International Journal of Engineering and Future Technology,
Year 2021; Volume 18; Issue No. 2;
ISSN 2455-6432

Impact of Meltdown and Spectre on CPU Manufacture Security Issues

Roza Dastres[1] and **Mohsen Soori** [2*]

[1] Department of Computer Engineering, Cyprus International University, North Cyprus, Turkey;
Email : roza.dastres@yahoo.com

[2] Department of Mechanical Engineering, Eastern Mediterranean University, Famagusta, North Cyprus, Via Mersin 10, Turkey
* *Corresponding author's* Email : mohsen.soori@gmail.com, mohsen.soori@emu.edu.tr

ABSTRACT

The Meltdown and spectre holes are two security deficiencies which can provide access to personal data for hackers and can potentially affect performances of Linux, Mac systems, and Windows devices plus other operating systems. In order to prevent the capturing data on computer or smartphones by attackers, two vulnerabilities as meltdown and spectre are recently detected on CPU manufacture. Vulnerabilities are part of the hardware design of the processor by changing the processor structures in terms of security enhancement of the CPU manufacture. Meltdown hole is run on a wide range of operating systems including IOS, Linux, MacOS, and Windows which can affect many service providers and cloud services. There are some fixes from manufacturer of OS and BIOS which are trying to fix exploits. Software patches should be used while undergo updating operations should also be applied in order to enhance the security of operating systems. In this paper, the impact of meltdown hole on various processors and operating systems are studied and methods to deal with the security issues of the processors are also discussed.

Keywords: Meltdown, Spectre, Cloud, Virtualization, Cyber Attacks.

Mathematics Subject Classification: 68M10, 68M15, 68M20

Computing Classification System: C.2.0

1. INTRODUCTION

A lot of concern is recently created from the security created by the Spectre and Meltdown as the duo can be used to steal data from nearly any computer, as well as iPhones and iPads and other mobile devices. The research conducted in early 2018 have shown that all of the computer security chips produced in the past 20 years have major defects (Suryateja 2018). Security defects under the names of meltdown (Lipp et al. 2018) and spectre (Kocher et al. 2019) have been found and spread in Intel, AMD, and ARM processors. Differences between manufacturers (e.g., Intel vs. AMD) and architectures (e.g., x86-64 vs. Arm) make some processors vulnerable to more variants than others. While these are fundamentally hardware design flaws, attempts to remediate on a software level have seen some success. Given these vulnerabilities, destructive processes bring about the permission to access the Contents of other applications in the virtual memory. Meltdown and spectre holes are the destructors that attack billions of mobiles and computers ("Security ulnerability"). These holes directly

impact the central processor of the devices and make the robbery of information being processed likely. The specter hole is related to the speculative execution method in the processor ("Security ulnerability"). Spectre and Meltdown enable attackers to extract encryption keys and passwords from compromised systems, enabling other attacks dependent on access to compromised systems. Leveraging Spectre and Meltdown does not require a user to run a particular maliciously-formed executable, as JavaScript-based proofs-of-concept demonstrate the potential of exploiting these vulnerabilities inside a web browser. Leaking Data on Meltdown-resistant CPUs is investigated by Schwarz et al. (Schwarz et al. 2019) to ensure proper isolation between the kernel and user space. The Impact of Meltdown and Spectre Attacks is also studied by Efe and Güngör (Efe and Güngör) to discuss and suggest the recent methods in security issues of the processors.

For cloud computing, Spectre and Meltdown can be leveraged by attackers to escape software containers, paravirtualized systems, and virtual machines. Understanding of Spectre and Meltdown has increased significantly since the initial disclosure, and security researchers continue to study these vulnerabilities. Presently, 13 Spectre variants and 14 Meltdown variants have been identified. Initially, AMD processors were thought to be immune to Meltdown, though one variant has been successfully demonstrated on AMD systems.

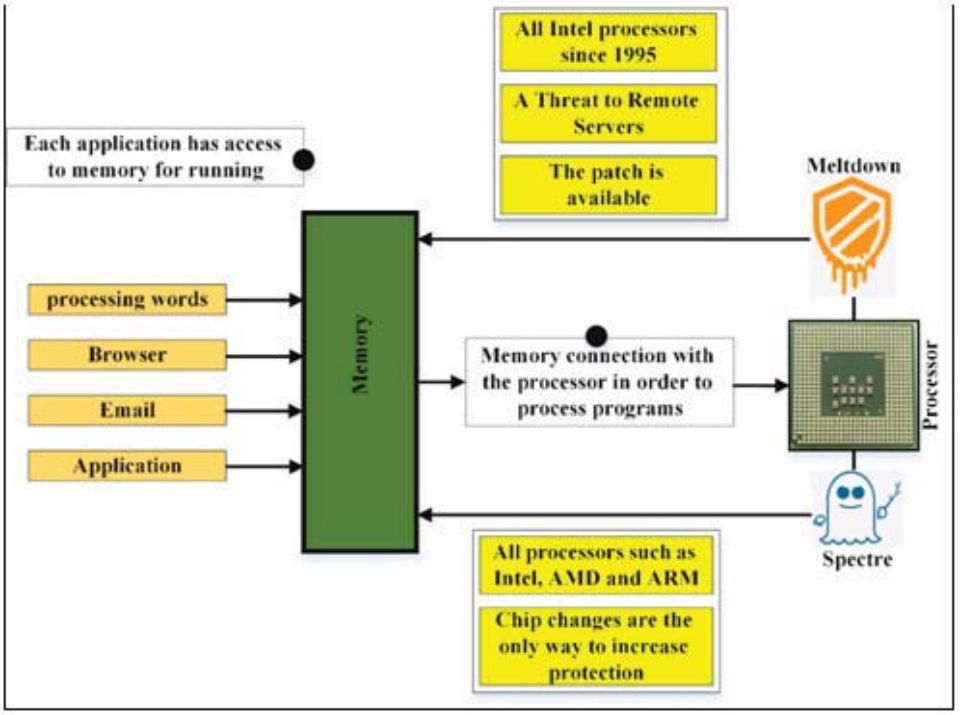

Fig. 1 The diagram of meltdown and spectre holes penetration into the systems (Tabe et al.).

Operating system kernel is a low quality software which controls output and input requests coming from other software and hardware. Kernel is the mediator between the programs and the hardware;

namely, any request that each of the programs (even the operating system itself) has to use the hardware sources is first sent to the kernel to be analyzed ("Meltdown-spectre-bugs" 2020). Kernel has also other roles including managing system sources, preparing operating systems and the applications, managing the addresses and the memory. The kernel of the operating system should always be updated otherwise it can cause specific issues such as security-related ones for the system. Figure (1) shows the diagram of penetration into the systems by meltdown and specter holes (Tabe et al.).

2. DISCUSSION

As a result of security holes in the CPU, the attackers can manipulate the top memory of a processor taking advantage of the parallel administration of the processes. They also enable the attackers to access the memory using JavaScript code being processed in a browser. The contents of memory can have compact information, passwords, coding keys, other virtual system data, or other valuable information.

Spectre, according to the original authors of the Spectre paper, "[induces] a victim to speculatively perform operations that would not occur during strictly serialized in-order processing of the program's instructions, and which leak victim's confidential information via a covert channel to the adversary ("Meltdown-spectre-bugs" 2020)." Spectre attacks are conducted in three steps:

- The setup phase, in which the processor is mistrained to make "an exploitably erroneous speculative prediction."
- The processor speculatively executes instructions from the target context into a microarchitectural covert channel.
- The sensitive data is recovered. This can be done by timing access to memory addresses in the CPU cache ("A comprehensive guide of Spectre and meltdown" 2020).

Meltdown exploits a race condition between memory access and privilege level checking while an instruction is being processed. In conjunction with a CPU cache side-channel attack, privilege level checks can be bypassed, allowing access to memory used by an operating system, or other running processes. In certain circumstances, this can be used to read memory in paravirtualized software containers [9]. Meltdown attacks, according to the original authors of the Meltdown paper, are conducted in three steps:

- The content of an attacker-chosen memory location, which is inaccessible to the attacker, is loaded into a register.
- A transient instruction accesses a cache line based on the secret content of the register.
- The attacker uses Flush+Reload to determine the accessed cache line and hence the secret stored at the chosen memory location .

Because of the nature of Spectre and Meltdown, ensuring the latest installed available patches for your system is necessary. Troublingly, initial patches for Spectre and Meltdown is focused on preventing exploitation of a specific methodology, not addressing the microarchitectural vulnerability enabling those attacks. As of November 2018, on systems with the latest available patches,

exploitation of some Spectre and Meltdown variants remained possible under specific circumstances. Patches for Spectre and Meltdown should be considered a work in progress, with initial patching strategies introduced and rolled back due to instability or findings indicating they were ineffective against specific variants. It is unclear if the pair of vulnerabilities can be completely patched through microcode and software updates, though this uncertainty should not discourage users or administrators from deploying available patches.

processors	**spectre**	**spectre**	**Meltdown**
	CVE-2017-5753	**CVE-2017-5715**	**CVE-2017-5754**
AMD Opteron & EPYC X86	All processors Kernel updates	All processors Kernel updates	Not susceptible No updates required
Cavium ThunderX Armv8	ThunderX2 firmware and kernel updates	ThunderX2 firmware and kernel updates	Not susceptible No updates required
IBM Power	Power7 firmware and kernel updates	Power7 firmware and kernel updates	Power7 firmware and kernel updates
IBM System z	All processors Kernel updates	All processors Kernel updates	Not susceptible No updates required
Intel Itanium	Not susceptible No updates required	Not susceptible No updates required	Not susceptible No updates required
Intel Xeon X86	All processors Kernel updates	All processors kernel and compiler updates	All processors Kernel updates
Oracle Sparc V9	susceptible OS patches	susceptible OS patches	Not susceptible No updates required
Qualcomm Centriq Armv8	susceptible Kernel updates	susceptible firmware and kernel and compiler updates	susceptible Kernel updates
Accelerator	**spectre**	**spectre**	**Meltdown**
	CVE-2017-5753	**CVE-2017-5715**	**CVE-2017-5754**
AMD Radeon Instinct & Pro	Not susceptible	Not susceptible	Not susceptible
Intel Xeon Phi	3200,5200,7200 Series	3200,5200,7200 Series	3200,5200,7200 Series
Nvidia Tesla	Not susceptible	Not susceptible	Not susceptible

Table 1. The suggestions and necessary items to prevent spectre and meltdown attacks on various processors ("Datacenters-brace-spectre-meltdown-impact").

Every software company proposed patches as follows to resist security holes. Microsoft has released an update for Windows 10 and has patched these vulnerabilities. Apple has patched these vulnerabilities in MacOS High Sierra 10.13.2 update and probably with the release of MacOS 10.13.3 version patches maybe be completely improved. Linux kernel developers have put kernel memory in a completely separated space by implementing the isolation of page tables (Jimenez, Papadakis, and Le Traon 2016; Kim and Lee 2008). Also, Google has updated Nexus and Pixel devices and patched the vulnerabilities. In Table (1), the suggestions and necessary items to prevent specter and meltdown attacks on various processors have been demonstrated ("Datacenters-brace-spectre-meltdown-impact").

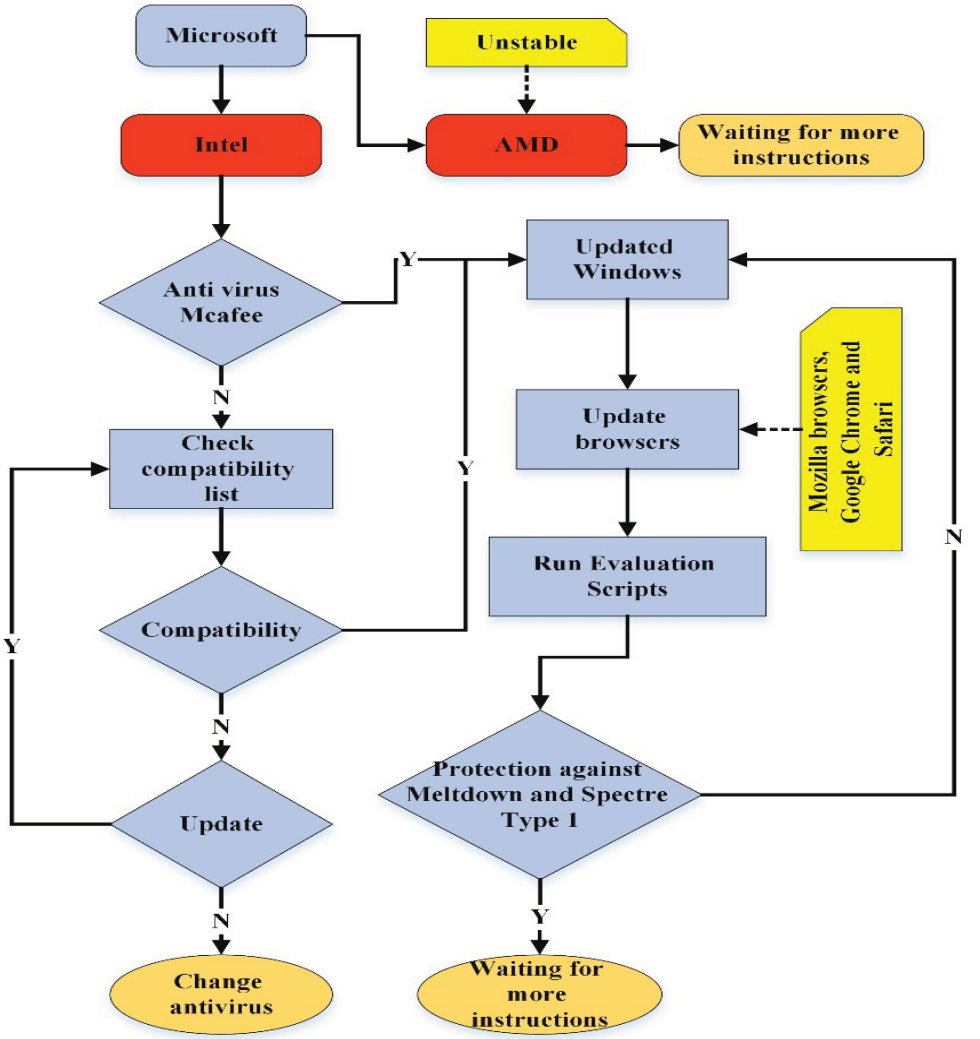

Fig. 2. The structure of resisting meltdown and spectre holes on Microsoft Company products ("About Meltdown Spectre").

Different ways of preventing meltdown and spectre holes on different processors and operating systems are presented in the Figures (2), (3), and (4) ("About Meltdown Spectre"). The structure of spectre and meltdown holes on the products of the Microsoft Company is shown in the Figure (2) ("About Meltdown Spectre"). The most important items to prevent the penetration of attackers are using updated anti-virus and the browsers. Every browser has its own defects which are removed in the updated versions. Antiviruses have the roles of identifying bad ware and destructive programs and announcing their penetration into the system.

The structure of resisting meltdown and spectre holes on UNIX and Linux operating systems is presented in the Figure (3) ("About Meltdown Spectre"). In this structure the kernel of operating systems are assessed and the patches required to deal with security issues are produced.

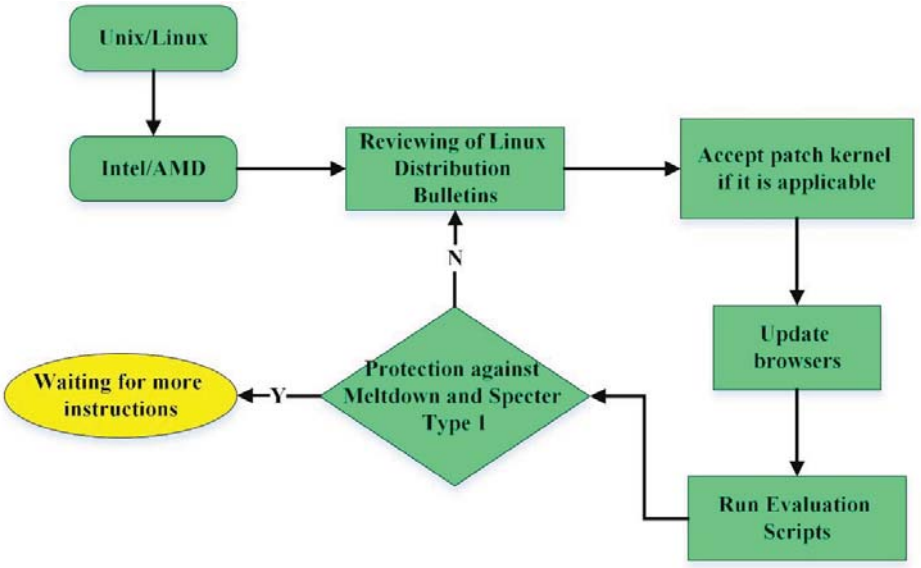

Fig. 3 The structure of resisting meltdown and spectre holes on UNIX and Linux operating systems ("About Meltdown Spectre").

Figure (4) ("About Meltdown Spectre") shows the structure of resisting meltdown and spectre holes on MacOS operating system. The structure of Figure (4) is comprised of two operating systems including El Capitan, Sierra & High Sierra. Security patches required for every operating system should be produced and the browsers should be updated and the ways of penetrating the system should be blocked.

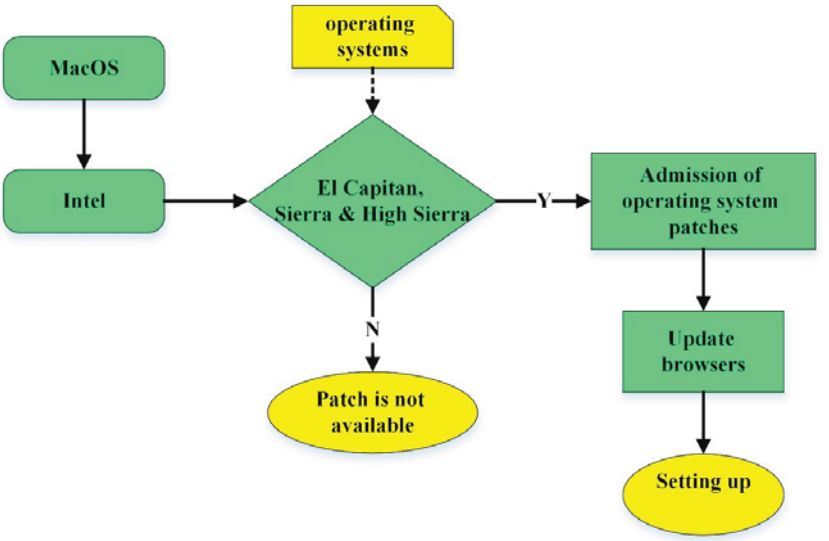

Figure 4. The structure of resisting meltdown and spectre holes on MacOS operating system ("About Meltdown Spectre").

3. CONCLUSION

Meltdown and spectre holes are two security deficiencies by which hackers can have access to personal data and can potentially affect Linux, Mac systems, and Windows devices plus other operating systems. These vulnerabilities occur through hardware and are carried out specifically through the processors. Kernel memory space is hidden and protected from the access of processes and the programs and users cannot easily gain access to the device memory by logging into the system, but destructive software designed for penetrating holes and some Java Script codes can obtain access to the secret information provided in kernel memory. Meltdown and spectre holes can have access to the user models plus the kernel and make disruptions between various processes that are being run. A destructive process can have access to the shared memory. As a result, to prevent the penetration and carry out repairs, each operating system should use a set of patches.

4. REFERENCES

"About Meltdown Spectre." 2020. https://wiki.epfl.ch/secure-it/meltdown-spectre-en.

"A comprehensive guide of Spectre and meltdown." https://www.techrepublic.com/article/spectre-and-meltdown-explained-a-comprehensive-guide-for-professionals/.

"Datacenters-brace-spectre-meltdown-impact."2020. https://www.nextplatform.com/2018/01/18/datacenters-brace-spectre-meltdown-impact/.

Efe, Ahmet, and Muhammed Onur Güngör. "The Impact of Meltdown and Spectre Attacks." Review of. *International Journal of Multidisciplinary Studies and Innovative Technologies* **3 (1)**:38-43.

Jimenez, Matthieu, Mike Papadakis, and Yves Le Traon. 2016. An empirical analysis of vulnerabilities in openssl and the linux kernel. Paper presented at the 2016 23rd Asia-Pacific Software Engineering Conference (APSEC).

Kim, Jaekwang, and Jee-Hyong Lee. 2008. A methodology for finding source-level vulnerabilities of the Linux kernel variables. Paper presented at the 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence).

Kocher, Paul, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, and Thomas Prescher. 2019. Spectre attacks: Exploiting speculative execution. Paper presented at the 2019 IEEE Symposium on Security and Privacy (SP).

Lipp, Moritz, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. 2018. "Meltdown." Review of. *arXiv preprint arXiv:1801.01207*.

"Meltdown-spectre-bugs." https://blog.barkly.com/meltdown-spectre-bugs-explained.

Schwarz, Michael, Claudio Canella, Lukas Giner, and Daniel Gruss. 2019. "Store-to-leak forwarding: Leaking data on meltdown-resistant cpus." Review of. *arXiv preprint arXiv:1905.05725*.

"Security ulnerability." 2020. https://en.wikipedia.org/wiki/Meltdown.

Suryateja, PS. 2018. "Threats and vulnerabilities of cloud computing: a review." Review of. *International Journal of Computer Sciences and Engineering* **6 (3)**:297-302.

Tabe, Arash, Seyyed Keyvan Mousavi, Kaveh Shaker, and Payam Hatamzadeh. "AN INVESTIGATION OF THE IMPACT OF MELTDOWN ON OPERATING SYSTEMS." Review of.