x86 Processor Vulnerabilities

MS19814520 : Dasitha Maduranga G.L.

Faculty of Computing, Sri Lanka Institute of Information Technology New Kandy Rd, Malabe 10115, Sri Lanka
dasithafit@gmail.com

Abstract
This research paper will focus on the discovery of certain x86 processor vulnerabilities and the far-reaching consequences on the entire computing world, up to and including a complete kernel redesign for most major operating systems. A basic comparison between the vulnerabilities is also highlighted in this paper. Furthermore, this paper will also explore the future of the micro-processor landscape which has been irreversibly altered due to the discovery of these vulnerabilities.
***Index Terms* – Spectre; Meltdown; Vulnerabilities; x86 Processor vulnerabilities; Hardware vulnerabilities**

I. INTRODUCTION

Microprocessors or processors as they are commonly called, are the foundation of any computer's operations, a processor is often referred to as the "brain" of the computer. This means that any vulnerability in a processor can be potentially devastating to security. This applies doubly to hardware vulnerabilities, as updated hardware must be designed and released to mitigate the vulnerability, which makes the vulnerability window much larger than it would be with a software vulnerability.[1]

We will briefly go over 2 specific vulnerabilities, namely; Spectre and Meltdown. We will also touch briefly on the newly discovered Microarichitectuiral Data Sampling, (MDS) attack in the evolution section. [2]

Meltdown

"Meltdown" gets its name from the nature of the exploit wherein it "melts" the security boundaries between user level memory and kernel memory. This allows attackers that are using Meltdown to read the entire physical memory of the device they are targeting.

Meltdown acts by targeting a race condition which occurs while an instruction is being processed, it allows Meltdown to bypass privilege level checks and access memory locations it should not have access to. [3]

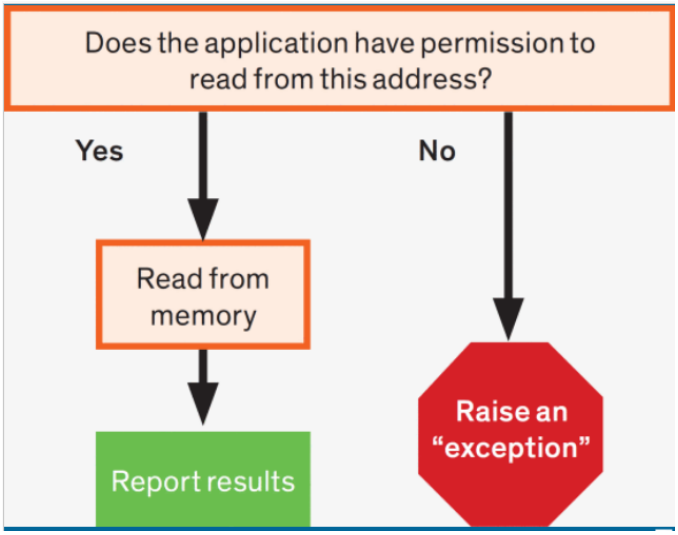

Figure 01 Memory read surface function [01]

Reading from memory will, on the surface, function as shown in the Figure 01. Intel processors, on the other hand, perform these moves out of order to save time as shown in Figure 02.

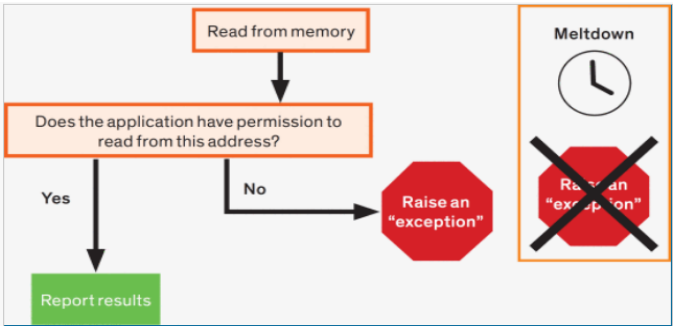

Figure 02 Meltdown secret data retrieve [01]

Meltdown can steal hidden data by concealing anomalies and using a side channel at the point how long it would take to retrieve from memory. [4,5]

Meltdown works mainly on Intel CPUS and on some ARM CPUS, AMD CPUS are largely unaffected due to architectural differences.

Spectre

Spectre works by tricking applications into executing code that they would normally never execute, by exploiting a branch prediction vulnerability in the processor. [6]

Branch prediction is a performance optimization which is present in most modern processors, it allows a processor to evaluate possible logical paths a program may take in the future and compute functions required for both paths. This will speed up processing once the program chooses one of the paths as some processing will already be done. This will allow Spectre to leak any personal user information the application may have access to. This means that even the most secure applications are vulnerable as there is no direct attack happening. [7]

Spectre works on any CPU architecture (Intel, AMD, ARM), which makes it extremely potent, as it is effective regardless of which type of device is in use.

Comparisons between the two

The main difference between Spectre and Meltdown is that Spectre exploits a branch prediction vulnerability that most modern processors whereas Meltdown is based around exploiting out of order execution which is employed by modern processors to reduce latency.

Spectre also must be customized to the target process' software environment, hence it has a setup phase much longer than Meltdown does. [8]

There are similarities between the two, including where they both use transient execution; Spectre triggers transient execution through misprediction events in branch predictions, while Meltdown exploits transient out of order instructions which follow an exception.

II. Evolution

History and mitigations

On June 1st 2017, Intel, ARM, and AMD were notified of the Spectre and Meltdown vulnerabilities by Google's Project Zero team. In the ensuing 7 months all vendors, be it software or hardware, scrambled to mitigate the vulnerability by deploying stealth patches to their systems. Even though these vulnerabilities were discovered relatively recently, they have been present for at least 20 years.[9]

A mitigation for Meltdown was found in the called KAISER (Kernel Address Isolation to have Side-channels Efficiently Removed) patch which was developed around the same time for Linux system, purely coincidentally. This patch effectively prevents Meltdown attacks, but the fundamental hardware vulnerability is still present, leaving room for other exploits to be developed. [11]

Current events

More recently, on the 14th of May 2019, researchers discovered another exploitable vulnerability in Intel processors, which can be used by four different attacks that enable an intruder to gain retrieve confidential information stored on a CPU.

This vulnerability uses speculative execution like Spectre does, allowing an attacker to trick the processor into capturing sensitive data moving between components of the chip, this is a serious flaw, allowing an attacker to potentially grab information ranging from website history to secret keys that could decrypt user hard drives. [12]

As of now software patches have already been applied to the affected Intel chips, but a more serious hardware overhaul is required to fully patch the bug.

Security researchers also recommend disabling hyper-threading on Intel CPUS to help prevent this attack, but this will come at a serious performance cost (around 20% in some cases), which Intel will be unable to overcome until hardware revisions are live. As such, Intel has classified these threats as "medium" which is up for debate in the security community, some view this to be Intel not wanting to lose customer confidence and satisfaction, which would be the end result of disabling hyper-threading. [13]

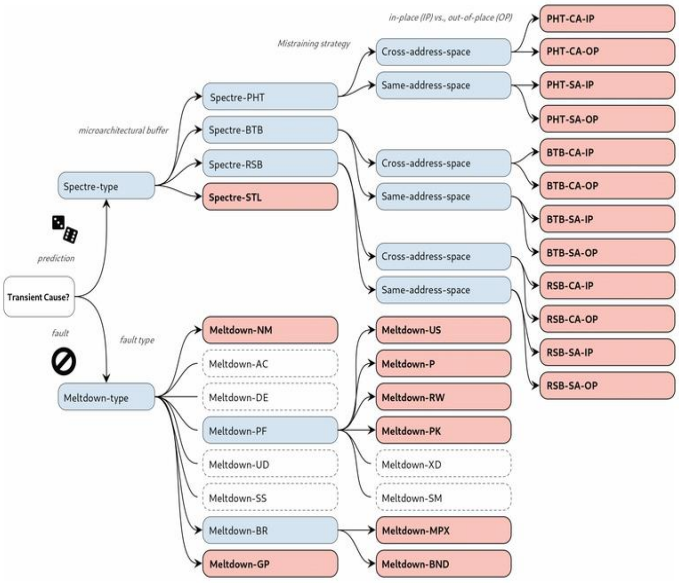

Image courtesy of Tech Republic [10]

Variants

Spectre

There are four primary attack types for Spectre;

1. Spectre PHT – exploits the pattern history table
2. Spectre BTB – exploits the Branch Target Buffer
3. Spectre RSB – exploits the Return Stack Buffer
4. Spectre STL – exploits CPU store-to-load forwarding

The first three attack forms depend on the branch predictor being mistrained. [14]

Spectre STL does not actually exploit mistraining of the processor, this means it only possible to reach memory with the same authorize level as it.

Meltdown

Attack Variant	Memory	Cache	Register	Cross Privilege Level
Meltdown-US	Yes	Yes	No	Yes
Meltdown-P	Partial	Yes	No	Yes
Meltdown-GP	No	No	Yes	Yes
Meltdown-NM	No	No	Yes	Yes
Meltdown-RW	Yes	Yes	No	No
Meltdown-PK	No	Yes	No	No
Meltdown-BR	Yes	Yes	No	No

Table Data: Canella et al.

Table courtesy of Tech Republic [10]

These are some variants of Meltdown [15]

1. Meltdown-US (Supervisor only) the first discovered example of a Meltdown vulnerability
2. Meltdown-P (Virtual Translation Bypass) This variant of Meltdown allows attackers to read any data in the L1 cache.
3. Meltdown-GP (System Register Bypass) This variant allows attackers to read privileged system registers
4. Meltdown-NM (FPU Register Bypass) This variant allows attackers to retrieve AES-NI keys.
5. Meltdown-RW (Read-only Bypass) This is the first variant which is able to bypass "page-table based access rights within the current privilege level. This exploit allows read-only data to be overwritten using transient execution.
6. Meltdown-PK (Protection Key Bypass) This variant exploits Memory Protection Keys for User-space which was first implemented in Intel's Skylake Xeon processors. This exploit can only be fixed by updating hardware.
7. Meltdown-BR (Bounds Check Bypass) This variant exploits a bound-range exceeded exception which exists in x86 processors. This is the only variant of Meltdown that works on AMD CPUs.

III. Spectre and Meltdown Prevention

Spectre and Meltdown mitigations are given via BIOS and OS updates for servers and desktops. Apple has released software and firmware updates to address the Spectre and Meltdown vulnerabilities. The first batch of patches for Android users were released at the 2018-01-05 security patch level. For cloud platforms, in 2018 released Virtual Machine updates which has been mainly addressed the Spectre and Meltdown vulnerabilities.

IV. Future developments in the area

These vulnerabilities shook the foundations of the industry. Intel in particular has been heavily focused on speed improvements from generation to generation

The discovery of MDS in particular displays a worrisome trend; a whole new class of security vulnerabilities has been discovered and it is still relatively early into its lifespan. There is no saying what kind of vulnerabilities will be created as researchers test new techniques to try and exploit newer features such as speculative execution. [9]

I believe there will be far more hardware vulnerabilities discovered with regards to processors, and not just related to speculative execution, as there are parts that have not yet been explored by researchers which may have been optimized by manufacturers for maximum speed instead of security, leaving them open for exploitation. This will only be true if manufacturers do not take the necessary steps to change their architectures as needed however, but even if they do, there will be a period of vulnerability before the new architecture is adopted by mass consumers, leaving them vulnerable to attack with only software mitigations to protect them.

In addition to hardware revisions, revisions must be done to operating systems as well, even though KAISER helps prevent Meltdown, even this may not be enough in the long run, this means that operating system vendors may have to consider further isolation to reduce the attack surface.

This brings up a dilemma for the vendors; how much
flexibility are they willing to trade for security and performance?

V. Conclusion

In conclusion, I would like to expand on some key points:

First, Spectre and Meltdown are clearly the first of a new class of exploits, based around hardware vulnerabilities in a processor itself. As such, it is important to stay up to date on the newest vulnerabilities and to ensure that any software mitigations are installed immediately, as an exploit in a processor will be completely undetectable by other protections in place such as encryption or anti-virus software.

In the case of some older processors, specifically Intel CPUs released between 2007 and 2011, a hardware upgrade will be required, as Intel has not patched CPUs released in this time frame.

Secondly, with respect to desktop processors, there have been many advancements made in the last few years with regards to performance, to achieve these performance gains, critical components have added various layers of optimizations, these layers introduce separate security risks that have not been seen in the industry before. In the case of some of these risks, manufacturers must consider some of their previous design choices and decide whether an alternative implementation that is optimized for security is required.

Finally, it goes without saying that the advent of these two exploits will have far-reaching consequences for the future of computer security, forcing hardware vendors to change their focus from performance optimization, which has been their sole goal for the last 10 years, to security optimizations. This fundamental shift in mindset will certainly usher in an interesting era in microprocessor development.

VI. Acknowledgements

I would like to thank Dr. Lakmal Rupasinghe, for the remarkable guidance, insightful comments and suggestions, and all the support, throughout the course of this work. His research knowledge and experience in all aspects of being a good researcher are extremely appreciated.

VII. References

1. N. Abu-Ghazaleh, D. Ponomarev and D. Evtyushkin, "How the spectre and meltdown hacks really worked," in IEEE Spectrum, vol. 56, no. 3, pp. 42-49, March 2019, doi: 10.1109/MSPEC.2019.8651934.

2. T. M. Conte, E. P. DeBenedictis, A. Mendelson and D. Milojičić, "Rebooting Computers to Avoid Meltdown and Spectre," in Computer, vol. 51, no. 4, pp. 74-77, April 2018, doi: 10.1109/MC.2018.2141022.

3. J. Horne, "Reading Privileged Memory with a Side-Channel", Project Zero, Apr. 2021, [online] Available: https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html.

4. J. Sianipar, M. Sukmana and C. Meinel, "Moving Sensitive Data Against Live Memory Dumping, Spectre and Meltdown Attacks," 2018 26th International Conference on Systems Engineering (ICSEng), 2018, pp. 1-8, doi: 10.1109/ICSENG.2018.8638178.

5. A. Baumann et al., "The Multikernel: A New OS Architecture for Scalable Multicore Systems", Proc. ACM SIGOPS 22nd Symp. Operating Systems Principles (SOSP 09), pp. 29-44, 2009.

6. *Prout et al., "Measuring the Impact of Spectre and Meltdown," 2018 IEEE High Performance extreme Computing Conference (HPEC), 2018, pp. 1-5, doi: 10.1109/HPEC.2018.8547554.*

7. M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, et al., Meltdown, Apr. 2021, [online] Available:

8. M. D. Hill, J. Masters, P. Ranganathan, P. Turner and J. L. Hennessy, "On the Spectre and Meltdown Processor Security Vulnerabilities," in IEEE Micro, vol. 39, no. 2, pp. 9-19, 1 March-April 2019, doi: 10.1109/MM.2019.2897677.

9. Z. Wang and R. B. Lee, "Covert and side channels due to processor architecture", Proc. 22nd Annu. Comput. Secur. Appl. Conf., pp. 473-482, 2006.

10. "Spectre and Meltdown explained: A comprehensive guide for professionals", TechRepublic, 2021. [Online].Available: https://www.techrepublic.com/article/spectre-and-meltdown-explained-a-comprehensive-guide-for-professionals/. [Accessed: 08- May- 2021]

11. P. Kocher et al., "Spectre Attacks: Exploiting Speculative Execution," 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 1-19, doi: 10.1109/SP.2019.00002.

12. A. Prout et al., "Measuring the Impact of Spectre and Meltdown," 2018 IEEE High Performance extreme Computing Conference (HPEC), 2018, pp. 1-5, doi: 10.1109/HPEC.2018.8547554.

13. O. Alhubaiti and E. M. El-Alfy, "Impact of Spectre/Meltdown Kernel Patches on Crypto-Algorithms on Windows Platforms," 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2019, pp. 1-6, doi: 10.1109/3ICT.2019.8910282.

14 P. Li, L. Zhao, R. Hou, L. Zhang and D. Meng, "Conditional Speculation: An Effective Approach to Safeguard Out-of-Order Execution Against Spectre Attacks," 2019 IEEE International Symposium on High Performance Computer Architecture (HPCA), 2019, pp. 264-276

15. C. Li and J. Gaudiot, "Online Detection of Spectre Attacks Using Microarchitectural Traces from Performance Counters," 2018 30th International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD), 2018, pp. 25-28, doi: 10.1109/CAHPC.2018.8645918.