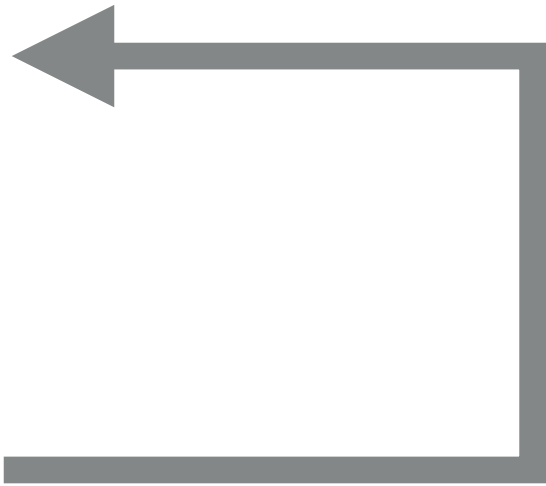
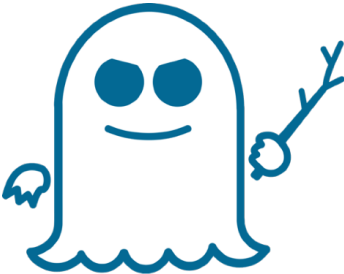






**VICTIM PROCESS**







**SPECTRE: SPECTACULAR EXERCUTION**

48



A

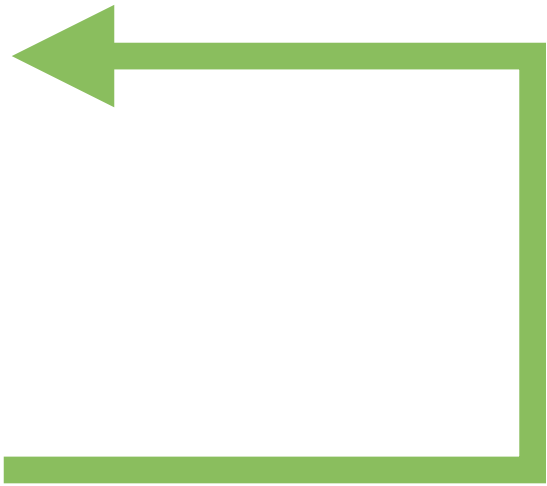
B



c

D

E



D

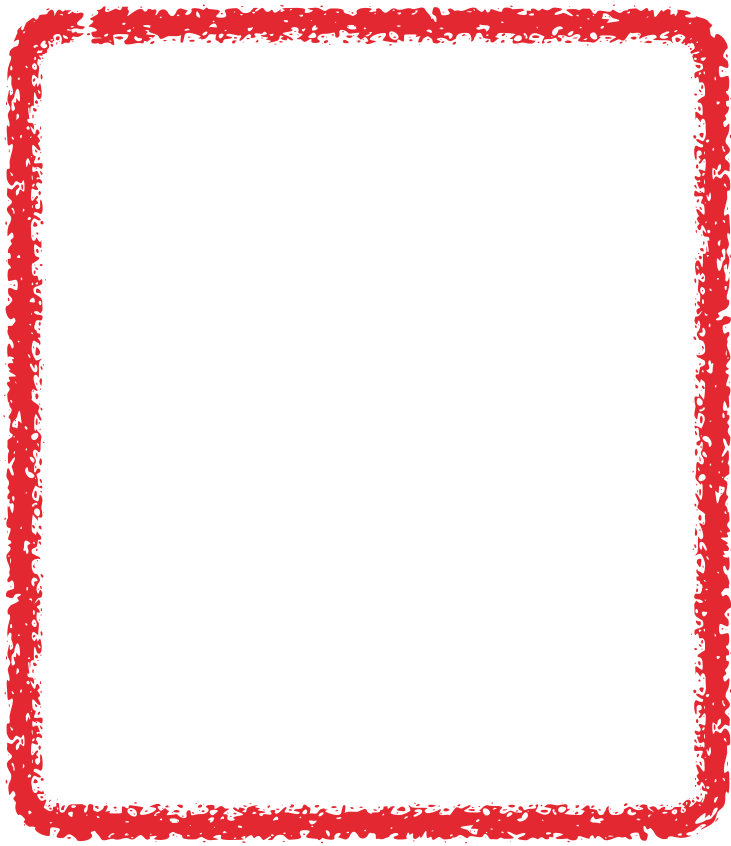
Attacker can influence the CPUs branch prediction of victim.

Making the victim *speculatively* execute "wrong" code.

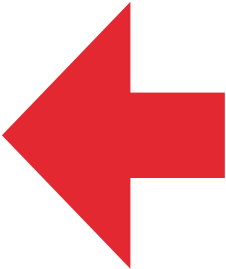
E.g. loop even when Counter is `== 0`.







**ATTACKER PROCESS**



0





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

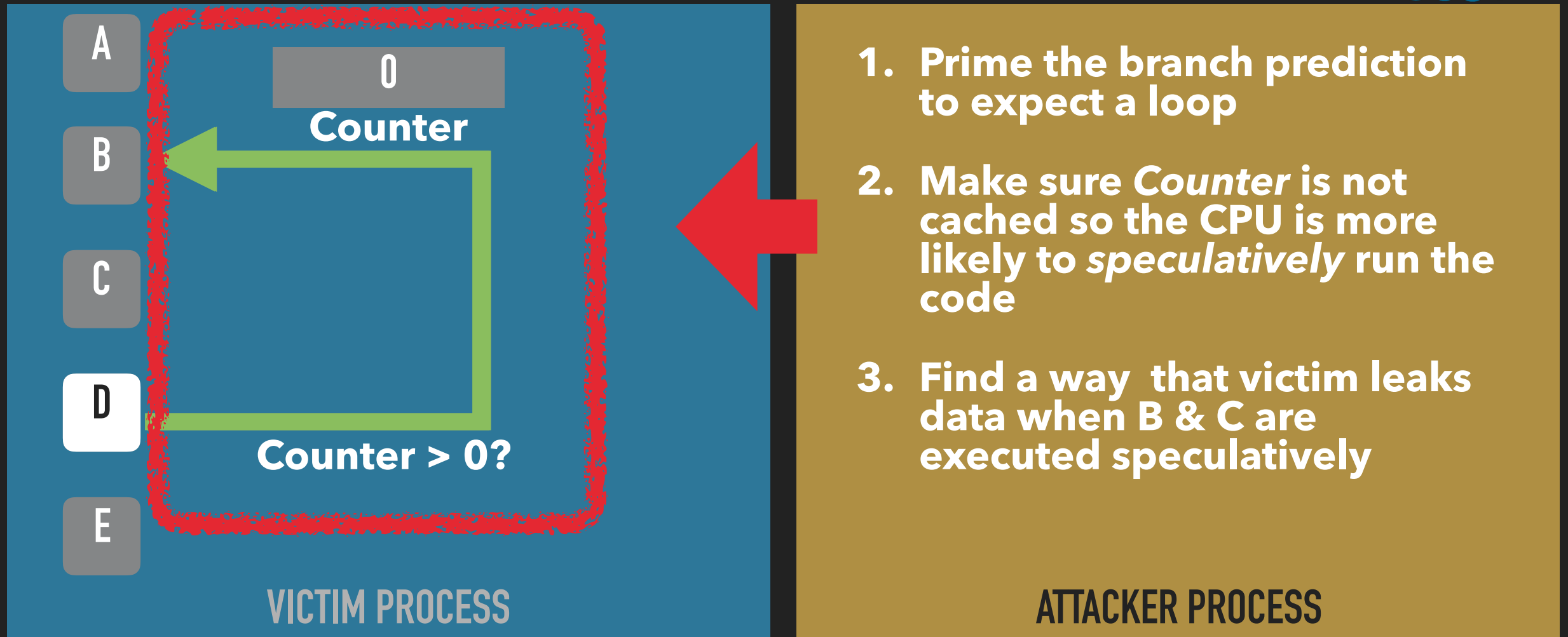


```
if (x < array1_size)
    y = array2[array1[x] * 256];
```

- ▶ 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



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