New side-channel attack vulnerability found in Intel CPU

April 26 2023, by Peter Grad

Credit: CC0 Public Domain

Add one more vulnerability to the list of side-channel attacks that have long dogged Intel CPUs.

Researchers at Tsinghua University, the University of Maryland and Beijing University of Posts and Telecommunications said they have uncovered a previously undetected flaw in Intel processors that permits data leakage through the EFLAGS register. Their work is published on the *arXiv* preprint server.

Unlike a host of previous side-channel vulnerabilities, this new exploit does not rely on the cache system. Rather, it focuses on timing analysis of transient executions. This approach makes it more difficult to detect such attacks.

Yu Jin, a co-author of the paper released last week, said a change of the EFLAGS register in transient execution could slow down subsequent JCC instructions. The vulnerability, which the team used in conjunction with a Meltdown attack, allows intruders to use timing analysis to decipher code it would otherwise not have access to.

The team demonstrated the vulnerabilities on Intel Core i7-6700, i7-770 and i9-10980XE CPUs.

Jin said, "The increasing complexity and aggressive optimizations of modern CPUs, with their many microarchitectural features… are the root cause of many security issues, including side-channel attacks."

Side-channel attacks can come in many forms. They are not viruses, but rather intrusions into computer systems that gain access by reading non-code-related patterns such as timing, power consumption, and electromagnetic and acoustic emissions.

Daniel Genkin, a University of Michigan professor, explained in a 2020 interview, "Usually when we design an algorithm, we think about inputs and outputs. We don't think about anything else that happens when the program runs. But computers don't run on paper, they run on physics.

When you shift from paper to physics, there are all sorts of physical effects that computation has: time, power, sound. A side channel exploits one of those effects to get more information and glean the secrets in the algorithm."

Side-channel attacks in recent years include Meltdown, Spectre, Fallout and Zombieload.

The team states it is not certain of the specific cause of the vulnerability.

"The root causes of this attack are still not fully understood," Jin said. "We guess that there is some buffer in the execution unit of the Intel CPU which needs some time to revert if the execution should be withdrawn. This withdrawal process will cause a stall if the following instruction depends on the target of the buffer."

Jin also indicated that this vulnerability relies on other transient execution attacks to effect "a real-world attack."

"But it is still a new side-channel attack and worth further exploration," he said. "This attack may bring insight for new microarchitecture attacks and give a new way to build side-channel attacks in cache side-channel resistant CPU."

Intel 11th generation CPUs appear to be more resistant to such attacks. Moreover, Intel's new 13th generation vPro processors are equipped with stronger defenses against side-channel attacks.

More information: Yu Jin et al, Timing the Transient Execution: A New Side-Channel Attack on Intel CPUs, *arXiv* (2023). DOI: 10.48550/arxiv.2304.10877