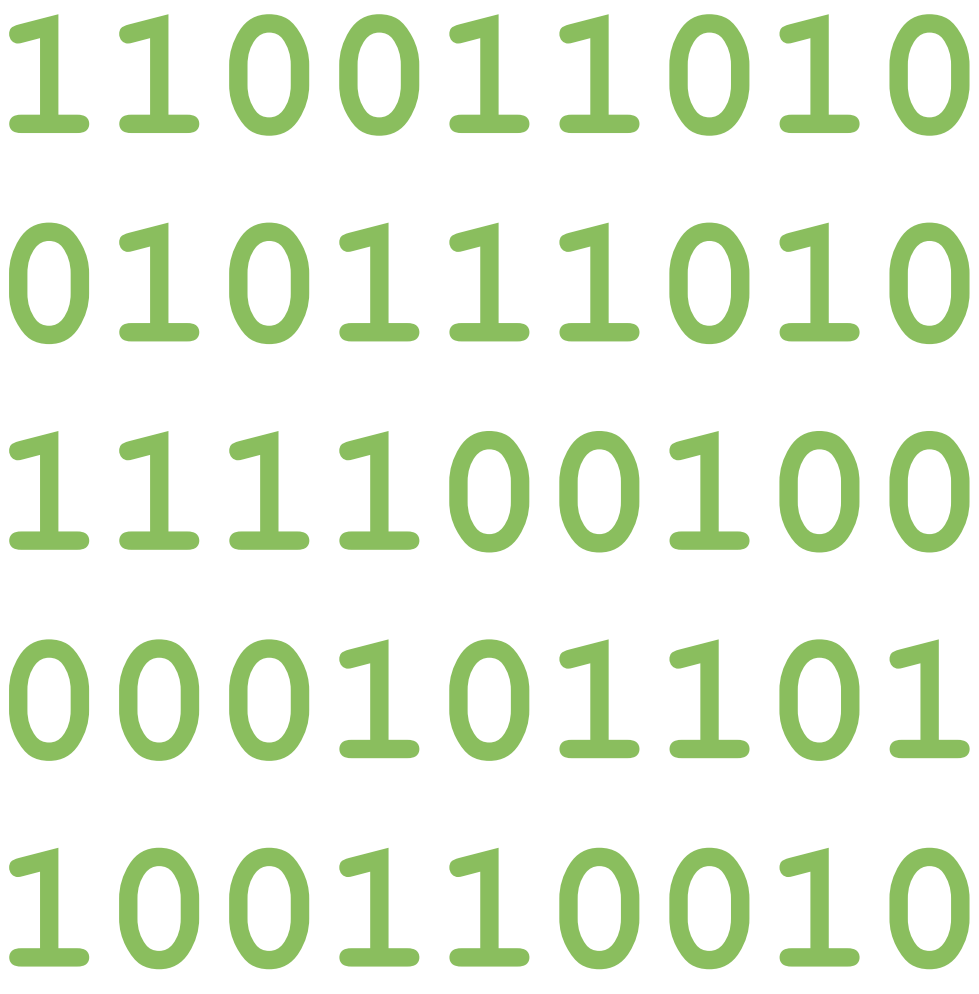
“IT’S A 1”



Collector

110011010
010111010
111100100
000101101
100110010
Spy

MELTDOWN & SPECTRE FOR NORMAL PEOPLE

MELTDOWN: THE ATTACK

30

1. **Spy** will read the **secret**

2. Depending on the **value**, **Spy** will cache a grey block[1]

3. CPU detects **Spys** access validation and terminates **Spy**

4. **Collector** now reads all grey blocks and stops the time

1. Block “It’s a 3” will be the block read the fastest

“IT’S A 2”


RAM

“IT’S A 3”

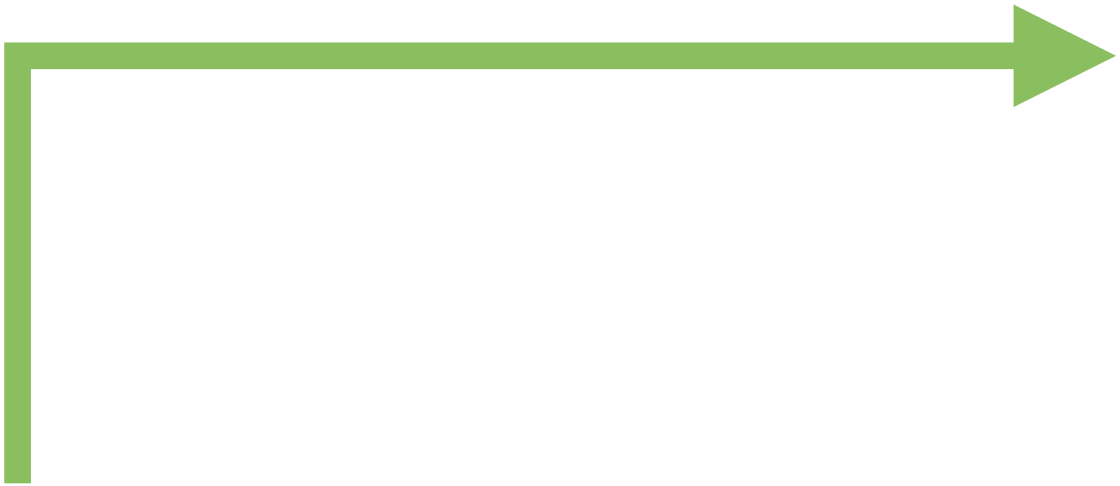
“IT’S A 1”

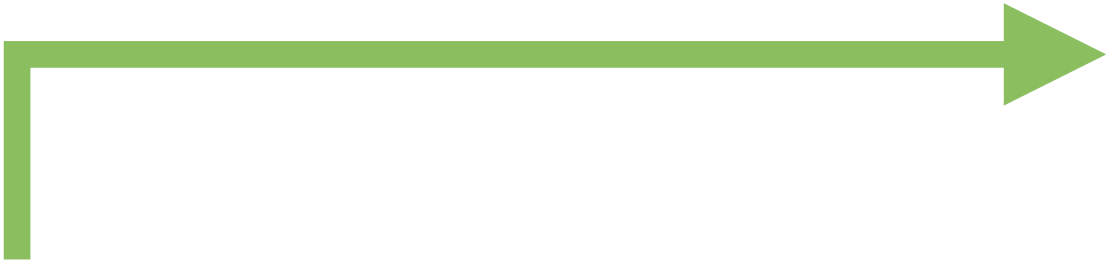
SECRET (“3”)

Cache

SECRET (“3”)

“IT’S A 3”





“IT’S A 2”

read: 103ns (uncached read)

read: 103ns (uncached read)

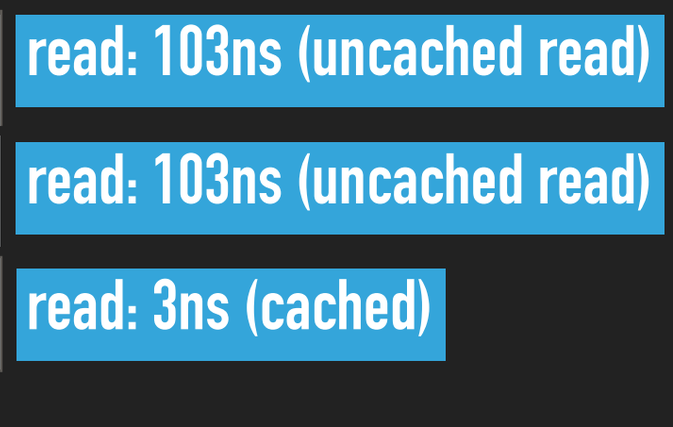
read: 3ns (cached)


2


1

[1] Actually Spy will cache the *address* of block #3 and Collector will read the blocks *addresses*

MELTDOWN: THE ATTACK



2 1. **Spy** will read the **secret**

2 2 Depending on the **value**, **Spy** will cache a grey block[1]

1 3. CPU detects **Spys** access validation and terminates **Spy**

4. **Collector** now reads all grey blocks and stops the time

1. Block "It's a 3" will be the block read the fastest

[1] Actually Spy will cache the *address* of block #3 and Collector will read the blocks *addresses*

MELTDOWN

Meltdown exploits two properties of modern CPUs

- *Out of order execution* of OPs and µOPs
- Timing side channels for the cache

This allows an attacker to

- Read all memory mapped[1] in a process
- This often includes all other processes memory
- This does NOT allow reading “outside of a VM[2]”

[1] Virtual vs. physical memory is a subject for another time [2] For fully virtualised VMs