MELTDOWN & SPECTRE FOR NORMAL PEOPLE

MEMORY MODEL

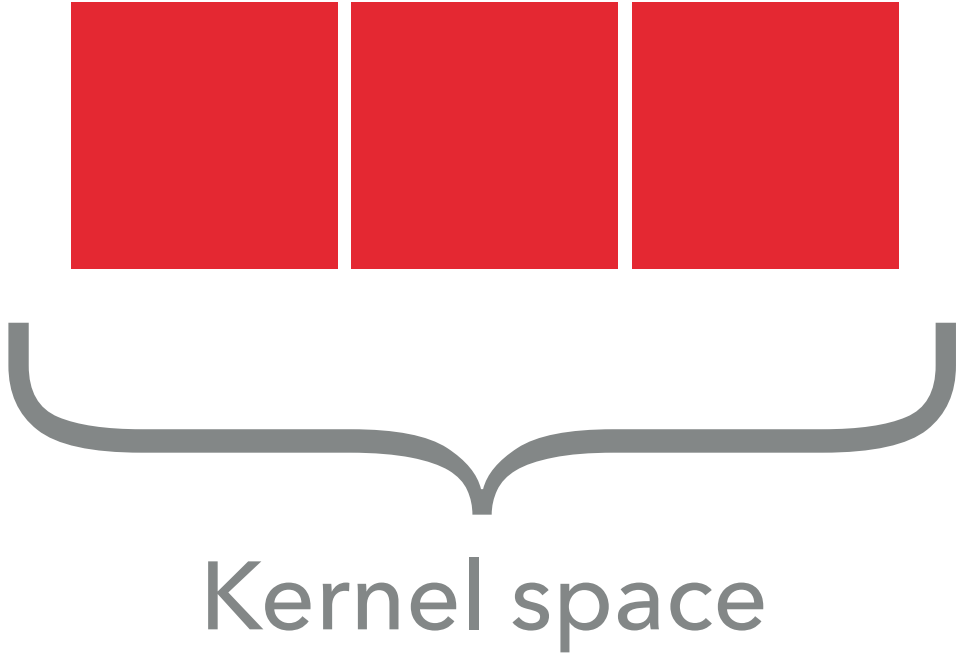

PROCESS
A

- Memory is split into *pages* (each 4KiB on x86)

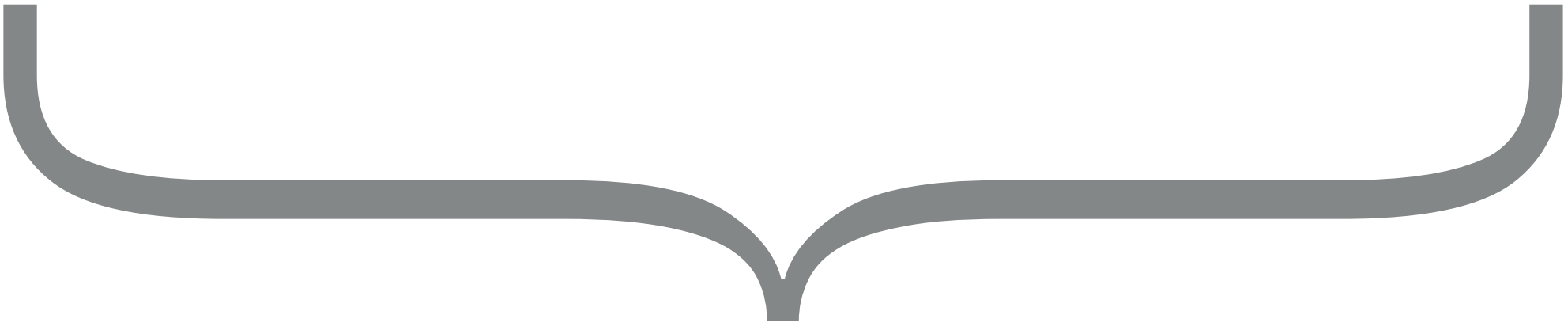
- The kernel *maps* its own memory into each process

- This “kernel” memory is only accessible by the kernel

User space


Kernel space


c)

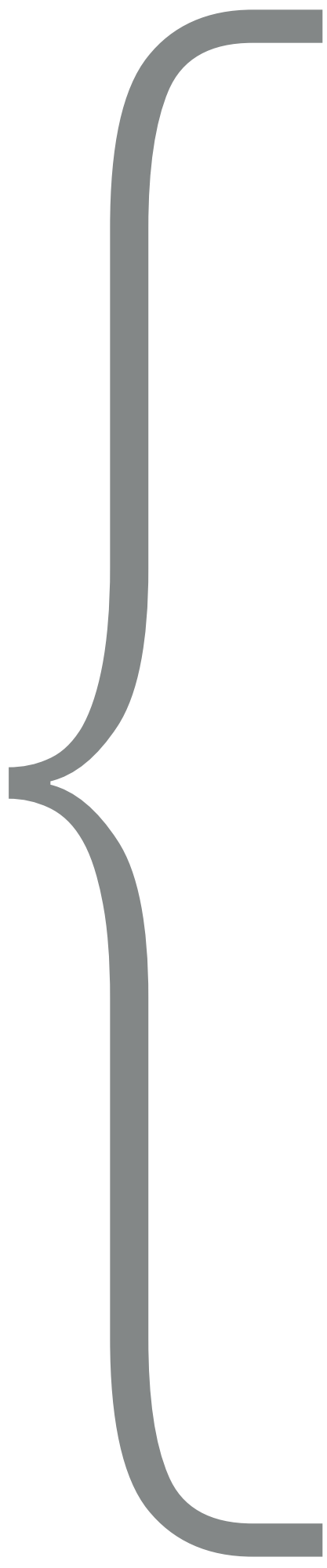


b) and c) are completely different error scenarios

process could try to access the pages via a pointer

- **b)** Process **B** has no possibility to even *describe* the address

- c) Kernel memory pages are marked “kernel only” but the



PROCESS


B

0x0000..0

b)

c)