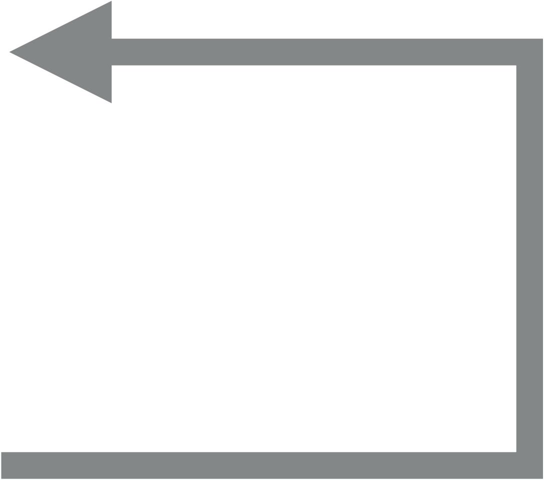
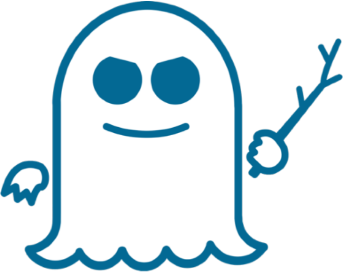




SPECTRE: VARIANT 2 (CVE-2017-5715)

43

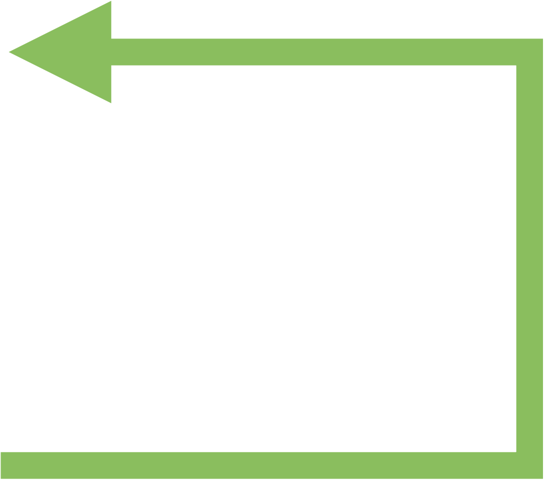
A

B

C

D

E

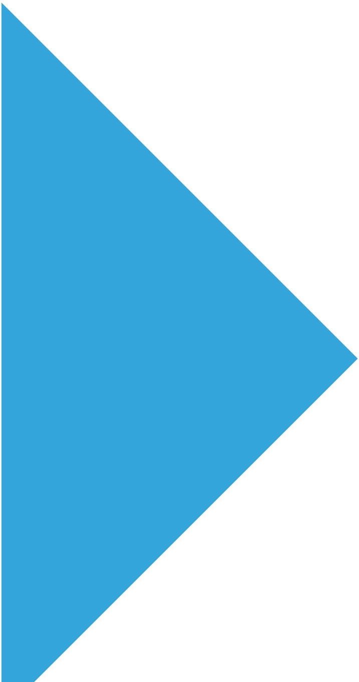


D

- The conditional jump (branch) 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).



3

Counter

2

1

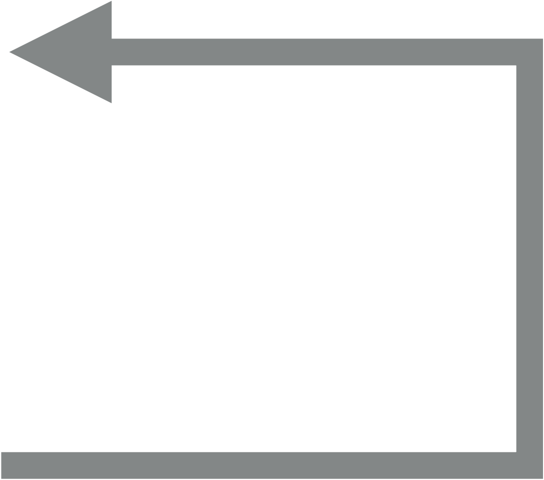
(1) Counter > 0?

B

(2) Read next instruction address

(3) Jump to indirect address

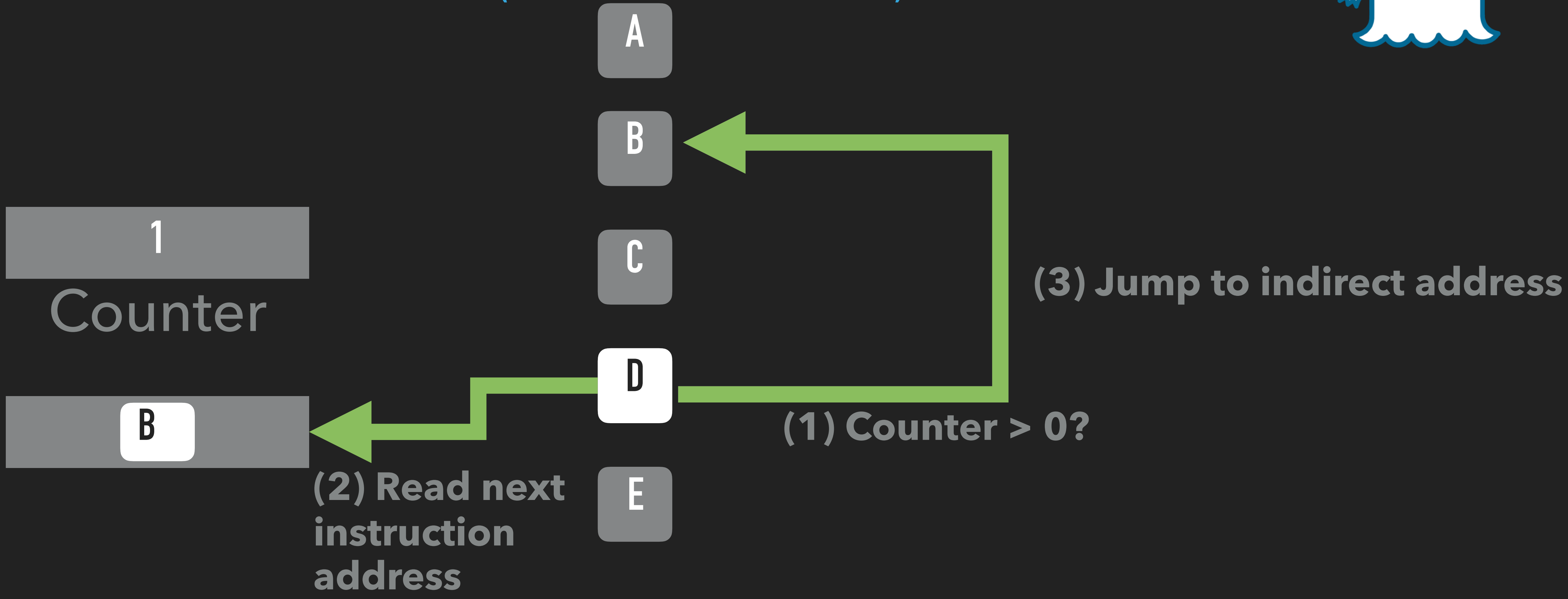
D



𝄞 ♫ INTERLUDE ♫

MEMORY MODEL

SPECTRE: VARIANT 2 (CVE-2017-5715)


A
B
C
D
E
1
Counter
B
(1) Counter > 0?
(2) Read next instruction address
(3) Jump to indirect address

- 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).