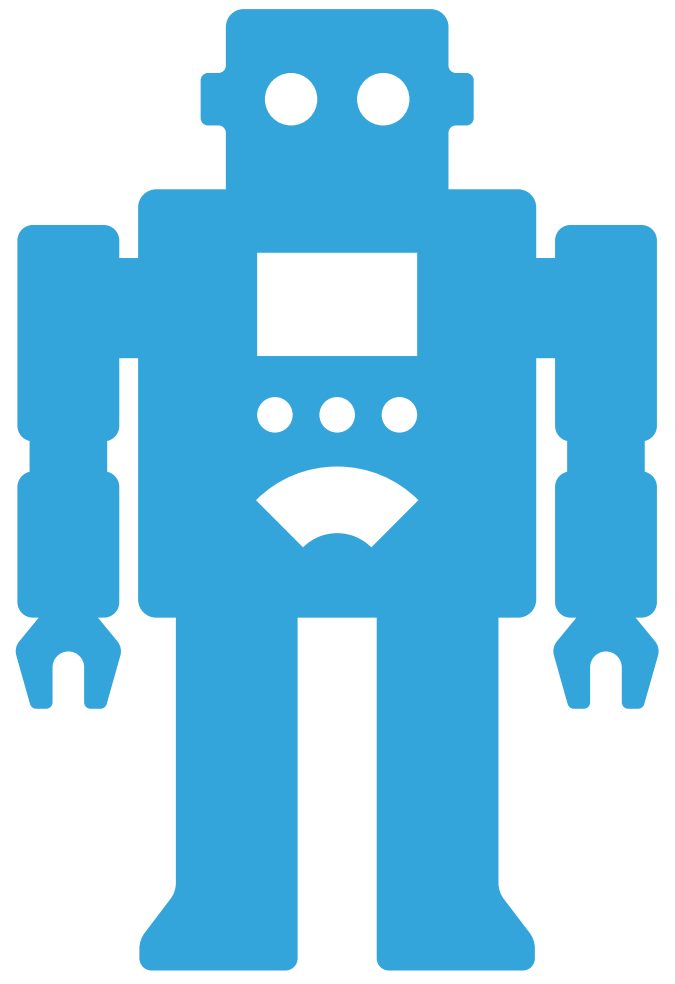
MELTDOWN & SPECTRE FOR NORMAL PEOPLE

MELTDOWN: STASHING AWAY – SIDECHANNEL

31



CPU core


RAM

- Data is stored in RAM
- RAM is very slow
- Reading one byte stalls the CPU for hundreds of µOPs

Read
RAM

value
100ns

VALUE

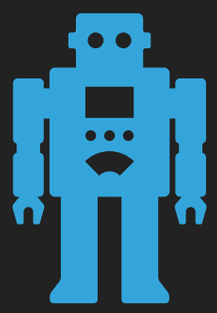
value at address

address

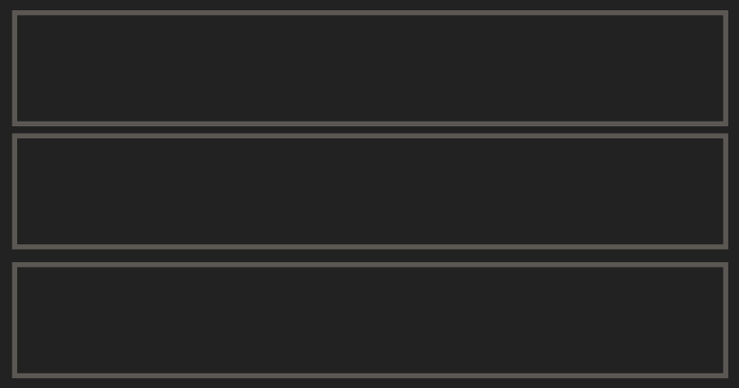
MELTDOWN: STASHING AWAY – SIDECHANNEL

- Data is stored in RAM
- RAM is very slow
- Reading one byte stalls the CPU for hundreds of µOPs

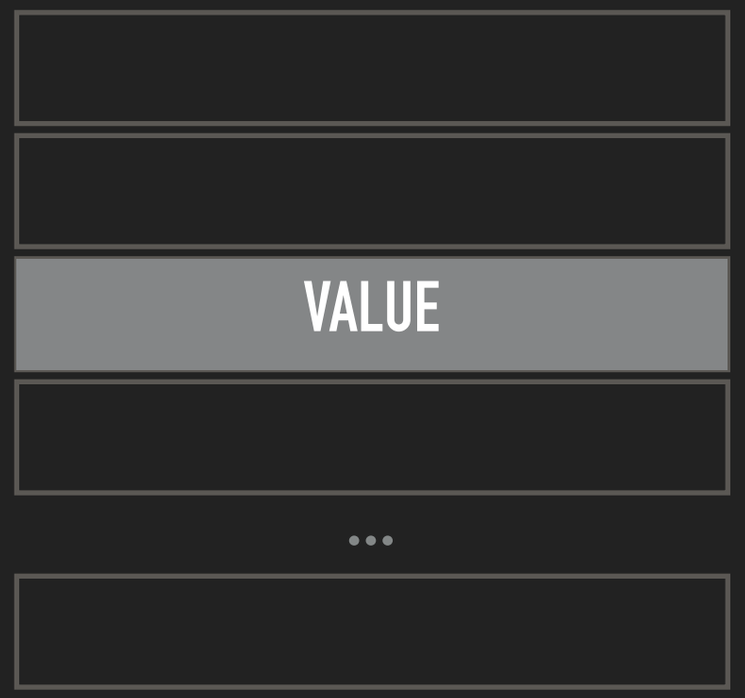
MELTDOWN: STASHING AWAY – SIDECHANNEL



CPU core



Cache



RAM

- Reading one byte stalls the CPU for hundreds of µOPs
- 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"*