

System services:            The inside story 2

The kernel side:

user process triggers kernel activity with the use of INT

CPU uses address in Interrupt Descriptor Table Register

to find the IDT in memory and reads 8 byte entry for

INT 0x80.

Processor now starts executing in kernel mode and jumps to `system_call()` handler.

kernel does housekeeping to save user values in registers and reads value from EAX, which references the needed service.

The value in EAX is an index into the `sys_call_table`, this contains the address of the kernel code to be executed