



MELTDOWN & SPECTRE FOR NORMAL PEOPLE

SPECTRE: SPECULATIVE EXECUTION

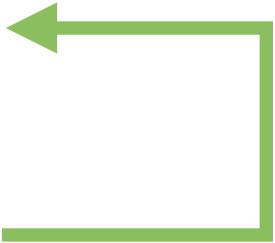














The CPU has learned that Counter probably is > 0

Reading Counter from memory is very slow

The CPU speculatively executes to improve performance



Counter





Counter > 0?



SPECTRE: SPECULATIVE EXECUTION A B C

Counter



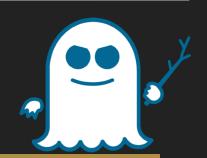
The CPU has learned that Counter probably is > 0

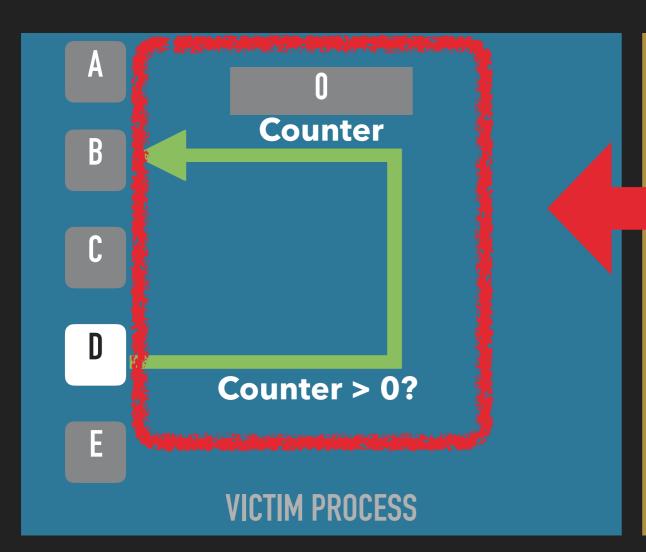
Counter > 0?

Reading Counter from memory is very slow

The CPU *speculatively* executes B to improve performance

SPECTRE: SPECULATIVE EXECUTION





- 1. Prime the branch prediction to expect a loop
- 2. Make sure Counter is not cached so the CPU is more likely to speculatively run the code
- 3. Find a way victim leaks data when B &C are executed speculatively

ATTACKER PROCESS

Attacker can influence the CPUs branch prediction of victim.

Making the victim speculatively execute "wrong" code.

E.g. loop even when Counter is == 0.