**Hardware Vulnerability Research**

**CYBR3020**

**Vulnerabilities and Exploits**

Arr Domingo

Student ID: 200458099

Instructor: Clayton Amelia

Table of Contents

[Introduction 1](#_Toc211456348)

[What is Meltdown 1](#_Toc211456349)

[Subtopic 1.1 1](#_Toc211456350)

[How meltdown works 1](#_Toc211456351)

[Subtopic 2.1 1](#_Toc211456352)

[Subtopic 2.2 1](#_Toc211456353)

[How to Prevent the Exploitation 1](#_Toc211456354)

[Subtopic 3.1 1](#_Toc211456355)

[Subtopic 3.2 1](#_Toc211456356)

# Introduction

Hardware Vulnerability refer to weaknesses or flaws in the physical components of computing devices, such as processors, memory, and firmware. It has emerged as a critical concern in the rapidly evolving cybersecurity landscape. Unlike software vulnerabilities, which can often be patched or updated, hardware vulnerabilities are more challenging to address because they are literally part of the physical machine. One of the most common hardware exploitations is Meltdown.

# What is Meltdown (Report describes the Vulnerability)

Meltdown (CVE-2017-5754)

This hardware vulnerabilities work on personal computers, mobile devices, and in the cloud. Every Intel processor which implements out-of-order execution is potentially affected by Meltdown.

Both Meltdown and Spectre use side-channel to obtain the information from the accessed memory location, termed “Kernel-memory-leaking”. While Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory, Spectre tricks other applications into accessing arbitrary locations in their memory. Leaked information could include passwords stored in a password manager or browser, personal photos, emails, instant messages and documents

## Subtopic 1.1

IAAA (Identification, Authentication, Authorization, Accountability) is the foundation of Identity and Access Management (IAM). IAM is a discipline and a type of framework for solving the challenge of secure access to digital resources.

# How meltdown works (Report explains how the exploit works)

## Subtopic 2.1

## Subtopic 2.2

# What was vulnerable (Report describes what was/is vulnerable)

Report describes the vulnerability clearly and with sufficient detail that the reader can understand the concept

Computer PC, etc

## Subtopic 3.1

## Subtopic 3.2

# How to Prevent Exploitation (Report describes how to prevent exploitation)

# References

*Installing GitHub Desktop on Debian/Ubuntu [closed]*. (n.d.). Retrieved from StackOverflow: https://stackoverflow.com/questions/73980172/installing-github-desktop-on-debian-ubuntu

*isec-tugraz / meltdown*. (n.d.). Retrieved from Github: https://github.com/isec-tugraz/meltdown

*Understanding Hardware Vulnerabilities and Advanced Persistent Threats*. (2024, October 2). Retrieved from Linkedin: https://www.linkedin.com/pulse/understanding-hardware-vulnerabilities-advanced-persistent-giffe#:~:text=Hardware%20vulnerabilities%20refer%20to%20weaknesses,processors%2C%20memory%2C%20and%20firmware.

<https://www.cyber.gc.ca/en/alerts-advisories/meltdown-and-spectre-side-channel-vulnerabilities>

**Conclusion**

Hardware vulnerabilities pose significant risks to the security and functionality of systems. Addressing these vulnerabilities requires a comprehensive approach that includes secure design, rigorous testing, and robust supply chain management. By understanding and mitigating these risks, organizations can better protect their hardware from exploitation and ensure the integrity and security of their systems. https://clocked-out.com/what-is-hardware-vulnerabilities/