Reports: Intel chips have new security flaws

11 June 2020, by Peter Grad

Credit: Pixabay/CC0 Public Domain

A pair of new security threats to Intel-based computer systems have been revealed. The beleaguered semiconductor chip manufacturer has faced a seemingly endless series of vulnerabilities over the past two years.

Although no known attacks have occurred, two teams of researchers have confirmed vulnerabilities in what is supposed to be the safest neighborhood within Intel processor architecture.

One attack, dubbed SGAxe, can gain entry into Intel's Software Guard eXtensions (SGX) services that were specifically designed to protect critical data in the event of massive assault elsewhere in a system. A hacker theoretically can steal cryptographic keys stored in SGX and use them to break security measures protecting sensitive data such as financial records, copyrighted content or passwords.

Researchers say SGAxe operates in a fashion similar to the Meltdown and Spectre threats of 2018. Both of those threats overrode measures to isolate programs and tricked applications into revealing information that enabled access to memory banks holding sensitive data.

In their paper "SGAxe: How SGX Fails in Practice," researchers from the University of Michigan and the University of Adelaide attribute inadequate fortification of SGX that allows side-channel attacks. Such attacks rely on timing information, power consumption, sound waves or electromagnetic fields rather than coding flaws to gain unauthorized access to systems. The earliest instance of electromagnetic eavesdropping was the infamous Van Eck phreaking attack of 1985, in which computer researcher Wim van Eck showed he cold eavesdrop on a major computer system from hundreds of yards away using $15 worth of equipment and a TV set.

"Notwithstanding its strong security guarantees, SGX does not protect against … side channel attacks," the report stated in its explanation of SGAxe. "As acknowledged by Intel, 'SGX does not defend against this adversary.'"

Elaborating further, the researchers said: "With the machine's production attestation keys compromised, any secrets provided by [the] server are immediately readable by the client's untrusted host application while all outputs allegedly produced by enclaves running on the client cannot be trusted for correctness." Attestation keys protect a device against unauthorized firmware and software modification.

The other vulnerability, CrossTalk, was uncovered by researchers at Vrije University in Amsterdam and the Swiss Federal Institute of Technology in Zurich.

Crosstalk relies on data obtained through "transient executions" of code in the CPU the researchers said. Challenging the notion that isolating defense systems on their own cores can prevent such attacks, the researchers asserted that "sensitive information [can] leak across cores in modern Intel CPUs, via a staging buffer that is shared across cores."

"The security implications of this behavior are

serious," the report said, "as it allows attackers to mount transient execution attacks across CPU cores, which implies that mitigations separating security domains at the granularity of cores are insufficient."

Traditional protective measures along with periodic updates for hardware, software and operating systems are "costly and incomplete," the researchers added.

While no actual assaults by these latest threats have been detected beyond academic research, Intel says it is working on a comprehensive solution and hopes to issue an update soon.

Intel units released between 2015 and 2019 are affected. Intel released a list of affected processors on its Developer Zone page. software.intel.com/sec … on-product-cpu-model

More information: sgaxe.com/files/SGAxe.pdf
download.vusec.net/papers/crosstalk_sp21.pdf

APA citation: Reports: Intel chips have new security flaws (2020, June 11) retrieved 20 September 2021 from https://techxplore.com/news/2020-06-intel-chips-flaws.html