveal cryptographic keys and make applications that use them less secure than they would be without the TPM.

Flaw in Intel fTPM

One of the security flaws Intel patched today is in a cryptographic library—in the fTPM set inside the Intel Management Engine processor. With this vulnerability, researchers used the timing leakage to recover the signature key in less than two minutes. Intel is patching the security flaw with an update to the library.

Intel's fTPM is a widely used TPM product that runs in a dedicated

microprocessor for carrying out cryptographic operations, like making sure data has not been maliciously altered, ensuring data remains confidential, and proving the identity of both the sender and recipient of the data. The microprocessor is embedded with multiple physical security measures, designed to make it tamper resistant.

WPI's Moghimi explained that if hackers gained access to the fTPM, they could forge digital signatures, enabling them to alter, delete, or steal information.

STMicroelectronics Flaw

The research team discovered a flaw in the STMicroelectronics' TPM, which is based on the company's popular ST33 chip, an embedded security platform used in many SIM modules, using integrated circuits designed to securely store authentication information. The chip maker announced earlier this year that more than 1 billion ST33 chips have been sold.

The vulnerability in STMicroelectronics' TPM basically leaks the signature key, which should remain safely inside the hardware. It is designed to enhance the system's security. With the key, a hacker could access, steal or alter encrypted electronic documents. Using the flaw in the STMicroelectronics chip, researchers extracted the private ECDSA key from the hardware after less than one and a half hours of data collection.

"STMicroelectronics developed a new ST33 chip with vulnerability countermeasures in the firmware," said Moghimi. "We verified the new chip. It is not vulnerable to TPM-Fail."

The vulnerable chip has received a CC4+ rating from Common Criteria, which ranks security levels from one (lowest) to seven (highest).

"The certification has failed," said Sunar. "Such certifications are intended to ensure protection against a wide range of attacks, including physical and side-channel attacks against its cryptographic capabilities. This clearly underlines the need to reevaluate the CC process."

Provided by Worcester Polytechnic Institute