Unix System Call

User Space

Application Program

_____
_____

size_t count = **read**(fd, &buffer, size);

_____
_____

PC -> stack
size -> stack
&buffer -> stack
fd -> stack

PC <- stack

System Call User Space Routine

syscall# -> register

Call TRAP (syscall)

Call RET

Hardware

mode(PSW) <- user
PC <- stack

mode(PSW) <- kernel
PC -> stack
Call **TRAP handler**(syscall)

Kernel Space

TRAP Handler
Kernel Space
Routine

Call **syscall kernel routine**

Call IRET

PC -> stack

PC <- stack

Retrieve **syscall#** from register
Find *read service routine* from
syscall#

Syscall Kernel
Space Routine

Call **read service routine**

Call RET

PC -> stack

Retrieve '**fd**', '**&buffer**', '**size**'
from stack
Read 'size' number of bytes from
'fd' into '&buffer'

PC <- stack

Call RET

Read Kernel Space
Service Routine