

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



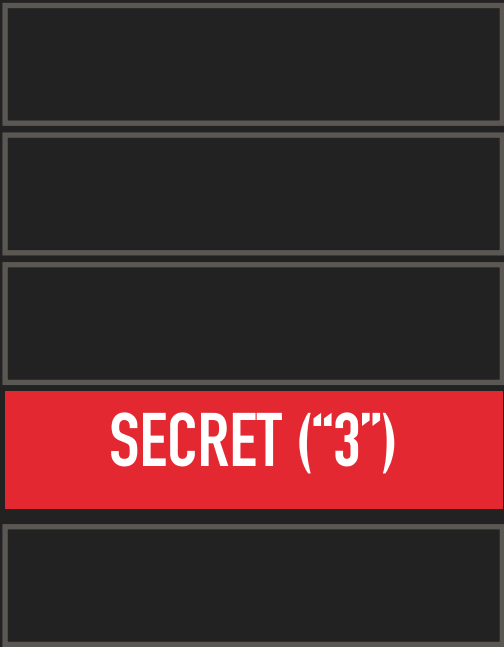
MELTDOWN: THE ATTACK

110011010
010111010
111100100
000101101
100110010

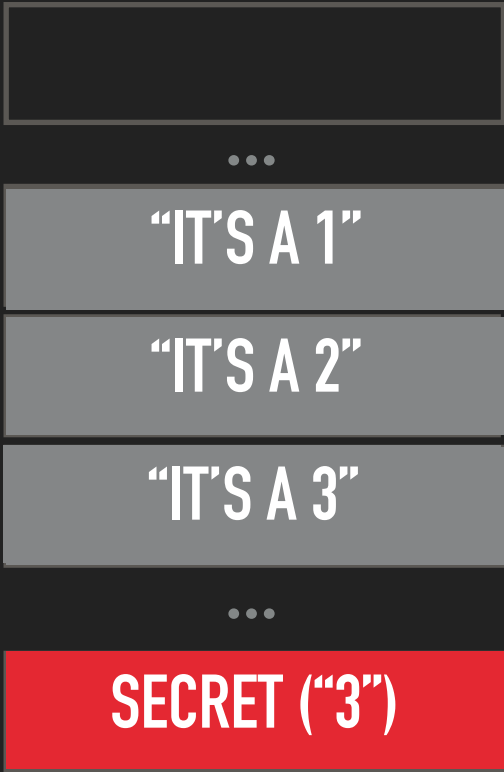
Spy

110011010
010111010
111100100
000101101
100110010

Collector



Cache



RAM