System call

William ZHENG

Example: Linux “Write”

… printf(“Hello World\n”);…

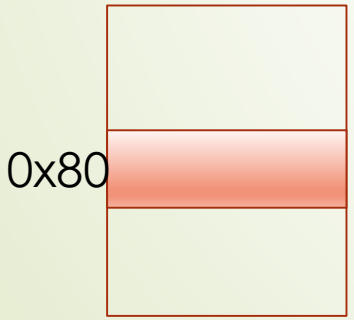
User mode

Libc: %eax = sys_write; int 80h;

---

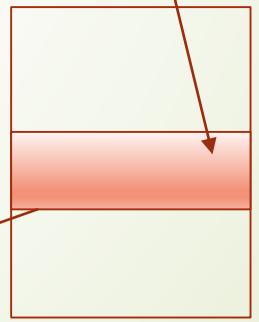
system_call () { sc = sys_call_table[%eax];}

Kernel mode



0x80

sys_write
{ //handler for write }



System Call Table

Interrupt Vector Table

How a system call happens