RECENT SECURITY ISSUES

AGENDA

- Meltdown (2017/2018)
- Spectre (2017/2018)
- Foreshadow (2018)
- Zombieload v1, v2 (2019)

CVE

CVE - Common Vulnerabilities and Exposures. A dictionary of publicly known information security vulnerabilities and exposures.

- https://nvd.nist.gov
- http://www.cve.mitre.org/
- http://www.cvedetails.com/

SPECTRE AND MELTDOWN

- Discovered in 2017 - OS vendors had head start to patch.
- Released early 2018
- Targeted Hardware
- Now: Brief recap of computer architecture and a preview of OS topic

CPU

CPU → Brain of the computer

Fast brain → Clockspeed

Increased until ~4.0GHZ

Very hard to get faster... new ideas implemented: Speculative Execution

SPECULATIVE EXECUTION

```
y = x+1
z = y+2
```

If x is to be fetched from memory (slow) the processor can select to guess y to execute the second statement: **Speculative Execution**

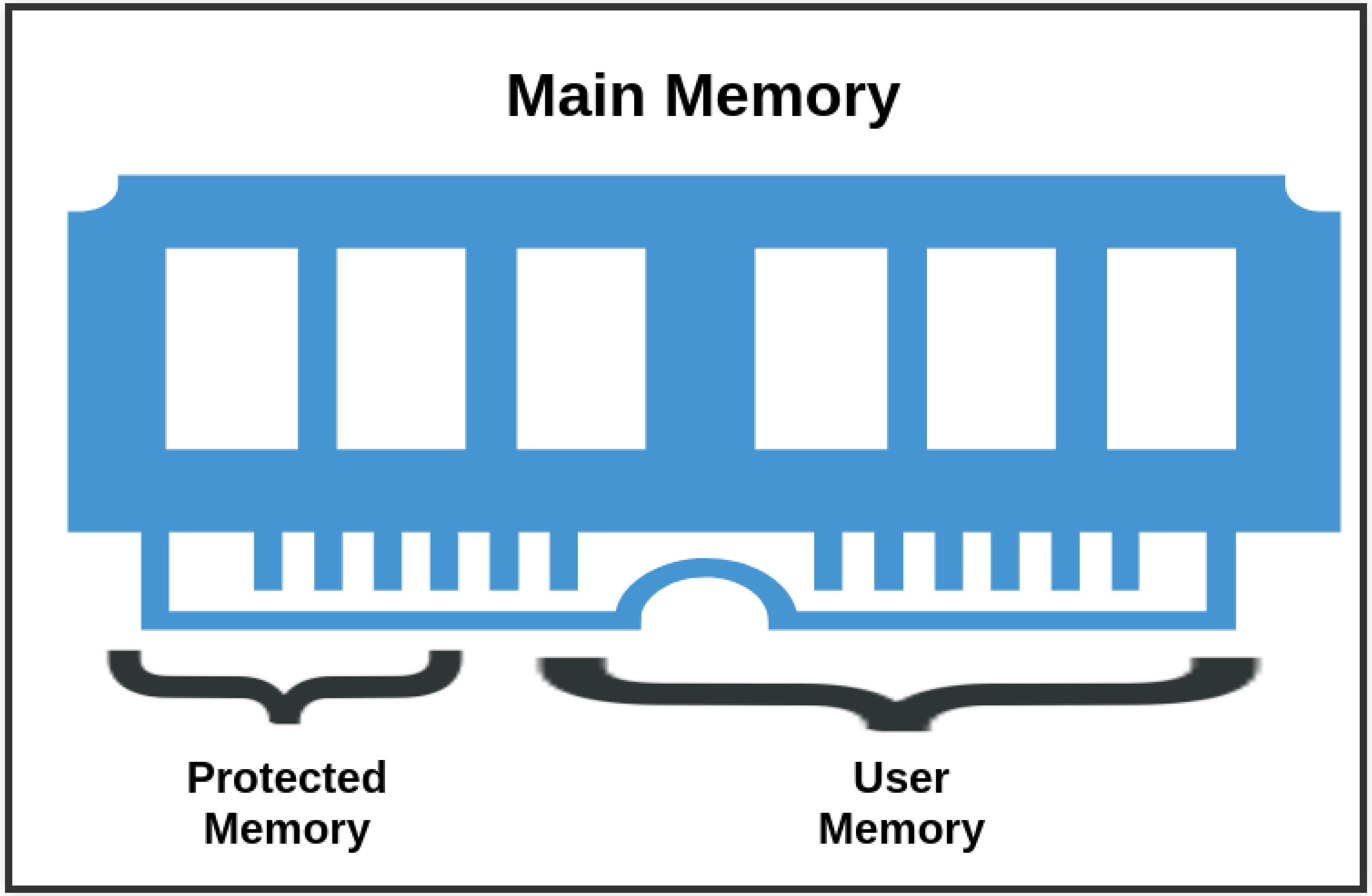
Once y is available the processor would **discard** or **commit** the result

MEMORY

Main Memory/RAM → Somewhat slow :(

CPU Cache → Fast → Data copied here from RAM before use by CPU

MAIN MEMORY



OS Writes to Protected Memory (Not allowed for user proces directly)

VIRTUEL MACHINE

A little OS preview too

VIRTUEL MACHINE

A Virtual Machine is a software emulator of a physical computer.

Virtual machines are often used in compute clouds (fx Amazon’s AWS or Microsoft’s Azure) where, instead of maintaining their own infrastructure, customers can pay for the time the cloud infrastructure spends on running the customer’s machine (and the computations within it).

VM AND CLOUDS

As clouds typically run more than one virtual machine on the same physical hardware, it is important that the cloud's Virtual Machine Manager (VMM) or hypervisor prevents information leakage across VM boundaries by ensuring complete isolation between two virtual machines and between the virtual machines and the hypervisor.

MELTDOWN

RAM CONTINUED

Protected Memory is for OS access only.

But speculative execution ignores this…

it will remove the value if it was not allowed to do instruction

EXPLOIT

Try to guess your wifi password

```
if( readMemory(183212) === 'W' ) {
    readPixel(1) 1
}
```

1 Executed while speculative execution ⇒ Copy stored in CPU Cache

EXPLOIT

Have second program: Time to read pixel 1

- **FAST** ⇒ CPU Cache ⇒ Password starts with "W"
- **SLOW** ⇒ Not in CPU Cache ⇒ Password NOT starts with "W"

MELTDOWN IN 1 SENTENCE

Allow programs to read protected memory

⚠ Intel CPU’s only

MATERIAL

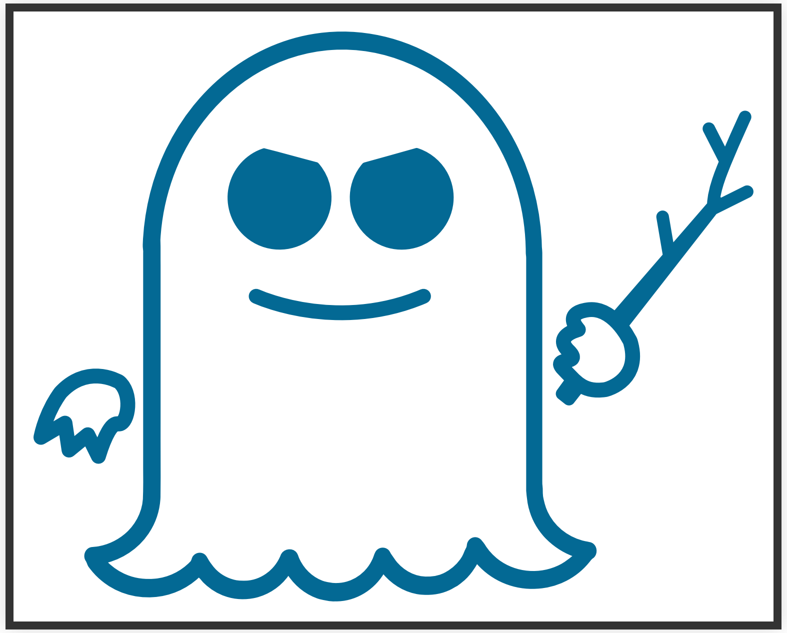
- https://meltdownattack.com/
- https://meltdownattack.com/meltdown.pdf

CREDITS

Meltdown was independently discovered and reported by three teams:

- Jann Horn (Google Project Zero),
- Werner Haas, Thomas Prescher (Cyberus Technology),
- Daniel Gruss, Moritz Lipp, Stefan Mangard, Michael Schwarz (Graz University of Technology)

SPECTRE



Spectre: Ghost type creature

EXPLOIT

```
if( x < array_1_length) {
    y = array2[array1[x]] 1
}
```

1 This is the statement we would lure the processor into speculatively execute

EXPLOIT

Idea:

1. Train the CPU with a lot of values of `x` that is less than `array_1_length`.
2. CPU will learn that statement is likely executed
3. Fire value of `x` higher than `array_1_length` ⇒ CPU will speculatively execute statement
4. Listen for the memory space, catch value before CPU performs **discard**

SPECTRE IN 1 SENTENCE

Trick CPU into speculatively execute statement and listen for value before it is discarded.

⚠ Intel, AMD, ARM cpu's all vulnerable

MATERIAL

- https://spectreattack.com
- https://spectreattack.com/spectre.pdf

CREDITS

Spectre was independently discovered and reported by two people:

- Jann Horn (Google Project Zero) and
- Paul Kocher in collaboration with, in alphabetical order, Daniel Genkin, Mike Hamburg, Moritz Lipp, and Yuval Yarom

FORESHADOW

- Operating systems and System Management Mode (SMM) — CVE-2018-3620
- Virtualization software and Virtual Machine Monitors (VMM) — CVE-2018-3646

FORESHADOW IN 1 SENTENCE

Foreshadow is a speculative execution attack on Intel processors which allows an attacker to steal sensitive information stored inside personal computers or third party clouds.

FORESHADOW

- SGX is a new feature in modern Intel CPUs which allows computers to protect users' data even if the entire system falls under the attacker's control.
- Previously believed that SGX is resilient to speculative execution attacks (Meltdown, Spectre)
- Foreshadow demonstrates how speculative execution can be exploited for reading the contents of SGX-protected memory

FORESHADOW

Mitigations at the both software and microcode level. This includes updates to most operating systems, hypervisors as well as CPU microcode updates.

💡 Foreshadow-NG breaks the virtual machine isolation.

MATERIAL

- https://foreshadowattack.eu/
- https://foreshadowattack.eu/foreshadow.pdf

ZOMBIELOAD (V1 + V2)

V2 just disclosed (Nov. 14th) - discovered back in May

ZOMBIELOAD

While programs normally only see their own data, a malicious program can exploit internal CPU buffers to get hold of secrets currently processed by other running programs.

These secrets can be user-level secrets, such as browser history, website content, user keys, and passwords, or system-level secrets, such as disk encryption keys.

ZOMBIELOAD IN 1 SENTENCE

The ZombieLoad attack allows stealing sensitive data and keys while the computer accesses them.

ZOMBIELOAD V2

A new variant of ZombieLoad that enables the attack on CPUs that include hardware mitigations against MDS in silicon.

With Variant 2 (TAA), data can still be leaked on microarchitectures like Cascade Lake (patched against many other similar attacks)

CREDITS

- Michael Schwarz, Moritz Lipp, Daniel Gruss (Graz University of Technology)
- Jo Van Bulck (imec-DistriNet, KU Leuven)

DEMO

https://zombieloadattack.com/#demo

MATERIAL

- https://zombieloadattack.com
- https://zombieloadattack.com/zombieload.pdf
- https://www.youtube.com/watch?v=3AtQIKE7pvM
- https://github.com/IAIK/ZombieLoad - PoC attack

QUESTIONS