An Analysis on Effects after Mitigating Meltdown and Spectre Vulnerabilities

By

Partha Sarothi Deb
(142-35-709)

A thesis submitted in partial fulfillment of the requirement for the degree of

Bachelor of Science in Software Engineering

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Fall – 2018

APPROVAL

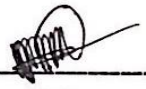
This **Thesis** titled "**An Analysis on Effects after Mitigating Meltdown and Spectre Vulnerabilities**", submitted by **Partha Sarothi Deb**, **ID: 142-35-709** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc in Software Engineering and approved as to its style and contents.

BOARD OF EXAMINERS

Prof. Dr. Touhid Bhuiyan — **Chairman**
Professor and Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

K. M. Imtiaz-Ud-Din — **Internal Examiner 1**
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Asif Khan Shakir — **Internal Examiner 2**
Lecturer
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



Dr. Md. Nasim Akhtar — **External Examiner**
Professor
Department of Computer Science and Engineering
Faculty of Electrical and Electronic Engineering
Dhaka University of Engineering & Technology, Gazipur

DECLEARATION

We hereby declare that we have taken this thesis under the supervision of **Afsana Begum, Senior Lecturer, Department of Software Engineering, Daffodil International University.** We also declare that neither this thesis nor any part of this has been submitted elsewhere for award of any degree.

26.12.18

Partha Sarothi Deb
ID: 142-35-709
Batch : 14th
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Certified by:

26/12/2018

Afsana Begum
Senior Lecturer
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Acknowledgement

I would like to thank a lot of people whose help was very precious to this research. However first of all I am grateful to the God for the good health and wellbeing that were necessary to complete this research.

I wish to express my sincere thanks to my supervisor **Mrs. Afsana Begum, Lecturer, Department of Software Engineering** for her tireless guidance to complete the research and also for providing me with all the necessary facilities for the research. I would also like to thank **Dr. Touhid Bhuiyan**, **Professor and Head of the Department of Software Engineering** for his immeasurable inspiration to conduct this research. Again I would like thank **Mr. Asif Khan Shakir**, **lecturer**, **Department of Software Engineering** and **Md. Maruf Hassan**, **Assistant Professor**, **Department of Software Engineering** for reviewing my research paper and giving proper instruction to make it perfect. At last I will also thank Mr. Delwar Alam for sharing his precious knowledge during the period of the research.

Finally I would like to thank my parents for their never-ending encouragement, support and attention.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

ABSTRACT

Background

Meltdown and Spectre are two of the most dangerous vulnerabilities that are discovered by the researchers of google from "Google zero project". These vulnerabilities are hardware based processor vulnerability. Sensitive information's like username, password, email and many other necessary data can be disclosed by the proper execution of side channel attacks. As these vulnerabilities are mainly hardware based processors vulnerability, its proper mitigations are only possible if hardware architecture modifications are performed. However, patching the system is the only solution. Although respective vendors has already released patches to mitigate the effects, that resulting continuously slowing down the system and reducing the performance.

Research Gap

As previous researches are done on this kind of performance measurement on super computer but not for personal computer, so we decided to conduct this.

Objective

The main objective of this research is to analyze the effects of the patches on different processor and determine which types of processor are facing which kind of performance issues.

Methodology

For the sake of performing the research and determine the effect on the performance of processor we will choose processors of different vendors and test and calculate the performance before and after installing the patches. Than we will compare several processors performance and determine which processors are more affected.

Result

In this research we have selected two Intel's core i5 processors of 7^{th} and 6^{th} generation. We tested their performance before and after installing the patches. We will calculate and compare the results and show it.

Audience

The targeted audience of the research are the people who has no or a little idea about the Meltdown and Spectre vulnerability and great interest about this vulnerability. This research will also help those people who are interested to learn how performance measurement are done on processor.

Conclusion

In this research our main focus is to show the performance analysis before and after the patches on different processor

Keywords: Meltdown, Spectre, Side-Channel Attack, Patching, Performance Analysis, Phoronix Test Suite tool.

Chapter 1

INTRODUCTION

1.1 Background

Meltdown and Spectre the fiercest vulnerabilities of current period is discovered at June 2017 by the researchers of Google Zero Project (Lipp, 2018) (Kocher, 2018). However at that time the findings were only shared with several vendors like Intel, AMD, and Microsoft under a non-disclosure terms and provided them time to create the fixes and patches. Later on 3rd January 2018 the details of these vulnerabilities are disclosed publically (Lipp, 2018) ("Reading privileged memory with a side-channel", 2018). All though there are no news of mass exploitation however it remains a topic of concern because processors of different vendors like Intel, AMD, and ARM are affected by this vulnerabilities (Tabe, 2018). Researchers revealed that all though other chip vendors are also affected to some extent however Intel's processors are mostly vulnerable due to some performance optimization technique they used in their chips since 1995 ("Protect your Windows devices ", 2018) [8]. As if Meltdown and Spectre are two of the vulnerabilities which occurs due to the processors architectural design flaw so, it can be said that they are going to stay here for a while(Larrea, 2018)(Lipp, 2018).

Meltdown and Spectre triggered due to some performance optimization features. Those features are Out-of-order Execution, Speculative Execution, and use of cache memory ("Meltdown and Spectre, explained", 2018) ("Meltdown, Spectre, and the State of Technology", 2018) ("Spectre and Meltdown explained: what they are, how they work, what's at risk", 2018). All of these features are used to increase the performance of a PC or a server. However all this features can be exploited too. According to the researchers of google project zero till now there are three main variants of meltdown and spectre. Those variants are Bound check Bypass (Common Vulnerabilities and Exposure-2017-5754), Branch Target Injection (CVE-2017-5715) and Rouge Data Cache Load (CVE-2017-5754). First two variants are combinedly called Spectre and the last variant is called Meltdown ("Reading privileged memory with a side-channel", 2018) (Lipp, 2018) (Kocher, 2018). All these variants can be exploited by "**Reading privileged memory with Side Channel**". Later this year more variant has made their entrance to complicate the situation. **MeltdownPrime** and **SpectrePrime** are two of the latest variants of this vulnerability (Trippel, 2018).

The effect of Meltdown and Spectre are widespread. Personal computing as well as cloud computing both are vastly affected by this. Businesses can be affected too. Mostly large businesses like banks or other organizations can become the victim of this vulnerability besides patching can reduce the performance therefore it can put a huge impact on businesses ("The impact of Meltdown and Spectre on your business", 2018). Small data centers can't afford to hire professionals to create patches because it will cost them a lot. Rather than creating patches they will depend on big cloud based companies services because they have enough manpower to handle this situation ("11 Potential effects of Meltdown and Spectre on Tech industry", 2018). Most of the big companies already patched their device however patching isn't always the solution. Patch can obviously mitigate the danger however the

security hole is always there ("11 Potential effects of Meltdown and Spectre on Tech industry", 2018). IOT devices can also be affected by these vulnerabilities. Another thing that we have to notice that these vulnerabilities are hardware based not software based. Patching or updating OS or Firmware can be a good option for mitigation however this problem can't be fixed from the root. To solve the problem from the root modification of working logics in the processors are need to be changed as soon as possible ("Meltdown and Spectre: Understanding the Performance Impact", 2018).

It was expected that all this patches will mitigate the problem. However after installing both firmware and operating system patches it appeared that it is slowing down the system gradually as well as creating a frequent reboot issue ("Belay that order: Intel says you should NOT install its Meltdown firmware fixes", 2018) ("Meltdown and Spectre Patches May Increase CPU Load ", 2018)("Intel Security Issue Update: Initial Performance Data Results for Client Systems", 2018). Besides there were a lot of compatibility issues too. Windows users generally use a lot of third party antiviruses. Those third party antiviruses make unsupported system calls to windows kernel which causes "Stop Errors" and "blue screen of death" ("Important: Windows security updates and antivirus software", 2018). This is why Intel made an announcement through blog post and requested all the recipient not to install those initial patches ("Belay that order: Intel says you should NOT install its Meltdown firmware fixes", 2018). Initially it was assumed that performance reduction will be up to 30% however after a few improved patches the performance decrease rate is now within the single digits ("Meltdown and Spectre Patches May Increase CPU Load ", 2018) ("Intel Security Issue Update: Initial Performance Data Results for Client Systems", 2018). This patches also created great impact on the servers and cloud storages too. According to Redhat Servers are getting slow according to their workloads and the percentages varies from 1% to 19% ("How the Meltdown and Spectre security holes fixes will affect you", 2018) ("Speculative Execution Exploit Performance Impacts ", 2018). Mostly the patches doesn't slow the systems with newer CPUs. Nevertheless CPUs which are produced more than 5 years ago are taking the heats. Besides the performance reduction not only depends on patch updates, it also depends on the configuration and workload of the systems.

1.2 Side Channel Attack Variants

Several performance increasing features are the main reason behind all this Meltdown and Spectre vulnerabilities. Meltdown and Spectre vulnerabilities are exploited by using side channel attacks. There are a lot of variants of CPU vulnerabilities which is exploited by side channel attacks. Those variants are stated below.

Table 1.1: List of the variants of meltdown and spectre which is exploited by using several side channel attacks

Variant no.	Name of the Variants	Date of Disclosure	Disclosed by
1.	Spectre (CVE-2017-5753) Bound Check Bypass	3rd January, 2018	Google Project Zero
2.	Spectre (CVE-2017-5715) Branch Target Injection	3rd January, 2018	Google Project Zero
3.	Meltdown (CVE-2017-5754) Rouge Data Cache Load	3rd January, 2018	Google Project Zero
3A.	Meltdown (CVE-2018-3640) Rouge System Register Read	21st May, 2018	***Ken Johnson***(Microsoft Security Research Center & ***Jan Horn(***Google Project Zero)
4.	Spectre (CVE-2018-3639) Speculative Store Bypass	21st May, 2018	***Ken Johnson***(Microsoft Security Research Center & ***Jan Horn(***Google Project Zero)
5.	L1 Terminal fault/ Foreshadow attack		
5A.	L1 Terminal fault – SGX (CVE-2018-3615)	14th August, 2018	***Jon Van Bluck***, ***Frank Piessens***, ***Raoul Strackx*** (imec-DistriNet, KU Leuven)
5B	L1 Terminal fault – OS, SMM (CVE-2018-3620)	14th August, 2018	Same
5C	L1 Terminal Fault – VMM (CVE-2018-3646)	14th August, 2018	Same

1.3 Effects of Meltdown and Spectre

The effects of Meltdown and Spectre are widespread. Devices like Laptop, desktop, servers and mobiles are all affected by these vulnerabilities. All the effects of these vulnerabilities are listed below.

1. **Cost Increase**
   After applying a patch or mitigation the overall cost becomes increases for user due to additional expenditure ("11 Potential effects of Meltdown and Spectre on Tech industry", 2018).

2. **Slower device**
   According to **Naresh Soni** ("11 Potential effects of Meltdown and Spectre on Tech industry", 2018) (CTO of Tsunami AR/VR, Sierrabolics, AI Software Company) said that after the breakout of meltdown and spectre vulnerabilities giant vendors like Microsoft, Google, Intel, and Firefox released firmware, operating system and browser patches respectively. Those patches are responsible for slow performance of the devices.

3. **Future exploitation of unpatched hardware**
   Vik Patel (Board of Directors Center of Excellence, Nexcess, and Forbes Technology Council) noticed that vendors like Intel aren't providing patches to the older generation of processors. However during the **WannaCry** ransomware situation they provided patches for those old hardware's too. Now it seems that older generation hardware's are the most vulnerable ones. Beside there are lots of organizations who still uses those hardware's. Therefore, it is quite possible that in future those old unpatched hardware's will be targeted by the hackers. ("11 Potential effects of Meltdown and Spectre on Tech industry. ", 2018)

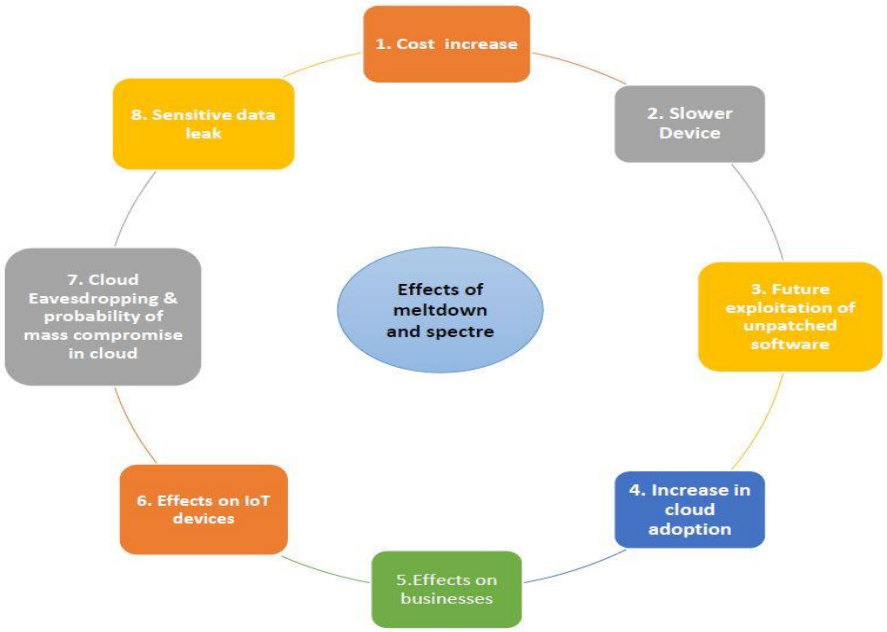


Figure 1.1: Effects of meltdowns and spectre.

4. **Increase in cloud adoption**
   According to **Rich Campagna** (CMO at Bitglass, Inc.), Small businesses and data centers will be affected by this vulnerability too however they can't afford to hire security expert to create patches to mitigate the effect of the vulnerabilities. Hence, they will have to shift to giant vendors services like AWS (Amazon Web Service) because they are capable enough to hire security personnel to create and distribute patches.

5. **Effects on Business**
   According to reference no ("The impact of Meltdown and Spectre on your business", 2018) we found that these vulnerabilities can put an impact in stealing sensitive data from business organizations tech infrastructure.

6. **Effects on IoT**
   According to reference no ("Implications of Meltdown and Spectre for IoT", 2018) most of the IoT devices and infrastructures uses several chips and sensors to acquire data and process them.

7. **Cloud eavesdropping and probability of mass compromise in cloud**
   According to reference ("The Effects of the Spectre and Meltdown Vulnerabilities - Schneier on Security", 2018) we found that several companies use same server space to store their sensitive information. It is quite possible for an attacker to rent a space for his own application and exploit those vulnerabilities by tricking the processor of that particular.

8. **Sensitive data leake**
   According to reference ("The Effects of the Spectre and Meltdown Vulnerabilities - Schneier on Security", 2018) we found that Sensitive data of the processor can be leaked through the exploitation of these vulnerabilities.

1.4 Mitigation Strategy

Meltdown and Spectre is one of the most perilous vulnerabilities that has exaggerated the tech world in a great extent. Preventing system or infrastructures from these vulnerabilities are tough but it is quite possible to mitigate the effects. Here are some steps that can be taken to mitigate the effects of Meltdown and Spectre.

1. **Creating a detailed inventory**
   According to Gartner researchers "nearly every single devices like computer, smartphone, network and storage appliances are affected to meltdown and spectre vulnerabilities ("5 Ways to Prevent a Spectre or Meltdown Attack", 2018). Therefore to mitigate this it will take cautious and phased remediation plan. First step could be creating a detailed inventory of affected systems. "

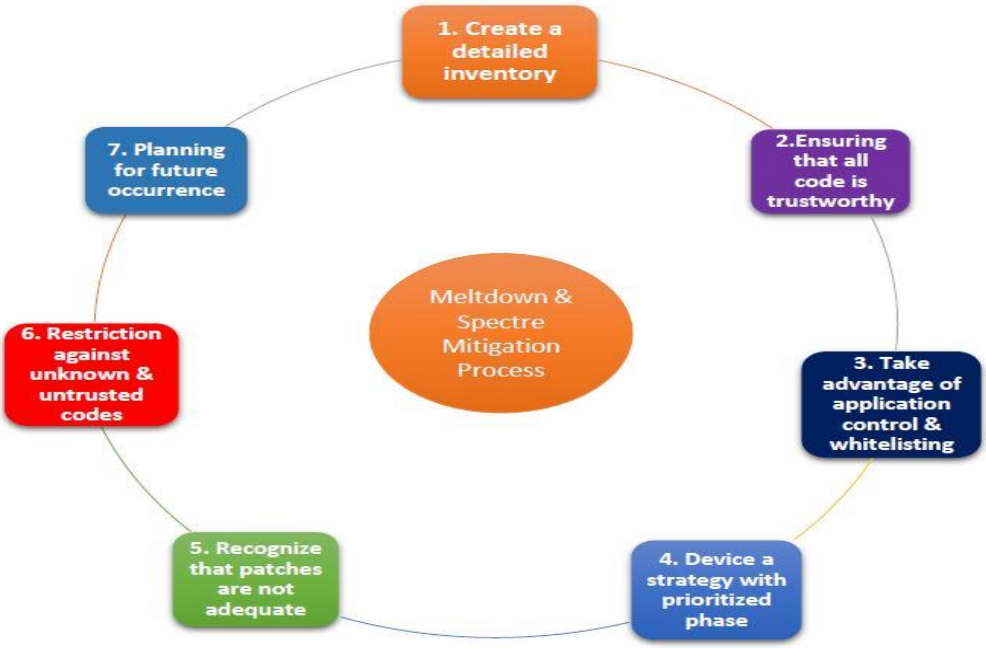


Figure 1.2: Mitigation process of Meltdown & Spectre vulnerability.

2. **Ensuring that all codes are trustworthy**
   According to Gartner Research "Modern operating system and hypervisors depend in structured, layered permission model to deliver isolation and separation" ("6 steps firms can take to mitigate Spectre and Meltdown risks", 2018).The exploitable design is under the os, therefore all this software layers above are vulnerable. Successful attack may results in reading the systems memory, altering it isn't possible. Successful exploits requires to execute untrusted code on the system. Therefore, every kind of untrusted code should be prohibited to run on the system. ("6 steps firms can take to mitigate Spectre and Meltdown risks", 2018)

3. **Take advantage of application control and whitelisting**
   According to Gartner researchers "the vulnerabilities are not remotely exploitable" ("6 steps firms can take to mitigate Spectre and Meltdown risks", 2018). They also explained that "A successful attack requires the attacker to execute code on the system. As such application white control and whitelisting on all systems greatly reduce the risk of unknown code execution. However, share infrastructure as a service (IaaS) infrastructure is particularly vulnerable until the cloud provider update their underlying firmware and hypervisor layer. Strong separation of duties (SOD) and privileged account management (PAM) reduce the risk of the introduction of untrusted code ("6 steps firms can take to mitigate Spectre and Meltdown risks", 2018)."

4. **Device a Strategy with prioritized phase**
   To mitigate the effects of meltdown and spectre it is now quite necessary to develop a remediation strategy. Several vendors are releasing remedies for their customers. In order

to develop a remediation plan Gartner researchers recommends a prioritized phase wise plan. Most vulnerable system should be given the priority in the case of applying the remediation plan. [40, 42].

5. **Recognizing that patches are not always adequate**
   Till now we all know the effects of Meltdown and Spectre vulnerabilities. Several giant vendors developed various patches to mitigate vulnerabilities. However patches are slowing down the systems. Therefore it is a burning question whether to patch or not to patch the system. Gartner researchers suggested that industry leaders should not opt to patch the personal and organizational systems unless those patches are stable. [40, 41, 42]."

6. **Restriction against unknown and untrusted codes**
   Gartner researchers suggested that "system that are unpatched or partially patched, several mitigation policies can be taken to reduce risks. The single most important measure is to restrict putting unknown and untrusted code on the system. The attack requires local code execution that it is a default deny approach. Besides Application control and whitelisting as well as traditional end point protection platform and network based intrusion detection systems also mitigate the risks."("Gartner Provides Seven Steps for Security Leaders ", 2018)("6 steps firms can take to mitigate Spectre and Meltdown risks", 2018)

7. **Planning for the future occurrence**
   Gartner researcher said that "complete elimination of the exploitable implementation requires new type of improved hardware's which won't be available within the next 12 to 24 months. This is why the inventory of systems will serve as a critical roadmap for future mitigation efforts. To lessen the risk of future attacks of all types of vulnerabilities use of application control and whitelisting on server should be increased. Besides researches on the design flaws to discover new variants as well as additional patches for OS, Firmware and Browser should be done.("5 Ways to Prevent a Spectre or Meltdown Attack", 2018)("6 steps firms can take to mitigate Spectre and Meltdown risks", 2018)

1.5 Patching

To eradicate the effect of meltdown and spectre giant vendors provided the customers with several patches. Patches that will mitigate meltdown and the two existing variants of spectre. Proper patching is another factor here.

a) Proper Patching Method

To secure the system or an infrastructure a person should have to know how to patch or update them properly. Proper update includes 1) Updating the operating system 2) Updating the browser and 3) Updating the Bios/Firmware. Each of them are described

below ("A Clear Guide to Meltdown and Spectre Patches", 2018), ("Mitigating Meltdown and Spectre", 2018), ("Protect your Windows devices ", 2018), ("Meltdown and Spectre Vulnerabilities", 2018), ("Mitigating Meltdown and Spectre – Linux", 2018), ("How to protect your PC from the Meltdown and Spectre CPU flaws", 2018)

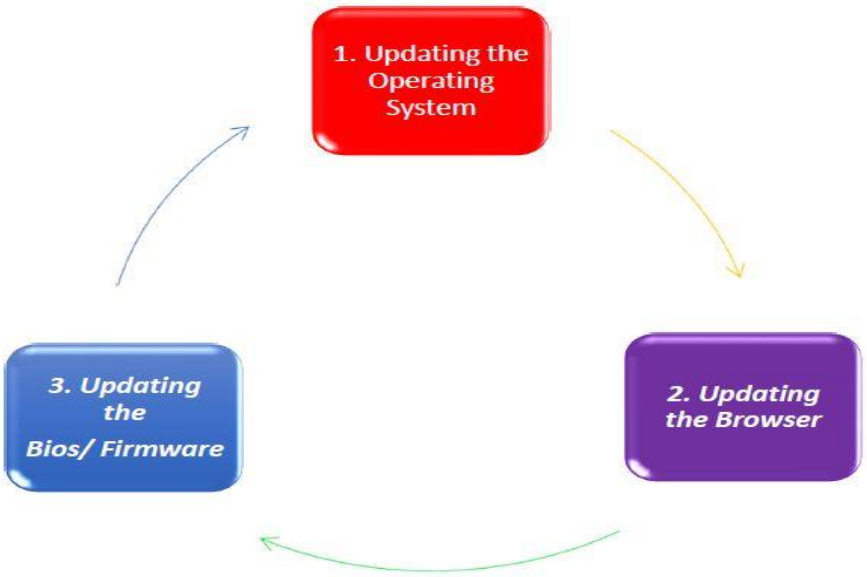


Figure 1.3: The proper patching method to mitigate the effects of Meltdown and Spectre.

1.6 Motivation of the research

Meltdown and Spectre vulnerabilities came to light through a blog post of google project zero team. Thereafter searched a lot about those vulnerabilities on google and found the proof of concept papers (Lipp, 2018) (Kocher, 2018). There were shortage of resources. Besides that it's being said that the performance of the processors are being reduced due to patch installation. Several independent developers were testing those patches and analyzing the consequences. However at that period those results weren't trustworthy because of unstable patches released by the respective vendors. Currently when all the patches are all most stable, testing the performance of the processors of various kinds seems to be a good idea.

1.7 Problem Statement

Meltdown and specter are hardware based processor vulnerabilities capable of leaking data from processors (Lipp, 2018). The vulnerability which was discovered earlier in 2018 has a far reaching effects (Prout, 2018). In the earlier stage, there were a very few resources available that could helped people to know about this vulnerability. Besides that in the later part of the year respective vendors had released patches to mitigate the effects of those vulnerabilities and those patches had their effects too. Those patches were making the systems slow ("Meltdown and Spectre: Understanding the Performance Impact", 2018)(Prout, 2018). Therefore it could have been a great initiative to collect all the necessary

information that can help people to know more about this vulnerability and prepare themselves to face it. Also analyzing the effect of patches on the performance of a system will help people to decide whether they should patch the system sacrifice the performance or remain unpatched.

1.8 Research Question

Based on the problem statement mentioned before, the following question are constructed:

- What kind of performance we get from a processor during pre-patch and post patch situation?
- Which kind of processors are facing most performance reduction after patch installation?

1.9 Research Objective

- To find out available information about the Meltdown and Spectre vulnerability and organize them.
- To find out different types of processors and measuring their performance during pre-patch and post-patch state.
- To find out and compare the performance of different types of processors during the pre-patch and post-patch state and determine which types or which generations processor are having which kind of impact on their performance after the installation of Meltdown and Spectre patches.

1.10 Research Scope

This research is conducted to determine the effects of Meltdown and Spectre patches on several types of processor. All though in recent time a lot of research is done in this area but most of the researches are conducted to mitigate the effects of meltdown and spectre or to find a new architecture for a processor which will disable or modify the way how speculative execution works. There were also a few researches on measuring the performance reduction of a system on pre-patch and post-patch phase but most of those researches are performed on Super Computers. There are a little or almost no researches were conducted to measure the performance reduction on personal computers.

As a parameter for measuring the performance researchers used **Network Connection Establishment**, **Disk access** and **Computation of intensive codes** on the system. However in our research we designed the environment in our own way. We selected Ubuntu 16.04 LTS version as our os of the system which is vulnerable to Meltdown and Spectre. As the processors of the system we used two of Intel's processors. We considered disk read-write speed, main memory's processing speed, Processors performance on performing intensive tasks and dedicated graphics cards performance as a parameter of measuring the performance of the processors.

1.11 Area of Contribution

In this research our main contribution is to measure and analyze the performance reduction of the processors on personal computers which is triggered due to the installation of Meltdown and Spectre patches.

1.12 Thesis Organization

The thesis organization of our paper is: In Chapter-I we discussed about the background of Meltdown and Spectre vulnerability, existing variants of this vulnerability, their effects, mitigation strategy and patching method. In chapter-II we discussed about the recent researches on Meltdown and Spectre and their drawbacks. We discussed about the methodology that we had followed throughout the research to determine the impact of installing patches on different systems in Section III. We collected the result that we had got from Chapter-III and analyzed in Chapter- IV and finally the conclusion in Chapter-V.

Chapter 2

LITERATURE REVIEW

Meltdown and Spectre are the most dangerous vulnerabilities that the IT world is facing currently. Those vulnerabilities are not remotely exploitable, to exploit those vulnerabilities one should have to apply malicious code into the system manually. There are reports of the rapid released patches by several vendors and the effect of this patches. In this paper we intend to represent the current situation regarding those vulnerabilities and also test the performance decrease of particular systems due to the installation of the released patches.

2.1 Previous Researches

Meltdown (Common Vulnerability and Exposure-2017-5754) is a recent vulnerability which is discovered by the researcher of google zero project (Lipp, 2018). This vulnerability mainly melts the boundaries between the kernel space and the user space is a system ("Spectre and Meltdown explained: what they are, how they work, what's at risk", 2018). It happens due to the faulty structure of processors. Vendors like Intel, AMD and ARM sometimes focuses on the performance of the chip speed which causes some vulnerability. One of them is "out of order execution" (Lipp, 2018) (Kocher, 2018). This feature helps to increase the processing speeds. In our computers there are several tasks that are scheduled properly. Generally Processors performs the task one by one ("Meltdown and Spectre, explained", 2018). To perform those task processors gather required resources from different register or cache memories. Sometime processors try to perform a task which is scheduled nevertheless can't perform it due to the unavailability of the resources (Lipp, 2018) ("Meltdown and Spectre, explained", 2018). Therefore the processor chose another task which has required resources at that time ("Meltdown, Spectre, and the State of Technology", 2018). This feature of the processor is called out-of-order execution. This feature is responsible for the exploitation of Meltdown vulnerability. This feature of the processor can be exploited by side channel cache attacks (Lipp, 2018).

Spectre is another vulnerability which is also discovered by the researcher of the Google Zero project (Kocher, 2018). It has two variants such as CVE-2017-5753(Bound check bypass) and CVE-2017-5715(Branch target injection) (Kocher, 2018) ("Meltdown and Spectre, explained", 2018) (CVE-2018-3639, 2018). Spectre is also a little bit similar to Meltdown nevertheless they aren't the same. Spectre occurs due to a chip feature "Speculative Execution" which is used by different CPU vendors like Intel, AMD and ARM etc. (Kocher, 2018) [9] . "Speculative Execution" are mainly used to increase the performance of the processor ("Reading privileged memory with a side-channel", 2018) ("Meltdown and Spectre, explained", 2018). Most of the modern day processors are good at multi-tasking. This sort of multi-tasking is possible due to speculative execution. This feature of the modern chips can be exploited by the side channel timing attacks (Lipp, 2018) (Kocher, 2018) (Khasawneh, 2018).

In recent time there were a lot of researches performed to mitigate the effects of Meltdown and Spectre vulnerabilities. Most of the researches were performed to find better alternate CPU architecture. There were few researches conducted on determining the performance reduction on the processors. In this section we would like to know more about the current significant researches that has been performed around the world and try to find their drawbacks.

a) SafeSpec: Banishing the Spectre of a Meltdown with Leakage-Free Speculation

Speculative Execution a performance enhancer feature of processors are mainly responsible for Meltdown and Spectre vulnerability (Khasawneh, 2018) (Lipp, 2018) (Kocher, 2018). An unprivileged user can read privileged data of a system by using side channel cache attacks. Khasawneh K. N., and his fellow researchers has proposed a new type of speculative execution **SafeSpec** which is immune to the side channel leakage necessary for attack such as Meltdown and Spectre.(Khasawneh, 2018) In particular, SafeSpec stores the side effects of speculation in separate structures while the instructions are speculative. The speculative is then either committed to the main CPU structures if the branch commits, or squashed if it does not. It makes all the direct side effects of speculative code invisible.

b) Rebooting Computers to Avoid Meltdown and Spectre

In a research conducted by Conte, T.M (Conte, 2018) proposed a model for processors working architecture. He suggested to use temporary registers instead of cache memory, which actually reboot the whole concept of computing.

c) oo7: Low-overhead Defense against Spectre Attacks via binary Analysis

To prevent micro architectural attacks like Meltdown and Spectre Wang G. (Wang, 2018) and fellow researchers proposed a binary analysis framework which is **oo7** to check and fix code snippets against potential vulnerability to Meltdown and Spectre attack. This proposed model **oo7** employs control flow extraction, taint analysis and address analysis to detect tainted conditional branches and their ability to impact memory accesses. (Wang, 2018)

d) Detecting Spectre Attacks by identifying Cache Side-Channel Attacks using Machine Learning

Recently discovered spectre vulnerabilities exploits the design flaws in the architecture of the processors and pose a threat to the systems security (Kocher, 2018) (Depoix, 2018). To fix this vulnerability major change in the processors architecture of current processors are essential.(Kocher, 2018) (Depoix,2018) In this research Depoix, J. and Altmeyer, P., are presenting a real time detection system, which recognizes Spectre attacks by detecting cache side channel attacks (Depoix,2018). They built the system on the data of previously conducted research in the field of cache side channel attack detection. They used neural network to analyze the data and recognize the patterns of the attack.

e) Processors performance measurement

Several researches had been conducted to measure the effect of Meltdown and Spectre Patches on the systems. However most of the time researches conducted their researches on different super computers to understand the patches effects. Prout, A. and fellow researchers conducted a research to understand the impact on several workload relevant to HPC systems (Prout, 2018).

The impacts were significant both synthetic and realistic workloads. They showed that the performance penalties are difficult to avoid (Prout, 2018). In another research Larrea, V.G.V and his fellow researchers (Larrea, 2018) measured the effect of Meltdown and Spectre patches on Cray supercomputers and supporting systems at Oak Ridge Leadership Computing Facility. In other research Watson, R.N.M and his fellow researcher had conducted similar type or research on another supercomputer which is Capability Hardware Enhanced RISC Instructions (CHERI) computer architecture (Watson, 2018).

2.2 Anticipated Area of Research

From the above mentioned researches it's obvious that there are lot of researches going on in this area. However most of the researches are mainly being conducted to find out a new CPU architecture or modifying the existing architectures. Also there are researches conducted on the exploitation of the new variants of the vulnerability. In later part we observed that there were some researches on performance measurement. Although these performance tests are done on supercomputer, we did not find out the result on personal computer. In this research we would like to conduct such kind of tests on the processors of personal computer.

Chapter 3

RESEARCH METHODOLOGY

In this chapter we would like to discuss about the methodology that we will follow to calculate the performance reduction of the various processors due to installing meltdown and spectre patches. To calculate the performance reduction, a few tools will be required. We will use those tools to stress the processor and measure their performance.

3.1 Working Procedure

The entire working procedure consists of various stages like creating the environment for testing, Executing the performance tests and collecting the result, patching the systems with latest OS and BIOS patches released by the respective vendors and again executing the performance tests to analyze the effects on the processors. The flow chart below will be used to explain the working procedure.

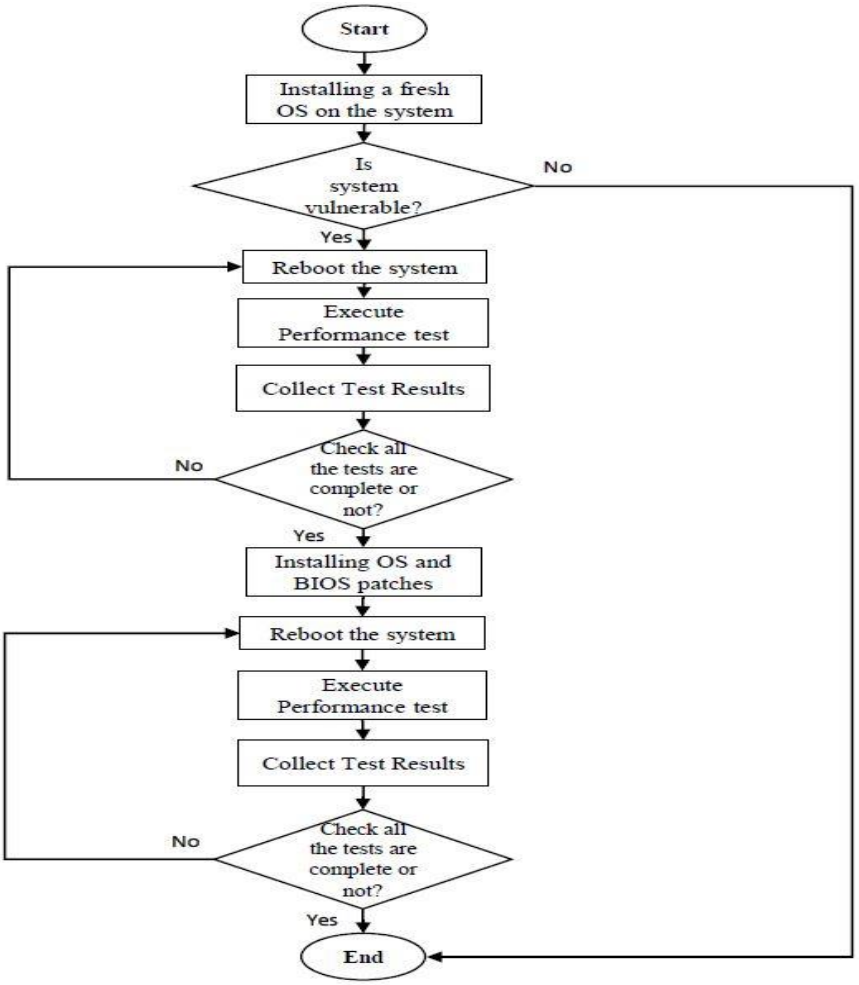


Figure 3.1: Complete procedure of executing performance tests to determine the impacts of Meltdown & Spectre on various processors.

3.1.1 Installing a fresh OS

To execute the performance test, first of all we will install a fresh operating system to our pc. In this the case we will use linux based operating system which is "Ubuntu 16.04 LTS." "Ubuntu 16.04 LTS" was released is April 21st , 2016 during the pre Meltdown era. It uses 4.4.0-31generic Kernel which by default vulnerable to Meltdown and Spectre vulnerability. However any operating system can be used to perform the tests.

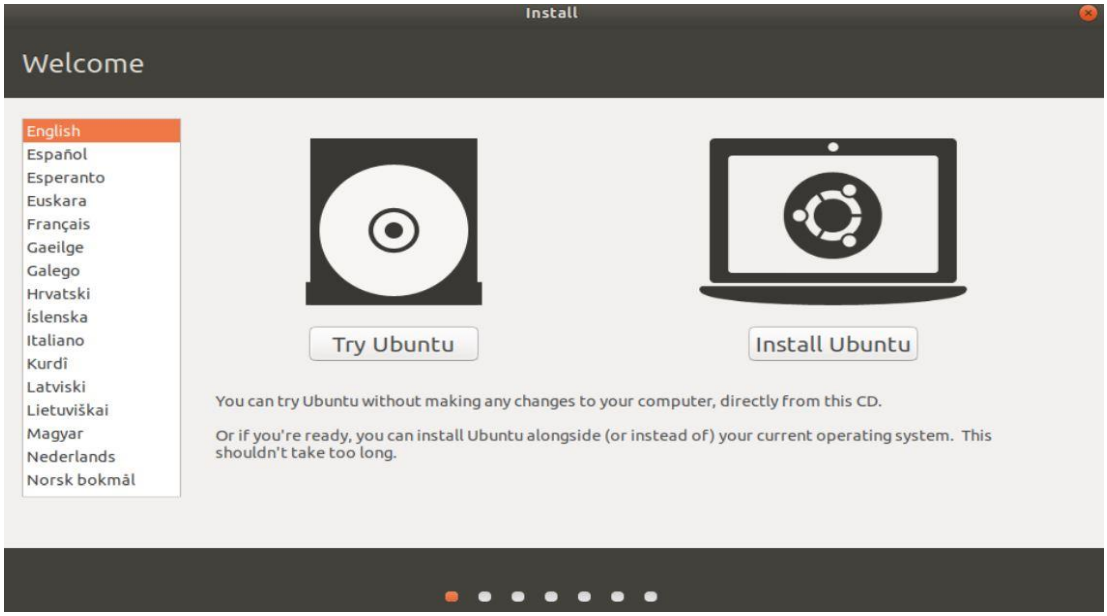


Figure 3.2: Installing of a fresh OS on the system.

3.1.2 Checking Whether the system is vulnerable or not

After installing the operating system we should have to check whether the system is vulnerable to "Meltdown and Spctre" vulnerability. To check whether the system is vulnerable or not we used a script "Spectre & Meltdown Checker" (Conte, 2018). After running the script on shell it produces a result which indicates that whether the system is vulnerable to how many variants of Meltdown and Spctre. It also represents that which defence mechanism or patches are installed in the system and which patches can be installed to mititgate the effects of Meltdown and Spectre on the system. If the result of the script is positive than we will proceed to the next step of the working procedure otherwise we will end the whole process.

Figure 3.3: Systems vulnerability status.

3.1.3 Rebooting the System

Before performing every single test we will always reboot the system. It will prevent annoying program from running on the system. We want those programs to run on this system which is appsulately necessary. Any annoying anonimous program running on the system can put a serious impact on the performance.

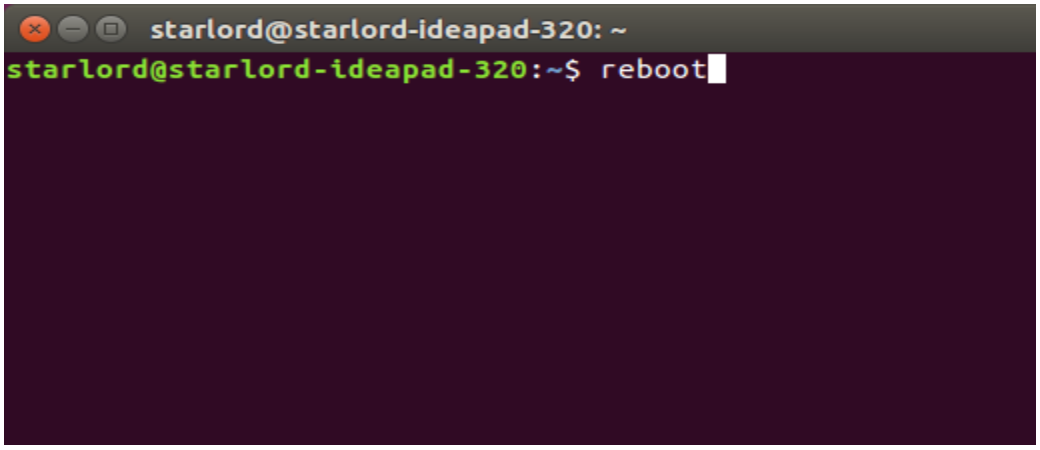


Figure 3.4: System reboot.

3.1.4 Execute Performance Test

To determine the impacts of the patches on a pre-patched system we have to run several tests on the system. Mainly we will run several tests to evaluate the performance of disk,RAM, processor and graphics of a particular system. In order to run those test we will be required performance measuruing tools. “Phoronix Test Suite” a free, open source software for linux operating system can be used for the purpose. This tool consist of

various types of tests to stress the processor and provide us visible result that we can use to compare between different hardwares.

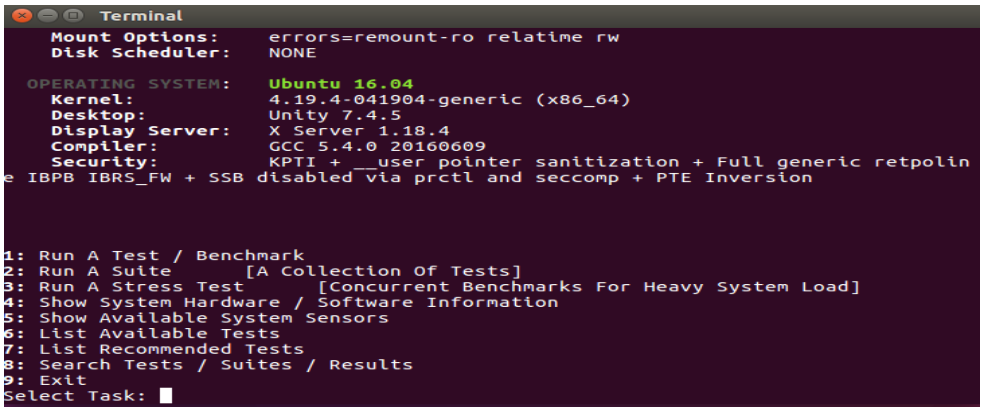


Figure 3.5: Phoronix Test Suite tool

We will perform six tests to stretch the processor. Those six test and what actually we will measure are explained bellow.

3.1.4.1 Disk Performance

To caulucate the disk performance we will use **IOzone** test.

a) IOzone Test

This **IOzone** benchmarking tests the hard disk drive/ file system performance. It calculates the disk reading and writing speed.

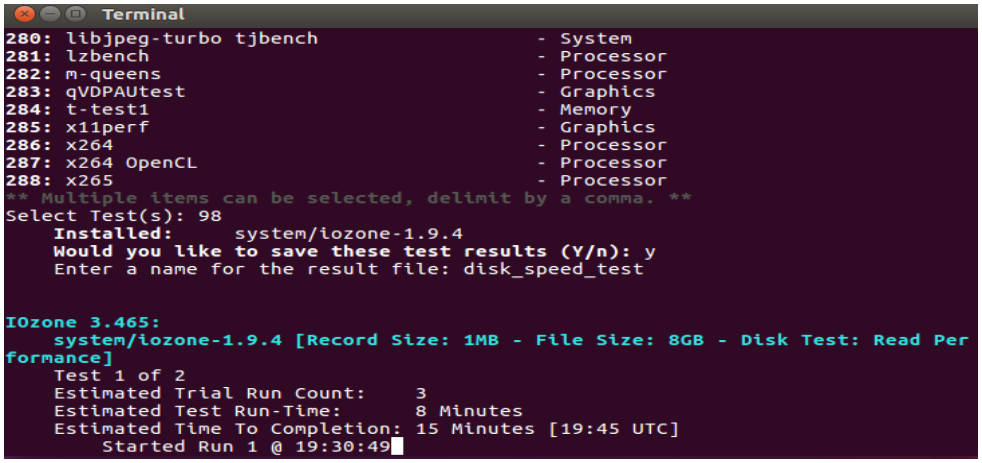


Figure 3.6: IOzone test for disk read/write speed calculation

3.1.4.2 RAM Performance

To determine main memory or RAM performance we will use **RAMspeed SMP** test**.**

a) RAMspeed SMP

RAMspedd SMP benchmark tests the system memory (RAM) performance. It tests the system memory in two stages. In stage one it calculates how fast system memory(RAM) can process integer data and in stage two it calculates how fast system memory(RAM) processes the floating point data.

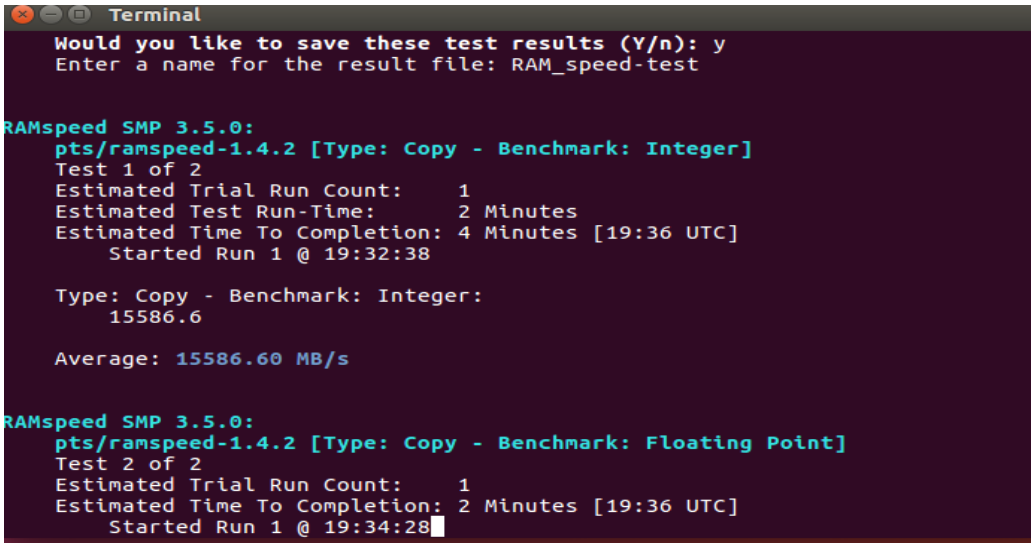


Figure 3.7: RAMspedd SMP test for measuring main memory performance.

3.1.4.3 Processors Performance

Determining the impact on performance of the processors are the most important part of this performance testing. Meltdown and Spectre are micro architectural attack. They affects the processor the most. To determine the performance of a the processor we will apply three tests. They are C-Ray test, Encryption test and Compression test. Description of those tests are stated below.

a) C-Ray test

This is a test of C-Ray, a simple raytracer designed to test the floating-point CPU performance. This test is multi-threaded (16 threads per core), will shoot 8 rays per pixel for anti-aliasing, and will generate a 1600 x 1200 image and calculate the time that is needed to generate the image.

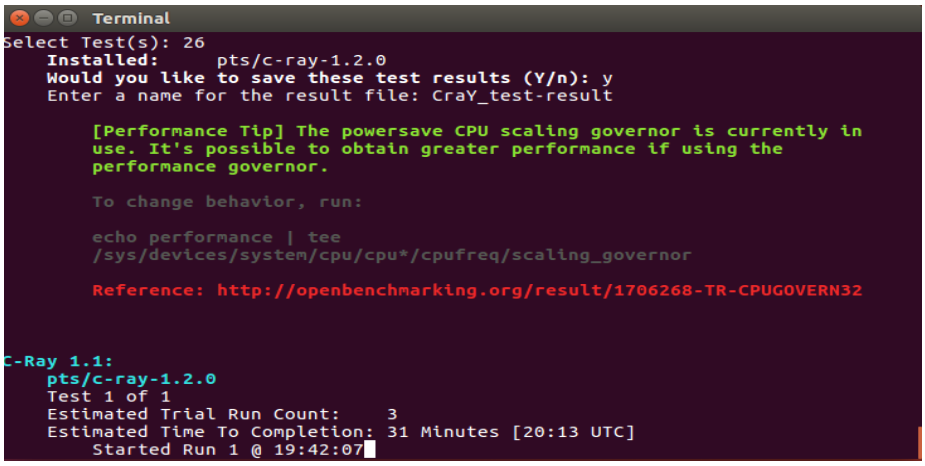


Figure 3.8: C-Ray test for processors performance clculation

b) Encryption test(GnuPG test)

GnuPG tests the amount of time it requires to encrypt a certain amount of file. In this case file is allmost 2GB.

Figure 3.9: GnuPG test for processors performance calculation.

c) Compression Test(Gzip Compression test)

Gzip Compression test actually calculate the time needed to compress two copies of linux kernel tree by using Gzip Compression.

Figure 3.10: Gzip Compression test for processors performance calculation.

3.1.4.4 Graphics Performance

To calculate the graphical performance we used Unigine Heaven test.

a) Unigene Heaven Tests

In Unigene Heaven test it calculates the average frame rates within the heaven demo in Unigene enigine. This test put high amount of stress on the processor. It is highly required to use a graphics card but in this test we are not using any extra graphics card. We are only using the integrated graphics card that comes with the processor by default.

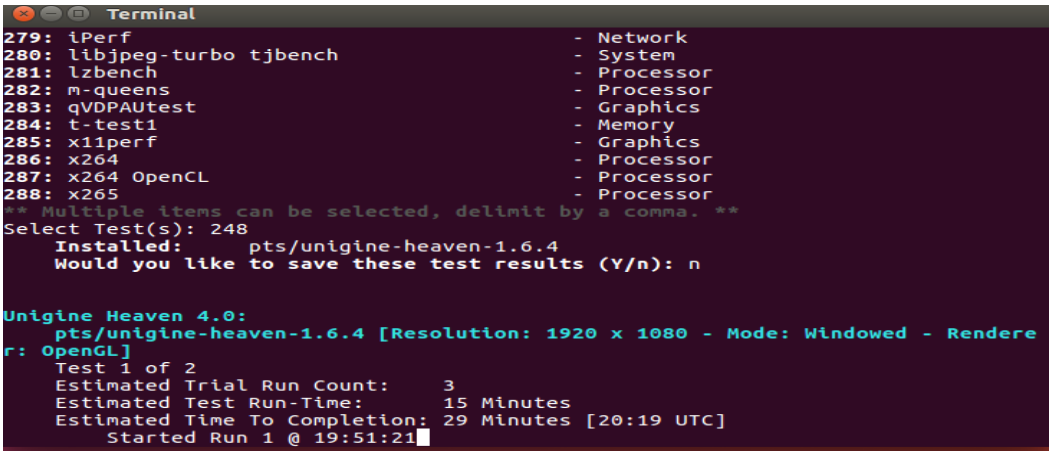


Figure 3.11: Unigene Heaven test for processors graphical performance calculation.

3.1.5 Collecting Test Results

After completing every single tests, we will collect the results. Collecteed results will be used for further tasks like comparing pre-patch and post-patch performance data.

3.1.6 Checking the completition of tests

In this step we have to make sure that all the required tests are finished or not? If the test are finished that we will proceed towards the next step. Otherwise we will perform the the remaining tests.

3.1.7 Installing OS and BIOS patches

So far we had performed tests on the vulnerable system and collected the results. Our main intention was to collect data from both pre-patched and post-patched stages of a particular processor. Now that we had already collected required pre-patched performance data, it's time to patch the system properly and than run some tests and collects post-patched data. To patch a properly we have to install bosth OS and BIOS patch.

First of all we will install the OS patches. In this case we will install the latest kernel version for our system. We installed latest 4.19.3 kernel which includes all the mitigation that is required to mitigate meltdown and spectre vulnerabilities.

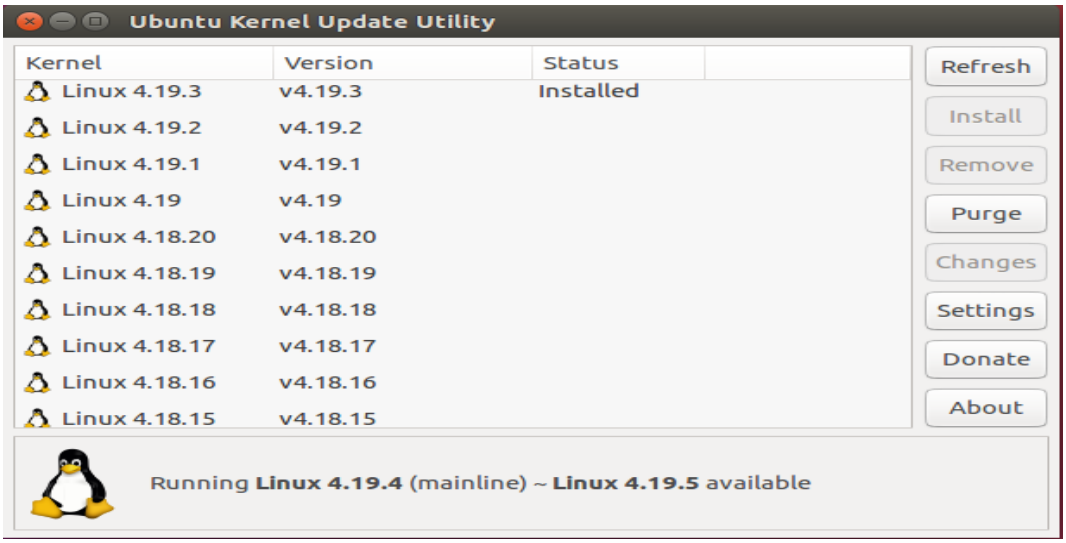


Figure 3.12: Updating to the latest kernel version.

And then we will download the required BIOS patches from appropriate vendors website and install the BIOS on the system.

3.1.8 Rebooting The System

After installing the patches, we reboot the system. In that case we have followed the same procedure as given in the article 3.1.3 .

3.1.9 Execute Performance Test

After rebooting the system we will start to execute the performance tests. We will perform several tests to calculate the performance of disk,system memory (RAM), processor and Graphics. In that case we have follooed the same procedure as given in the article 3.1.4 .

3.1.10 Collecting Test Results

After completing every single tests, we will collect the results. Collecteed results will be used for further tasks like comparing pre-patch and post-patch performance data.

3.1.11 Checking the completition of tests

In this stage we will again check that all the that we needed to perform to calculate the performance of a particular processor in post-patched situation is completed or not? If the tests are completed than we will proceed to the next step and end the task , otherwise we will execute the remaining tests.

Chapter 4

RESULT AND DISCUSSION

4.1 Existing attack variants, Existing Patches, their Problems and probable solution

Here we will discuss about all the variants of the meltdown and spectre and their existing solution and the problem of existing solutions.

Table 4.1: Existing variants of Meltdown and Spectre, existing solution of the vulnerabilities and Problem of existing solutions.

Name of the vulnerability	**Solution (OS patch+ Microcode patch+ Browser patch)**	**Problem with existing Solution**	**Probable Solution (future solution)**	**References**
Spectre (CVE-2017-5753) Bound Check Bypass	Yes	Performance reduction	1.New type of speculative execution method (SafeSpec) 2. Using temporary register instead of cache memory.	(Khasawneh , 2018) (Conte, 2018)
Spectre (CVE-2017-5715) Branch Target Injection	Yes	Performance reduction	Same	(Khasawneh , 2018) (Conte, 2018)
Meltdown (CVE-2017-5754) rouge Data Cache Load	Yes	Performance reduction	Same	(Khasawneh , 2018) (Conte, 2018)
Meltdown (CVE-2018-3640) Rouge System Register Read	Yes	Performance reduction	Same	(Khasawneh , 2018) (Conte, 2018)
Spectre (CVE-2018-3639) Speculative Store Bypass	Yes	Performance reduction	Same	(Khasawneh , 2018) (Conte, 2018)

L1 Terminal fault –SGX (CVE-2018-3615)	Yes	No information yet	-	
L1 Terminal fault –OS, SMM (CVE-2018-3620)	Yes	No information yet	-	
L1 Terminal Fault – VMM (CVE-2018-3646)	Yes	No information yet		

4.2 PC Configuration

For Conducting our measurement as discussed in the Previous chapter we have considered the follwing PC configurations:

Table 4.2: Configuaration of the of our selected systems

PC Configuaration

Factors	PC-1	PC-2
Processor	Intel Core i5-7200U	Intel Core i5-6200U
Motherboard	LENOVO LNVNB161216	HP 8101
Chipset	Intel Sky Lake	Intel Kaby Lake
Disk	2000 GB	1000 GB
Memory (RAM)	8192 MB	8192 MB
Graphics	Intel® HD Graphics 520	Intel® HD Graphics 620
OS	Ubuntu 16.04 LTS	Ubuntu 16.04 LTS
Kernel	4.4.0-31 generic	4.4.0-31 generic
Desktop	Unity 7.4.5	Unity 7.4.5
Compiler	GCC 5.4.0 20160609	GCC 5.4.0 20160609
File System	ext4	ext4
Screen Resolution	1920*1080	1366*768

4.3 PC-1 Pre-Patch and Post-Patch Performance

In this stage we would like to discuss about the impacts of meltdown and spectre patches on systems performance.

Table 4.3: Pre-patch and Post-patch performance of PC-1

Disk Test Performance			
Pre-Patch Test Result	**Test Factors**	**Post-Patch Test Result**	**Rate of change**
130 MB/s	Read	127 MB/s	2.31% less in data read after patch installation.
120 MB/s	Write	114 MB/s	5% less in data write after patch installation.
RAM Test Performance			
Pre-Patch Test Result	**Test Factors**	**Post-Patch Test Result**	**Rate of change**
14968 MB/s	Copy –Integer	15750 MB/s	5.22% increase in processing integer type data.
14882 MB/s	Copy -Floating point	15575 MB/s	4.65% increase in processing float type data.
Processor Test Performance			
Pre-Patch Test Result	**Test Factors**	**Post-Patch Test Result**	**Rate of change**
469 s	C-Ray	479 s	2.13% extra time needed
44.18 s	Compression	44.40 s	0.50% extra time needed
15.82 s	Encryption	16.78 s	6.06% extra time needed
Graphics Test			
Pre-Patch Test Result	**Test Factors**	**Post-Patch Test Result**	**Rate of change**
13.44 frame/s	1920*1080 Window mode	10.35 frame/s	22.99% frame drop per second
7.72 frame/s	1920*1080 Full screen mode	8.82 frame/s	14.24% frame rate increased per second

4.4 PC-2 Pre-Patch and Post-Patch Performance

In this stage we would like to discuss about the impacts of meltdown and spectre patches on systems performance.

Table 4.4: Pre-patch and Post-patch performance of PC-2.

Disk Test Performance			
Pre-Patch Test Result	**Test Factors**	**Post-Patch Test Result**	**Rate of change**
86.83 MB/s	Read	75.76 MB/s	12.74% less in data read after patch installation.
83.17 MB/s	Write	74.49 MB/s	10.43% less in data write after patch installation.
RAM Test Performance			
Pre-Patch Test Result	**Test Factors**	**Post-Patch Test Result**	**Rate of change**
10285 MB/s	Copy –Integer	10003.04 MB/s	2.74% decrease in processing integer type data.
10315 MB/s	Copy -Floating point	10190.69 MB/s	1.20% decrease in processing integer type data.
Processor Test Performance			
Pre-Patch Test Result	**Test Factors**	**Post-Patch Test Result**	**Rate of change**
494 s	C-Ray	662.53 s	34.11% extra time needed
51.60 s	Compression	55.76 s	8.06% extra time needed
18.71 s	Encryption	22.71 s	21% extra time needed
Graphics Test			
Pre-Patch Test Result	**Test Factors**	**Post-Patch Test Result**	**Rate of change**
16.46 frame/s	1366*768 Window Mode	12.24 frame/s	25.63% frame drop
11.99 frame/s	1366*768 Full screen Mode	11.08 frame/s	7.58% frame drop

4.5 Result Analysis

Table 4.5: Performance change on the 6th and 7th Gen. Processor and further analysis on that result.

	Test Factors	PC-1 (7th gen processor)	PC-2 (6th gen processor)	Result Analysis
Disk Performance	Read	2.31% reading speed decreases in data read after patch installation.	12.74% reading speed decreases in data after patch installation.	After patching system containing 6th Gen. processor becomes slower than 7th generation Processor.
	Write	5% deduction of data writing speed after patch installation.	10.43% deduction of data writing speed after patch installation.	After patching system containing 6th Gen. processor becomes slower than 7th generation Processor.
RAM Performance	Copy -Integer	5.22% increase in processing integer type data.	2.74% decrease in processing integer type data.	After patch installation system containing 6th Gen. processor can process less amount of data in their main memory than 7th Gen. processor.
	Copy - Floating point	4.65% increase in processing float type data.	1.20% decrease in processing integer type data.	After patch installation system containing 6th Gen. processor can process less amount of data in their main memory than 7th Gen. processor.
Processors Performance	C-Ray	2.13% extra time needed	34.11% extra time needed	After patch installation it takes relatively more time for 6th Gen. processor rather than a 7th Gen. processor to load a 4k image.
	Compression	0.50% extra time needed	8.06% extra time needed	A 6th Gen. processor took relatively long time than 7th Gen. processor to compress a particular amount of data after patch installation.

	Encryption	6.06% extra time needed	21% extra time needed	It took more time for a 6th Gen. processor to Encrypt certain amount of data than a 7th Gen. processor because of the slowness of the system.
Graphics Performance	Window Mode	22.99% frame drop per second	25.63% frame drop per second	After patch installation a 6th Gen. processor drops relatively more frames rather than a 7th Gen. processor on window mode.
	Full screen Mode	14.24% frame rate increased per second	7.58% frame drop per second	After patch installation a 6th Gen. processor drops relatively more frames rather than a 7th Gen. processor on full screen mode.

4.6 Discussion

From the above mentioned table we can observe that the processors of different generations are having significant amount of impacts after installing, Meltdown and Spectre patches. We selected two of Intel's i5 processors with 6th and 7th generation.

During the research we conducted several test to the CPU and get their performances on that particular situation. We tested both 6th and 7th generation's processors. We tested the processors before and after applying the patches. From the tests we found that 6th generations processors performance are getting reduced on disk read and write speed, main memory's processing speed, processors required time to perform complex tasks and processors integrated graphics cards performance.

Therefore form the above data it can be said that all the Intel's processors till 7th generations are affected by meltdown and spectre vulnerabilities. Their performances are also decreased due to the installation of patches. Most significant fact is that, the older generations processors are having more performance reduction than latest processors.

Chapter 5

Conclusion

5.1 Conclusion

During the whole process of this research, we collected existing information about the Meltdown and Spectre vulnerability and presented them in an organized way. We collected different types of processors for testing their performance. We tested those processors before patching and then we patched those processors with appropriate OS and BIOS patches. Again we tested the performance of the processor. We compared both processors performance and came to a conclusion that almost all the processor performance till 7th generation are getting reduced by the installation of patches. However the old hardwires are facing more and more performance reduction level. Therefore, from the entire research period it is obvious that the older generations systems are having more performance reduction. This research will help people to know more about the current situation of the old or new hardwires. Now it's up to the user to decide whether they would choose performance over the security or they may choose their systems security and sacrifices the performance.

5.2 Limitations

Intel's 6th and 7th generation core i5 processor were used for performance testing during the research period. After performing those tests we get to the above conclusion, nevertheless result might get more accurate if we used other processors as like 5th or 4th generation's Intel processor. Besides that we could study and understand the impact of patches on various processors more effectively. However due to some limitation we weren't been able to test more processors. Therefore, being unable to test more processors were the limitation of this research.

5.3 Future Work

Future research should be devoted to the development of patches. Patches should be improved and optimized as if they don't put an impact on the performance of the processor whether it is old or new. There are millions of older devices such as desktop, laptop and mobile devices which are affected by the Meltdown and Spectre vulnerabilities. Replacing old hardware's with newer hardware's will be difficult as well as time and money consuming. Therefore, the development and optimization of the patches which will mitigate the effects of meltdown and spectre without sacrificing the performance of the system will be the goal of future research.

REFERENCES

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., … Hamburg M.(2018). Meltdown.

Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., … Yarom, Y.(2018). Spectre Attacks: Exploiting Speculative Execution.

Trippel, C., Lustig, D., & Martonosi, M. (2018). MeltdownPrime and SpectrePrime: Automatically-Synthesized Attacks Exploiting Invalidation-Based Coherence Protocols.

Reading privileged memory with a side-channel. (2018). Retrieved from https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

Meltdown and Spectre, explained. (2018). Retrieved from https://medium.com/@mattklein123/meltdown-spectre-explained-6bc8634cc0c2

Meltdown, Spectre, and the State of Technology. (2018). Retrieved from https://stratechery.com/2018/meltdown-spectre-and-the-state-of-technology/

Researchers Discover Two Major Flaws in the World's Computers. (2018). Retrieved from https://www.nytimes.com/2018/01/03/business/computer-flaws.html

The Effects of the Spectre and Meltdown Vulnerabilities - Schneier on Security. (2018). Retrieved from https://www.schneier.com/blog/archives/2018/01/the_effects_of_3.html

Spectre and Meltdown explained: what they are, how they work, what's at risk. (2018). Retrieved from https://www.csoonline.com/article/3247868/vulnerabilities/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html

11 Potential effects of Meltdown and Spectre on Tech industry. (2018). Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/03/21/11-potential-effects-of-meltdown-and-spectre-on-the-tech-industry/#1c789232e44c

Meltdown and Spectre: Understanding the Performance Impact, Current State & What's Next. (2018). Retrieved from https://www.citrix.com/blogs/2018/02/06/meltdown-and-spectre-understanding-the-performance-impact-current-state-whats-next/

The impact of Meltdown and Spectre on your business. (2018). Retrieved from https://mondo.com/blog-meltdown-spectre-business-impact/

What Are the Implications of Meltdown and Spectre for IoT. (2018). Retrieved from https://dzone.com/articles/what-are-the-implications-of-meltdown-and-spectre

Gruss, D., Lipp, M., Schwarz, M., Fellner, R., Maurice, C., & Mangard, S. (2018). KASLR is Dead: Long Live KASLR

KAISER: hiding the kernel from the user space. (2018). Retrieved from https://lwn.net/Articles/738975/

A Clear Guide to Meltdown and Spectre Patches. (2018). Retrieved from https://blog.barkly.com/meltdown-spectre-patches-list-windows-update-help

Mitigating Meltdown and Spectre - Windows Server. (2018). Retrieved from https://help.fasthosts.co.uk/app/answers/detail/a_id/3135/~/mitigating-meltdown-and-spectre---windows-server

Protect your Windows devices against Spectre and Meltdown. (2018). Retrieved from https://support.microsoft.com/en-us/help/4073757/protect-your-windows-devices-against-spectre-meltdown

Meltdown and Spectre Vulnerabilities. (2018). Retrieved from https://www.dell.com/support/contents/us/en/04/article/product-support/self-support-knowledgebase/software-and-downloads/support-for-meltdown-and-spectre

Mozilla Foundation Security Advisory 2018-01. (2018). Retrieved from https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

Mitigating speculative execution side-channel attacks in Microsoft Edge and Internet Explorer. (2018). Retrieved from https://blogs.windows.com/msedgedev/2018/01/03/speculative-execution-mitigations-microsoft-edge-internet-explorer/#hlgJckks2qu9Vxhm.97

Intel Releases Linux CPU Microcode's to fix Meltdown & Spectre Bugs. (2018). Retrieved from https://www.bleepingcomputer.com/news/security/intel-releases-linux-cpu-microcodes-to-fix-meltdown-and-spectre-bugs/

Important: Windows security updates and antivirus software. (2018). Retrieved from https://support.microsoft.com/en-us/help/4072699/windows-security-updates-and-antivirus-software

Mitigating Meltdown and Spectre – Linux. (2018). Retrieved from https://help.fasthosts.co.uk/app/answers/detail/a_id/3136/related/1

USN-3522-3: Linux kernel regression. (2018). Retrieved from https://usn.ubuntu.com/3522-3/

How to protect your PC from the Meltdown and Spectre CPU flaws. (2018). Retrieved from https://www.pcworld.com/article/3245810/security/how-to-protect-your-pc-meltdown-spectre-cpu-flaws.html

Google: We fixed Spectre and Meltdown with no performance loss. (2018). Retrieved from https://www.slashgear.com/google-we-fixed-spectre-and-meltdown-with-no-performance-loss-12515017/

Controlling the Performance Impact of Microcode and Security Patches for CVE-2017-5754 CVE-2017-5715 and CVE-2017-5753 using Red Hat Enterprise Linux Tunables. (2018). Retrieved from https://access.redhat.com/articles/3311301

Retpoline: a software construct for preventing branch-target-injection. (2018). Retrieved from https://support.google.com/faqs/answer/7625886

Belay that order: Intel says you should NOT install its Meltdown firmware fixes. (2018). Retrieved from https://www.computerworld.com/article/3250250/malware-vulnerabilities/belay-that-order-intel-says-you-should-not-install-its-meltdown-firmware-fixes.html

Meltdown and Spectre Patches May Increase CPU Load [Initial Findings]. (2018). Retrieved from https://www.lakesidesoftware.com/blog/meltdown-and-spectre-patches-may-increase-cpu-load-initial-findings

Intel Security Issue Update: Initial Performance Data Results for Client Systems. (2018). Retrieved from https://newsroom.intel.com/editorials/intel-security-issue-update-initial-performance-data-results-client-systems/

How the Meltdown and Spectre security holes fixes will affect you. (2018). Retrieved from https://www.zdnet.com/article/how-the-meltdown-and-spectre-security-holes-fixes-will-affect-you/

Speculative Execution Exploit Performance Impacts - Describing the performance impacts to security patches for CVE-2017-5754 CVE-2017-5753 and CVE-2017-5715. (2018). Retrieved from https://access.redhat.com/articles/3307751

Firmware Updates and Initial Performance Data for Data Center System. (2018). Retrieved from https://newsroom.intel.com/news/firmware-updates-and-initial-performance-data-for-data-center-systems/

Intel Security Issue Update: Initial Performance Data Results for Client Systems. Retrieved from https://newsroom.intel.com/editorials/intel-security-issue-update-initial-performance-data-results-client-systems/

Khasawneh, K. N., Koruyeh, E.M., Song, C., Evtyushkin, D., Ponomarev, D., & Abu-Ghazaleh, N. (2018). SafeSpec: Banishing the Spectre of a Meltdown with Leakage-Free Speculation.

INTEL OFFERS SECURITY UPDATES. (2018). Retrieved from https://newsroom.intel.com/news/intel-offers-security-issue-update/

Gartner Provides Seven Steps Security Leaders Can Take to Deal With Spectre and Meltdown. (2018). Retrieved from https://www.gartner.com/en/newsroom/press-releases/2018-02-15-gartner-provides-seven-steps-security-leaders-can-take-to-deal-with-spectre-and-meltdown

5 Ways to Prevent a Spectre or Meltdown Attack. (2018). Retrieved from https://www.gartner.com/smarterwithgartner/5-ways-to-prevent-a-spectre-or-meltdown-attack/

6 steps firms can take to mitigate Spectre and Meltdown risks. (2018). Retrieved from https://www.information-management.com/slideshow/6-steps-firms-can-take-to-defend-against-spectre-and-meltdown

About the security content of Safari 11.0.2. Retrieved from https://support.apple.com/en-us/HT208403

Mitigating Side-Channel Attacks. (2018). Retrieved from https://www.chromium.org/Home/chromium-security/ssca

AMD processor security updates. Retrieved from https://www.amd.com/en/corporate/security-updates

Bulck, J. V., Minkin, M., Weisse, O., Genkin, D., Kasikci, B., Piessens, F., …Strackx, R. (2018). FORESHADOW: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution.

Weisse, O., Bulck, J. V, Minkin, M., Genkin, D., Kasikci, B., Piessens1, F., … Yarom, Y. (2018). Foreshadow-NG: Breaking the Virtual Memory Abstraction with Transient Out-of-Order Execution

L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646. (2018). Retrieved from https://access.redhat.com/security/vulnerabilities/L1TF

L1 Terminal Fault / CVE-2018-3615, CVE-2018-3620,CVE-2018-3646 / INTEL-SA-00161. Retrieved from https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault

Q2 2018 Speculative Execution Side Channel Update. Retrieved from https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html

CVE-2018-3640. Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3640

CVE-2018-3639. Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3639

Conte, T. M., DeBenedictis, E. P., Mendelson, A., & Milojičić, D., (2018). Rebooting Computers to Avoid Meltdown and Spectre", https://ieeexplore.ieee.org/document/8352078

Prout, A., Arcand, W., Bestor, D., Bergeron, B., Byun, C., Gadepally, V., … Reuther, A. (2018). Measuring the effects of Meltdown and Spectre.

Tabe, A., Mousavi, S.k., Shaker, K., & Hatamzadeh, P. (2018). An Investigation of The Impact of Meltdown on Operating System.

Watson, R.N.M., Woodruf, J., Roe, M., Moore, S.W., & Neuman, P.G., (2018). Capability Hardware Enhanced RISC Instructions (CHERI): Noters on the Meltdown and Spectre Attacks.

Larrea, V.G., Brim, M.J., Joubert, W., Boehm, S., Baker, M., Hernandez, O., … Maxwell, D., (2018). Are We Witnessing the Spectre of an HPC Meltdown?

Wang, G., Chattopadhyay, S., Gotovchits, I., Mitra, T., & Roychoudhury, A., (2018). oo7: Low-overhead Defense against Spectre Attacks via Binary Analysis.

Depoix, J., & Altmeyer, P., (2018). Detecting Spectre Attacks by identifying Cache Side-Channel Attacks using Machine Learning

