"Stashing" and "retrieving" the secret works via *side channels*.

Side channels are *observable side effects* of actions.

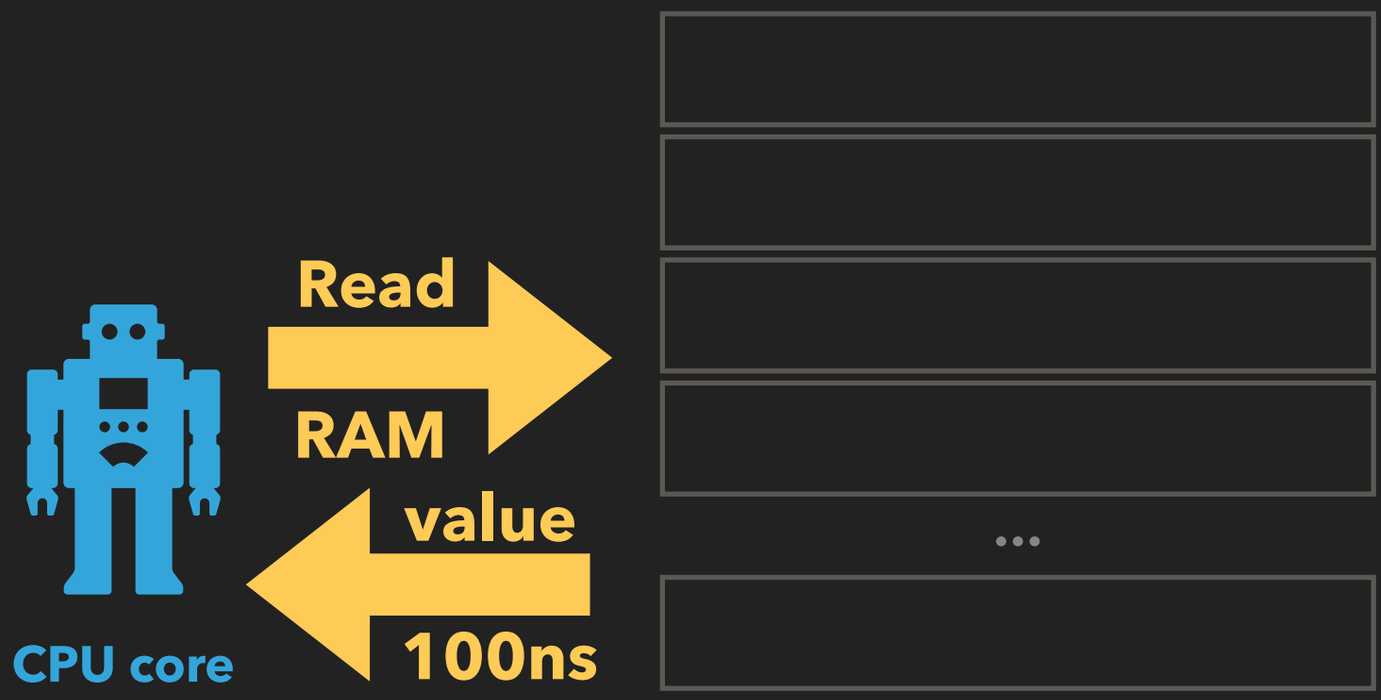
1. READ secret from forbidden address
2. Stash away secret by caching a memory location that depends on the secret
3. Retrieve secret by finding which memory location is cached

MELTDOWN & SPECTRE FOR NORMAL PEOPLE

MELTDOWN

23

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" and "retrieving" the secret works via *side channels*.

Side channels are *observable side effects* of actions.

- READ secret from forbidden address
- Stash away secret by caching a memory location that depends on the secret
- Retrieve secret by finding which memory location is cached