

Week 2

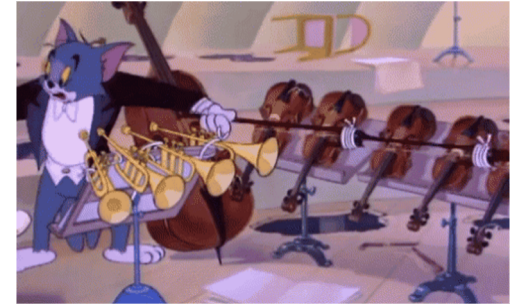
xv6 and System Calls

slides

- <https://github.com/jinlang226/CS537-discussion>

Review

What is context switching? When does it happen?

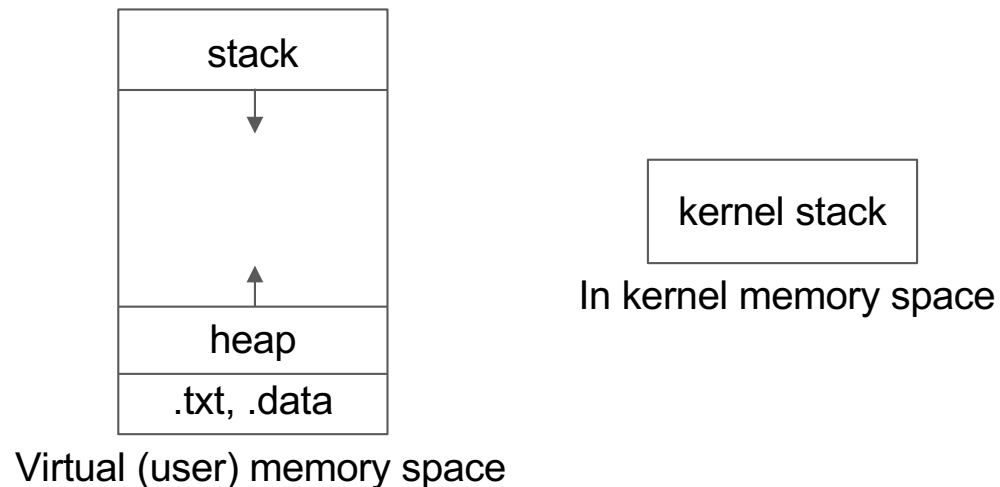


- Context switching happens if a new task will be scheduled when the current running one has not finished yet (preemption)
- It stores the current running context so that the preempted task can be resumed later
 - It saves the registers, memory maps, etc
- Used widely for multitasking (process / threads) and interrupt handling
 - Switching between kernel and user process (e.g., exception handling) does not necessarily incur a complete context switch

Review

What is the kernel stack?

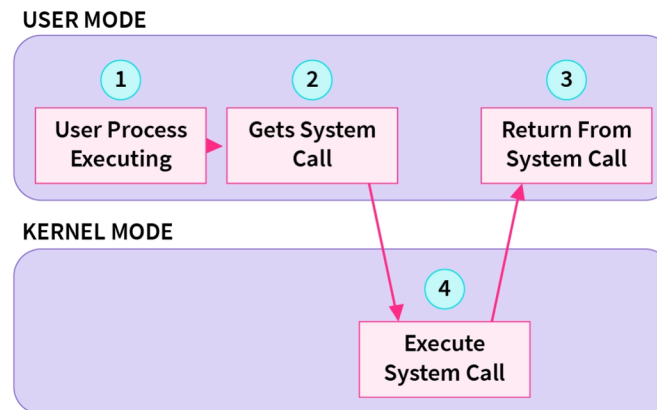
- A fix-sized memory region managed by kernel for each running process
- Used for the function call stack when running in kernel mode
- Stores registers from the userspace during system calls



System Calls

What is a system call?

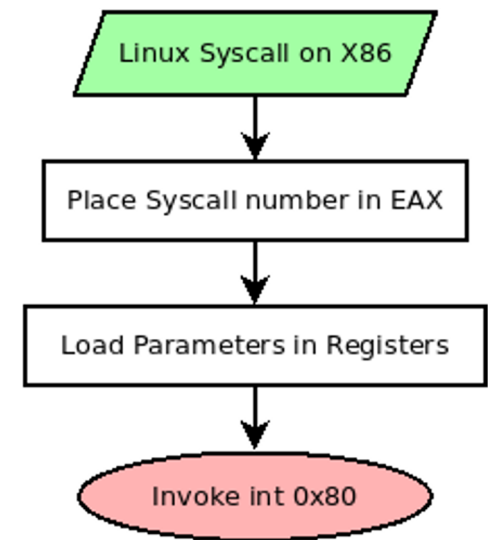
- Ways through which user programs request services from kernel
- Running processes will yield the CPU to kernel to fulfill the request (i.e. blocking / synchronous)
- E.g., getpid(), read() and write(), send() and recv(), fork(), etc.



System Calls

What is an interrupt?

- Event through which kernel is awaken
- Can be triggered by both hardware devices (disk, NIC, etc) and programs
- An interrupt number is passed to kernel to indicate the reason for interrupt
- Used to implement system calls in many operating systems
 - Linux and xv6 (on x86 architecture) uses `int 0x80` for system calls
- Trap vs Interrupt:
 - Trap is a different event used to implement system calls in older OS
 - The term is kept to refer to software-generated events
 - This include system calls and exceptions
 - Trap are often synchronous, while interrupts are mostly asynchronous



System Calls

What is the trap function?

- Kernel function that handles trap (also called trap handler)
- It checks the trap number to decide what to do

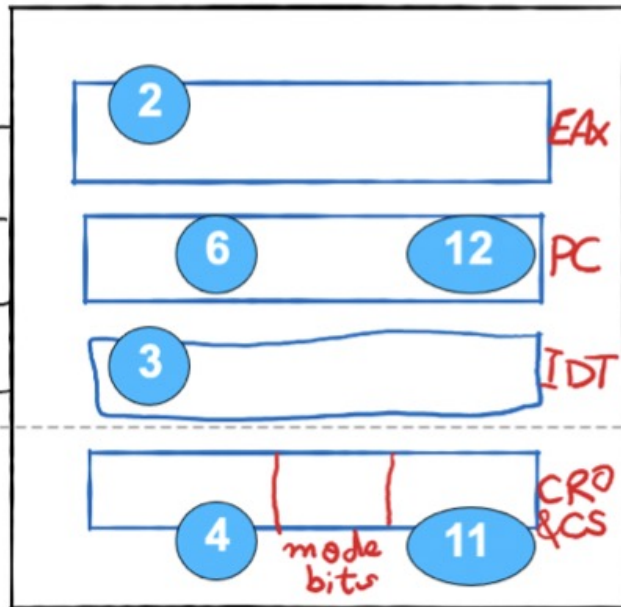
Note: In xv6 (and many other OS), the trap handler handles more than just traps: it also handles some hardware interrupts like timer interrupts.

System Calls

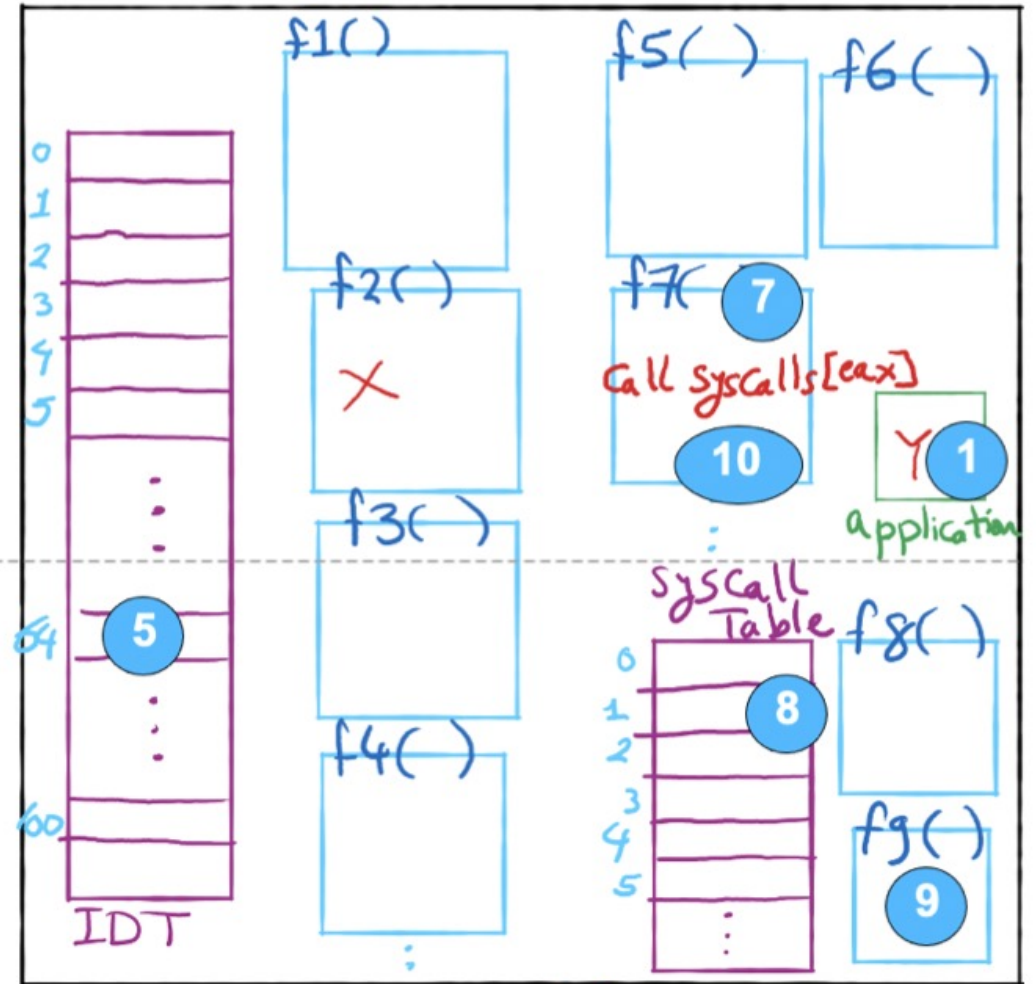
What is a system call table?

- Mapping from the system call number to the corresponding handler

keyboard 1
Hard disk 2
Network Card 3
Web Camera 4



CPU



Memory

xv6 Demo