IJMSIT

International Journal of Multidisciplinary Studies and Innovative Technologies

Volume : 3
Number: 1
Year: 2019
Pages: 38 - 43

# The Impact of Meltdown and Spectre Attacks

Ahmet EFE*[1], Muhammed Onur GÜNGÖR[2]

[1]*Ankara Development Agency, PhD, CISA, CRISC, PMP, Turkey*
[2]*Department of Computer, Faculty of Engineering, Yıldırım Beyazıt University, Ankara, Turkey*
** Corresponding author: icsiacag@gmail.com*

***Abstract-*** Two vulnerabilities which are meltdown and spectre have been detected recently. They are used to capturing data on computer or smartphones by attackers. Vulnerabilities are part of the hardware design of the processor. The only thing is changing the processor to get rid of these vulnerabilities. There are some fixes from manufacturer of OS and BIOS which are trying to fix exploits. In this paper, detailed analysis will be performed for the personal and business impact of meltdown and spectre vulnerabilities.

*Keywords- Meltdown, Spectre, Cloud, Virtualization, Cyber Attacks*

## I. INTRODUCTION

The power of the microprocessors is increasing day by day. Manufacturers compete to make their processor faster. In this competition, manufacturer misses the security of the processors. The memory isolation is one of the biggest issues for processors security. Memory isolation separates memory region of the applications which are running on processors. Memory isolation also separates the kernel space and user space. It is necessary to provide a safe sandbox to avoid the crashing the entire system. Isolation is not only required to prevent crashes but also it is required to provide safe workspace for applications.

Applications should not access each other memory space because of the sensitivity of the data. Two vulnerabilities which are meltdown and spectre have been detected recently. They violate the memory isolation. Root of the Vulnerabilities are not related with operating system. They exist in the CPU hardware itself. Meltdown (Lipp, et al., 2018) and Spectre (Kocher, et al., 2018) work on PCs, distributed systems, cloud computers and mobile systems.

Intel, AMD, ARM and nearly every processor are affected from the spectre vulnerability. Meltdown is more hazardous on Intel processors which are made in last 20 years. On the other hand, meltdown can be safely avoided. The vulnerably is based on memory sharing between kernel and user space. The solution is based on end of sharing between user and kernel space (Bright, 2018).

In this paper, it is aimed to show that how meltdown and spectre are impacting the personal and business user? Solution proposals which are offered from manufacturer microprocessors and operating systems will be investigated. Impacts of the mitigations on personal and business user will be detailed.

## II. PROBLEM DEFINITION

Intel, AMD and ARM processors in the process 'Meltdown' and 'Specter' has been announced that there are serious security vulnerabilities. As companies take action to repair vulnerabilities, Apple announced that all Mac and IOS devices are affected by these two vulnerabilities. However, the company said there were no signs of abuse of these deficits.

According to Firefox's Twitter statement, Google experts have identified vulnerabilities, even though the browser can be exploited. On Wednesday, January 3, it was named Meltdown and Specter, which affected nearly all processor families and operating systems. It is not known if there are sensitive data stolen by exploiting the gaps found. Because the exploiting codes do not leave any traces behind and security devices cannot detect these vulnerabilities yet.

The reason why the name Meltdown is given is that it overrides all existing security products. The malicious attackers who take advantage of the openness can access the memory areas of their applications and they can read the data they want. In this way, all information held on the application is decoded.

In fact, even on the virtual computer, the data on the memory of the other virtual servers on the main server could be read. Google experts, security vulnerabilities after sharing with the public operating systems for Windows 10, MacOS, Linux and Android security patches began to be published. Amazon and Microsoft have announced that they have started a comprehensive work to close the gap.

Finding codes assigned to these vulnerabilities:

*For Specter: CVE-2017-5753 and CVE-2017-5717*

*For Meltdown: CVE-2017-5754*

In the processors designed by leading companies such as Intel, AMD and ARM, there were serious security vulnerabilities that could lead to attackers gaining sensitive data such as passwords and bank information. The vulnerabilities called Meltdown and Specter were found by security experts from different countries working in Google's 'Zero Project'. These vulnerabilities have been affected by nearly all modern computers in the world, including smartphones, desktops and tablets. The Meltdown vulnerability is currently affected by Intel branded processors, which have been produced since 1995 as a mainstream. However, it was announced that the company did not include Itanium server chips and Atom processors produced before 2013.

The Meltdown vulnerability allows hackers to disable hardware barriers between users-operated applications and the computer's memory. It is also claimed that the actions to be taken to repair the Meltdown can create up to 30 percent reduction in the speed of some tasks on the computer. The Specter vulnerability found on Intel, AMD and ARM processors allows hackers to trick sensitive applications into other applications without error.

It is reported that the company Intel started to provide software and software-supported hardware updates to fix security vulnerabilities. However, the company has announced that it will not cause a slowdown for ordinary computer users who use the processors. Google and its security experts have not yet been able to determine if hackers are using these vulnerabilities. Experts from Apple and Microsoft have announced that they have developed a patch for Meldown vulnerable desktop users, and that this patch can be used for the Linux operating system.

Microsoft also reported that patch services for cloud services are running, and that on 2018 January 3, Windows updates security updates for Windows users. Apple has announced on its website that all iPhones, iPads and Macs have been affected by the newly discovered vulnerabilities in Meltdown and Specter. However, the company has not yet found any evidence of abuse of these deficits. IPhone operating system updates (iOS 11.2) and Mac system updates (macOS 10.13.2), Apple TV updates (tvOS 11.2) Meltdown defends the protection of products against the error.

Apple said that these updates did not slow down devices, and that the Meltdown gap did not affect Apple Watches. Apple advised all customers to download applications from the App Store only. Google, the latest security updates, using the Android system devices, including their own products, Nexus, Pixel and Chromebook is also under protection. ARM announces the release of patches with company partners, and said AMD is currently in near zero risk for AMD products.

## III. ANALYSIS

In this paper, current topic meltdown and Spectre will be explained and detailed in the light of literature reviews and case studies. Meltdown was reported by three independent teams, which are Jann Horn from Google Project Zero, Werner Haas and Thomas Prescher from Cyberus Technology and Daniel Gruss, Moritz Lipp, Stefan Mangard and Michael Schwarz from Graz University of Technology. Spectre was reported by two independent people who are Jann Horn from Google Project Zero and Paul Kocher in collaboration with, in alphabetical order, Daniel Genkin from University of Pennsylvania and University of Maryland, Mike Hamburg from Rambus, Moritz Lipp from Graz University of Technology and Yuval Yarom from University of Adelaide. (Meltdown, 2018).

Meltdown is a kind of attack that use side channel cache method. Even if the application has not right on the memory region, it will be retrieve to last-level cache (LLC). After caching, a page fault error will be occurred because application does not have access for this data. Even if error occurred, the data will be stored in LLC. (Meltdown, 2018).

Spectre is a kind of attack that uses *speculative execution* beside the *side channel cache method*. The instruction has a jump after and comparison line. Although compare result is false, microprocessor will attempt to access data to increase the speed of the execution. After compare result, CPU will ignore the attempted data and there will be no page fault error. This attack is quitter when compared with meltdown. Even if the data is ignored, the attacker can access the attempted data which is in cache memory.

### *A. Speculative Execution*

Speculative execution is used to improve the operating capacity of the modern high-performance processors. Logic of the speculative execution is that instruction sets are executed N by N without waiting the order of the sequence. N group of instruction set is executed simultaneously without deciding necessity of instruction. If the speculative execution is not used, the performance of the execution will be decreased N times because of waiting for prior instructions to be executed and deciding to necessity of the instruction. If the instruction is necessary for further processing then it will be used, otherwise it will be ignored (Intel, 2018).

### *B. Side Channel Cache Methods*

Side channel method is not working like buffer overflows and other security exploits. Side channels do not effect on the data. They are not modifying or deleting the data or speculating the program. They are monitoring the system via microarchitectural properties of the system. A cache timing side channel decides the location

of the data in the processor using access time. Accessing memory time will be deciding the location of the data. Accessing the nearby cache will be take shorter time then accessing the far away cache. There are three methods, which are identified by Google Project Zero to use accessing private data using cache timing side channel (Intel, 2018).

## IV. AFFECTED SYSTEMS

Almost every system is vulnerable against spectre and meltdown because of the architecture of the vulnerability. The root of the vulnerability is microprocessors. It means every system which has microprocessors like Desktops, Laptops, Cloud Servers, HPCS (High Performance Computing Systems) and also Smart phones are affected. Spectre is detected on Intel, AMD and ARM processors. On the other hand, Meltdown is more dangerous on Intel processors, which are manufactured in the last 20 years.

In the business, side which includes cloud providers that operate on Intel microprocessors and Xen PV without mitigations will be affected from Meltdown vulnerability. Google, Apple, Microsoft and Firefox have patches on their sites. Their updates should be checked regularly to be as impressed as possible. Moreover, Docker, OpenVZ (Open Virtuozzo) or LXC (Linux Container) which are popular in business area will be affected from Meltdown because of their architecture which is sharing one kernel which use one kernel without hardware virtualization will be affected (Meltdown, 2018).

## V. DETECTION

Detection of the vulnerability is possible in theory, but it will be not easy as much as theory in practice. Meltdown and Spectre has different working mechanism. They will be detailed to show how they can be detected.

Meltdown leaves a trace behind it. It can be easily detected via controlling the page fault errors on kernel side. If one process has a great deal of page fault error than it can be suspected as meltdown attack. Recall and Precision values are high enough to satisfy. On the other hand, attacker can eliminate the exception using some special instructions which are provided by microprocessors (Trendmicro, 2018).

Spectre and meltdown use side channel cache methods which use L3 cache which is used by all cores. The L3 cores are the last memory before accessing the RAM. Caches are used to decrease the time of accessing memory. Accessing a data from RAM which is also located in cache is faster than accessing data from RAM. If the data is in cache than cache hit will be occurred otherwise cache miss will be occurred. Cache hit and cache miss can be understood via measuring the access time. There will be many cache misses to transfer data when there is a meltdown or spectre attack. Cache misses can be observed using performance counter of the microprocessors (Trendmicro, 2018).

Another detection method is using traditional malware detection which is tracking the pattern of the code. After some of the codes which using spectre and meltdown codes are known then antivirus systems can compare the code fragment with the known code to detect spectre and meltdown.

## VI. MITIGATIONS AND PERFORMANCE

Manufacturers offer some mitigation to prevent the vulnerable. In this chapter, mitigations will be detailed with their performance results for business and personal computer users. Intel has been published 3 mitigations for side channel methods which will be detailed in this chapter with their performance.

### [1] *Bound Check Bypass Mitigation*

The software mitigation, which is recommended by Intel to provide a barrier to prevent speculative execution. The instruction is called with the name of LFENCE. LFENCE stops the execution of younger instruction. LFENCE instruction should be added into the necessary lines of the application, but it should not use cavalierly. It reduces the performance of the microprocessor dramatically (Intel, 2018).

### [2] *Branch Target Injection Mitigation*

There are two mitigations techniques, which are offered by Intel to prevent the branch target injection. First technique is using a new designed interface, which is available future revision of the Intel processors. This technique requires the updated system software and microcode. The feature provides Indirect Branch Restricted Speculation (IBRS), Single Thread Indirect Branch Predictors (STIBP), and Indirect Branch Predictor Barrier (IBPB). IBRS restricts the indirect branches using speculation, STIPB inhibits sibling Hyperthread for indirect branch predictions and IBPB provide to deny control of the preceding code to posterior indirect branch predictions. (Intel, 2018). It does not provide retroactive benefit due to the need for new hardware.

The second technique is based on “return trampoline” which is called “Retpoline”. This technique is based on adding an dummy branch that has a return statement before the jump and call instruction to prevent branch Traget injection. (Intel, 2018). This method is better than the previous method because it can be applied retrospectively on many processors.

### [3] *Rogue Data Cache Load Mitigation*

Current systems have a single page table for each process. This mitigation offers the using two paging

structure for each user process. This approach was first proposed by KAISER (Gruss, et al., 2017) stands for "kernel address isolation to have side-channels efficiently removed". User paging structure should have the application pages and minimal subset of supervisor pages which are necessary for user side processor operation that are system calls and interrupts. Supervisor paging structure should have all kernel space pages. It can also have user side pages (Intel, 2018).

[4] *Performance*

Solutions for Meltdown and Spectre can be easy to apply but there is a significant performance impact for personal and business user. I/O operations need system call to get data from kernel space to user space. Most of the programs use I/O operations to complete their task. For instance, when a program wants to access the files on the disk then it will make a system call to the kernel space. In this situation, the microprocessor will switch from user space to kernel space and flush the memory lookup table cache. This operation has a significant cost especially the operation frequency is considered. I/O intensive applications for example database, e-commerce application or HPC programs will be worst affected. Applying the OS patch will be decrease the performance of the microprocessor about 10-30% for I/O intensive applications (Francis, 2018).

As we have seen, the Meltdown weakness is far more than a matter of concern with performance concerns and is a serious problem. In the sample exploit I have just shown, we have seen that the system can leak data from critical data structures by bypassing ASLR. Of course, those who want to exploit these weaknesses will try to steal this much more important data by taking it further. This data includes information such as encryption key, passwords, credit card information that you enter on online purchases, your identity information, and more than just the damages of classic computer malware.

One of these factors in the article that counts the factors that lead to Meltdown is explained that the virtual memory mechanism is visible to the user mode by the kernel memory space for some reasons. When we recall the information in that section, it would be easier to understand if the operating systems have solved this problem by completely isolating the User and Kernel mode address space from each other. As is mentioned before, if User mode processes are isolated from each other by page table change, this problem is tried to be solved by completely isolating the kernel and user address space.

When only the processes are scheduled on the processor, the switched page table means that it is necessary to perform the system calls to each Kernel mode. Unfortunately, the change of this page table in every system call is a costly process for the processor. It is obvious that the cost of this Page Table switch, which is based on the cost of switching to kernel mode, will adversely affect system performance. This is also due to the valid handling of an Interrupt that will occur when the processor is operating a user mode process.

In this case, if you do not do a lot of system calls, if you do not do a lot of work on the load that will create too many interrupts (network cards on servers, for example) as the end user, these patches will not cause a loss of performance at a level that is too intimidating. Especially in the new generation processors, this difference will probably not be felt.

These investigations have shown that, while designing architectures, they need to be examined more carefully, even if they are exploited, such as software. In fact, the problem-creating part is not that the architecture is designed incorrectly, but the design has prepared the ground for abuse. Of course, additional measures are necessary to prevent this abuse, and it is possible that these additional measures or changes in the design will overload the performance.

*Ways To Protect From Meltdown And Specter*

The bad side of Specter and Meltdown is Intel, AMD and ARM , which have emerged as an important security vulnerability that could lead to a change in processor designs ; device and operating system discrepancy. As we say at the beginning, Mac, iPhone, is the user; whether you are a Windows and Android phone user; you are under threat unless the manufacturer has submitted a software update that closes the vulnerability. The three major processors we are mentioning at this time are in a joint effort, and they are strongly encouraging users to update their systems. On the other hand, no device is hacked using this vulnerability was shared by Intel and Arm where it was necessary to run malware on the system for hacking to take place. It was also said that it would not be possible for the deficit to erase, alter or delete the data. It is important to note that Intel offers the update.

*Android Phones*

You need to start with Android phones because it is the most common mobile operating system worldwide. If you have a Google-branded phone (such as Nexus 5X or Nexus 6P), your phone will automatically download the security update on January 5; you will only stay install. It is even easier if you have a Pixel or Pixel 2 phone; The security update will be installed automatically. Google should offer the security update for their phones immediately, but it does not have the same sensitivity as other Android phone manufacturers. Unfortunately, at this point, there is nothing we can do other than to expect the manufacturer or operator to provide security updates as end users. You're lucky if you're using top-of-the-line phones like Samsung, LG, Sony.

*Windows PC*

Let us continue with Windows because it has more users on the desktop platform. Microsoft released the update on the evening of the day we were aware of the vulnerability. Because Windows 10 automatically downloads the necessary security updates (if you have not set otherwise), you just need to download and install. Of course, every important update is waiting for you like a long download, reboot after installation process. Do not forget to register without applying the update.

*MAC, iPhone / iPad*

We all know how fast Apple was when a security breach occurred. iOS, MacOS, offering frequent updates TVOSA the official explanation of the technology meltdown and Spectra security giant open the page can be found. In summary, the vulnerability that affects all Mac and iOS devices is no longer harmful to the end user. iOS 11.2, MacOS 10.13.2 and tvOS 11.2 updates include a patch that protects users against Meltdown. To protect against Specter, the Safari browser will be updated soon. Apple recommends users to download software download from trusted sources such as the App Store.

*Google Chrome*

Windows, Mac, Linux, and Android users love the web browser by making a small setting in Google Chrome may not be affected by this vulnerability. This exploit, also was buried in JavaScript codes can be run through the web site, to fix these flaws in Chrome users at "Site Isolation – Site Isolation" feature.

Windows, Mac, Linux, Chrome OS or Android "Strict Site Isolation" feature how to change is described below:

chrome://flags/#enable-site-per-process

Copy and paste it into the URL field at the top of your web browser Chrome, and then press Enter. View on-screen XIT "Strict Site Isolation" feature. After activating, you must restart Chrome.

## VII. CONCLUSION

In this paper, importance of the memory isolation for microprocessors is investigated and two deficits, which are meltdown and Spectre, detailed. Meltdown and Spectre vulnerabilities are part of the hardware design of the processors and there is no certain solution to protect the user from attackers without decreasing the performance of the microprocessors. Regardless of manufacturer or operating system almost all PCs, laptops, tablets and smart phones that threaten the AMD, ARM and Intel, which are including processors of potentially effective.

Meltdown not only core memory by attackers also target the physical memory on the machine and, therefore, other programs, and to read all the secrets of the operating system. Meltdown, user applications and the operating system is using to run to break the isolation between the speculative and the core of any application, including memory allocated for access to system memory.

Spectre does not seem easy to correct this deficit and this topic totally for elimination of changes in the architecture of the processor. This is a long process. Spectre attack, breaking the isolation between applications, an attacker can trick a program error-controlled programs, it programs its memory to read the desired zones of their confidential data leakage by forcing. This data can be read from the later side-channel. To analyze the user programs, in addition to the guest system information to choose among virtualization hypervisor can be used to leak.

Almost every system is affected from Meltdown and Spectre. Microprocessors' architecture of the Intel and Apple are vulnerable for both meltdown and spectre. On the other hand, microprocessors' architecture of ARM and AMD are vulnerable only for spectre. Detection of these attacks is not easy according to other attacks. Detection is based on monitoring the page fault errors and performance counter of the processor. Another detection method is tracking the pattern of the code. It can be possible after some of the malwares are detected and recorded into the database systems of the antiviruses.

The vendors are offering some mitigation for their users, which are slated for Spectre Variant 1 that is CVE-2017-5753 Bounds Check Bypass, Spectre Variant 2 that is CVE-2017-5715 Branch Target Injection and Meltdown Variant 3 that is CVE-2017-5754 Rogue Data Cache Load. The solutions can be applied easily by updating Operating System. Performance of the microprocessors will be decreased nearly 10-30% for I/O intensive applications.

## REFERENCES

[1]. Bright, P. (2018, 1 5). *Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it*. Retrieved from ARS TECHNICA: https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/

[2]. Trendmicro, (2018). *Detecting Attacks that Exploit Meltdown and Spectre with Performance Counters*. (2018, March 13). Retrieved from Trend Micro: https://blog.trendmicro.com/trendlabs-security-intelligence/detecting-attacks-that-exploit-meltdown-and-spectre-with-performance-counters/

[3]. Francis, R. (2018). *How the Meltdown and Spectre bugs work and what you can do to prevent a performance plummet.* Ellexus.

[4]. Grisenthwaite, R. (2018). *Cache Speculation Side-channels.* arm.

[5]. Gruss, D., Lipp, M., Schwarz, M., Fellner, R., Maurice, C., & Mangard, S. (2017). Kaslr is dead: long live kaslr.

*International Symposium on Engineering Secure Software and Systems*, 161-176.

[6]. Innus, M. D., Simakov, N. A., Jones, M. D., White, J. P., Gallo, S. M., DeLeon, R. L., & Furlani, T. R. (2018). Effect of Meltdown and Spectre Patches on the Performance of HPC Applications. *arXiv preprint arXiv:1801.04329*.

[7]. Intel. (2018). *Intel Analysis of Speculative Execution Side Channels.*

[8]. Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., . . . Yarom, Y. (2018). Spectre Attacks: Exploiting Speculative Execution. *arXiv preprint arXiv:1801.01203*.

[9]. Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., . . . Hamburg, M. (2018). Meltdown. *arXiv preprint arXiv:1801.01207*.

[10]. Meltdown. (2018). *Meltdown and Spectre*. (n.d.). Retrieved from Meltdown Attack: https://meltdownattack.com/