1 Summary

Meltdown (2018): The authors detail a software-based side-channel attack called Meltdown that allows an unprivileged user program or adversary to read memory locations belonging to other processes. Meltdown exploits the side effects from OOO execution to read these memories. In general, Meltdown makes the processor execute a transient instruction sequence (those instructions that wouldn't appear on the executed path) that leverages a "secret value" that an adversary wants to leak. Transient instructions commonly occur because techniques that minimize latency tend to also execute instructions (and cache memory accesses), but only commit them after preceding instructions have retired. Then, by leveraging side-channel attacks, such as Flush+Reload transferring cache state into architectural state, Meltdown can access the cache line in order to read the "leaked secret value" and eventually dump the entire physical memory. Their study draws attention to this critical vulnerability in the hardware, and that until it is fixed, this necessitates that all operating systems have countermeasures, such as KAISER, which can impede Meltdown, until a permanent fix is found.

2 Strengths

- Section 2 background explanation best illustrates the foundation of OOO execution vulnerabilities. And Section 3 is a good if not brief, walkthrough of how the exploit may work. The toy example helps to clarify specific aspects of Meltdown discussed in Sections 4 and 5.

3 Weaknesses

- No figures or quantitative data were provided in their evaluation of different operating systems with Meltdown, such as how consistent were the bandwidth across platforms, or what % of the target kernel memory was successfully leaked.
- In section 6.2, the Meltdown Proof-of-Concept performance was only done with one processor, the Intel Core i7-6700K. They did not mention which ARM or AMD CPUs they failed to reproduce the Meltdown bug with.

4 Rating: 5

5 Comments

The paper details an exploitable hardware vulnerability that comes from OOO execution or transient execution, which is a feature that enhances performance in modern processors. For the most part, the authors have demonstrated convincingly that Meltdown is a security issue that affects all operating systems. It has been more than 5 years since this paper was

published, more than a decade since chip companies were aware of this vulnerability, and several months since the authors' original Meltdown Proof-of-Concept on GitHub had been archived; therefore, there should be a follow-up paper that discusses Meltdown in this same depth here that also includes research on the topic that have been published since 2018, as well as address some of the weaker areas of the paper mentioned above. For example, their evaluation of Linux and Windows lacked specificity, they only measured Meltdown performance on one processor (Intel Core i7-6700K) when Table 1 lists several, this paper at the time only speculated that ARM and AMD chips could be affected by Meltdown, and the paper did not reference any real-world Meltdown attacks or lack thereof. While they did not find that AMD CPUs were affected by their Meltdown implementation, two more recent paper describe Meltdown-like side-channel leakages that could be exploited on AMD CPUs in 2021 [2] and 2022 [3]. Despite available patches for Spectre/Meltdown, research appears to still thrive for this topic, and will likely continue to thrive because these or similar hardware exploits inform how hardware optimizations are designed with respect to security vulnerabilities.

References

[1] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, Mike Hamburg. Meltdown. Jan 2018.

[2] Saidgani Musaev and Christof Fetzer. Transient Execution of Non-Canonical Accesses. 2021.

[3] Moritz Lipp, Daniel Gruss, Michael Schwarz (2022) AMD Prefetch Attacks through Power and Time. 31st USENIX Security Symposium. USENIX-Security Usenix Security Symposium. Aug 2022.

[4] ARM. Software implications for Spectre/Meltdown on Arm cores. June 2018.