

"IT'S A 1"



110011010

010111010

111100100

000101101

100110010

Collector

110011010

010111010

111100100

000101101

100110010

Spy



MELTDOWN & SPECTRE FOR ARMV8-A

MELTDOWN: THE ATTACK

3

1



1. **spy** will read the **secret**

2. Depending on the **value**, **Sp****y** will cache a grey block¹

3. CPlu detects **Spys** access validation and terminates **Spys**

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")



Gamechane

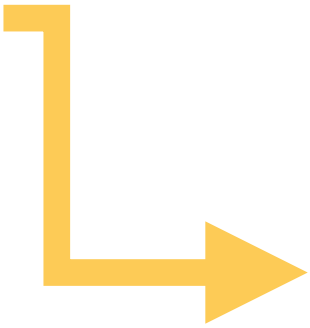


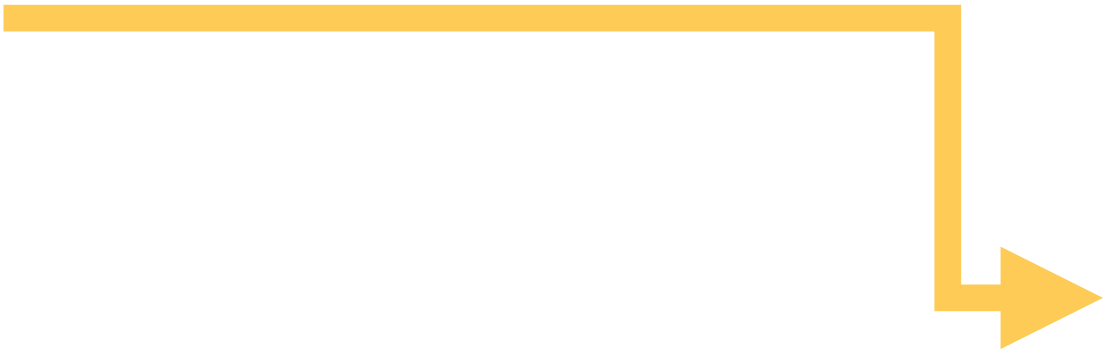


SECRET ("3")



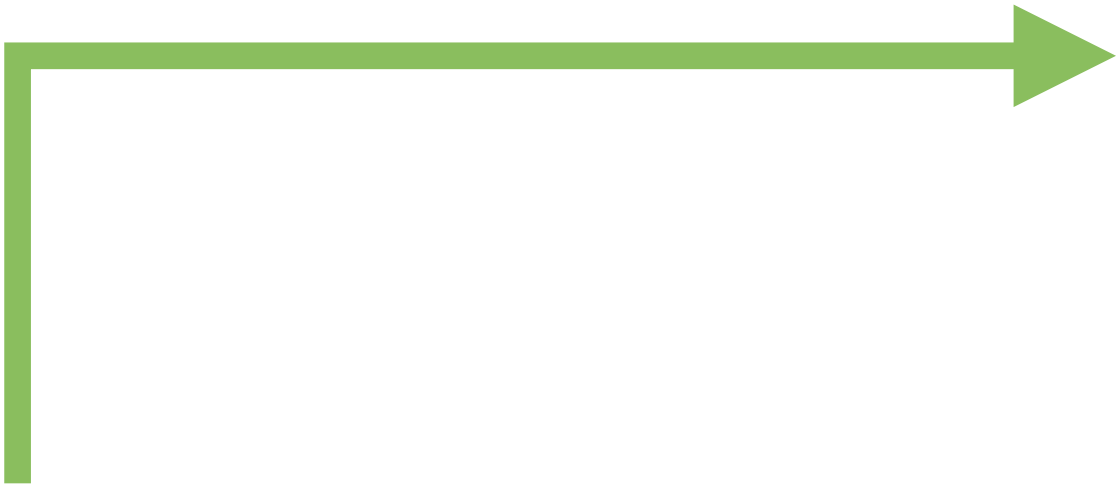


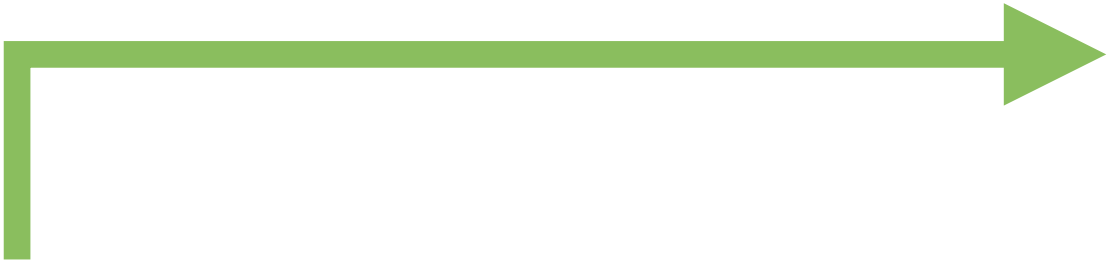




“IT’S A 3”







"IT'S A 2"



read: 103ns (uncached read)

read: 103ns (uncached read)

read: 3ns (cached)



2



1

¹Actually Spyy will cache the address of block #3 and Collect will read the blocks addresses

MELTDOWN: THE ATTACK

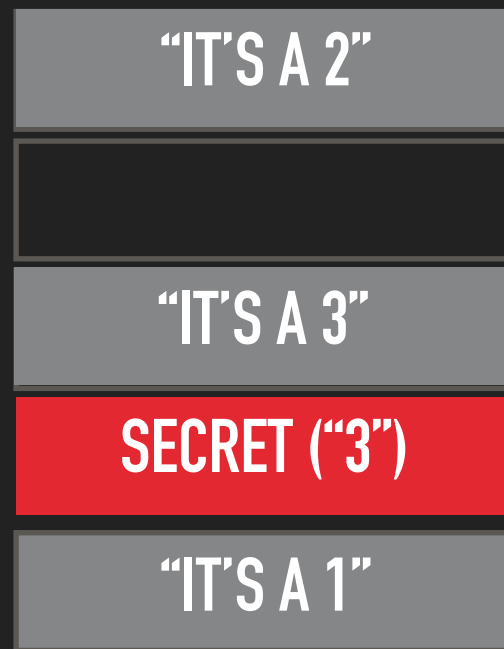


110011010
010111010
111100100
000101101
100110010

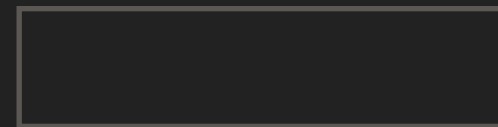
Spy

110011010
010111010
111100100
000101101
100110010

Collector



Cache



...

"IT'S A 1"

"IT'S A 2"

...

SECRET ("3")

read: 103ns (uncached read)

read: 103ns (uncached read)

read: 3ns (cached)

RAM

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

2. Depending on the **value**, **Spy** will cache a grey block¹

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 μ OPs
- ▶ Timing side channels for the cache

This allows an attacker to

- ▶ Read all memory mapped¹ in a process
- ▶ This often includes all other processes memory
- ▶ This does NOT allow reading “outside of a VM²”

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