# AN INVESTIGATION OF THE IMPACT OF MELTDOWN ON OPERATING SYSTEMS

Arash Tabe[1], Seyyed Keyvan Mousavi[2], Kaveh Shaker[3], Payam Hatamzadeh[4]

[1]Computer Engineering Student, Department of Computer,
Tabriz University Campuses, Tabriz, Iran
[2]PhD Student, Department of Computer, Urmia Branch,
Islamic Azad University, Urmia, Iran
[3]Computer Engineering Department, Mizan Higher Education Institute, Tabriz, Iran
[4]Faculty of Engineering, Department of Computer Engineering, University of Isfahan,
Isfahan, Iran

***ABSTRACT***

*Meltdown hole is a hardware vulnerability which affects Intel processors, IBM Power processors, and some other ARM based processors. Through this hole, a destructive process sets out to read memory even when the destructive process is not allowed to do so. Meltdown hole is run on a wide range of operating systems including IOS, Linux, MacOS, and Windows; in addition, it affects many service providers and cloud services. The security of operating systems should be provided using hardware and software factors in order to prevent the penetration of destructors. Operating system is entitled to manage and control hardware and run the applications. Software patches should be used in order to enhance the security of operating systems which should undergo updating operations. In operating systems, kernel completely controls the system and connects the applications to the processor, memory, and other hardware inside a system. Meltdown hole allows the attackers to access and read the contents of kernel memory. In this paper, the impact of meltdown hole on various processors and operating systems are investigated and the security solutions of hardware and software companies are compared so as to deal with the security issues of the processors.*

***KEYWORDS***

*Meltdown, destructor, operating system, kernel, security*

## 1. INTRODUCTION

The research conducted in early 2018 have shown that all of the computer security chips produced in the past 20 years have major defects [1]. Security defects under the names of meltdown [2] and spectre [3] have been found and spread in Intel, AMD, and ARM processors. 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 [4]. 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 [4]. Speculative execution is a technique used by most of the modern processors to optimize functioning. The role of this technique in the processor is to investigate the activities that it guesses the device will operate on them.

These vulnerabilities have been recognized by Google Project Zero and other researchers who have studied the security of operating systems independently and separately. According to the literature, all computer systems including laptops, tablets, and cell phones will be under the impact of this security hole. To date, three types of these vulnerabilities have been identified out of which the first two statuses are called spectre and the third one is called meltdown. Meltdown hole to which CVE-2017-5754 [5] vulnerability code has been assigned crosses from the layer between user software and operating system in a way that these attacks allow the destructive program to have access to the running memory and the secret information plus the operating system [6]. Linux kernel developers have released KPTI patch [7] in order to transfer kernel to a completely separate address space. Meltdown attacks can be prevented using KPTI, which has been designed to enhance security by separating kernel space from the user space memory. This patch is on the basis of KAISER patch [7].

Specter hole to which CVE-2017-5753 [5] and CVE-2017-5715 [5] vulnerability codes have been assigned allows the hackers to have access to the information in Kernel/Cached files or the data saved in the memory in the process of being run such as certificates (passwords, login keys, and etcetera). Specter bad ware affects Intel, AMD and ARM processors.

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 [8]. 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.

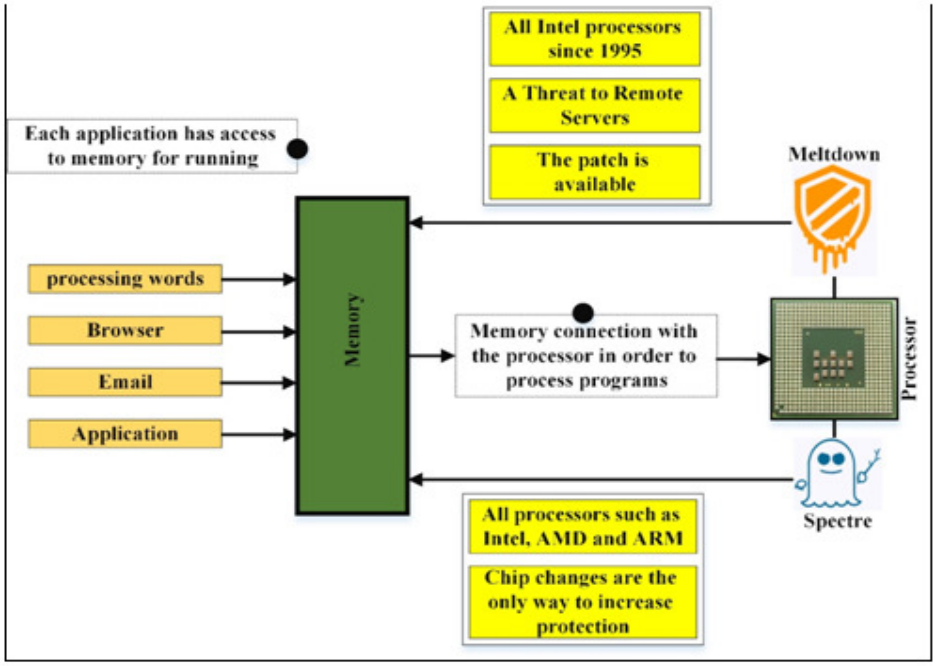


Figure 1. The diagram of meltdown and spectre holes penetration into the systems

Google Company has proposed a software method called Retpoline to prevent spectre attacks without patching hardware [9]. Retpoline is in fact a software structure by which the indirect

branches of the programs can be separated. Using Retpoline, Google managed to correct the programs directly and did not conduct updating operations related to hardware preventing system slowdown consequently [9]. After carrying out various tests, Google Company announced that it can patch the computers using Retpoline so that they can withstand specter attacks and not have slowdown or efficiency reduction.

Even the developers of cloud calculations such as Amazon and Microsoft are encountered with these two security defects [10]. Cloud calculations are an internet-based model which offers a pattern to supply, consume, and deliver information technology services (including software, information and shared sources) using internet [11]. In cloud calculations, access to information technology in time of need and based on the extent to which users make demands is delivered to the user through internet in a flexible and measurable manner. What a cloud calculation developer offers is online business programs which are made available to the users through web browser or other software. Practical software and information are stored on the servers and made available to the users according to their demands. Details remain hidden from the users and they do not need to have expertise and control on the underlying structure of cloud technology to able to use it. Through meltdown and spectre attacks, hackers can gain access to all cloud data as all the data are in a shared space [12].

## 2. DISCUSSION

Various security techniques should be used to enhance the security of computer systems and protect data. With the rapid and continuous development of the attacks of attackers and the exploration of holes there is the need to have smart tools to be able to react in time when facing a new attack. Meltdown hole enables the attacker to read not only the kernel memory but also the whole physical memory of the intended machine. Meltdown hole uses speculative execution to break the isolation between the user programs and the operating system and enables each program to have access to the whole memory of the system including special kernel memory [13].

Spectre and meltdown holes cause the hackers to gain access to the important information of the programs, passwords, and the keys. Spectre and meltdown holes are different from each other in two respects. First, meltdown is conducted on Intel and ARM processors and AMD processors are not faced with this problem. However, specter can be run on all kinds of processors. Second, using and running meltdown is easy but it is far more difficult to run spectre despite the fact that there are many techniques for this purpose. Of course, using each of these holes to penetrate and rob information is very difficult and complex. Although, hackers have recently demonstrated that there is no limitation. Various ARM processors that are under meltdown attack have been demonstrated in Table (1).

Table 1. Various ARM processors under meltdown attack

| **Process** | **Spectre** | | **Meltdown** | |
|---|---|---|---|---|
| | Type 1 | Type 2 | Type 3 | Type 3a |
| Cortex-R7 | Y | Y | N | N |
| Cortex-R8 | Y | Y | N | N |
| Cortex-A8 | Y | Y | N | N |
| Cortex-A9 | Y | Y | N | N |
| Cortex-A15 | Y | Y | N | Y |
| Cortex-A17 | Y | Y | N | N |
| Cortex-A57 | Y | Y | N | Y |
| Cortex-A72 | Y | Y | N | Y |
| Cortex-A73 | Y | Y | N | N |
| Cortex-A75 | Y | Y | Y | N |

Security holes make it possible for the attackers to 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. A list of various Linux distributions under the impact of meltdown hole is given in Table (2).

Table 2. The list of various Linux distributions based on irresistance against meltdown attacks

| # | List of operating systems |
|---|---|
| 1 | Red Hat Enterprise Linux 5 (including clones such as CentOS/Oracle/Scientific Linux 5) |
| 2 | Red Hat Enterprise Linux 6 (including clones such as CentOS/Oracle/Scientific Linux 6) |
| 3 | Red Hat Enterprise Linux 7 (including clones such as CentOS/Oracle/Scientific Linux 7) |
| 4 | Debian Linux wheezy |
| 5 | Debian Linux Jessie |
| 6 | Debian Linux stretch |
| 7 | Deiban Linux buster, sid |
| 8 | SUSE Linux Enterprise 11 |
| 9 | SUSE Linux Enterprise 12 |
| 10 | OpenSuse Linux based upon SUSE 12/11 |
| 11 | Fedora Linux 26 |
| 12 | Fedora Linux 27 |
| 13 | Amazon Linux AMI (Bulletin ID: ALAS-2018-939) |

Linux attempts to limit the extent of user space memory to which the kernel has access. The reason is that on penetration, the attacker tries to penetrate first into the user memory space and waits for the kernel orders to gain access to that space. This feature limits the attack level and narrows the possibility of the access of destructive code to the kernel which causes misusing the whole device.

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 [14, 15]. Also, Google has updated Nexus and Pixel devices and patched the vulnerabilities. In Table (3), the suggestions and necessary items to prevent specter and meltdown attacks on various processors have been demonstrated [16].

Table 3. The suggestions and necessary items to prevent spectre and meltdown attacks on various processors

| **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 |

Intel Company has released patches for its own processors to deal with the security vulnerabilities that affect millions of personal computers, servers, and devices connected to the internet and has asked the users to update their systems. Figures (2), (3), and (4) have demonstrated ways of preventing meltdown and spectre holes on different processors and operating systems. Figure (2) shows the structure of spectre and meltdown holes on the products of the Microsoft Company. 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. Anti-viruses have the roles of identifying bad ware and destructive programs and announcing their penetration into the system.

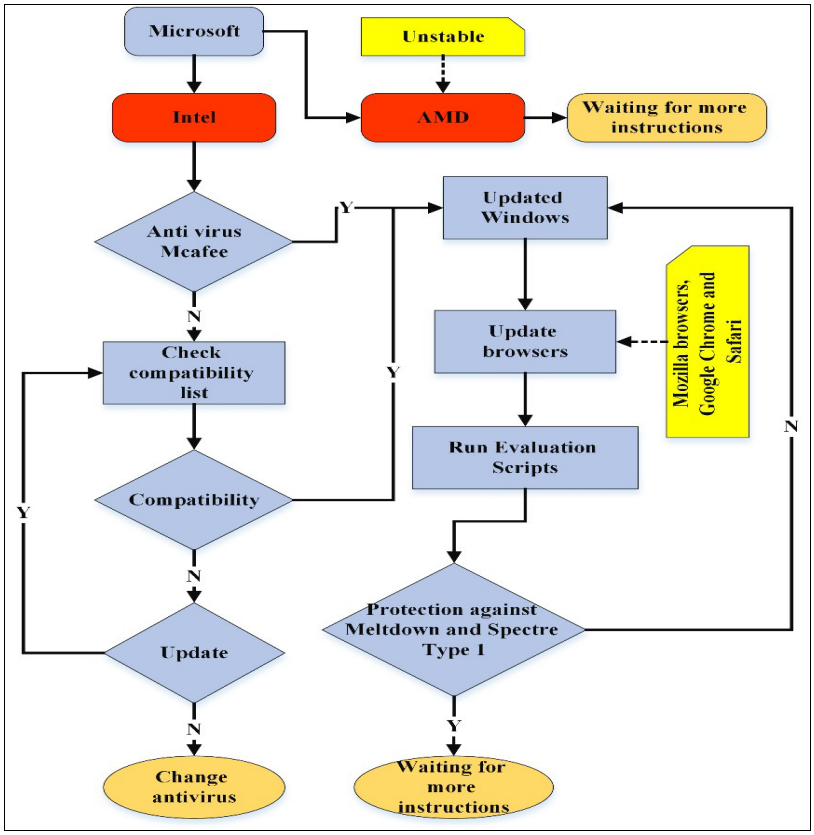


Figure 2. The structure of resisting meltdown and spectre holes on Microsoft Company products [17]

Figure (3) demonstrates the structure of resisting meltdown and spectre holes on UNIX and Linux operating systems. In this structure the kernel of operating systems are assessed and the patches required to deal with security issues are produced.

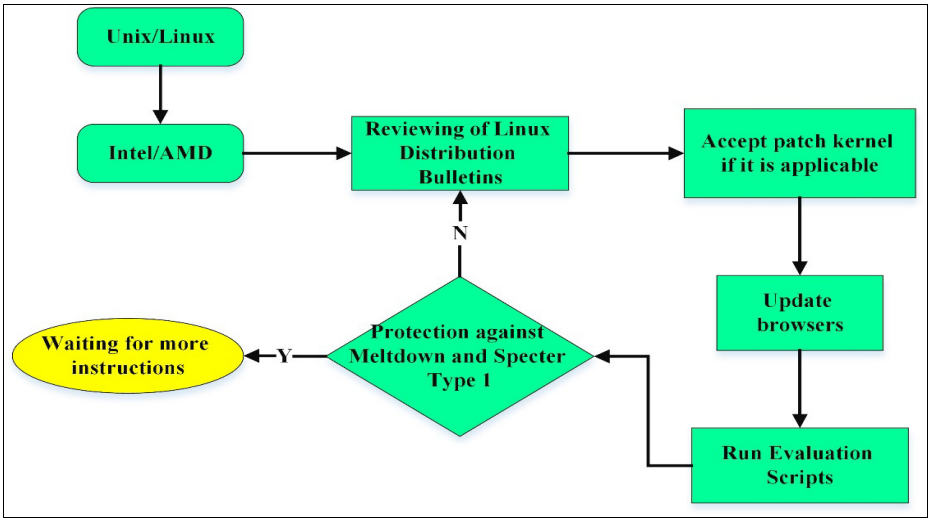


Figure 3. The structure of resisting meltdown and spectre holes on UNIX and Linux operating systems

Figure (4) 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.

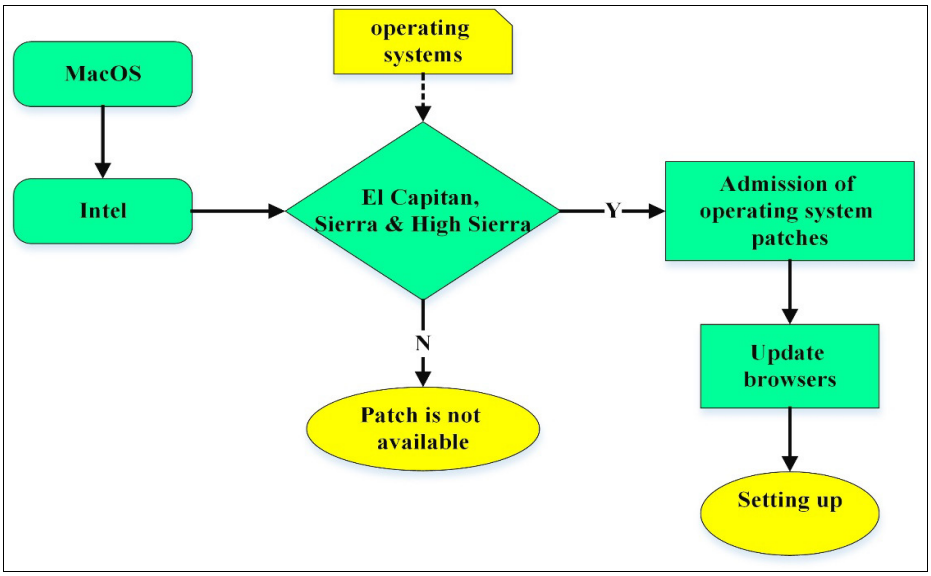


Figure 4. The structure of resisting meltdown and spectre holes on MacOS operating system [17]

Security Software are necessary and crucially important for the server operating systems especially services such as emails and/or file saving servers. Unlike Client operating systems, in server operating systems in case servers get virused given the fact that many users receive their services through them, all connected systems will be polluted [17]. In Table (4) patches required to deal with spectre and meltdown are indicated for every operating system [18].

Table 4: patches required for every operating system to deal with spectre and meltdown are indicated [18]

| OS | Version | spectre | spectre | meltdown |
|---|---|---|---|---|
| | | CVE-2017-5753 | CVE-2017-5715 | CVE-2017-5754 |
| windows | Server 2008 | NOT AVAILABLE | NOT AVAILABLE | NOT AVAILABLE |
| | Server 2008 R2 | DONE | DONE | DONE |
| | Server 2012 | NOT AVAILABLE | NOT AVAILABLE | NOT AVAILABLE |
| | Server 2012 R2 | DONE | DONE | DONE |
| | Server 2016 | DONE | DONE | DONE |
| VMware | vSphere 4.0/4.1/5.0/5.1 | NOT AVAILABLE | NOT AVAILABLE | NOT AVAILABLE |
| | vSphere 5.5 | WAIT | DONE | WAIT |
| | vSphere 6.0/6.5 | DONE | DONE | DONE |
| | Debian Wheezy | WAIT | WAIT | DONE |
| | Debian Jessie | WAIT | WAIT | DONE |
| | Debian Stretch | WAIT | WAIT | DONE |
| | Debian Buster | WAIT | WAIT | DONE |
| | Debian Sid | WAIT | WAIT | DONE |
| | Red Hat Enterprise Linux 7 | WAIT | WAIT | DONE |

| | | | | |
|---|---|---|---|---|
| Linux | Red Hat Enterprise Linux 6 | WAIT | WAIT | DONE |
| | Red Hat Enterprise Linux 5 | WAIT | WAIT | WAIT |
| | Red Hat Enterprise Linux OpenStack Platform 7.0 (Kilo) for RHEL 7 | WAIT | WAIT | WAIT |
| | Red Hat Enterprise Linux OpenStack Platform 6.0 (Juno) for RHEL 7 | WAIT | WAIT | WAIT |
| | Red Hat OpenStack Platform v 8/9/10/11/12 | WAIT | WAIT | WAIT |
| | CentOS 6 | DONE | WAIT | DONE |
| | CentOS 7 | DONE | WAIT | DONE |
| | Fedora 26 | WAIT | WAIT | DONE |
| | Fedora 27 | WAIT | WAIT | DONE |
| | SUSE OpenStack Cloud 6 | WAIT | WAIT | DONE |
| | SUSE Linux Enterprise Server 11 SP3-LTSS | WAIT | WAIT | DONE |
| | SUSE Linux Enterprise Server 11 SP4 | DONE | DONE | DONE |
| | SUSE Container as a Service Platform ALL | DONE | DONE | DONE |
| | Gentoo | WAIT | WAIT | WAIT |
| | Slackware 14 | WAIT | WAIT | DONE |
| | CloudLinux 6 | DONE | DONE | DONE |
| | CloudLinux 7 | DONE | DONE | DONE |
| | Ubuntu | DONE | DONE | DONE |
| | OpenSuse Linux based upon SUSE 12/11 | WAIT | WAIT | DONE |
| | Archlinux | WAIT | WAIT | DONE |
| | OpenVZ | DONE | DONE | DONE |
| | Proxmox 3.x | WAIT | WAIT | WAIT |
| | Proxmox 4.X | DONE | DONE | DONE |
| | Proxmox 5.X | DONE | DONE | DONE |
| | CoreOS Container Linux (channels Stable/Beta/Alpha) | WAIT | DONE | DONE |
| Solaris | SmartOS | WAIT | WAIT | WAIT |
| BSD | DragonFlyBSD | WAIT | WAIT | DONE |
| | FreeBSD | WAIT | WAIT | WAIT |
| | OpenBSD | WAIT | WAIT | WAIT |
| | NetBSD | WAIT | WAIT | WAIT |

## 3. CONCLUSIONS

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. Meltdown and spectre holes were investigated in this paper and the weak points of the systems were compared. It was also shown that each operating system should use a set of patches to prevent the penetration and carry out repairs.

## REFERENCES


[1] No authors available, Spectre and Meltdown processor flaws threaten billions of computers and mobile devices, Computer Fraud & Security, Elsevier Ltd, Vol. 2018, Issue 1, pp. 1-3, Jan 2018.

[2] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, M. Hamburg, Meltdown, Computer Science, Cryptography and Security, 3 Jan 2018.

[3] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, Y. Yarom, Spectre Attacks: Exploiting Speculative Execution, Computer Science, Cryptography and Security, 3 Jan 2018.

[4] https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability), [last visit: March-31-2018]

[5] https://blog.barkly.com/meltdown-spectre-bugs-explained, [last visit March-31-2018]

[6] https://hackernoon.com/spectre-meltdown-processor-vulnerabilities-a-technical-introduction-e3d09d6699a6, [last visit March-31-2018]

[7] http://www.brendangregg.com/blog/2018-02-09/kpti-kaiser-meltdown-performance.html, [last visit March-31-2018]

[8] https://devopsideas.com/steps-to-identify-and-address-meltdown-and-spectre-vulnerability-in-linux/, [last visit March-31-2018]

[9] https://medium.com/@mattklein123/meltdown-spectre-explained-6bc8634cc0c2, [last visit March-31-2018]

[10] https://aws.amazon.com/security/security-bulletins/AWS-2018-013/, [last visit March-31-2018]

[11] https://www.americanbanker.com/news/fears-mount-about-meltdown-spectre-threats-to-cloud-computing, [last visit March-31-2018]

[12] https://www.cloudwards.net/spectre-meltdown-and-the-cloud/, [last visit March-31-2018]

[13] Q. Liu, W. Cai, J. Shen, Z. Fu, X. Liu, N. Linge, A speculative execution strategy based on node classification and hierarchy index mechanism for heterogeneous Hadoop systems,19th International Conference on Advanced Communication Technology (ICACT), pp. 889-894, 2017.

[14] M. Jimenez, M. Papadakis, Y. Le Traon, An Empirical Analysis of Vulnerabilities in OpenSSL and the Linux Kernel, 23rd Asia-Pacific Software Engineering Conference (APSEC), IEEE, pp. 105-112, 2016.

[15] J. Kim, J.H. Lee, A methodology for finding source-level vulnerabilities of the Linux kernel variables, IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence), pp. 3717-3722, 2008.

[16] https://www.nextplatform.com/2018/01/18/datacenters-brace-spectre-meltdown-impact/, [last visit March-31-2018]

[17] https://wiki.epfl.ch/secure-it/meltdown-spectre-en, [last visit March-31-2018]

[18] https://docs.ovh.com/fr/dedicated/meltdown-spectre-kernel-update-per-operating-system/