



Spectre Attack

Agenda

- Theoretical intro

 - Processor & memory structure

 - Speculative execution

 - Timing attack

- Attack demonstration

- Code explanation

- Outcome

 - Other attacks

 - Solution finding and despair

Processor & Memory Structure

Processor

CPU cache

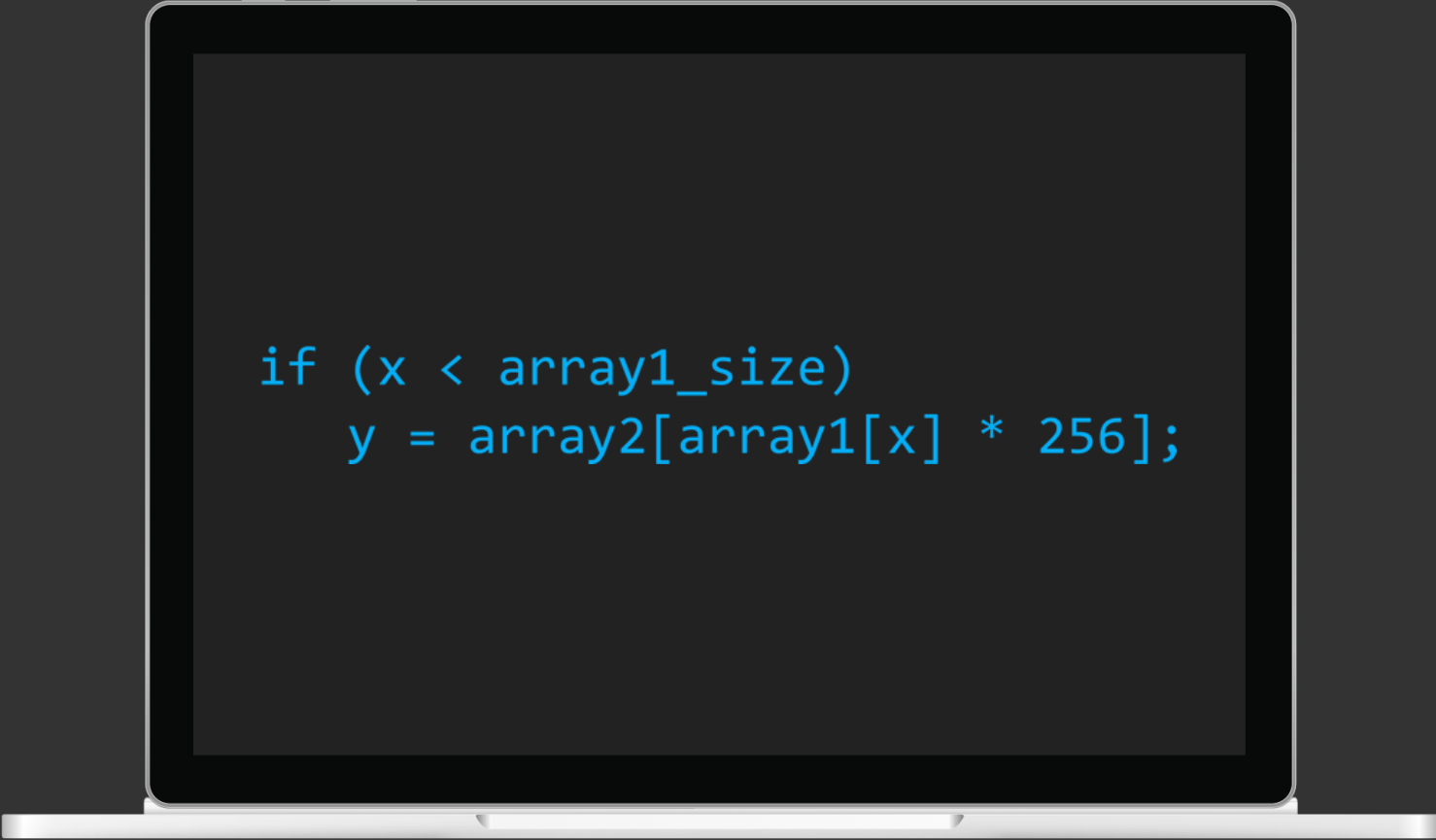
RAM

Disk (HDD, SSD, flash)

Memory Speed

operation	time, ns
execute typical instruction	1.0
fetch from L1 cache memory	0.5
branch misprediction	5
fetch from L2 cache memory	7
mutex lock/unclock	25
fetch from main memory	100
send 2 KB over 1 Gbps network	20,000
read 1 MB sequentially from main memory	250,000
fetch from new disk location (seek)	8,000,000
read 1 MB sequentially from disk	20,000,000
send packet from US to Europe and back	150,000,000

Speculative Execution

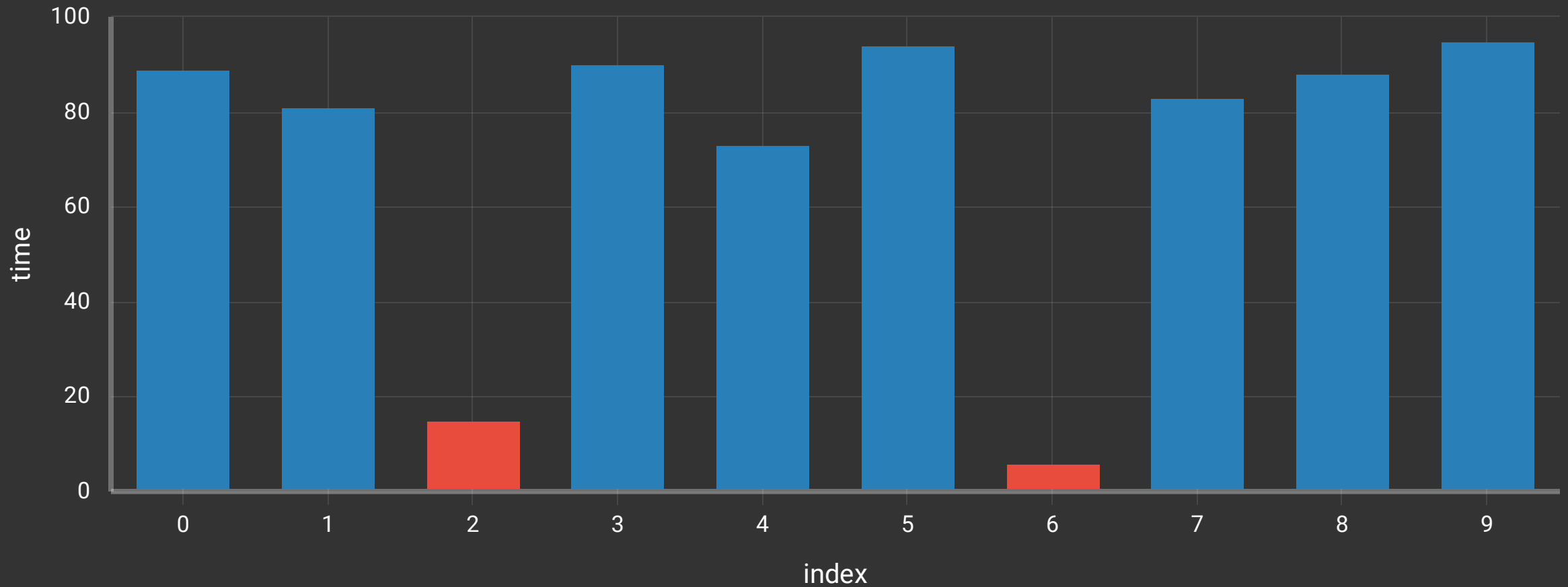
A laptop is shown from a front-facing perspective, slightly angled to the left. The screen is dark and displays two lines of code in a light blue font. The code is an if-statement that checks if 'x' is less than 'array1_size'. If true, it assigns a value to 'y' based on 'array1[x]' multiplied by 256, then accesses 'array2' at that index. The laptop has a silver bezel and a dark base.

```
if (x < array1_size)
    y = array2[array1[x] * 256];
```

- Do not wait for condition check
- Execute code out of order
- Save or discard result depending on condition
- Everything is fine, but...

Timing Attack

HIT MISS



Attack Basis



If you want a guarantee,
buy a toaster

Clint Eastwood