

Spectre attacks other processes by forcing them to
speculatively run other code paths

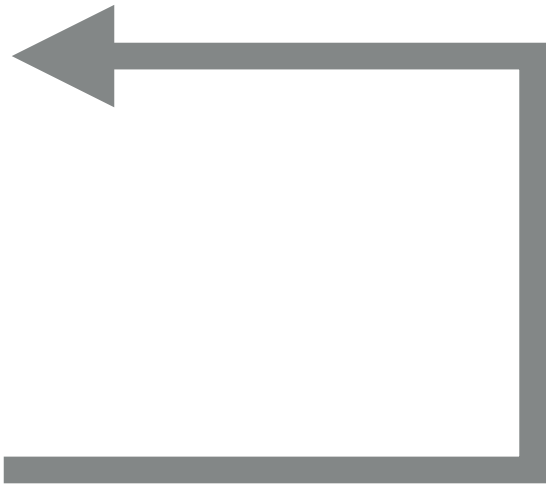


SPECTRE

3

5

VICTIM PROCESS



A

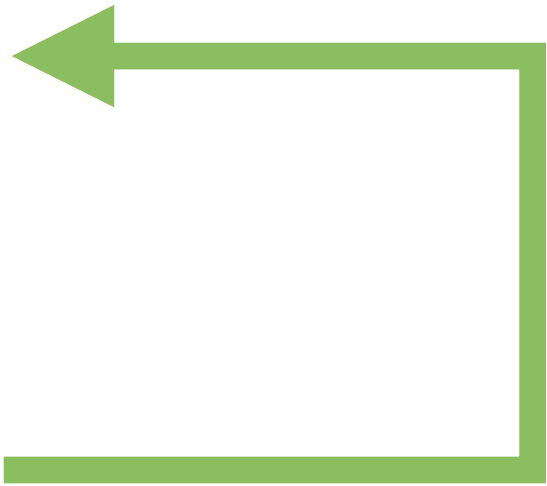
B



c

D

E

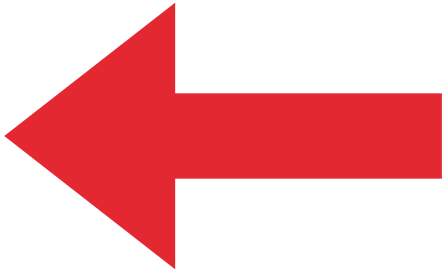


D

counter=0?






ATTACKER PROCESS



SPECTRE



Spectre works like this:

-  force victim to leak secret
-  stash away secret
-  retrieve secret

SPECTRE



Spectre attacks other processes by forcing them to *speculatively* run other code paths

