

Invoking a System Call

5) the system call function executes and (possibly returns value by pushing them onto the stack of the interrupted program

prog

stack



usermode

kennebennodde

A speech bubble with a dark gray border and a light gray background. The bubble has a tail pointing towards the bottom-left corner. Inside the bubble, there is a line of code.

...

`write("hello world")`

kernel

process

1) the program calls a library function

lib/write



syscall num

arg #0

2) the library function pushes the syscall number and its arguments onto the stack and triggers a software interrupt

```
write(s):  
    push("write")  
    push(s)  
    int x80
```



x80 interrupt
handler

3) the interrupt handler reads the stack of the interrupted program to extract the system call number and the arguments



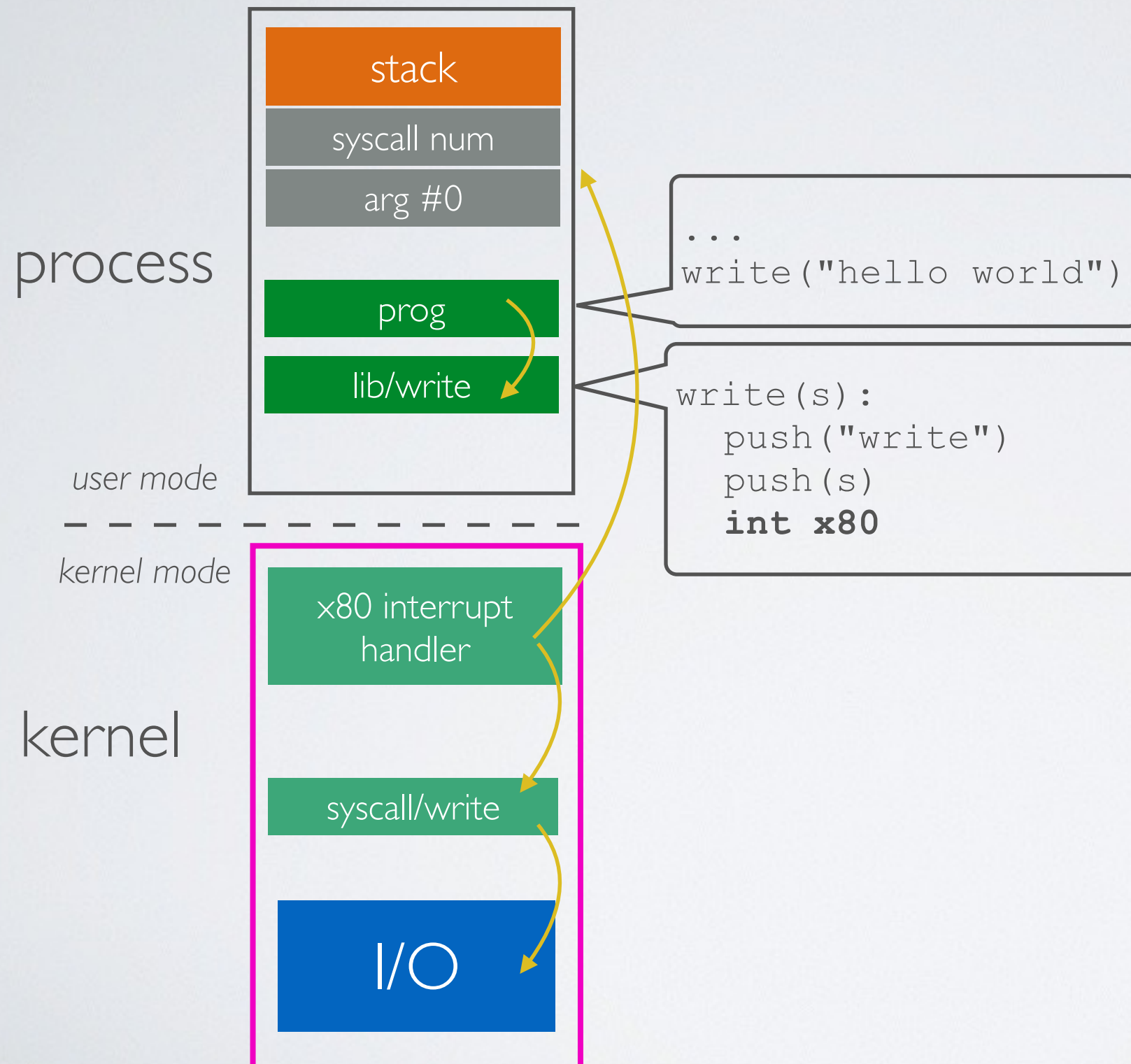
syscall/write

4) the interrupt handler calls the corresponding kernel system call function

1/0



Invoking a System Call



1) the program calls a library function

2) the library function pushes the syscall number and its arguments onto the stack and triggers a software interrupt

3) the interrupt handler reads the stack of the interrupted program to extract the system call number and the arguments

4) the interrupt handler calls the corresponding kernel system call function

5) the system call function executes and (possibly returns value by pushing them onto the stack of the interrupted program

Process