



## MELTDOWN & SPECTRE FOR NORMAL PEOPLE

## SPECTRE: SPECULATIVE EXECUTION

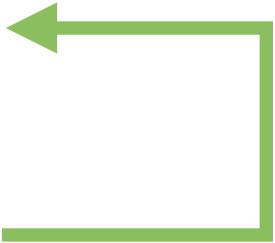








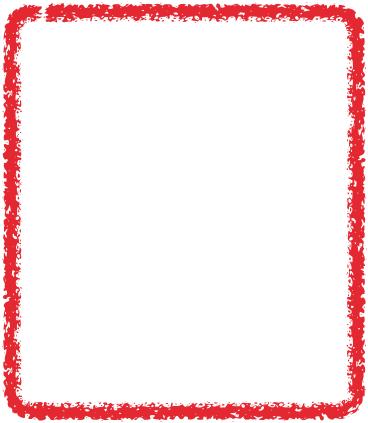






Attacker can influence the CPUs branch prediction of victim. Making the victim *speculatively* execute "wrong" code. E.g. loop even when Counter is == 0.

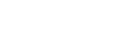










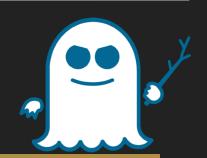


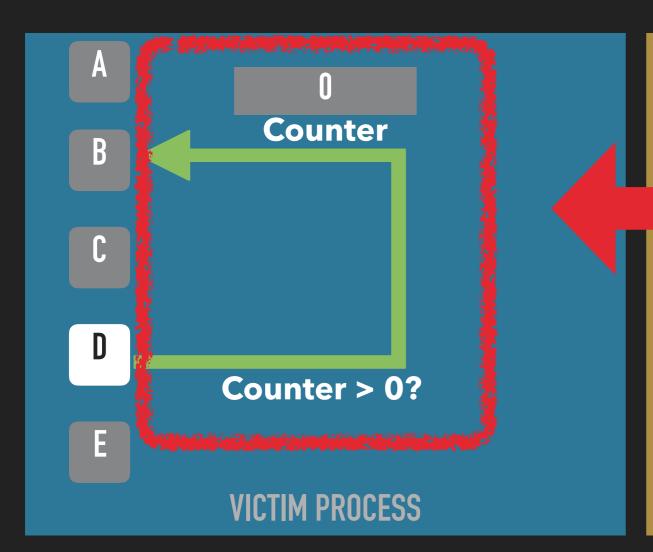
## **SPECTRE: VARIANT 1 (CVE-2017-5753)**



- This is code of the victim
- x is controlled by the attacker
- attacker wants to read array1[x] out of bounds
- array2 is used to leak the value of y (like in Meltdown)

## **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 that 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.