**Abstract**

This report is about examining the various security flaws that exist in the microarchitectures of Intel’s products. The report begins by introducing Intel as one of the biggest companies in Silicon Valley. The company has been around for over fifty years. The company develops advanced technologies with the goal of improving people's lives all over the world. Intel's advanced technologies include artificial intelligence, pervasive connectivity, cloud infrastructure, and ubiquitous computing. A literature review of the research is presented. Initially, a team of researchers from the following institutions; the University of Adelaide, the University of Michigan, and Austrian University, delved into this matter. The research discusses the various security flaws that the researchers found. The researchers found three major flaws, which are Meltdown, spectre, and RIDL. The research ends with a conclusion in regards to the discussed security flaws.

**Introduction**

This report is about the security flaws of a technology company called Intel. Intel is one of the renowned tech firms in the proverbial Silicon Valley. The company has been in existence for over fifty years. The company creates advanced technologies that are aimed at improving the lives of people across the world. Some of the advanced technologies at Intel include the following; artificial intelligence, pervasive connectivity, cloud infrastructure, and ubiquitous computing (Lieder, Segal, and Hope, 2019). In recent years, customers all over the world have raised complaints about the security problems in the processors of Intel's products. This essay seeks to explore the relationship between security issues and microarchitecture.

**Literature Review**

This section deals with research that has been conducted initially regarding the security problems of Intel's product. The literature review is very significant in that it provides this research with a background on where to begin. The literature review will focus on the research that was done by scientists from the University of Adelaide, the University of Michigan, and the Austrian University (Moghimi, 2020). The teams of researchers had been conducted by the company itself to do research about security flaws that could be found in its microarchitectures. The group of researchers found the following are the major security problems; Meltdown, spectre, ZombieLoad, and RIDL.

**Discussion**

This section discusses the various kinds of security flaws that were found to be affecting the microarchitectures of Intel's products. They are discussed below:

1. **Meltdown and Spectre**

These two vulnerabilities go hand in hand because they are almost similar. These are security flaws that permit a program to gain accessibility to the memory. In the process, the program is able to get access to get the secrets of the operating systems and other programs that are found there (Herzog, Reif, and Preis, 2021). However, it should be noted that they are not the same. They are two different vulnerabilities that are almost similar in nature. Meltdown and spectre are extremely dangerous to the hardware components of a firm. The two have the capability of allowing malicious people to gain accessibility to the organization's systems, such as servers, CPUs, and smartphones, among others.

Spectre and Meltdown are examples of "transient execution" security issues, which depend on defects in the hardware plan of modern CPUs' enactments of notional execution, instruction pipelining, and out-of-order execution. While this trio is critical to modern processor performance optimizations, implementations vary between CPU manufacturers and microarchitectures; as a result, not all Spectre and Meltdown variants are exploitable on all microarchitectures (Herzog, Reif, and Preis, 2021). However, the researchers found out that it is hard to understand meltdown and spectre vulnerabilities because of the following reasons:

1. After the first disclosure, the scientists found out that there were some technical differences in the variances.
2. The degree to which different microarchitecture types are vulnerable to transient execution attacks (Herzog, Reif, and Preis, 2021).
3. The manners in which spectre and Meltdown can be mitigated are not only difficult, but they also differ.
4. The capital blow that processor producers and hardware vendors fear.
5. There is great politics in the information

**Meltdown and Spectre Risks**

Spectre and Meltdown permit malicious people or hackers to excerpt encryption keys and passwords from systems that are compromised, thus; permitting other attacks that depend on compromised systems to be carried out. Since JavaScript-based proofs-of-concept validate the capability of exploiting these susceptibilities inside a web browser, exploiting Spectre and Meltdown does not require a user to run a specific maliciously-formed executable (Herzog, Reif and Preis, 2021). As an impartial weakness, Spectre and Meltdown are relatively inept for mass data exfiltration, with Meltdown retrieving data at about 120 KB/s and Spectre at 1.5 to 2 KB/s, according to the initial study. Furthermore, Spectre-BTB (Variant 2) takes approximately ten to 30 minutes to reset on a system with 64 GB RAM and is expected to scale "roughly linearly" as host RAM size increases.

**Variants of Meltdown**

The researchers found out that there were numerous variants of Meltdown as discussed below:

1. Meltdown-US – This kind of Meltdown was originally called Variant 3. It was the kind of Meltdown to be discovered. For the purpose of designating ownership of virtual memory folios, many processors include "user" and "supervisor" page-table characteristics; Meltdown-US validates the capability of reading kernel memory from user space on pipelined processors that fail to transiently enforce these flags (Khasawneh and Song', 2019). Meltdown-US modifications that use transactional harmonization leeway permit malicious individuals to increase data access speed. Additionally, Meltdown-US can excerpt uncached data from memory.
2. Meltdown-P – This kind of meltdown is known as Foreshadow. Meltdown-P causes page culpability in the event that unauthorized access to page-table memory transpires, providing an exploitable way of reading protected memory. When researchers reported Foreshadow to Intel, the company discovered Foreshadow-NG the following variants CVE-2018-3620 and CVE-2018-3646, which consent invaders to read any information that is stored in the L1 cache, including System Management Mode, host OS kernel, and hypervisor data (Khasawneh and Song', 2019). These variants can permit cloud platform assailants to read data from other virtual machines on the same physical hardware.
3. Meltdown-RW - According to the Systematic Evaluation, Meltdown-RW is the primary to detour "page-table based access rights within the current privilege level." Additionally, Meltdown-RW demonstrates that "transient execution disregards thread/write' page-table trait." The capacity to quickly overwrite read-only data within the current privilege level can evade software-based sandboxes that depend on hardware read-only memory implementation." Meltdown-RW was initially labeled as "Spectre Variant 1.2," but because the cause of transient execution is a page-fault exception, the correct classification is Meltdown (Khasawneh and Song', 2019). Meltdown-RW was successfully demonstrated by researchers on Intel and Arm processors.
4. Meltdown-PK - Meltdown-PK takes advantage of "Memory Protection Keys for Userspace," which were originally affected in Intel's Skylake-based Xeon CPUs. This variant circumvents PKU's read and writes remoteness within the containing progression (Khasawneh and Song', 2019). Bestowing to the Systematic Evaluation that presented this variant, "there is no software workaround in contrast to cross-privilege level Meltdown attack variants." "Intel can only fix Meltdown-PK with new hardware or possibly through a microcode update," though the functionality is only available in Linux if the kernel was configured and built with support enabled.
5. **ZombieLoad Attacks**

This is the second security flaw in Intel's microarchitecture. This mode of attack makes it possible for sensitive data to be stolen. This is achieved courtesy of malicious programs. The malicious programs exploit the CPU internally, thereby accessing sensitive information (Schwarz, Lipp, and Gruss, 2019). Zombieland is a type of vulnerability known as Microarchitectural Data Sampling, abbreviated as MDS, vulnerabilities, whose main target is the CPU's microarchitectural data structures such as the load, store, and line fills buffer caches. ZombieLoad, in precise, uses the line buffer cache to excerpt information from a CPU's internal cache. RIDL and Fallout are two other MDS attacks.

1. **RIDL**

This is an abbreviation of Raw Internal Data Library. The research found out that this is one of the vulnerabilities to the microarchitecture of Intel's hardware components. The main focus of this kind of attack is the data structures of a CPU's architecture, such as buffer caches, stores, and the load (Schwarz, Lipp, and Gruss, 2019). Specifically, RIDL takes advantage of a hardware design flaw in the line buffer cache to extract sensitive data from a CPU.

**Conclusion**

In the world of information technology, data protection plays a crucial role. Protection of data from people with malicious intentions ensures that vital information is not accessed by unauthorized people. This research focused on how security flaws exist in Intel's microarchitectures. The company contracted researchers from reputable institutions of higher learning to conduct research on the various vulnerabilities of its microarchitectures components. This came after there were complaints from customers across the world. Other tech firms should also emulate this from Intel since it is a way of getting to know these flaws and thereby deriving ways of preventing or avoiding them all. The following are the flaws that were found by the researchers; meltdown, spectre, zombieload, and RIDL. Meltdown and spectre were the severest vulnerabilities. Moreover, in as much as these two were different, they were almost the same. The two allow malicious people or hackers to extract encryption keys and passwords from compromised systems, allowing other attacks that rely on compromised systems to be carried out. Exploiting Spectre and Meltdown does not require a user to run a specific maliciously-formed executable because JavaScript-based proofs-of-concept validate the capability of exploiting these vulnerabilities inside a web browser. According to preliminary research, Spectre and Meltdown are relatively inept for mass data exfiltration, with Meltdown retrieving data at about 120 KB/s and Spectre retrieving data at 1.5 to 2 KB/s.