Syscalls and interrupts

CAOS 2019

Interrupts

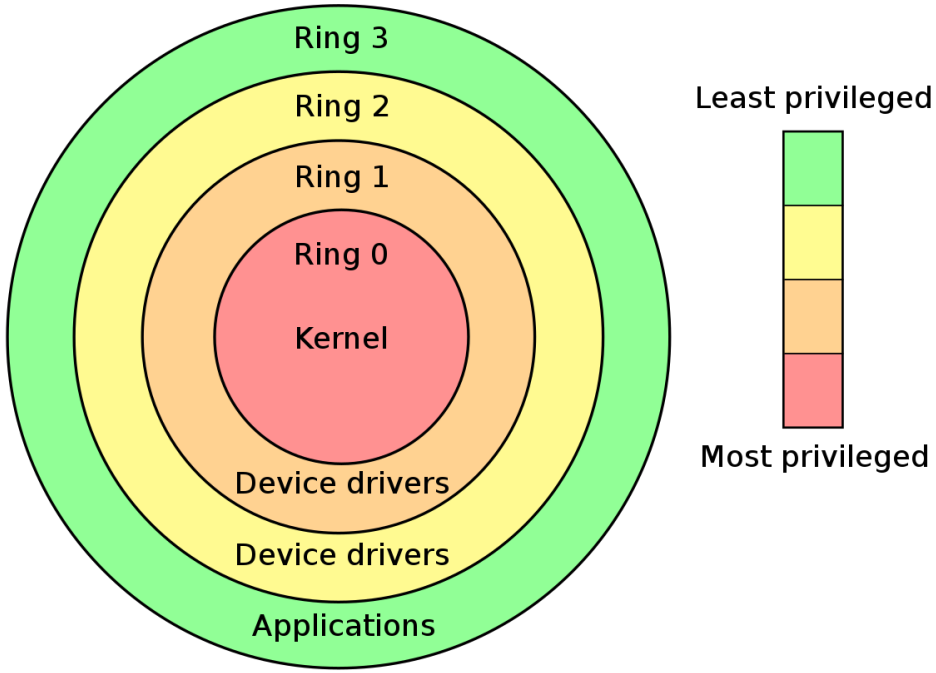
- Buttons pressed
- Tick of the timer
- Data bus got new byte from peripheral devices

How to proceed them

- CPU pause normal execution
- Saves IP on stack
- Sets IF flag
- Jumps to instruction from IDTR (interrupts table pointer) registry
  - If no special handler assigned just returns to normal execution
  - Otherwise, executes handler
- Restores address space of the process (special case: sysenter/syscall)

What interrupt handler does

- Interacts with peripheral device
- Needs access to ports and physical memory



IBM PC Hardware Interrupt Table

IRQ0	8	timer (55ms intervals, 18.2 per second)
IRQ1	9	keyboard service required
IRQ2	A	slave 8259 or EGA/VGA vertical retrace
IRQ8	70	real time clock (AT,XT286,PS50+)
IRQ9	71	software redirected to IRQ2 (AT,XT286,PS50+)
IRQ10	72	reserved (AT,XT286,PS50+)
IRQ11	73	reserved (AT,XT286,PS50+)
IRQ12	74	mouse interrupt (PS50+)
IRQ13	75	numeric coprocessor error (AT,XT286,PS50+)
IRQ14	76	fixed disk controller (AT,XT286,PS50+)
IRQ15	77	reserved (AT,XT286,PS50+)
IRQ3	B	COM2 or COM4 service required, (COM3-COM8 on MCA PS/2)
IRQ4	C	COM1 or COM3 service required
IRQ5	D	fixed disk or data request from LPT2
IRQ6	E	floppy disk service required
IRQ7	F	data request from LPT1 (unreliable on IBM mono)

http://stanislavs.org/helppc/int_table.html

Interrupts in 86/286/386/486

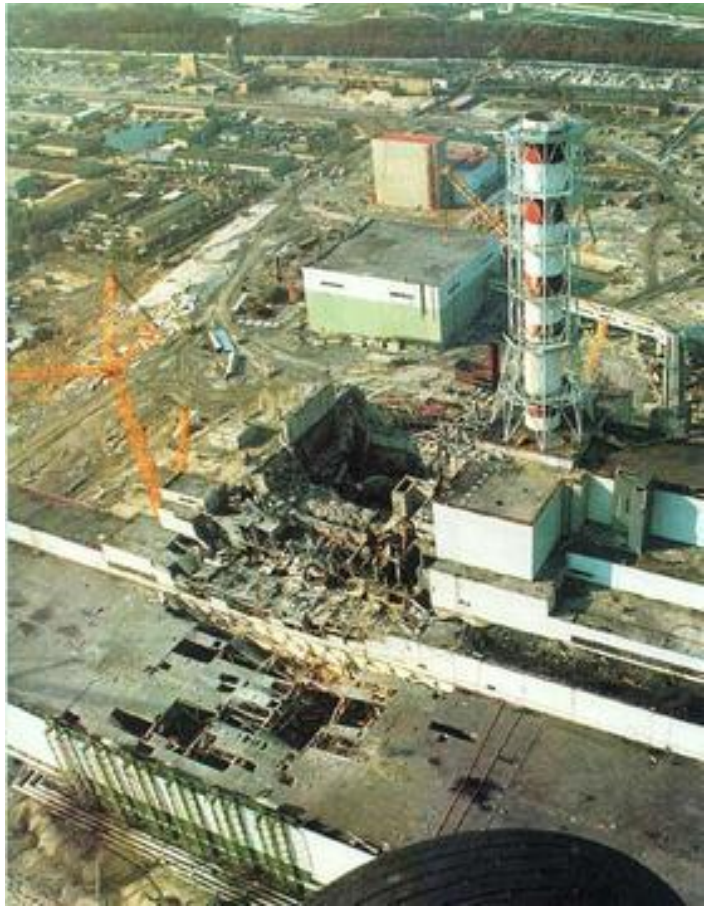
- Every device passes electric impulse
- Signals are multiplexed with priorities
- CPU knows only about existence of some interrupt
- CPU asks PIC about current interrupt

Interrupts with PCI/PCI Express

- Smart I/O APIC controller
- Devices send messaged about interrupts into interrupt queue
- Priority of interrupt defined on program level

Non-maskable interrupt

- To handle non-recoverable errors which need immediate attention
- Has the biggest priority
- (Cannot be masked)



Software interrupts

- Asm: int <NUM>
- Same processing as for hardware
- Before OS loading: BIOS interrupts
- After: OS can rewrite by own interrupts

- Examples: DOS Functions: Print a string message, Exit, Character Input, Printer Output

Kernel

- A set of programs that have the most privileged level of access
- Loads after BIOS
- Provides API for external programs – system calls
- Checks whether the caller can access the part of the system it asks

Int 0x80

- Number of an interrupt for initiating system calls
- Eax – number of a particular system call (see unistd_32.h)
- Arguments are in ebx, ecx, edx, esi, edi, ebp
- Return value is in eax