Hardware Vulnerabilities
Meltdown Spectre Attack

Hardware Vulnerabilities

As organizations strengthen their **software defenses**, attackers increasingly target **hardware components to exploit inherent weaknesses**. **Advanced Persistent Threats (APTs)** — highly sophisticated and targeted attacks often backed by **nation-states** — leverage these hardware vulnerabilities to compromise systems at a fundamental level, **bypassing conventional security measures.**

Hardware Vulnerabilities

Hardware vulnerabilities refer to **weaknesses or flaws in the physical components of computing devices, such as processors, memory, and firmware**.

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.**

These vulnerabilities may arise from **design flaws, manufacturing defects, or inadequate security considerations during development.**

Hardware Vulnerabilities

- **Physical in nature**: Exist in the physical components of a system.
- **Firmware or chip-level**: Affect the firmware or chips within a device.
- **Difficult to patch**: Often require hardware replacement or redesign.
- **Exploited through physical access**: Require physical access to the device.
- **Examples: Spectre, Meltdown, Rowhammer, and hardware Trojans.**

Software Vulnerabilities

- Logical in nature: Exist in the code or programming of a system.
- Application or OS-level: Affect the software running on a device.
- Easier to patch: Can often be fixed with software updates or patches.
- Exploited through network or user interaction: Can be exploited remotely or through user interaction.
- **Examples: Buffer overflows, SQL injection, and cross-site scripting (XSS).**

Differences

- **Origin**: Hardware vulnerabilities originate from design or manufacturing flaws, while software vulnerabilities originate from coding errors or design flaws.
- **Exploitation**: Hardware vulnerabilities often require physical access, while software vulnerabilities can be exploited remotely.
- **Mitigation:** Hardware vulnerabilities are harder to patch and may require hardware replacement, while software vulnerabilities can often be fixed with software updates.
- **Impact**: Both types of vulnerabilities can have significant impacts, but hardware vulnerabilities can be more difficult to detect and mitigate.

Hardware Vulnerabilities

- **Spectre and Meltdown (2018):** CPU vulnerabilities affecting Intel, AMD, and ARM processors, allowing unauthorized access to sensitive data.
- **Foreshadow (2018):** A variant of Spectre, exploiting Intel's SGX (Software Guard Extensions) to access sensitive data.
- **Fallout (2019):** A vulnerability in Intel's Converged Security and Management Engine (CSME), allowing attackers to access sensitive data.

Meltdown Hardware Attack

Meltdown is a hardware vulnerability affecting **Intel x86 microprocessors**, **IBM POWER processors**, and some **ARM-based microprocessors**. It allows a rogue process to read all memory, even when it is not authorized to do so.

Meltdown affects a wide range of systems. At the time of disclosure, this included all devices running any but the most recent and patched versions of iOS, Linux, macOS,or Windows.

Meltdown Hardware Attack

The New York Times

Researchers Discover Two Major Flaws in the World's Computers

The two problems, called Meltdown and Spectre, could allow hackers to steal the entire memory contents of computers, including mobile devices, personal computers and servers running in so-called cloud computer networks.

How Meltdown Works

- Meltdown exploits a Race condition between memory access and privilege level checking while an instruction is being processed.
- In conjunction with a CPU cache side-channel attack, privilege level checks can be bypassed, allowing access to memory used by an operating system, or other running processes.

Meltdown Hardware Attack : BACKGROUND

- Improvements in performance in modern processors are derived from a number of techniques. Limitations in augmenting the physical attributes of processors (shrinking transistor size and increasing clock frequencies) require architectural changes to how processors work in order to **deliver higher-performing parts.**
- These changes focus largely on **parallelism:** Optimizing and lengthening instruction pipelines, allowing multiple operations to be performed in parallel in a logical core (thread), and increasing the number of logical and physical cores on a processor.

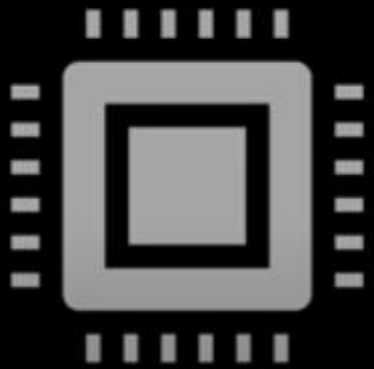
Meltdown Hardware Attack : BACKGROUND

- Other properties in modern processors include virtual (paged) memory, a method that streamlines memory management across processes, privilege levels, which allow operating systems to control which areas of virtual memory can be read by other processes, and CPU cache, in which data in system RAM is cached in order to reduce latency.
- Two independent optimization techniques of modern processors, used in conjunction, are key to understanding how Spectre and Meltdown are hardware-level vulnerabilities.

Two independent optimization techniques

- **Speculative execution** allows processors to speculate on future instruction directions and proactively execute instructions along these paths before knowing if the instructions are correct.
- **Out-of-order execution** allows for the simultaneous use of all the execution units in a CPU core. Instead of processing instructions strictly in the sequential program order, the CPU executes them as soon as all required resources are available.

Speculative out-of-order execution



```
Instruction 1
Instruction 2
Instruction 3
Instruction 4
```

Meltdown Attack : Solution

- Patches for Spectre and Meltdown should be considered, with initial patching strategies introduced and rolled back due to instability or findings indicating they were ineffective against specific variants.
- It is unclear if the pair of vulnerabilities can be completely patched through microcode and software updates, though this uncertainty should not discourage users or administrators from deploying available patches.

Servers, desktops, and notebooks

- Mitigations for Spectre and Meltdown are delivered through **BIOS and OS updates**. For BIOS updates, check with your manufacturer to determine if BIOS updates are available.
- Generally speaking, OS updates are delivered automatically through Windows Update, the App Store (on Mac OS), or through the package manager on Linux systems.

iOS and Android devices

- For users of Apple devices, including iPhone, iPad, and Apple TV devices, software and firmware updates have been issued to address Spectre and Meltdown.
- For Android users, the first round of patches were delivered in the 2018 security patch level.

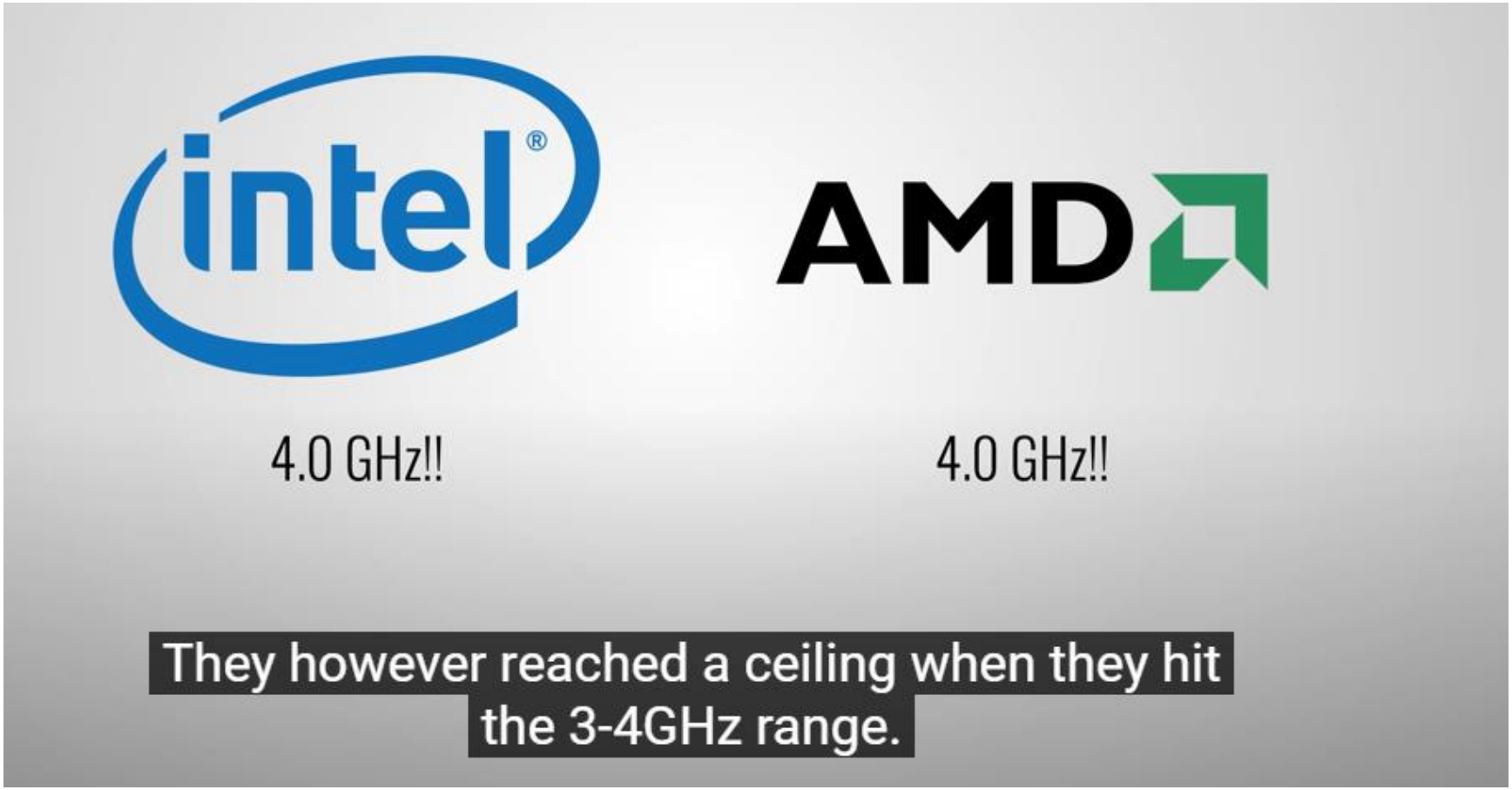
Cloud computing services

- Generally, users of cloud computing services are reliant on the platform provider to update the underlying infrastructure. Users of cloud-powered virtual machines may need to update their VMs.

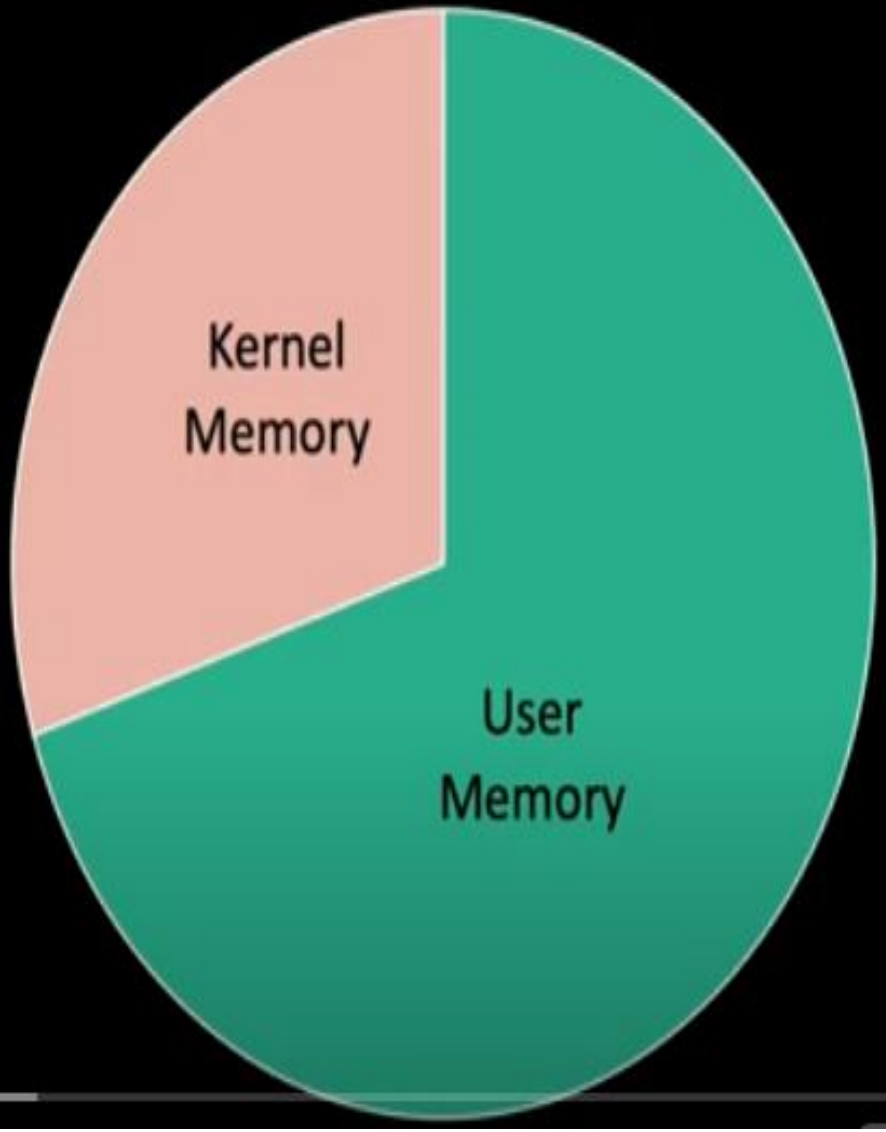
Will buying a new processor help protect against Spectre and Meltdown?

- New processors do address the Spectre and Meltdown vulnerabilities at a hardware level,

Clock Speed

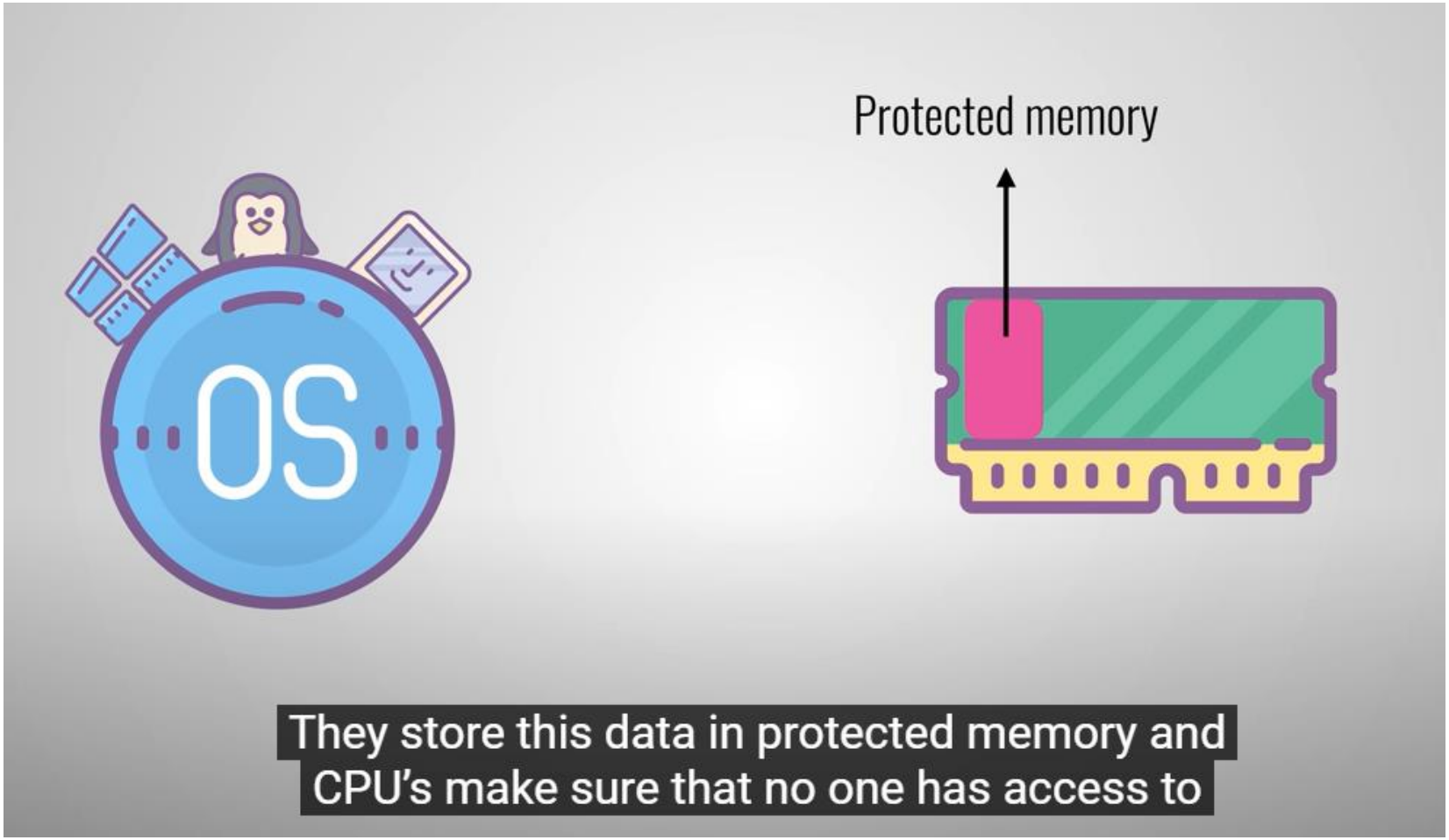

intel
AMD
4.0 GHz!!
4.0 GHz!!
They however reached a ceiling when they hit the 3-4GHz range.

High privilege
Managed by OS
Memory space shared
Access to all physical memory



Low privilege
Managed by user
Memory space unique
Access to own memory space

Memory


Protected memory
OS
They store this data in protected memory and
CPU's make sure that no one has access to


```
if ( readMemory(182379) === “S”){
   readPixel(1)
}
```

Executed while speculating

All the website has to do now is run a second program that times how long it takes to read