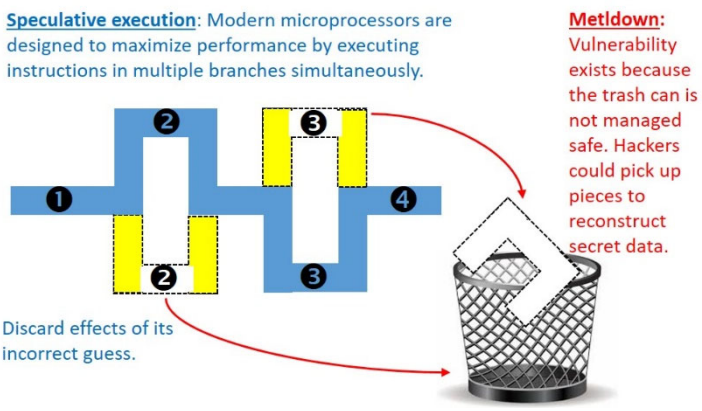
SCENARIO #2: **Meltdown & Spectre**

Scenario:



In 2015, Google's Project Zero team identified a hardware vulnerability known as Meltdown and Spectre, impacting Intel x86, IBM POWER, and certain ARM-based microprocessors [1]. This vulnerability stems from the use of "speculative execution" in modern processors to enhance performance. For instance, in the C/Java statement "if (condition) {A} else {B}," the CPU speculatively executes both A and B ahead of time, discarding the incorrect one after evaluating the condition. The vulnerability arises from the lack of secure management of the "trash can". Meltdown and Spectre attacks involve inducing a victim to speculatively perform operations not occurring during correct program execution, leaking confidential information via a side channel to adversaries.

This side-channel attack affects a broad range of systems. At disclosure, it impacted devices running versions of iOS, Linux, macOS, or Windows that were not the most recent and patched. Consequently, servers, cloud services, and numerous smart and embedded devices with ARM-based processors (e.g., mobile devices, smart TVs, printers) were affected, alongside a variety of networking equipment. A software workaround to Meltdown has been assessed to potentially slow computers by 5 to 30 percent in specific workloads, although minimal impact has been reported in general benchmark testing [2]. No reported attacks have occurred to date fortunately.

Within this scenario, students will comprehend the attack and secure CPU implementations. Additionally, they will scrutinize legal issues and risks associated with hardware vulnerabilities in the realm of cybersecurity, including the allocation of responsibility for identifying vulnerabilities, potential liability for organizations affected by cyberattacks, and advising clients on disclosure protocols. Apple, for instance, faced a class action lawsuit, alleging that it knowingly sold devices with security flaws without informing customers about potential performance slowdowns [3]. Intel also encountered lawsuits related to these security flaws, including a class action suit filed by Rifkin's law firm, Wolf Haldenstein.

Hardware security has gained significant attention in recent research. In 2015, researchers discovered the "row hammer attack," demonstrating that repeatedly accessing nearby memory cells could alter data contents in computer memory [4]. Another example is the "power analysis attack," involving the visual examination of power consumption graphs over time to infer program flow and potentially leak secret values [5]. Another important hardware attack is based upon the fact that many semiconductor intellectual property (IP) core vendors provide reusable units of logic or cell that can be licensed and used in the design of system-on-chips (SoCs) solutions. Notably, "supply chain attacks" have become prevalent, where adversaries insert

malicious components into trusted hardware, posing commercial and national security concerns [6]. Regarding Spectre, a recent report suggests that Apple's Safari browser remains vulnerable to Spectre attacks as of October 2023 [7].

NICE Workforce Framework for Cybersecurity:

Scenario #1 & #2 will cover the following Knowledge areas.
K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0004 Knowledge of cybersecurity and privacy principles.
K0005 Knowledge of cyber threats and vulnerabilities.
K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0116 Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
K0131 Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
K0205 Knowledge of basic system, network, and OS hardening techniques.
K0210 Knowledge of data backup and restoration concepts.
K0373 Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0392 Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K0452 Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.
K0627 Knowledge of the importance of ingress filtering to protect against automated threats that rely on spoofed network addresses.

References:

[1] Bright, Peter (2018-01-05). “Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it". Ars Technica, https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/
[2] “Industry Testing Shows Recently Released Security Updates Not Impacting Performance in Real-World Deployments". https://www.webwire.com/ViewPressRel.asp?aId=218518
[3] Newsweek, January 18, 2018, https://www.newsweek.com/apple-faces-class-action-lawsuit-over-meltdown-and-spectre-bugs-784496
[4] Row hammer attack, https://en.wikipedia.org/wiki/Row_hammer
[5] Power analysis attack, https://en.wikipedia.org/wiki/Power_analysis
[6] What is a Supply Chain Attack, Wired, May 31, 2021, https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/
[7] Apple Safari still vulnerable to Spectre attacks, https://news.rub.de/english/press-releases/2023-10-26-security-gap-apples-safari-browser-still-vulnerable-spectre-attacks