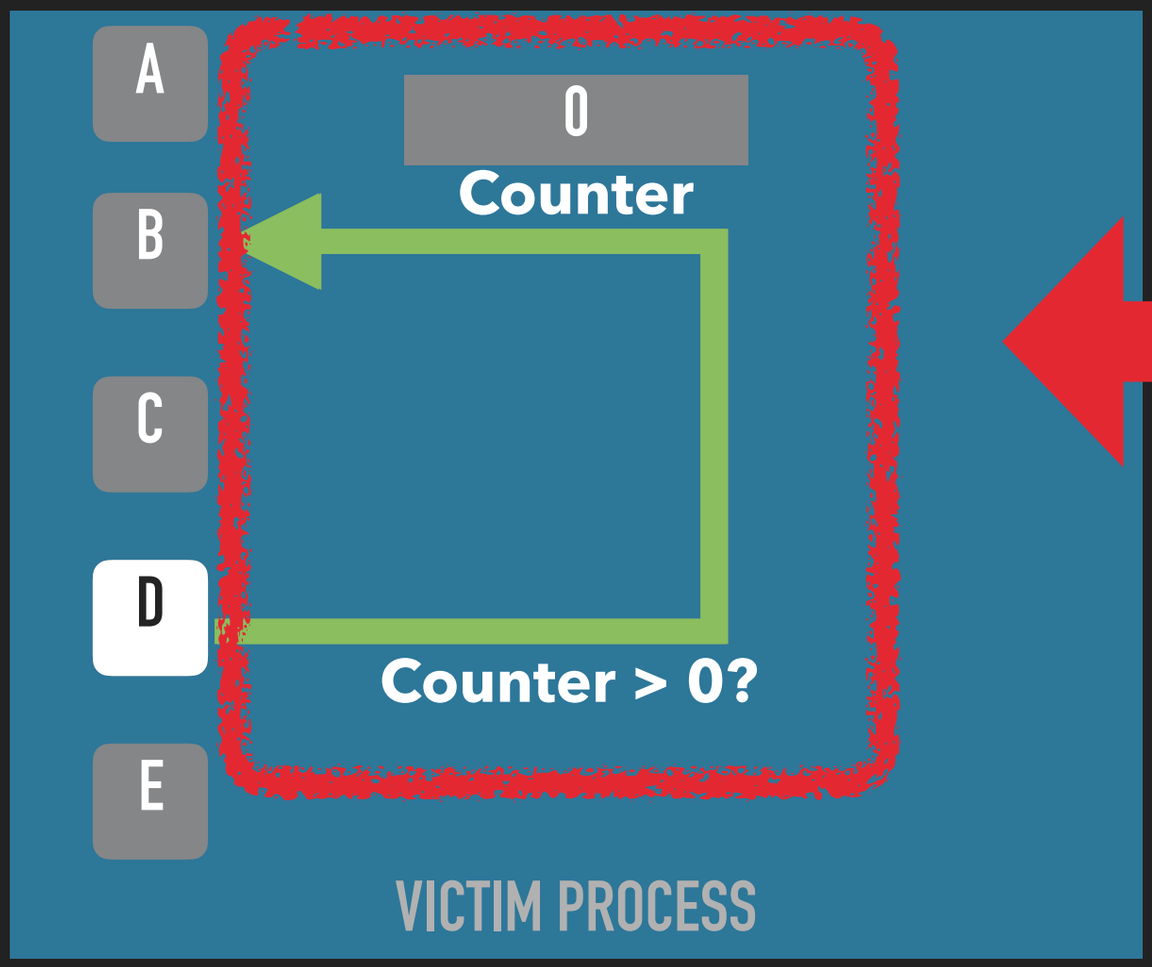
SPECTRE: SPECULATIVE EXECUTION



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**

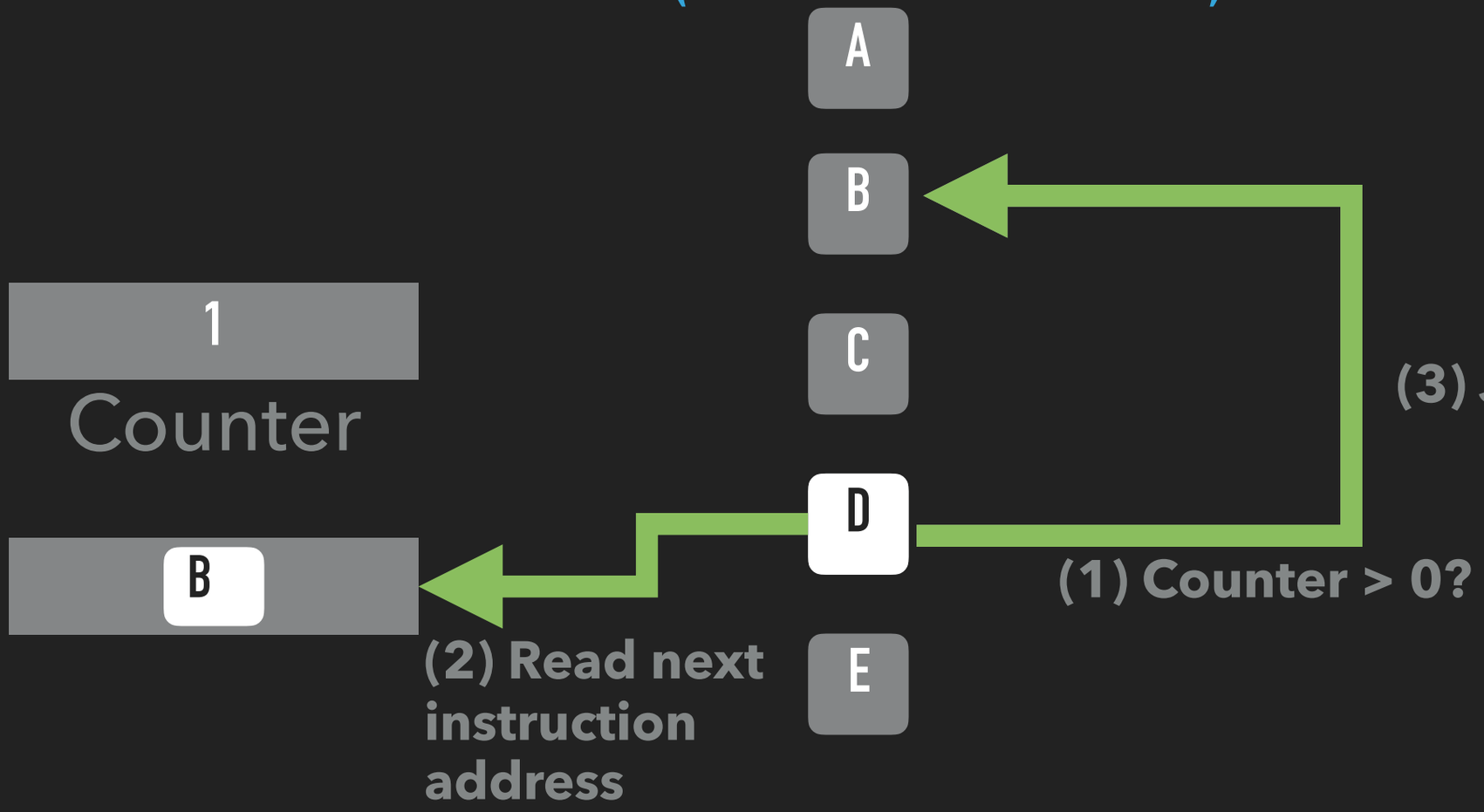
ATTACKER PROCESS

Attacker can influence the CPUs branch prediction of victim.

Making the victim *speculatively* execute “wrong” code.

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

SPECTRE: VARIANT 2 (CVE-2017-5715)



- The conditional jump (branch) D now is an *indirect jump*.
- Indirect jumps use addresses stored "somewhere else".
- This can also be used to *speculatively* execute any code found in the target process (kernel).