Meltdown and Spectre

Index

- Modern Processors
- Computer's Memory
- What is Meltdown
- What is Spectre
- What is the difference
- What we should do about it

Modern Processors

- CPU is brain of the device
- Responsible to execute instructions.
- Processing time depends on clockspeed.
- Vendors came up with something called “Speculative Execution”

Speculative Execution

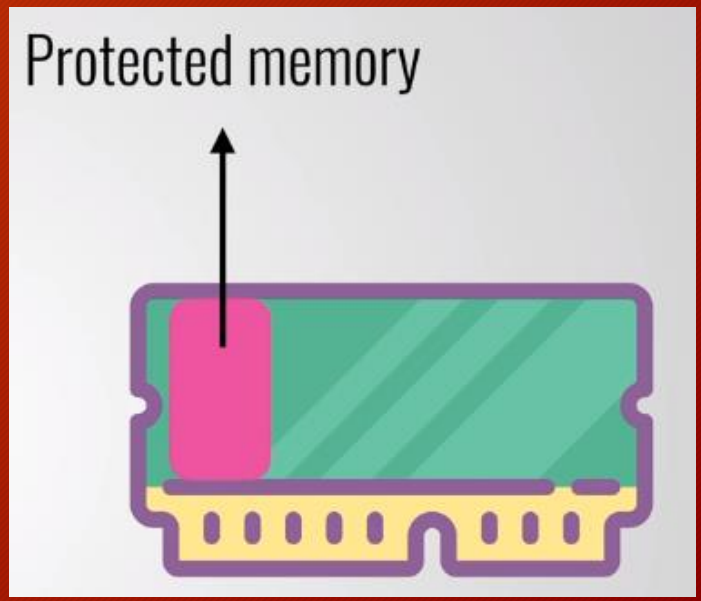
- Optimization technique where a computer system performs some task that may not be needed
- Function is carried out to prevent a delay.
- The Work is done in background before it is known whether it is actually needed or not

Memory

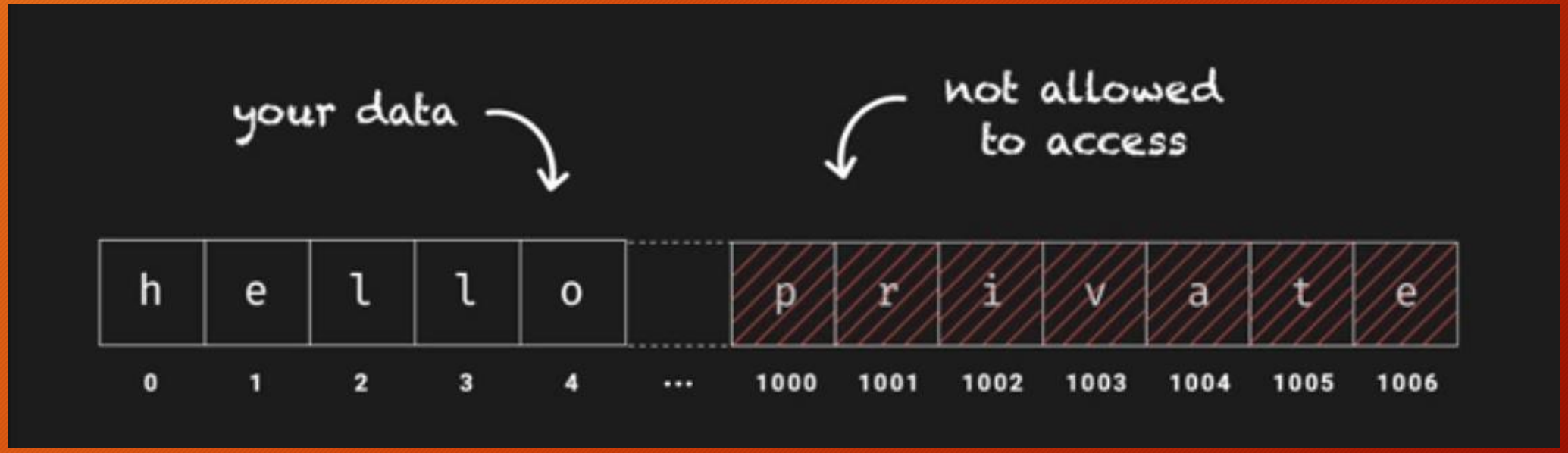
- Main two types : Main Memory and CPU Cache
- CPU read and write data from main memory
- CPU cache was introduced because main memory is way slower then the CPU.

Meltdown

- OS stores sensitive information in the main memory of our device.
- CPU make sure that no one has access to this except OS
- This rule isn't enforce when processor is speculating exections
- That's where the vulnerability is.



How Meltdown is carried out



How Meltdown is carried out

private address

```
secret = readCharacter(1000);
```

How Meltdown is carried out

```
secret = readCharacter(1000);

characters = ['A', 'B', 'C', ... 'Z'];

characters[secret];          60ms
characters[secret + 1];      60ms
characters[secret + 15];     3ms
```

Spectre

- Spectre breaks the isolation between different applications.
- It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets.
- Spectre is harder to exploit than Meltdown, but it is also harder to mitigate.

How Spectre is carried out

```
data = [1, 2, 3, 4]

input = 1000

if (input < data.size) {
    secret = data[input]
}
```

is true

speculative execution

leads to access private data

Spectre

- This attacks involve inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary.

Main difference between them

- Spectre tricks other applications into accessing arbitrary locations in their memory.
  - Both attacks use side channels to obtain the information from the accessed memory location.
- Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory.
  - Consequently, applications can access system memory.

Who are at risk?

- **ALMOST EVERYONE**
- Many Desktop, Laptop and Cloud Computers may be affected.
- Every intel processors since 1995 were effect by this vulnerabilities.
- Some of the ARM processors were also affected.

What should you do?

- Update your Operating system with latest patches of hardware and software of your computer.
- For Cloud Services, Check with your provider to see if they run the affected chips that make them vulnerable
- Most Mobile device manufacturers have developed patches as well.

References

- https://meltdownattack.com/
- https://www.redhat.com/en/blog/what-are-meltdown-and-spectre-heres-what-you-need-know
- https://www.Wikipedia.com
- https://www.youtube.com/watch?v=bs0xswK0eZk
- https://www.youtube.com/watch?v=NArwG6yaWJ8

Thank You!

Any Questions?