Meltdown and Spectre Vulnerability in x86 CPUs: How Does the Security Patches Affect Speed?

Ryan Ecarma and Lucien Ngalamou,

Lewis University, CAMS Dept., 1 University Parkway, Romeoville, IL 60446, USA

Summary

Security vulnerabilities are a major concern for computer systems in general especially at the hardware level. Whether it be an undiscovered backdoor or a bad sector of a CPU design lithography which wasn't verified during manufacturing, these are major concerns to consider. There were recently possible hardware security vulnerabilities found in modern x86 CPUs. Operating System level patches were created to mitigate these security flaws. The main problem for the patches is the speed of the hardware that is suspected to be less than before patching. This paper presents an in depth study of the security vulnerabilities, and analyze whether the patches for Windows 10 do significantly affect the speed with various benchmark tests before and after patches.

Keywords:

Vulnerabilities, Patches, Operating Systems, CPU (Central Processing Unit).

1. Introduction

Humanity is increasingly relying on technology for business and personal matters. With technology increasingly replacing old methods of yesteryear; Is the rate of security measures proportionate to the consumer/business electronics and other technologies being researched and developed? Are the software and or hardware designs formally and thoroughly verified before production? The fact of the matter is that there will almost always be a potential security vulnerability. The question that ponders many if there is always a potential security vulnerability, when will the security vulnerability be found and brought to light? How does a major hardware/software company combat these security vulnerabilities? The usual way to combat majority of the security vulnerabilities in today's software would to issue an update or security patch. That solution would then have to have the user to apply the patches vigilantly to their system. However, for some systems these patches can be delivered over-the-air (OTA) from the internet. This would be the solution that today's popular operating systems use to deploy security patches. What if the security vulnerability is in the hardware level, like a CPU bug? Can hardware really be patched like software? If the hardware can be patched how will it affect the speed of the hardware? If there is a speed deficit post patch, will the deficit be worth the security? Is the security vulnerability a big deal in the first place? This paper presents the recently discovered security vulnerability that has affected majority of consumer and enterprise x86 CPUs and test to see if the proposed patches for Windows 10 will affect the speed of an Intel based system. This paper is organized in five sections. Section two presents a background study, followed by the section that present a study of speed deficit. Section four presents the different test followed by the conclusion.

2. Background

2.1 What are the Meltdown and Spectre Security Vulnerability?

Meltdown and Spectre are two closely related security vulnerabilities that exploit certain features found in modern day CPUs found in desktops, laptops, and other compute devices. These security vulnerabilities were made public on January 3, 2018 by the release of two white papers by independent researchers. These discoveries took the field of computer security research by storm. The Meltdown security vulnerability was independently discovered and reported by three teams:

- Jann Horn (Google Project Zero),
- Werner Hass, Thomas Prescher (Cyberus Technology),
- Daniel Gruss, Mortiz Lipp, Stefan Mangard, Michael Schwarz (Graz University of Technology).

Figure. 1 Meltdown logo from meltdownattack.com.

Manuscript received August 5, 2025
Manuscript revised August 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.8.8

The Spectre security vulnerability was independently discovered and reported by two people:

- Jann Horn (Google Project Zero),
- Paul Kocher in collaboration with Daniel Genkin (University of Pennsylvania and University of Maryland), Mike Hamburg (Rambus), Mortiz Lipp (Graz University of Technology), and Yuval Yarom (University of Adelaide and Data61).

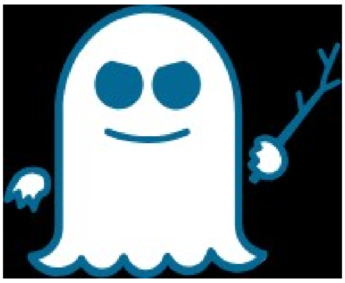

Figure 2. Spectre logo from meltdownattack.com

2.2 Meltdown

The fundamental security of computer systems is the memory isolation in the operating system. For example, kernel address ranges are marked as non-user-accessible and are protected from unwanted user access [1]. Typically, operating systems must ensure that applications cannot mess with each other's memory spaces. These areas of memory are supposed to be isolated from each other. This is to prevent instances like user applications with the wrong privileges reading or writing to the kernel memory. Memory isolation is one of the most notable features in computing environments, which makes running multiple applications on a computer possible. Meltdown is a powerful attack that allows the attacker to read arbitrary physical memory from an unprivileged user program. The meltdown security vulnerability exploits one of the key features of modern CPUs, out of order execution. Out-of-order execution is an important performance enhancement built into many modern CPUs today. Out-of-order execution is where instructions for the CPU are dynamically scheduled. Thus, while instructions submitted to the CPU by the operating systems are in order, the CPU might execute these instructions in a different order. In short, out-of-order execution works by making efficient use of CPU instruction cycles that otherwise would have been wasted idling.

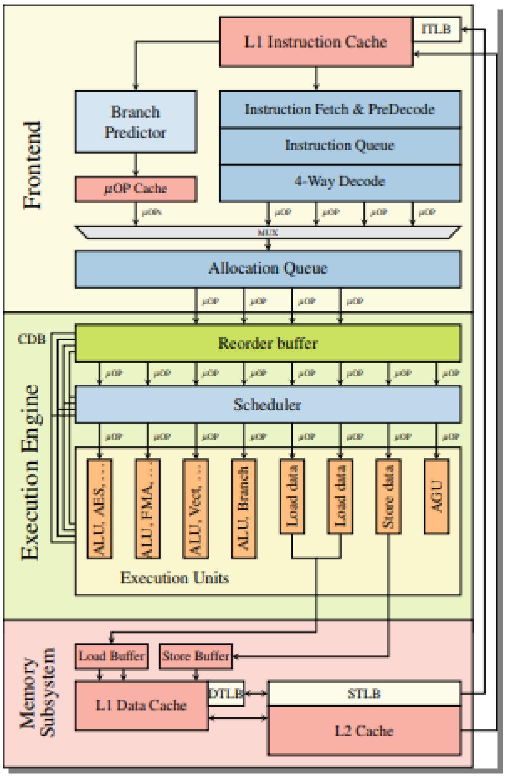

Figure 3: A simple illustration of a single core in Intel's microarchitecture. Instructions are loaded into the reorder buffer and decoded into µOPs, then executed out of order [1].

The reason why out-of-order execution is discussed is because there is an inherent side effect to this performance benefit and is the main driving force for this exploit. In vulnerable CPUs the out-of-order execution allows for an unprivileged process access from a privileged (kernel or physical) address into a temporary CPU register [1]. With this access to certain parts of memory without the need of heightened privileges, this is potentially dangerous, and this can be exploitable with attacks like a side-channel attack. More specifically, a cache side- channel attack whereas the attack exploits the target memory location by flushing and reloading shared cache by using the *clflush* function. Meltdown mainly effects the out-of-order execution performance features of modern Intel CPUs. Thus, it is to be expected that majority of Intel CPUs made from 1995 onward are affected by this attack.

2.3 Spectre

Branch and speculative prediction is another prominent feature that modern CPUs employ for performance enhancements. These performance enhancements are to be expected in many modern x86 CPUs today. It works by increasing performance by guessing the next execution paths and executing them prematurely. This is to maximize CPU clock cycles and not waste them idling waiting for the next instruction. Spectre attacks works by exploiting this feature and induce the victim into a state of vulnerability by executing speculative operations that normally would not have occurred under normal circumstances [2]. This breaks the isolation between different applications and processes. This potentially leads to having the victim's information leaked via a side channel attack. Moreover, this security vulnerability is even more widespread due to non-x86 CPUs like the ARM CPUs incorporating branch and speculative prediction into their silicon. The team that released this information confirmed that CPUs on AMD, including the newly released Ryzen microarchitecture line as well as the Samsung and Qualcomm ARM processors (found in phones and tablets) were able to successfully execute the Spectre attacks.

2.4 Mitigation

These exploits post a serious threat to vulnerable systems such as datacenters that deploy these processors as well as normal consumers who have these processors in their personal devices. The code that utilizes the exploits work on Windows, Linux, etc., as this is not a software but a hardware security issue [3]. For GNU/Linux users, there was a patch deployed to mitigate Meltdown called "KAISER," which is an acronym for "kernel address isolation to have side-channels efficiently removed [4]." This patch for Linux provided an implementation of separated address spaces for x86 and x86-x64 kernel. For Windows users, various system patches have been deployed by Microsoft for Windows 10, 8.1, 8 and Server 2012, 7 and Server 2008, to circumvent some aspects of Meltdown. Since the list of patches are extensive, we will only go over a summation of windows 10 which includes the first package for Windows 10 version 1507, KB4056893, which was issued January 03, 2018 to Windows 10 version 1709, KB4090007, which was issued on March 1, 2018 [5]. The KB4090007 patch in summary issues microcode updates for Intel Skylake, Kaby Lake, and Coffee Lake processors. For Spectre mitigation on Windows, software updates were introduced to Microsoft Visual C++ (MSVC) compiler and Microsoft urged the developers to recompile their code with the new /Qspectre feature and redeploy their code immediately. However, with all these mitigations in place for Meltdown and Spectre, the best mitigation for these security exploits will have to be a hardware revision or a refresh.

3. The Speed Deficit Study

The mitigations set in place for Meltdown and Spectre attacks are temporary measures to a permanent problem. The patches that were deployed helped mitigate these attack exploits to a certain degree, however there is a perceived side affect to these patches. This side effect is the resulted speed deficit that are introduced to the system as the CPU must make exceptions so that programs do not bypass their memory bounds and gain access to other programs. Since Windows 10 will be the main operating system for this study it is important to note that there have been reports of speed deficits across the board with multiple generations of Intel CPUs. Depending on what generation of CPUs (Sandy Bridge, Ivy Bridge, Haswell, Broadwell, Skylake, Kaby Lake, and Coffee Lake), the speed deficits can range from minor single digit percent losses to significant performance losses on some applications, however the applications tested weren't mentioned [6].

3.1. Test Methodology

This study will be conducted on a Windows 10 based test system as majority of computer owners own a Windows based computer. The test system was a 2011 Lenovo ThinkPad x220 which represents the typical casual PC user. This Lenovo ThinkPad x220 incorporates these specs:

- 2nd Generation Sandy Bridge Intel Core i5-2540M @ 2.60Ghz 2-core/4-threads
- Intel HD 3000 Integrated Graphics
- 2x4gb DDR3 @ 1333Mhz (Dual Channel)
- 180GB Intel SSD
- Windows 10 Professional Version 1709 OS Build 16299.15

The benchmarks used for this study will be Cinebench r15 [7], CPU-Z [8], and PassMark PerformanceTest 9 [9]. These benchmarks are all available for free from the internet. Cinebench r15 is a cross platform performance test suite that tests the capabilities of a system buy running a series of renderings and OpenGL benchmarks. CPU-Z is a free CPU validator which is used to get information such as processor name, process, and package as well as providing real time measurement of each of the CPU's cores and frequencies. PassMark PerformanceTest is a free PC benchmarking suite that utilizes different speed tests such as CPU tests and 2D graphics tests to compare results to other computers.

The benchmarks will run on pre and post patched Windows 10 Professional on the Lenovo ThinkPad x220. The Windows 10 Professional Version 1709 OS Build 16299.15 also known as the Fall Creator's Update, is a relatively outdated version of Windows which dates back October 10, 2017, note that this was before Meltdown and Spectre were brought to public which was January 3, 2018. The initial January 3, 2018 mitigation patches for Windows 10 Professional Version 1709 is KB4056892, which brings the OS Build to 16299.192. However, we ran into issues installing the update as installing manual updates are not able to install. The other version of Windows 10 Professional that will be tested will be the most recent 1803 April Update. This is to further test the speed deficits a vigilant Windows 10 user with the most up to date software patches applied running on older pre-2016 Intel silicon should experience. Each test of Windows 10 versions will be conducted on their own separate SSD's on the Lenovo ThinkPad x220:

- 180GB Intel 530 Series SSD: Windows 10 Professional 1709 pre-patch
- 180GB Intel 520 Series SSD: Windows 10 Professional 1803 current-patch

The SSDs will be imaged using Achronis True Image to ensure that each SSD will have the same starting point before the patches and updates are applied. SSD's are used to eliminate potential I/O bottlenecks. The three benchmarks will be run on instances of three runs in which the results will take the average of the 3 runs on each version of Windows 10. The laptop will be running AC power with the high-performance power profile to ensure maximum clock speeds. The results will then be graphed via Microsoft Excel 2016. The goal of the study is to run several benchmarks found in the consumer spectrum then compile and analyze the results. There should be performance deficits, but we shall analyze to what extent these security patches warrant the speed deficit.

4. Test

The benchmark tests were run in this order: Cinebench r15, CPU-Z, PassMark PerformanceTest. Cinebench r15 has two modes of render testing single thread and multi-threaded, both will be included. Also, CPU-Z has two modes of CPU benchmarks both single and multi-threaded scores. PassMark has several CPU tests, however this will result in a composite score

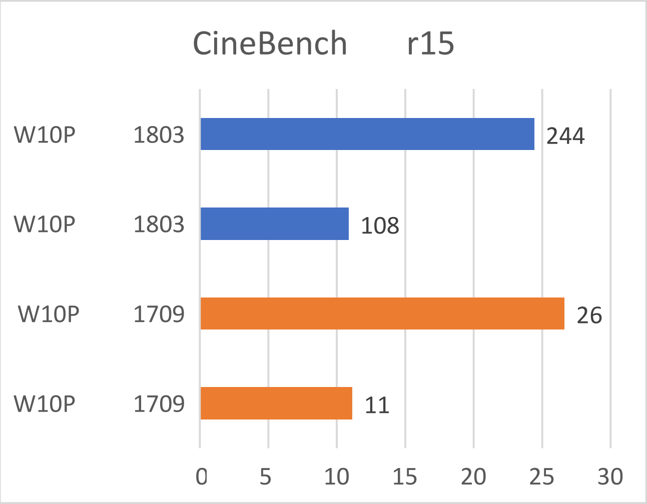

Figure 4: Cinebench r15 average scores for both single-core and multi-core. Higher value indicates higher performance

The Cinebench r15 benchmark was ran back to back three times for both multi-core and single threaded workloads on both Windows 10 versions. Regarding the results in figure 4, the pre-patched Windows 10 Professional 1709 resulted in an average 266 multi-core score and 111 single-core score. The post-patch Windows 10 Profession 1803 resulted in an average 244 multi-core score and a 108.3 single-core score. It is important to note that the units of these scores are not standard and only apply to CineBench r15. So, when directly compared to each other, the single-core score resulted in an average 2.67 points decrease in score which is a 2.4% decrease in performance after Windows 10 1803 update was applied. The same can be said with the multi-core tests, which resulted in an average 22 points decrease in the score, an 8.4% decrease in performance after Windows 10 1803 update was applied.

CineBench r15 showed a measurable drop in performance after the April 2018 Windows patch was applied to the x220. These drops are relatively minor and there could be some unknown variables that could have otherwise affected the score.

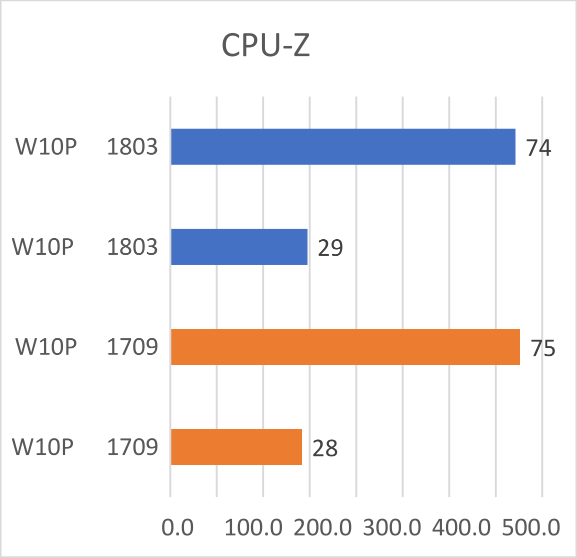

Figure.5: CPU-Z average of three scores for both single-core and multi-core. Higher value indicates higher performance.

The CPU-Z Benchmark was run back to back three times for each Windows 10 versions. From the graph referenced from Figure. 5, Windows 10 1709 single-core score resulted in 752.9 points and the multi-core score resulted in 283.3 points. The Windows 10 1803 single-core score resulted in 295.3 points and the multi-core score resulted in 743.1 points. It is important to note that the units of these scores do not represent a standard unit and only apply to CPU-Z. Comparing the results of both Windows 10 versions, there is an average 11.93-point increase in single core performance, which is a 4.2% increase with version 1803. For multi-core, there was an average 9.87-point decrease in performance, which is a 1.3% decrease in performance after the 1803 patch was applied.

CPU-Z's benchmark was quite interesting as the results do show a speed deficiency in the multi-core testing. However, it is interesting to note that the Lenovo x220 was able to reliably achieve a higher single-core score in the benchmark. There could be several assumptions that can be made. One assumption would be that the April 2018 Update for Windows 10 could have included a revamped CPU scheduler that is different than the initial Windows 10 Fall Creator's Update Version 1709.The PassMark PerformanceTest 9 benchmark was run back to back three times on both versions of Windows 10. PassMark Performance offers other tests like 2D, 3D, and Memory tests. But for this study the focus is on CPU performance, so only the CPU benchmark was run. Regarding the graph from figure 6, composite score for Windows 10 version 1709 resulted in 4351.7 points while the composite score for Windows 10 version 1803 resulted in 4106 points. Note that these scores do not represent any other standard units and only apply to PassMark PerformanceTest 9. Comparing the results from the different Windows versions, version 1803 resulted in a 245.67-point decrease from version 1709. This is a 5.6% decrease in performance from version 1709. The PassMark PerformanceTest 9 benchmark resulted in some interesting results as compared to the other tests, this benchmark resulted in a sizable drop in overall CPU performance.

5. Conclusion

The Windows 10 April 2018 update patch which includes the security patches for Meltdown and Spectre did result in performance decrease in majority of the tests with exception for single core performance on CPU-Z. There were a lot of other variables to consider as well like certain background processes that must run for Windows and scheduling. While the speed deficiency is indeed measurable, the average consumer might not notice these differences. The test provided somewhat of a real-world scenario of the speed deficiency a user might experience with these updates. Because the speed deficiency was minor in these consumer benchmarks, this ultimately resulted in the patch being worth installing for regular users. However, in the enterprise space where security and performance are a top priority these patches might significantly affect the business. Especially when these patches introduced a speed deficit, this might cost these businesses large amounts of money. While these patches mitigate the potential exploits that Meltdown and Spectre can perform on a system, due to the nature of the vulnerability in the hardware itself, there is always a chance that there can be another way a system can be exploited in future patches. Thus, to truly protect yourself from these security vulnerabilities would be to wait for an eventual hardware refresh or revision from your CPU manufacturer. Meltdown and Spectre affects everyone and with this security vulnerability being rooted from an microarchitectural standpoint it is to be expected that a new field of security research will under go development to prevent such attacks in the future.

6. References

[1] Lipp Mortiz., Schwarz Michael., Gruss Daniel., Prescher Thomas., Haas Werner., Mangard Stefan., Kocher Paul., Genkin Daniel., Yarom Yuval., Hamburg

Mike. “Meltdown” (2018).

[2] Kocher Paul., Genkin Daniel., Gruss Daniel., Haas Werner., Hamburg Mike., Lipp Mortiz., Mangard Stefan., Prescher Thomas., Schwarz Michael., Yarom Yuval. “Spectre Attacks: Exploiting Speculative Execution*” (2018).

[3] J. Galowicz, "Cyberus Technology Blog - Meltdown", *Blog.cyberus-technology.de*, 2018. [Online]. Available: http://blog.cyberus-technology.de/posts/2018-01-03-meltdown.html. [Accessed: 27- Apr- 2018].

[4] J. Corbet, "KAISER: hiding the kernel from user space [LWN.net]", *Lwn.net*, 2017. [Online]. Available: https://lwn.net/Articles/738975/. [Accessed: 28- Apr-2018].

[5] J. Crowe, "A Clear Guide to Meltdown and Spectre Patches", *Blog.barkly.com*, 2018. [Online]. Available: https://blog.barkly.com/meltdown-spectre-patches-list-windows-update-help#OS-updates. [Accessed: 28- Apr-2018].

[6] T. Myerson, "Understanding the performance impact of Spectre and Meltdown mitigations on Windows Systems", *Cloudblogs.microsoft.com*, 2018.

[7] CPUID CPU-Z System Information Software [Online]. Available: https://www.cpuid.com/softwares/cpu-z.html.

[8] Passmark PerformanceTest Benchmark [Online]. Available: https://www.passmark.com/products/pt.htm