1495

Computing Science

CS4040: Impact of Meltdown & Spectre

Konrad Dryja

No portion of the work contained in this document has been submitted in support of an application for a degree or qualification of this or any other university or other institution of learning. All verbatim extracts have been distinguished by quotation marks, and all sources of information have been specifically acknowledged.

Signed:

Date: October 14, 2019

CS4040 Report

Department of Computing Science **October 2019**
University of Aberdeen
King’s College
Aberdeen AB24 3UE

CS4040: Impact of Meltdown & Spectre

Konrad Dryja

Department of Computing Science
University of Aberdeen

October 14, 2019

Abstract: The aftermath of discovery of side-channel attacks on the performance of modern chips.

1 Introduction

With speculative execution no longer considered safe, modern CPU manufacturers were forced to drop these features in favour of enhancing security. But at the same time, it resulted in sacrificing the performance of the chips. Probably the most harming aspect was that speculative execution was at the time an industry standard - after the processor designers hit a ceiling with potential clock speed, being hit by Moore's Law [5]. I will not be focusing on the origin and details of the vulnerabilities, but rather the patches that followed - although will overview the basics in the next section.

Personally, I found the topic the most interesting, as the aftermath is still haunting security researches to this day, since the fault was not the software, but inherent architecture was flawed. Moreover, frequently we are hearing news how the newest vulnerability based on side-channel execution has been discovered - with the definite fix being complete hardware replacement with a chip produced after 2017. This forced Intel, AMD, ARM to release very aggressive patches, greatly hurting the benchmarks.

This has also raised ethical questions - since some of the machines suffered as much as 50& drop in performance. In the eyes of law, this could classify as false advertising followed by with many class-action lawsuits. As stated by Intel in their 2017 Annual report, as of February 2018, they were facing 30 customer faced suits along with two securities [1]. Intel perhaps is the company that was the most under fire, since Variant 1, also known as Meltdown, was mostly apparent in their chips

2 Background and related work

When speaking about Spectre and Meltdown, it's very important to start from the very beginning - when in July 2017, a researcher Jann Horn from Google's Project Zero has discovered the vulnerability. Due to the severity and potential implications resulting from premature releasing of the findings, those were first communicated directly - on NDA basis - with manufacturers, hoping for an immediate fix. On January 2018, two papers were released by J. Horn et al. illustrating in-depth the vulnerability and how it could be replicated [3, 2]. The papers present a throughout overview of the attack - the exploitation here is based on **Branch Prediction** (BP) along with **Out of Order Execution** (OOE). Those are optimizations techniques used by almost all CPUs on the market.

- BP lets the processor ”predict” the direction will go towards without explicitly evaluating the condition. For example, in a situation where **if** statement was successful for 100 iterations, we can assume that 101st will be successful as well and thus prematurely execute the included code-block
- OOE, on the other hand will often reorder scheduled operations leaving the most time-consuming actions till the end, executing the ones present in CPU cache immediately - assuming that those do not depend on each other, e.g., it’s a simple summation.

Together they create a cheap and clever way to speed up the execution of binaries, but unbeknownst opened a pathway for side-channel attacks, exploiting the fact that CPU was executing the code that it wasn’t meant to in the first place.

Multiple patches have been created ever since to mitigate the negative effect, trying to minimize the impact on performance. M. Löw [4] provides an overview of created patches and affected hardware.

3 Research question

Given the problem context (Section 1) and background (Section 2), you should now be in a position to present what you have investigated. **Pose this as a question.**

Then you should present your approach to addressing this question.

Guide length: 500 words.

4 Experimental Design

What are your hypotheses? How are you going to test them? What is your target population? What are your datasets; i.e. your sample of the target population. What are the dependent and independent variables?

Guide length: 500 words.

5 Discussion

What do the results say? What have you learned from the experiments? Have you identified a correlation between variables, or causation? What are the limitations of what you’ve done? What further experiments might be of benefit?

Guide length: 400 words.

6 Conclusion

What have you done and why? What have you shown through your experiments?

Guide length: 100 words.

References

[1] Intel Corporation, 2017 Annual Report. `https://bit.ly/2pkjeqq`, February 2018.

[2] Paul Kocher, Jann Horn, Anders Fogh, , Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution. In *40th IEEE Symposium on Security and Privacy (S&P'19)*, 2019.

[3] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. Meltdown: Reading kernel memory from user space. In *27th USENIX Security Symposium (USENIX Security 18)*, 2018.

[4] Marc Löw. Overview of meltdown and spectre patches and their impacts. *Advanced Microkernel Operating Systems*, page 53, 2018.

[5] Robert R Schaller. Moore's law: past, present and future. *IEEE spectrum*, 34(6):52–59, 1997.