







MELTDOWN & SPECTRE FOR ARMV8 ARE PEOPLE

**MELTDOWN: STASHAWAY - SLEDGEHAMMER**

2

3







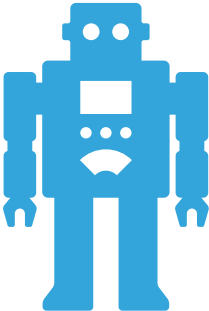












CPU core

RAM

- ▶ Data is stored in RAM
- ▶ RAM is very slow
- ▶ Reading one byte stalls the CPU for hundreds of  $\mu$ OPs



**Read**

**RAM**





**value**

**100ns**

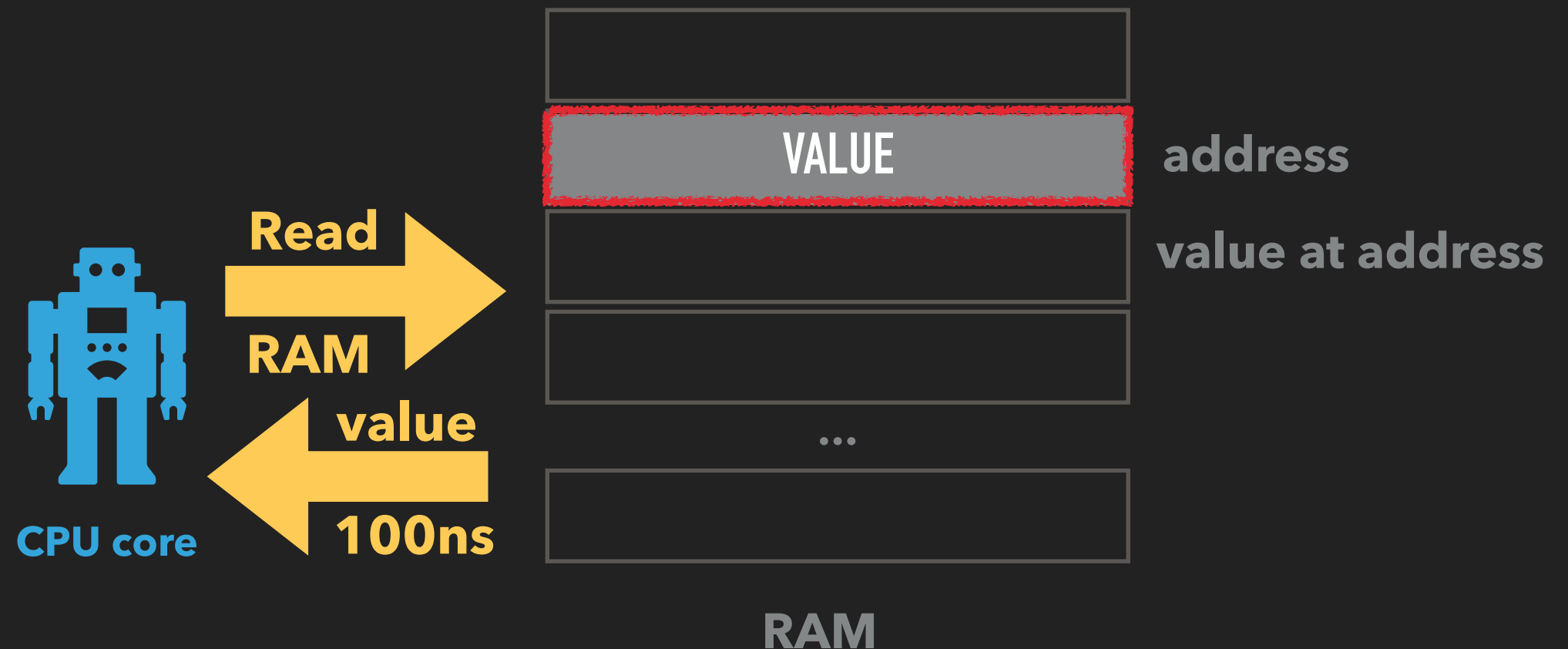
VALUE

value at address



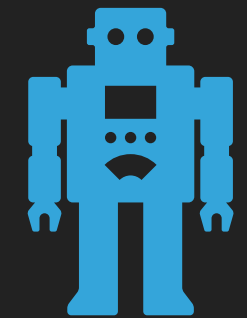
address

# MELTDOWN: STASHING AWAY – SIDECCHANNEL

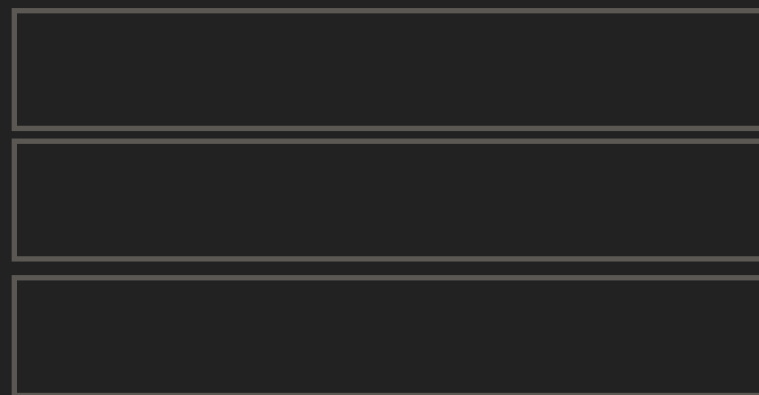


- ▶ Data is stored in RAM
- ▶ RAM is very slow
- ▶ Reading one byte stalls the CPU for hundreds of  $\mu$ OPs

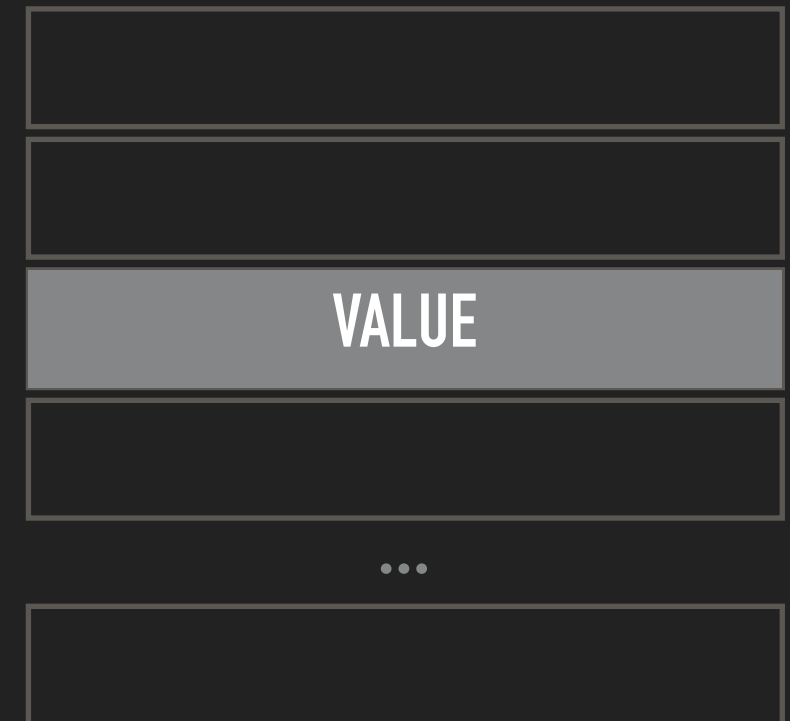
# MELTDOWN: STASHING AWAY – SIDECCHANNEL



CPU core



Cache



RAM

- ▶ Reading one byte stalls the CPU for hundreds of  $\mu$ OPs
- ▶ CPU caches considerably speed this up
- ▶ E.g. reading cached takes 3ns, reading uncached 103ns

The cache speeds up "what is the value at address X?". This is called "(address) X is cached"