



MELTDOWN & SPECTRE FOR ARMV8 ARE PEOPLE

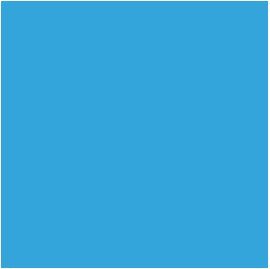
MEMORY MODEL

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









Userspace





Kernel space





MEMORY MODEL

b) and c) are completely different scenarios

process could try to access the pages via a printer

▶ c) Kernel modules are marked "kernel only" but the

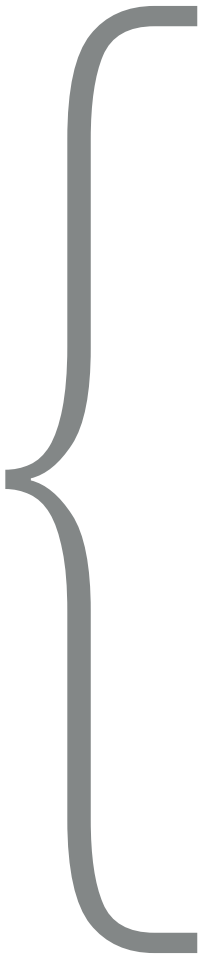
▶ **b)** Process **B** has no possibility to even *describe* the address











PROCES











OxOODOO.













