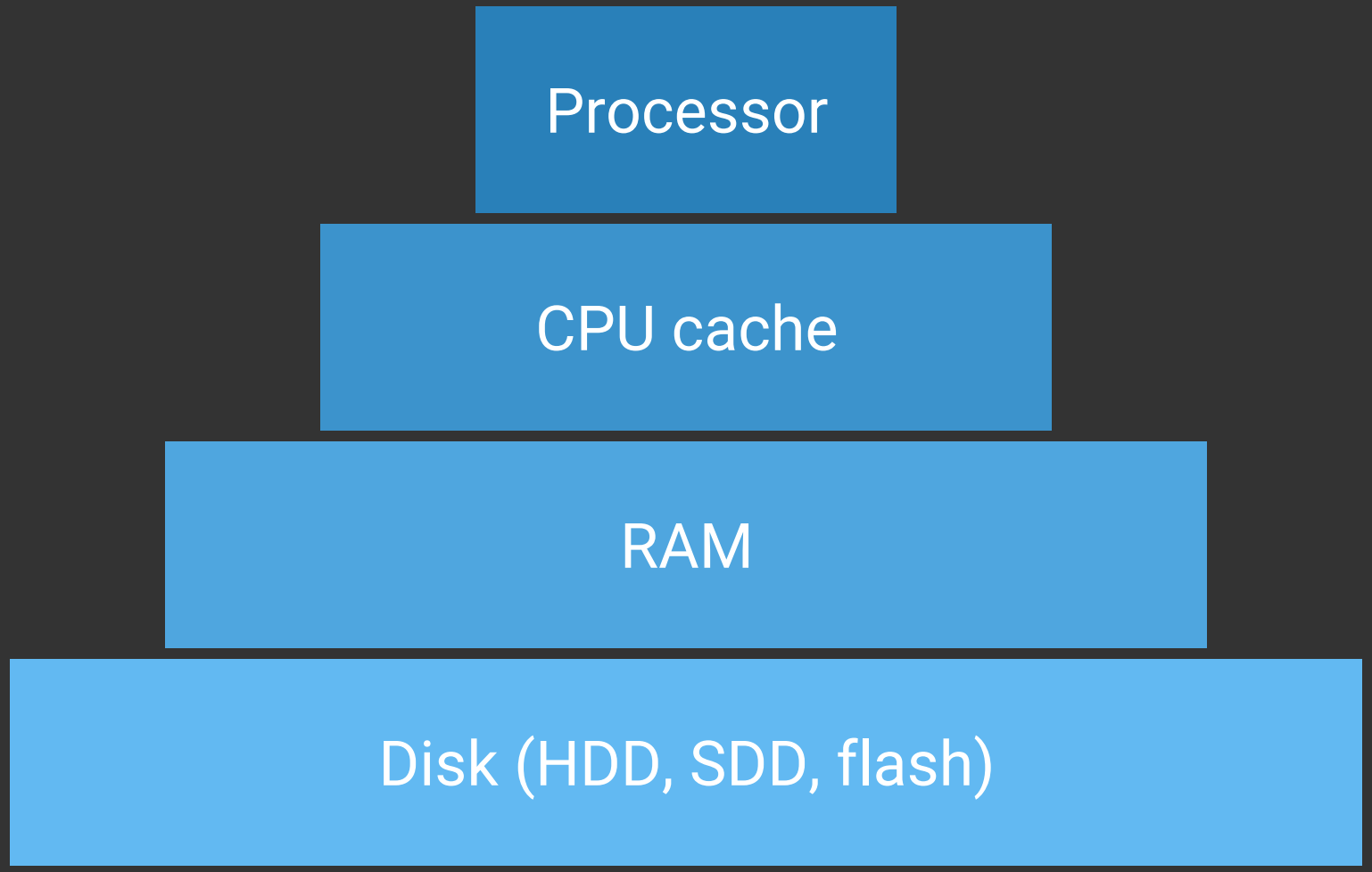
Spectre Attack

Agenda

- Theoretical intro
  - Processor & memory structure
  - Speculative execution
  - Timing attack
- Attack demonstration
- Code explanation
- Outcome
  - Other attacks
  - Solution finding and despair

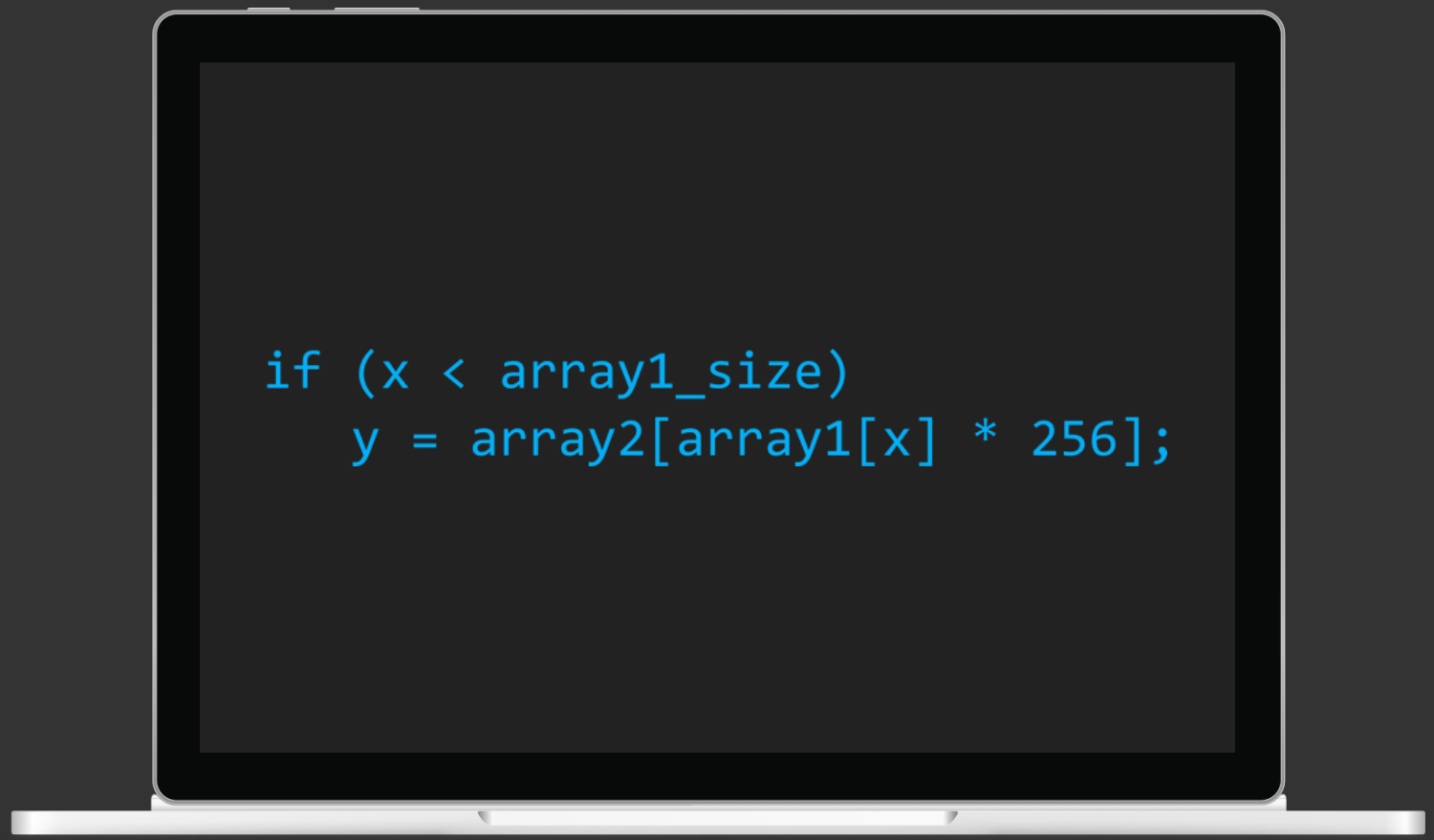
Processor & Memory Structure



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 form memory	250,000
fetch from new disk location (seek)	8,000,000
read 1 MB sequentially form disk	20,000,000
send packet US to Europe and back	150,000,000

Speculative Execution



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

Timing Attack

If you want a guarantee, buy a toaster

Clint Eastwood