



SPECTRE: VARIANT 2 (CVE-2017-5715)

42

A

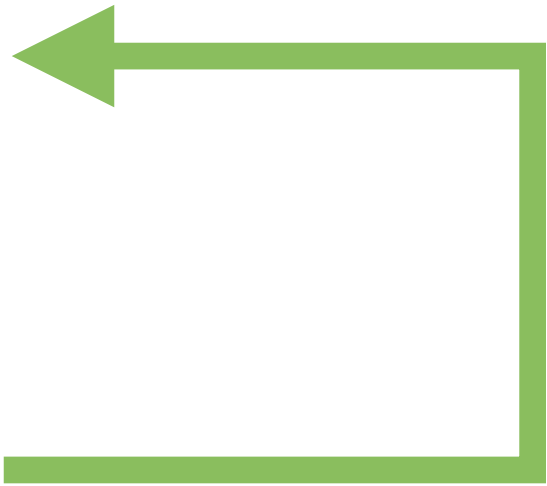
B



c

D

E



D

► The conditional jump (branch) `nbw` 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).



3



counter

2

1

(1) counter > 0?

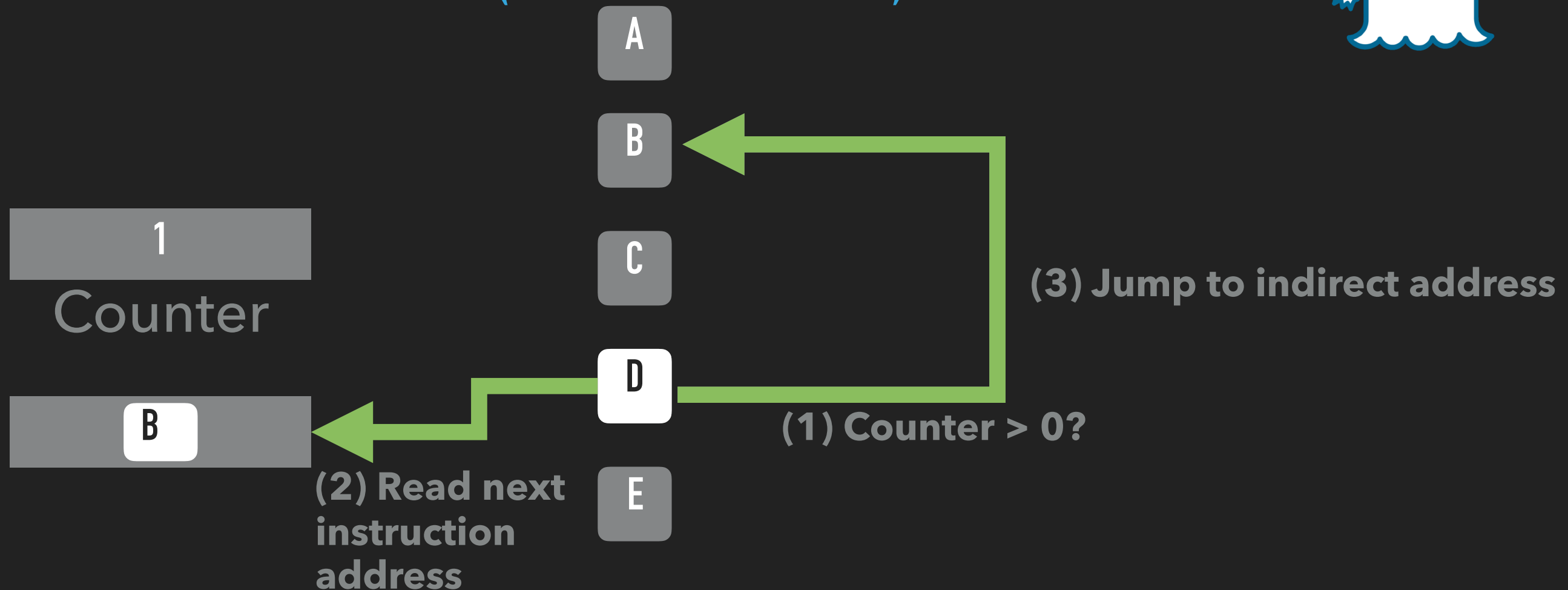
B

**(2) Read next
instruction
address**

(3) Jump to indirect address

D

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).



MELTDOWN AND
SPECTRE

CONCLUSION