SPECTRE: VARIANT 2 (CVE-2017-5715)

A

B

1

Counter

C

(3) Jump to indirect address

D

B

(1) Counter > 0?

(2) Read next instruction address

E
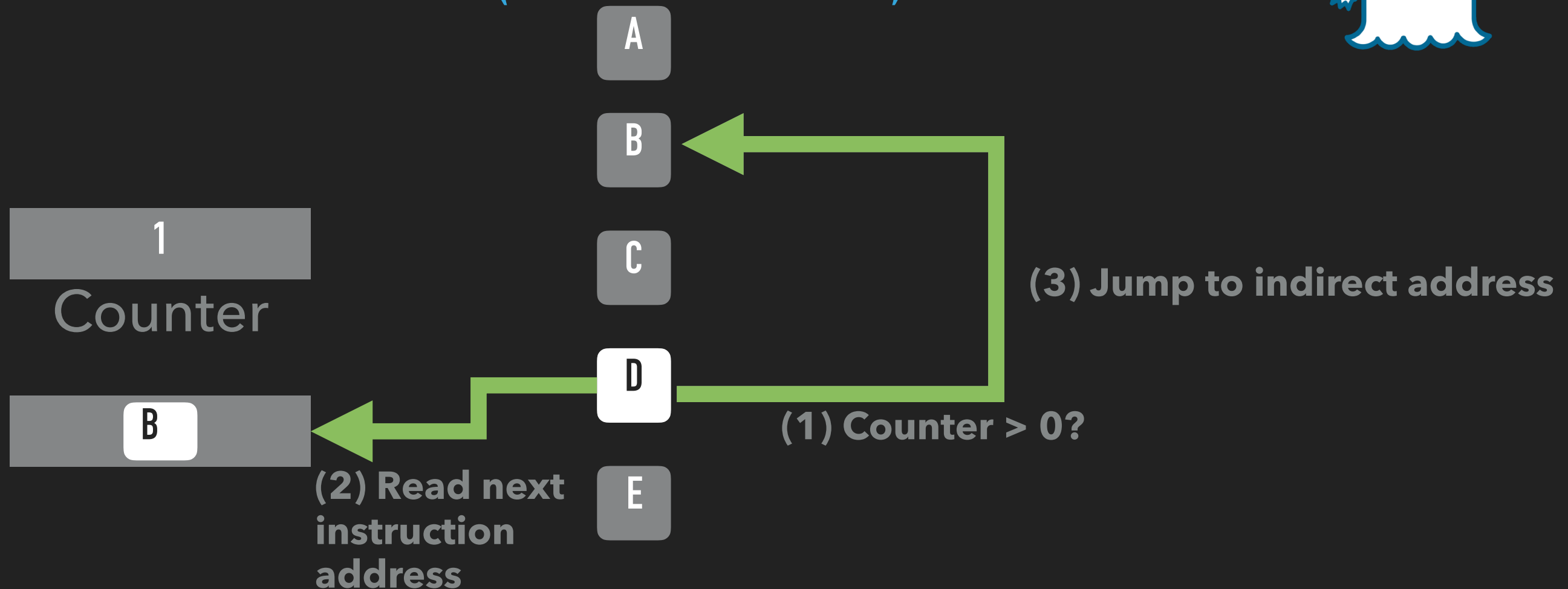
▸ The conditional jump (branch) D now is an *indirect jump*.

▸ 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