System calls

- What’s the exact process from user back to user?

  `451shell% physusage`

- In shell:

  ```
  ...
  syscall(__NR_physusage, ...)
  ...
  ```
System calls, cont’d

- In assembly:
  
  ```
  int $0x01
  ```

- Says: switch to kernel and tell it to call system call 01

- Kernel needs mapping from syscall number to backing C function
System calls, cont’d

- C function executes
- May copy to/from user space
- Return
Funky kernel programming

- Global variables
  - primary.c
    ```
    int array[2] = {1, 2};
    ```
  - secondary.c
    ```
    extern int array[];
    ```
- Static allocation
  - No magic numbers, please
  - Hmm, kmalloc?