- System calls use special interrupt (INT 80 in x86)
- Arguments stored in registers in specified order
- Interrupt switches to kernel mode, and uses table to lookup kernel function which processes system call
- system call returns value in register `rax`
- return value in range between -4095 and -1 indicates error.

Kernel code for system calls:

- Have system call table in `arch/x86/syscalls`
- Used during kernel compilation process to generate array of system calls
- Assembly code for handling system calls is in `arch/x86/kernel/entry_64.S`
- Argument handling done via special `SYSCALL_DEFINE` macros

No sanity checks of arguments made in system call code
$\Rightarrow$ kernel function needs to make all sanity checks