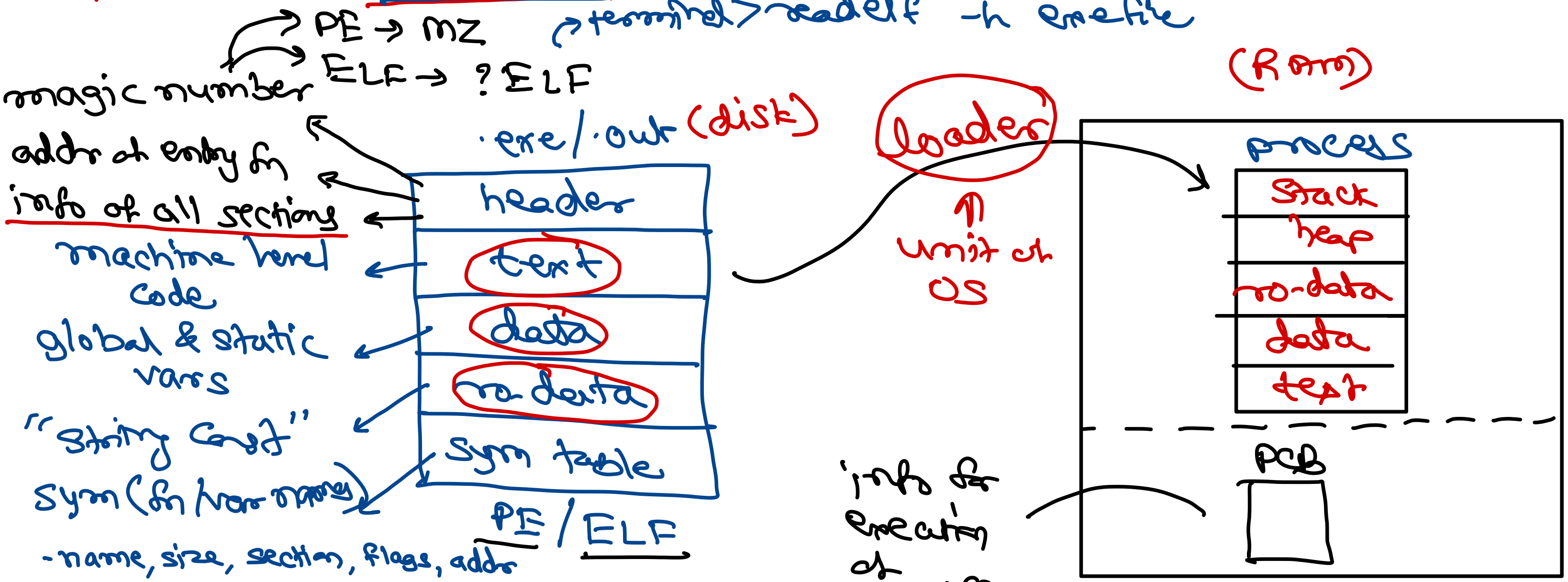
processes have lives and files have spaces. – UNIX.

UNIX OS = Process subsystem + File subsystem.

Process

program : set of instructions given to the computer, executable file

process : program under execution



```
terminal> readelf -h exefile
terminal> objdump -t exefile
```

File

file is collection of data/info on storage device

file = contents (data) + info (metadata)

↓ ↓

disk → data blocks

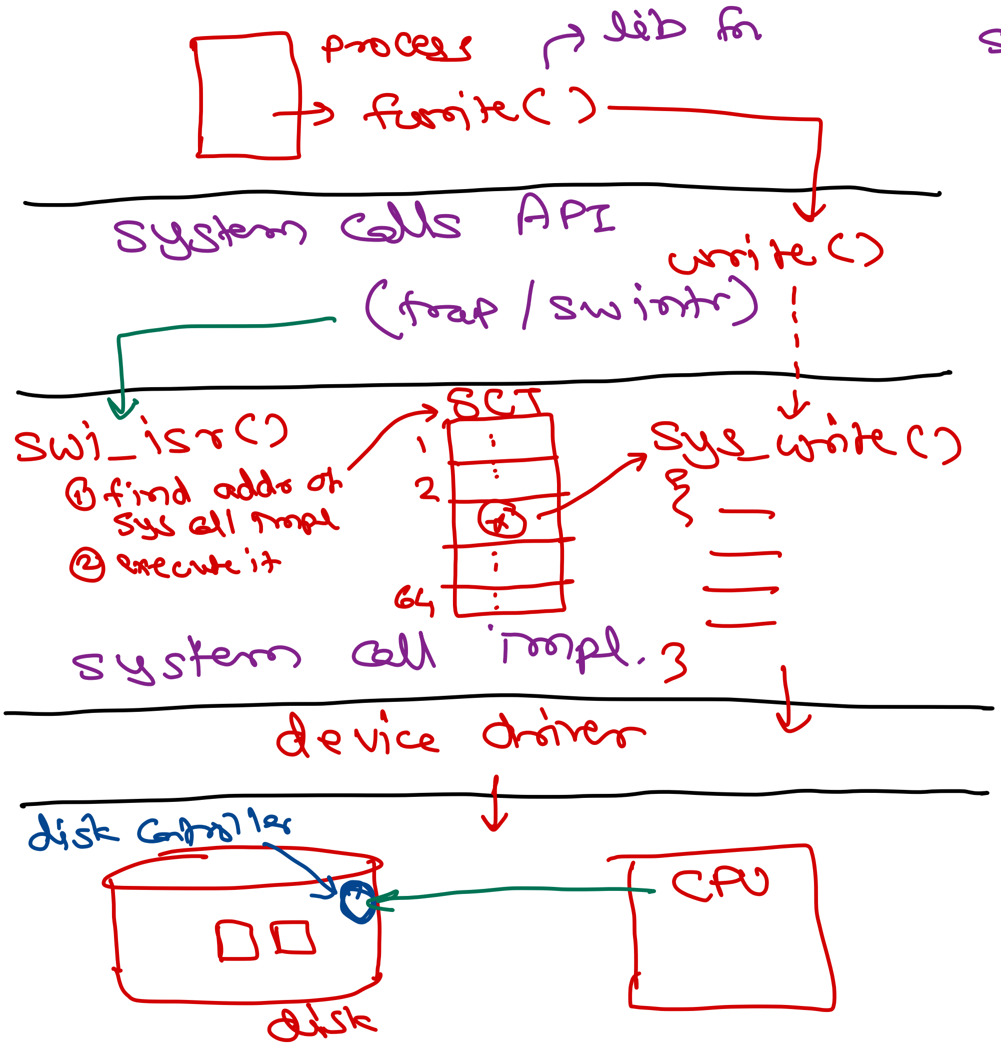
FCB (inode)

1. type
2. size
3. permissions (mode)
4. user & group
5. timestamps

...

Hardware Protection

- Early operating systems work as resident monitors.
- Then OS start doing additional jobs like I/O, resource allocator, etc.
- In multiprogramming environment, one program could disturb other program in memory by corrupting its data.
- The programming errors are detected by hardware and conveyed to operating system via interrupt. OS should take appropriate action like terminating victim program.
- The following protection mechanisms are available:
  - Dual-Mode Operation
  - I/O Protection
  - Memory Protection
  - CPU Protection



syscalls are fns exposed by the kernel, so that user programs can access kernel functionality

UNIX : 64 sys calls.

Linux : >300 sys calls.

Software interrupt

a special assembly instruction (arch dependent) → cause execution of ISR.

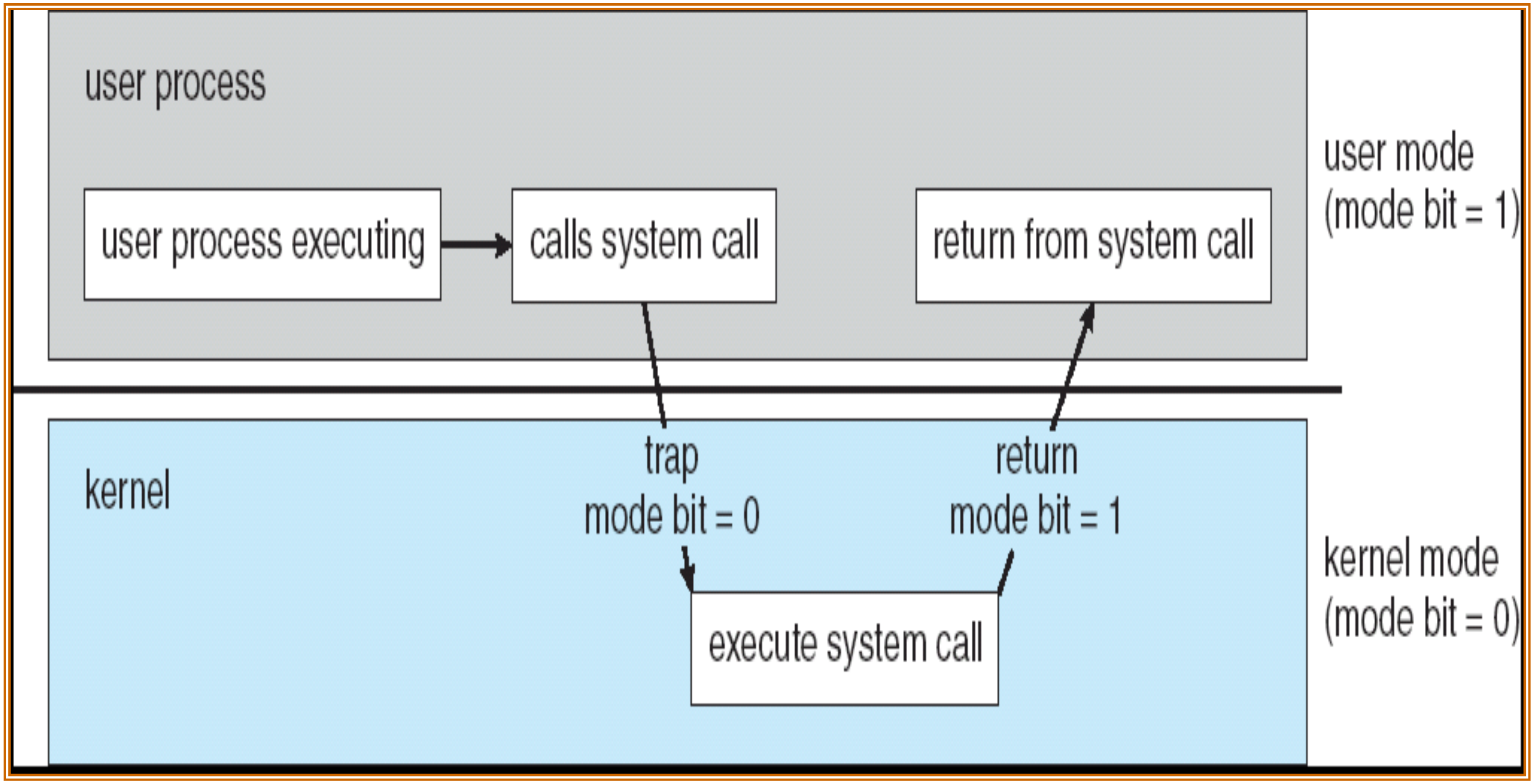
x86 : INT

ARM : SWI/SVC

Dual-Mode Operation

- Sharing system resources requires operating system to ensure that an incorrect program cannot cause other programs to execute incorrectly.
- Provide hardware support to differentiate between at least two modes of operations.
  - User mode – execution done on behalf of a user.
  - Monitor mode (also kernel mode or system mode) – execution done on behalf of operating system.
- Mode bit added to computer hardware to indicate the current mode: monitor (0) or user (1).
- When an interrupt or fault occurs hardware switches to monitor mode.

User mode and Kernel mode



Thank you!

Source: Galvin OS books/slides

Edited by: Nilesh Ghule