University of Texas at Arlington

Professional Practices: CSE-3314-002

Assignment #4

Protecting against Spectre and Meltdown in 2022

27 October 2022

Landon Moon – 1001906270

This Assignment is submitted towards and in support of the partial completion of the requirements for the Professional Practices Course

**Contents**

Introduction 3

Explanation and History 3

Advantages / Disadvantages 4

Conclusion 6

References 7

Protecting against Spectre and Meltdown in 2022

In today’s world, everything is just a fingertip away. The internet has connected us more than any other time in history. While the internet gives us access to vast amounts of information, it also brings security risks with it. One of these security risks is that of Spectre and Meltdown. Spectre and Meltdown are paired together because both exploits allow external programs to access the memory of another process. This allows private data to be scraped from your device without the operating system's authorization. Even though these exploits were discovered in 2017, their effects can still be seen today due to how lucrative the exploits are.

While Spectre and Meltdown were discovered nearly 5 years ago, the CPU and software industries are still being affected by the exploit. The Spectre and Meltdown exploits are not just a single algorithm to gain access to your data but instead are a family of security vulnerabilities. When one version gets patched by a newer CPU version, a new version pops up. A recent example of a new child of this family of exploits is the Branch History Injection (Nichols 2022). This exploit, if executed correctly could access your sensitive data such as plaintext passwords, encryption keys, banking information, and anything else that is being used on your device. Because this exploit was discovered recently, chip manufacturers and operating system developers might not have put a security update in place. The industry will always need to be on the lookout for these kinds of exploits.

To understand the decisions that must be made to be secure, we need to have at least a basic understanding of why Spectre and Meltdown exist in the first place. We have all learned about Moore’s law stating that “the number of transistors per silicon chip doubles every year.” (Britannica 2022). In recent years this law has been starting to slow down but the chip manufacturers need to keep advancing to stay on top. The leading CPU manufacturer, Intel, decided to put caches into almost every corner of their chip architecture to keep advancing. A cache is a small amount of memory that can be referenced and responds faster than RAM. These caches are the centerpiece of almost every Spectre and Meltdown exploit. If one process is temporarily stopped so another process can be processed, the values in the caches persist. If the new process needs a spot in the cache, then it is replaced with a new value which takes time. CPUs also use what is called speculative execution where some code can be executed before checking if it is valid. By using speculative execution and timing which cache values take longer to access, an external process can access the data of the previous process through any cache in a CPU.

A recent article by Kaspersky goes over how these security vulnerabilities are affecting us today and a couple of ways of guarding against them. There are three ways to protect against these vulnerabilities: modifying new CPUs, changing microcode, or releasing software updates (Root 2022). By changing one or more of these, a newly discovered security vulnerability can be partially or completely guarded against. Software updates provide an immediate solution to protecting your data. This prevents these vulnerabilities from being executed on different systems as long as they are up to date. Similarly, microcode can also be updated to provide an immediate response to save your private information from being spied on. Additional to these immediate patches, the design of the newer versions of CPUs is changed so that a specific type of exploit is physically unable to work on newer devices. All these solutions simply provide yourself and others the security they deserve, but while security at face value is desirable, there are costs to these changes that need to be considered.

As we discussed previously, there are three ways to protect against Spectre and Meltdown: software updates, microcode updates, and hardware. The first downside to these changes discussed in the article is that CPUs can “[disable] speculative code execution” (Root 2022). Speculative code execution is used so the CPU can start working before it gets an answer from RAM. By disabling it, these newer CPUs that are more secure against these vulnerabilities are inherently slower. The second downside to these measures of protecting against Spectre and Meltdown mentioned in the article is the optional security options when compiling the Linux kernel. Linux is most commonly used on large-scale databases and mainframes where speed and efficiency are extremely important. While speed is important, security is also a large requirement of these systems. By enabling all the “anti-Spectre precautions in the Linux OS” there is an average of a 25% performance decrease (Root 2022). While this performance hit wouldn’t be noticed too much if these precautions were on our personal machines, these large computer systems cost millions of dollars to build and upkeep. A 25% decrease in performance to keep the data secure will cost additional millions of dollars just to have the same performance as before. Lastly, all of these security vulnerabilities have to actively be fought against. When a new vulnerability is found, it is up to the chip companies and the software developers to secure their systems against it. Without constant upkeep and careful observation, our computer systems will eventually become vulnerable. This fact is especially important for old, unsupported systems such as windows 7 or older CPU models.

There is one main way of securing our private data while not sacrificing our devices’ performance: reducing the number of CPU caches. Most of these vulnerabilities do not affect AMD chips because instead of focusing on a faster CPU, they’ve focused on adding more cores and threads per chip. This doesn’t require the overuse of caches that Intel and other’s architectures require. By using fewer caches, AMD has unknowingly protected themselves from Spectre and Meltdown. in recent years AMD has finally started to take up a significant portion of the CPU market share because they got lucky with their CPU architecture. This doesn’t mean that the problem doesn’t exist for AMD though, they still need to keep a careful eye for exploits on the few caches they use and communicate with software developers about what precautions still need to be made.

In conclusion, Spectre and Meltdown are significant risks to our privacy when using our electronic devices. These vulnerabilities can be actively protected against but at the cost of the performance of our devices. This might cost us more for our devices or might cost companies more for their servers. While these vulnerabilities heavily affect intel’s CPU architecture, AMD chips are far less affected. This is one of the main reasons why AMD has seen a resurgence in popularity since 2017 and why Intel is likely to focus on increasing their core counts.

References

“Moore's Law.” *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 2 Sept. 2022, https://www.britannica.com/technology/Moores-law.

Nichols, Shaun. “Researchers Disclose New Spectre V2 Vulnerabilities.” *SearchSecurity*, TechTarget, 9 Mar. 2022, https://www.techtarget.com/searchsecurity/news/252514427/Researchers-disclose-new-Spectre-V2-vulnerabilities.

Root, E., Grustniy, L., Larkina, A., Aver, H., & Navar, E. (2022, February 1). *4 years since SPERCTRE vulnerability discovery*. Daily English USA usakasperskycomblog. Retrieved October 19, 2022, from https://usa.kaspersky.com/blog/spectre-meltdown-in-practice/26100/

**CSE - 4314**

**Professional Practices**

**Academic Integrity**

**In order for your Assignment/Homework/Project to be accepted you must read the following, sign this form and attach it to your papers (as the last page of your assignment).**

**Academic Integrity:** Students enrolled in this course are expected to adhere to the UT Arlington Honor Code:

*I pledge, on my honor, to uphold UT Arlington’s tradition of academic integrity, a tradition that values hard work and honest effort in the pursuit of academic excellence.*

*I promise that I will submit only work that I personally create or contribute to group collaborations, and I will appropriately reference any work from other sources. I will follow the highest standards of integrity and uphold the spirit of the Honor Code.*

Student Signature:



Student Id Number: 1001906270

*Note: Must be read, signed and attached (stapled) as last page of homework or assignment. If it is a team assignment then all team members must read, sign and attach a single copy of the Academic Integrity form to the team’s paper as the last page. If not properly attached as last page a 2 point penalty will be assessed after grade assigned.*