

"IT'S A 1"



110011010

010111010

111100100

000101101

100110010

Collector

110011010

010111010

111100100

000101101

100110010

Spy



MELTDOWN: THE CHANNEL (IDEA)

3

7



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

2. Depending on the **value**, **Spy** will mark a grey block

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

4. Collector now looks for *Spys* mark in all grey blocks













"IT'S A 2"

R
aces

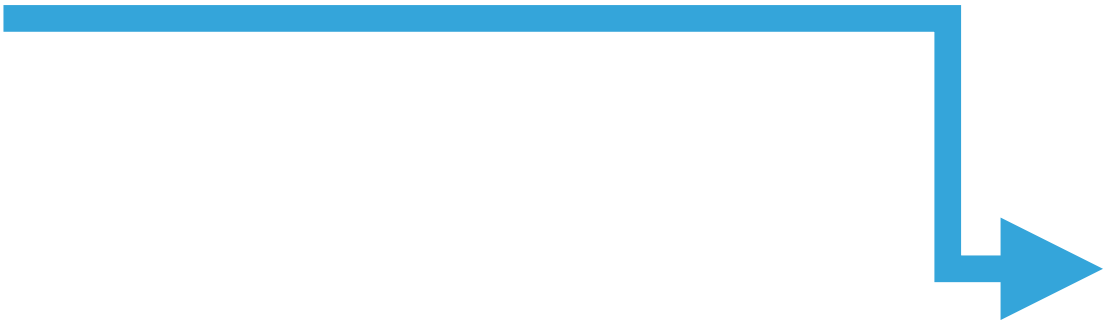
"IT'S A 3"

"IT'S A 1"

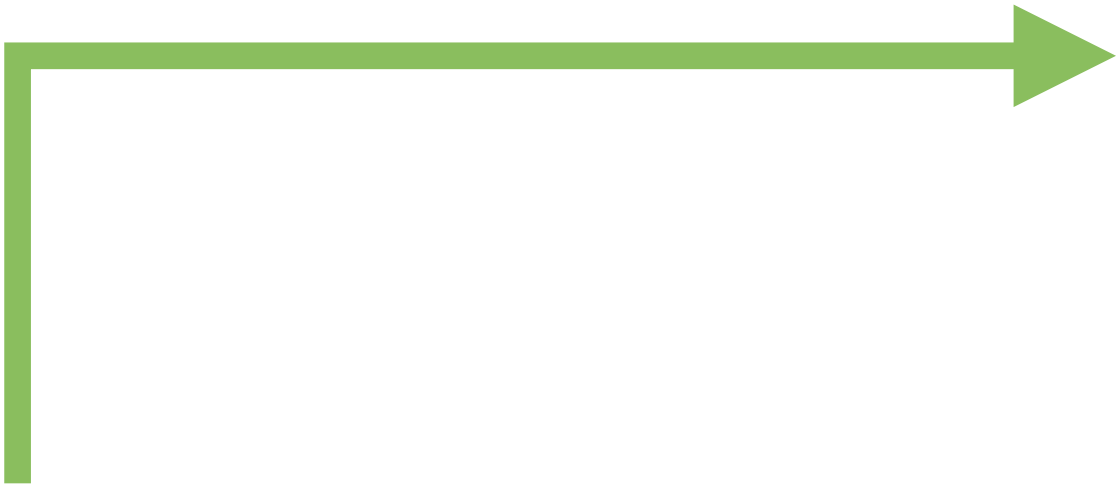
SECRET ("3")

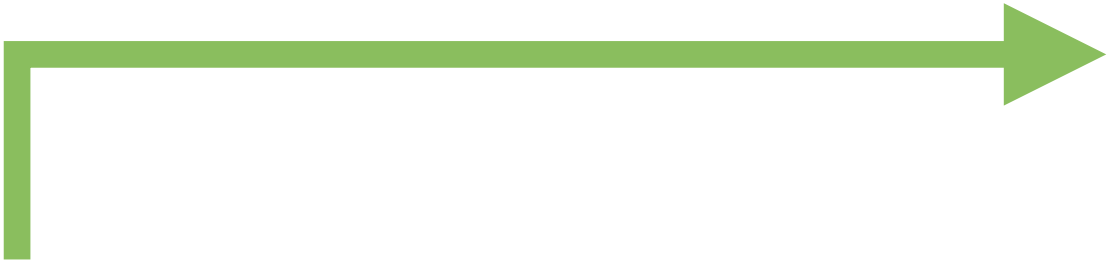




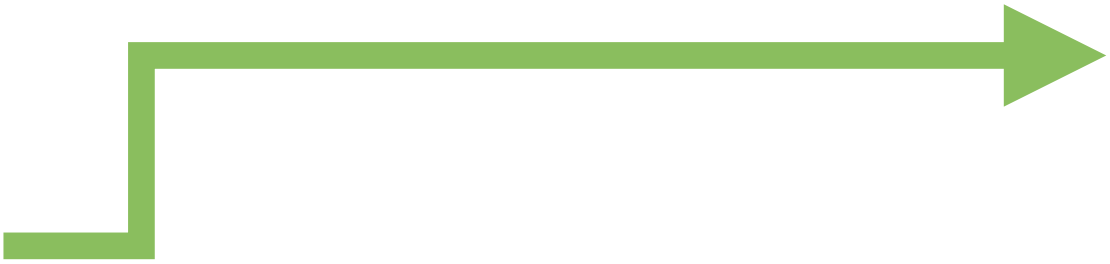








"IT'S A 2"













MELTDOWN: THE SIDECCHANNEL (IDEA)



-  **Spy** will read the **secret**
-  Depending on the **value**, **Spy** will mark a grey block
-  CPU detects **Spys** access validation and terminates **Spy**
-  **Collector** now looks for **Spys** mark in all grey blocks

MELTDOWN: THE ATTACK

110011010
010111010
111100100
000101101
100110010

Spy

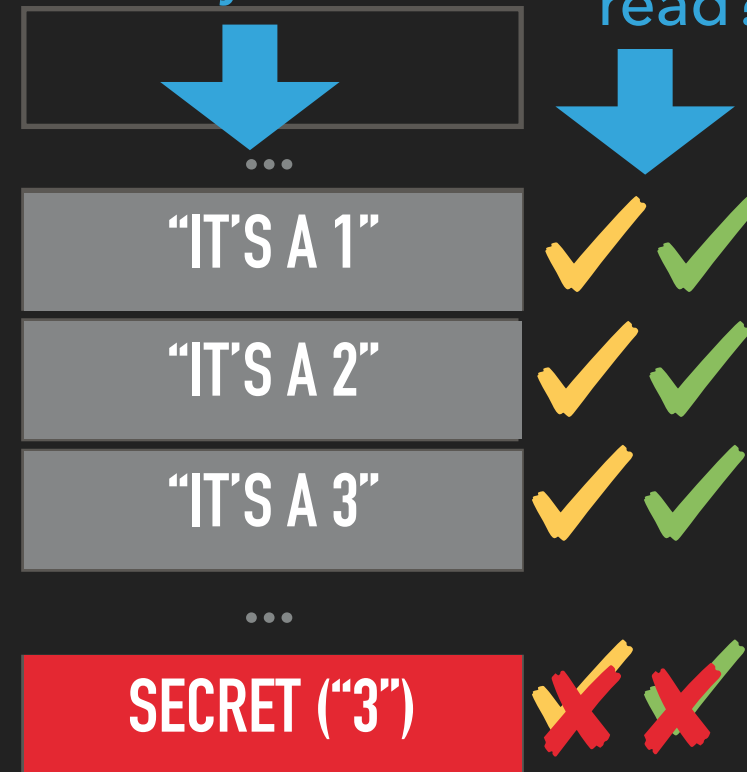
110011010
010111010
111100100
000101101
100110010

Collector



grey box:
memory block
tested by **Collector**

allowed to
read?



- ▶ Meltdown needs some preconditions
- ▶ The **secret** is in the cache (value: 3)
- ▶ Both **Spy** and **Collector** can read grey memory blocks