CSIT113

Computer and Information Technology

L-T-P 2-0-2

MODULE 2

Software

Software is a collection of instructions, data, or computer programs that are used to run machines and carry out particular activities.

System software

- **Operating system:** Manages resources and provides services for other software. There are many types of operating systems, including single-user, multi-user, mobile, and internet.
- **Device drivers:** Allow the operating system to communicate with hardware devices like printers, scanners, and graphics cards.

Application software

- **Spreadsheet:** Used to store data in tables and perform calculations.
- **Word processor**: Used to manipulate text and format documents.
- **Web browser**: Used to access the internet, such as Google Chrome or Firefox.
- **Multimedia:** Used to create, record, or play audio, video, or images.
- **Games**: Such as Candy Crush Saga or Ludo.
- **Smartphone apps**: Such as WhatsApp or Telegram.

AMITY UNIVERSITY Kolkata

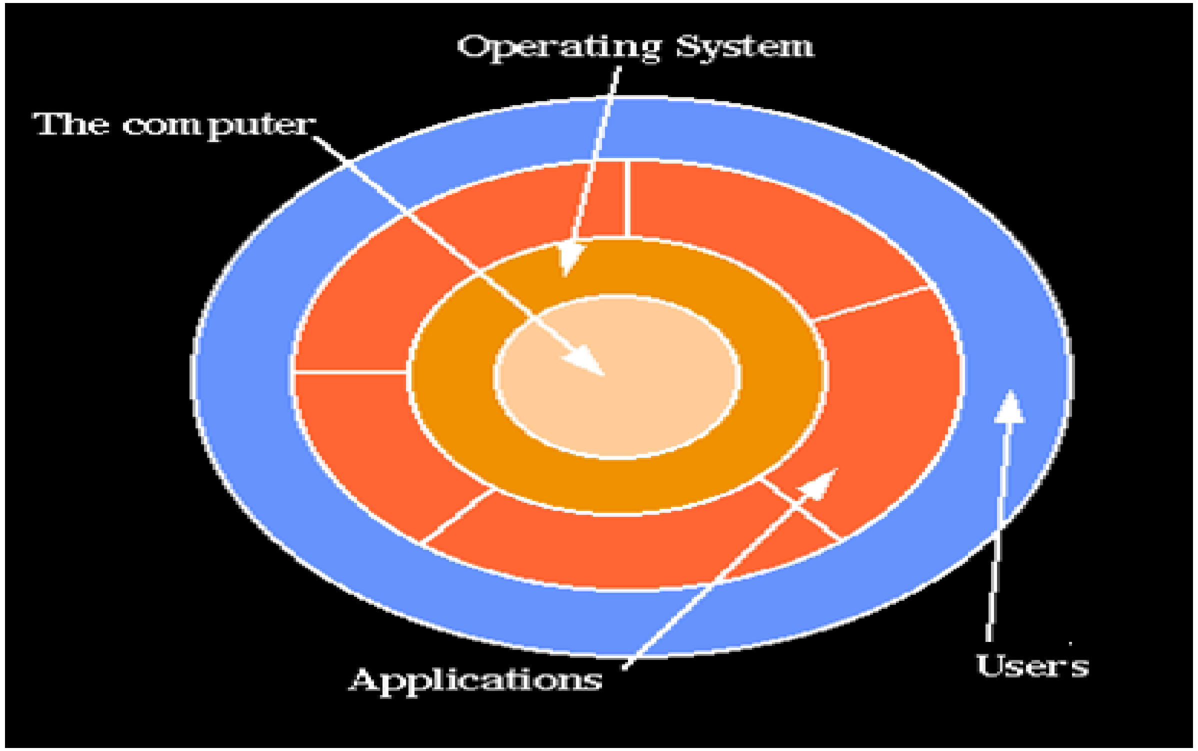
Operating Systems

What is an Operating System?

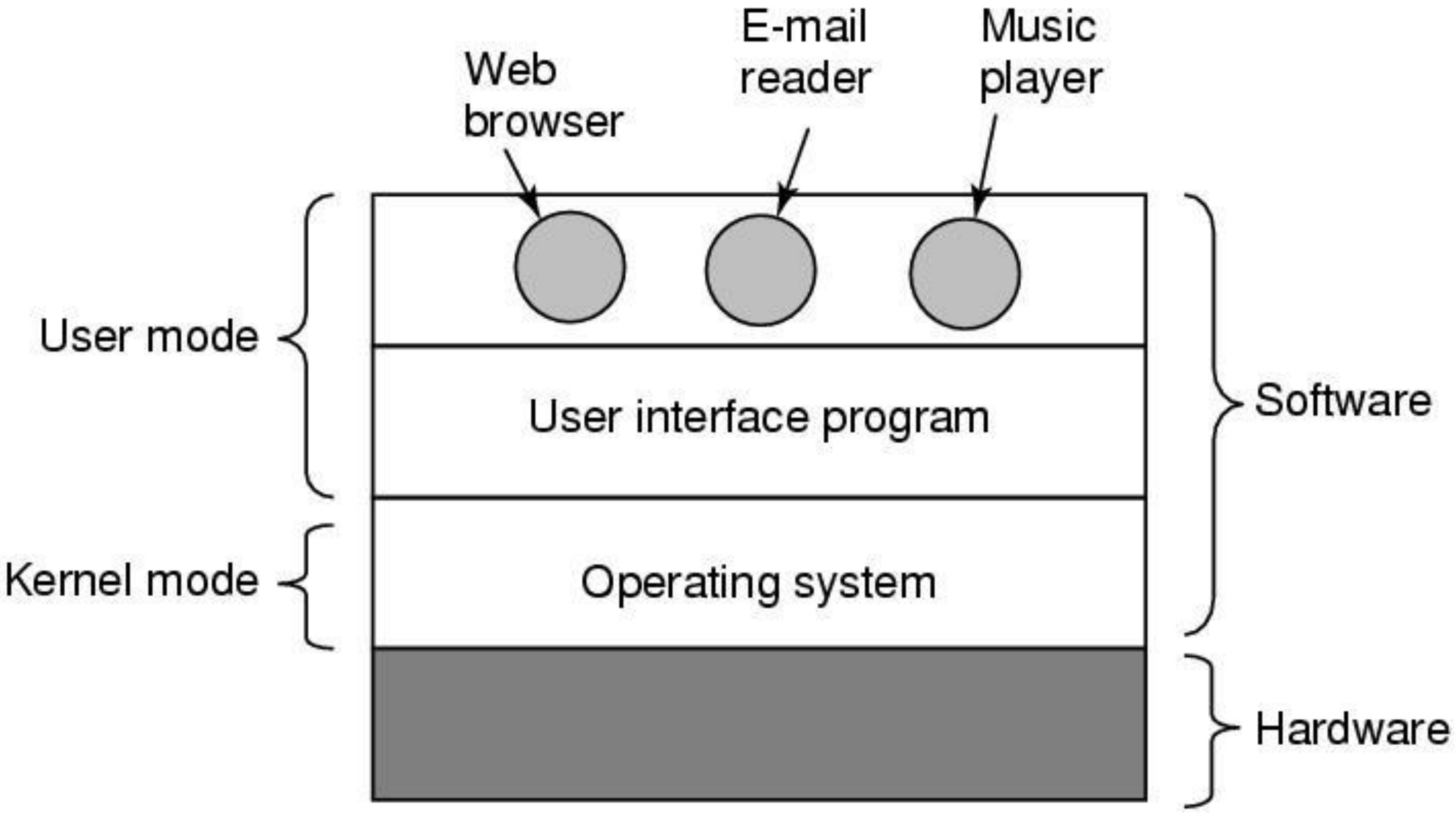
- A modern computer consists of:
  - ➢ One or more processors
  - ➢ Main memory
  - ➢ Disks
  - ➢ Various input/output devices.
- Managing all these varied components requires a layer of software – the **Operating System (OS).**

What is an Operating System?

- An Operating System is a program that acts as an intermediary/interface between a user of a computer and the computer hardware.



Where does the OS fit in?



Goals and Services

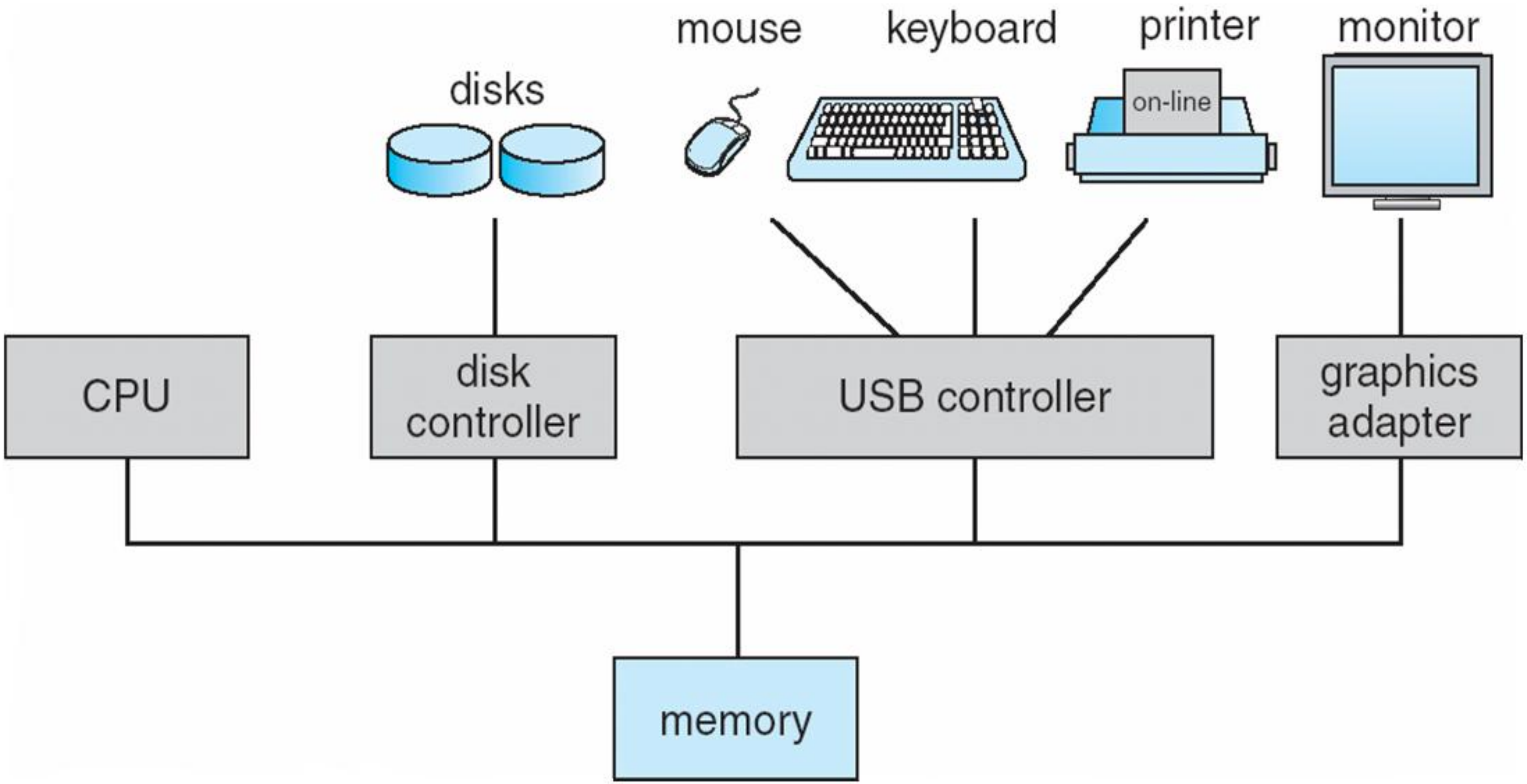
OS goals

- Control/execute user/application programs.
- Make the computer system convenient to use.
- Ease the solving of user problems.
- Use the computer hardware in an efficient manner.

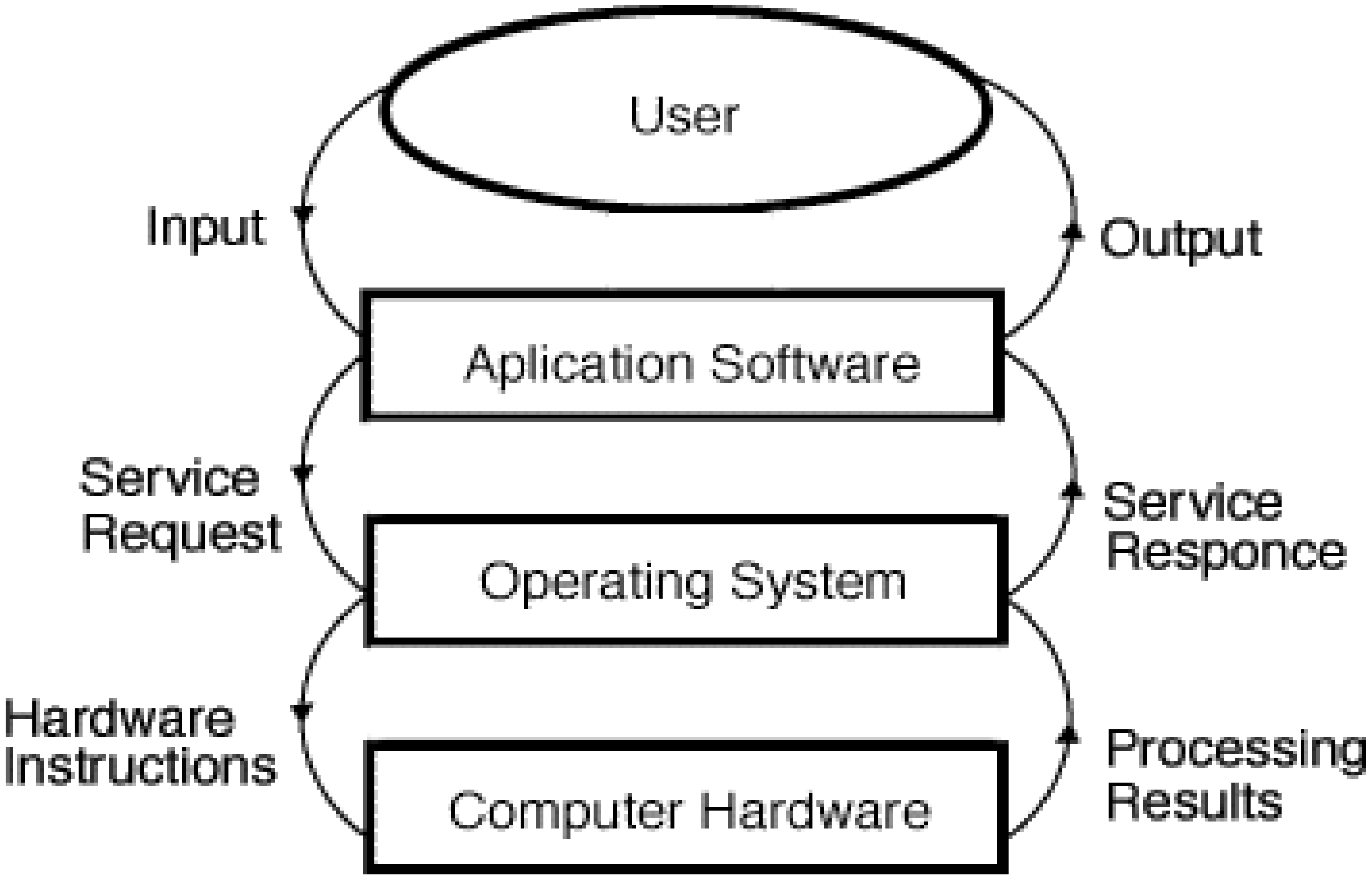
Services

- Facilities for program creation
  - editors, compilers, linkers, debuggers, etc.
- Program execution
  - loading in memory, I/O and file initialization.
- Access to I/O and files
  - deals with the specifics of I/O and file formats.
- System access
  - resolves conflicts for resource contention.
  - protection in access to resources and data.

Computer Hardware Organization



Dynamic View of System Components



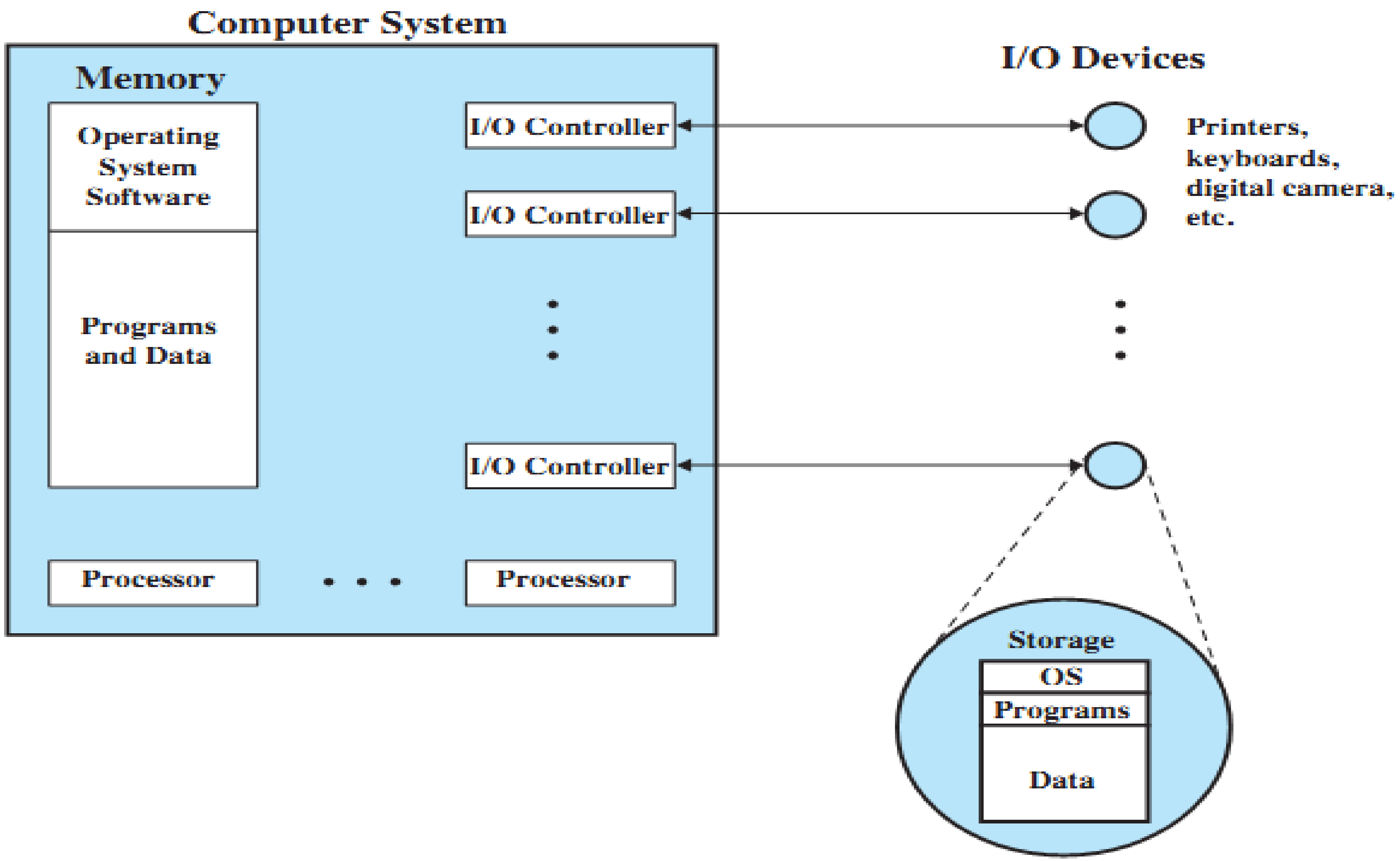
Operating System functions

- There are three classical functions:
  1. Resource Manager – manages and allocates resources.
  2. Control program – controls the execution of user programs and operations of I/O devices.
  3. Command Executer – Provides an environment for running user commands.
- But one more modern view: the Operating System as a Virtual Machine.

1. Resource Manager

- Resource Manager:
  - Manages and protects multiple computer resources: CPU, Processes, Internal/External memory, Tasks, Applications, Users, Communication channels, etc.
  - Handles and allocates resources to multiple users or multiple programs running at the same time and space (e.g., processor time, memory, I/O devices).
  - Decides between conflicting requests for efficient and fair resource use (e.g., maximize throughput, minimize response time).

OS as a Resource Manager



2. Control Program

- Control Program:
  - Manages all the components of a complex computer system in an integrated manner.
  - Controls the execution of user programs and I/O devices to prevent errors and improper use of computer resources.
  - Looks over and protects the computer: Monitor, Supervisor, Executive, Controller, Master, Coordinator

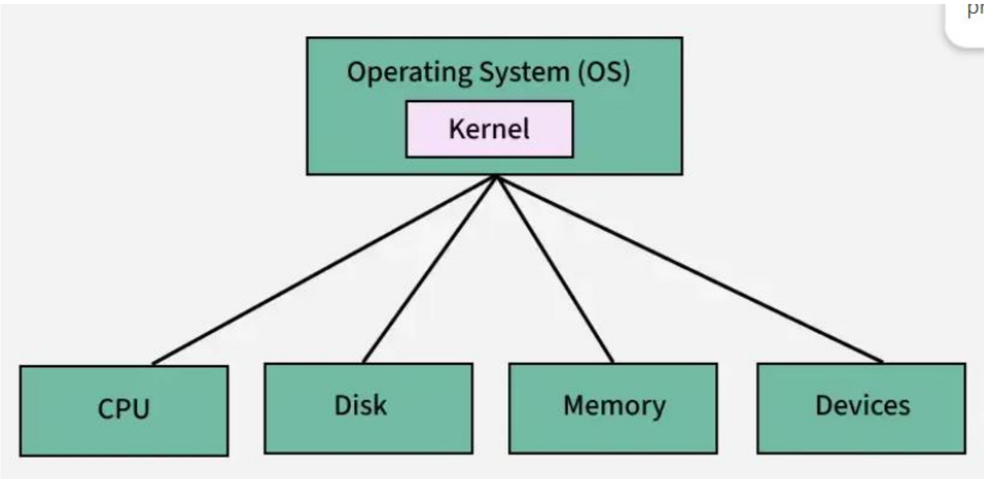
3. Command Executer

- Command Executer:
  - Interfaces between the users and machine.
  - Supplies services/utilities to users.
  - Provides the users with a convenient CLI (Command Language Interface), also called a Shell (in UNIX), for entering the user commands.

Kernel - Point of View

Kernel

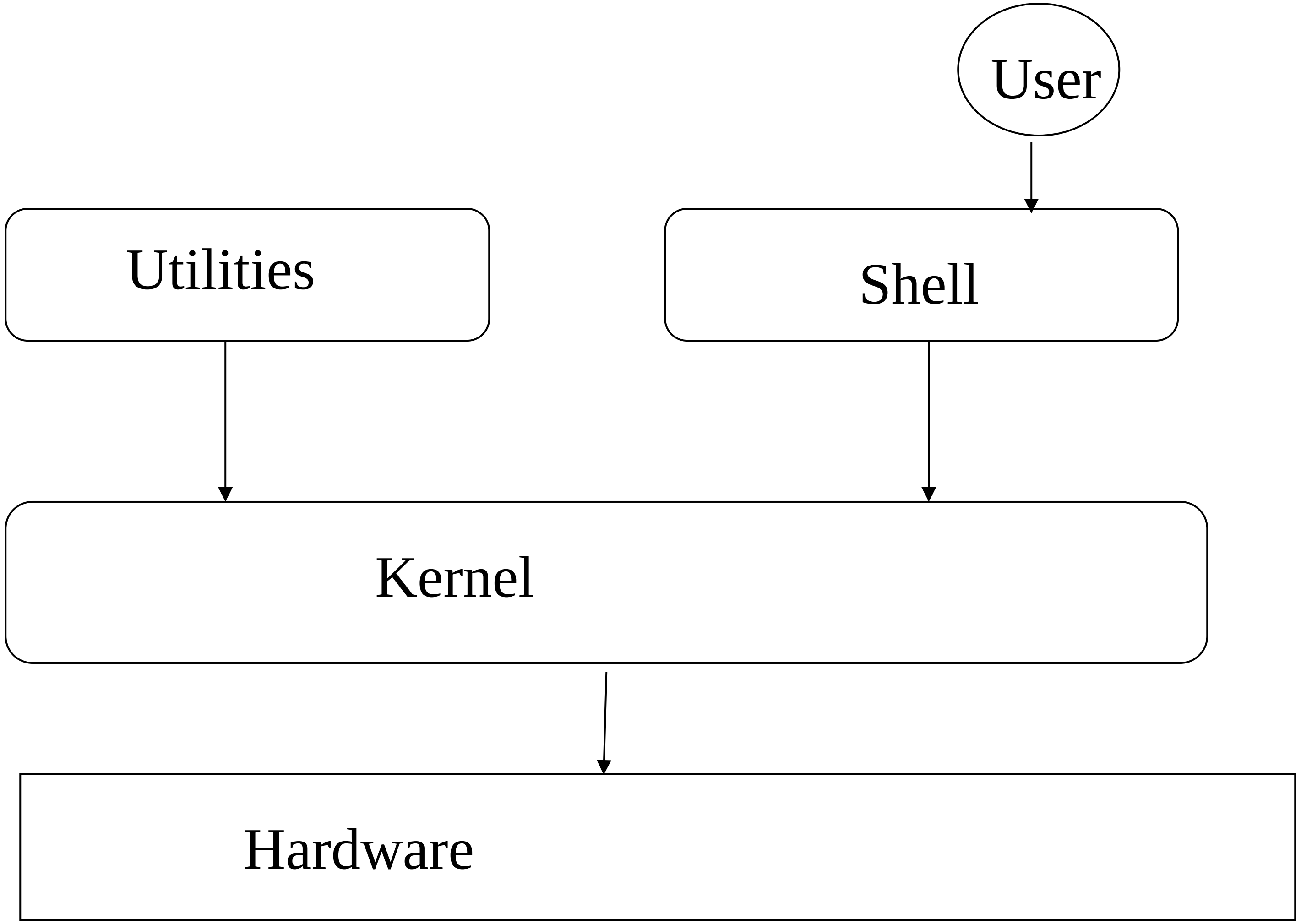
- The kernel is the main layer between the OS and the computer's hardware.
- It's responsible for managing system resources like memory, CPU, and devices.
- The kernel converts user queries into machine language.
- It also enforces system-level security by managing process permissions and controlling access to hardware.



Shell and Utilities

The kernel is the core of an operating system, while the **shell is a user interface** that allows users to interact with the operating system.

The kernel manages hardware resources and system calls, while the **shell translates user commands into binary language** that the kernel can execute.

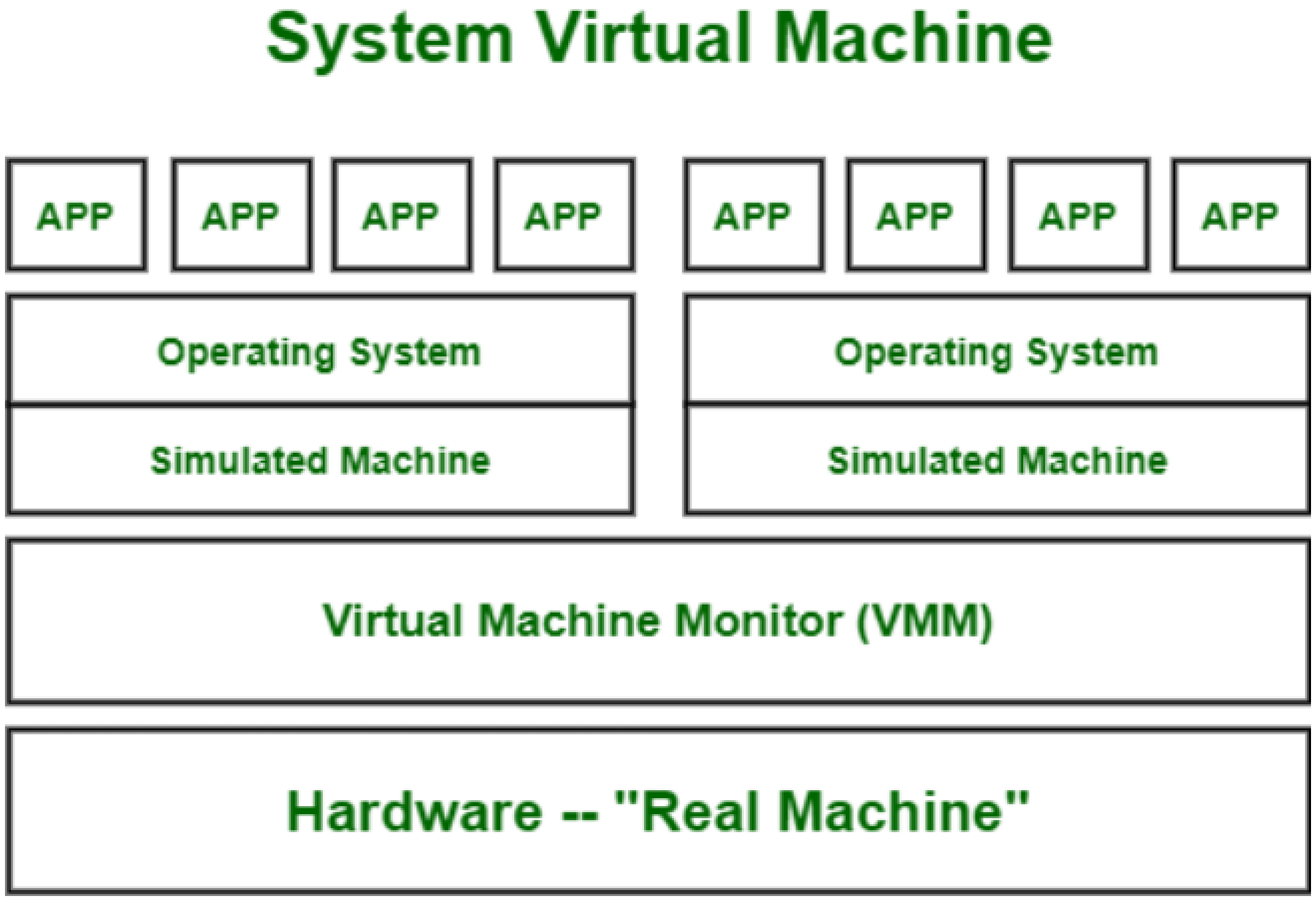


Virtual Machine

- A virtual machine (VM) is a software-based emulation of a complete computer, allowing you to run a separate operating system within your existing operating system, essentially creating a "computer within a computer" on the same physical hardware; meaning you can run multiple different operating systems on a single machine simultaneously by using virtual machines.

- **OS:** Windows 10 on your laptop.
- **VM:** Using software like VMware or VirtualBox to run a Linux operating system within your Windows 10 system.

Modern view: Virtual Machine



System Virtual Machine

APP APP APP APP

APP APP APP APP

Operating System

Simulated Machine

Operating System

Simulated Machine

Virtual Machine Monitor (VMM)

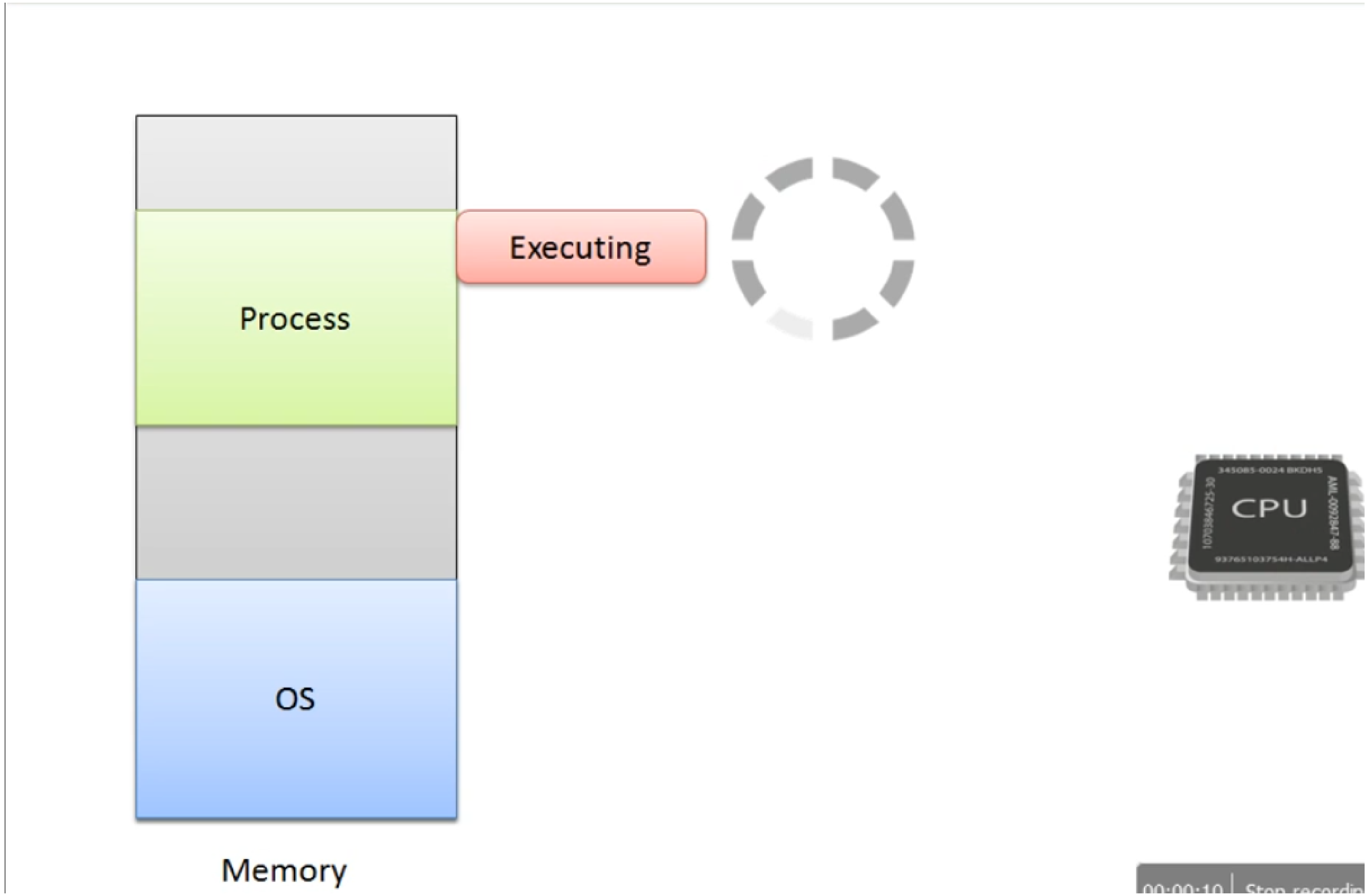
Hardware -- "Real Machine"

Types of modern operating systems

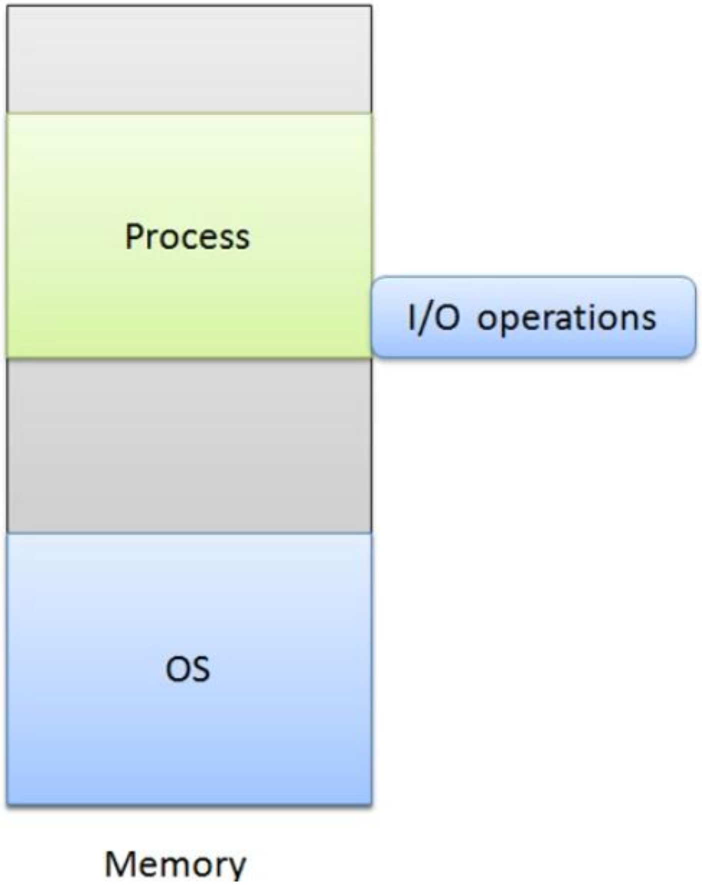
- Mainframe operating systems: MVS
- Server operating systems: FreeBSD, Solaris
- Multiprocessor operating systems: Cellular IRIX
- Personal computer operating systems: Windows, Unix
- Real-time operating systems: VxWorks
- Embedded operating systems
- Smart card operating systems

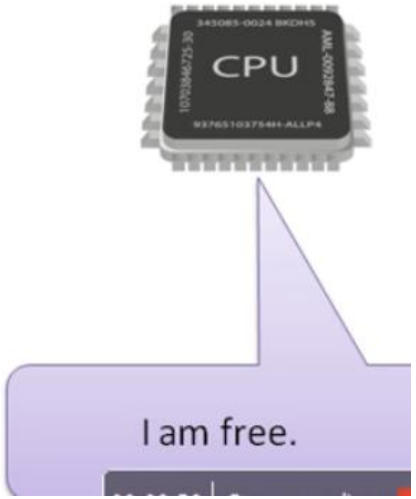
⇒Some operating systems can fit into more than one category

Single-process CPU

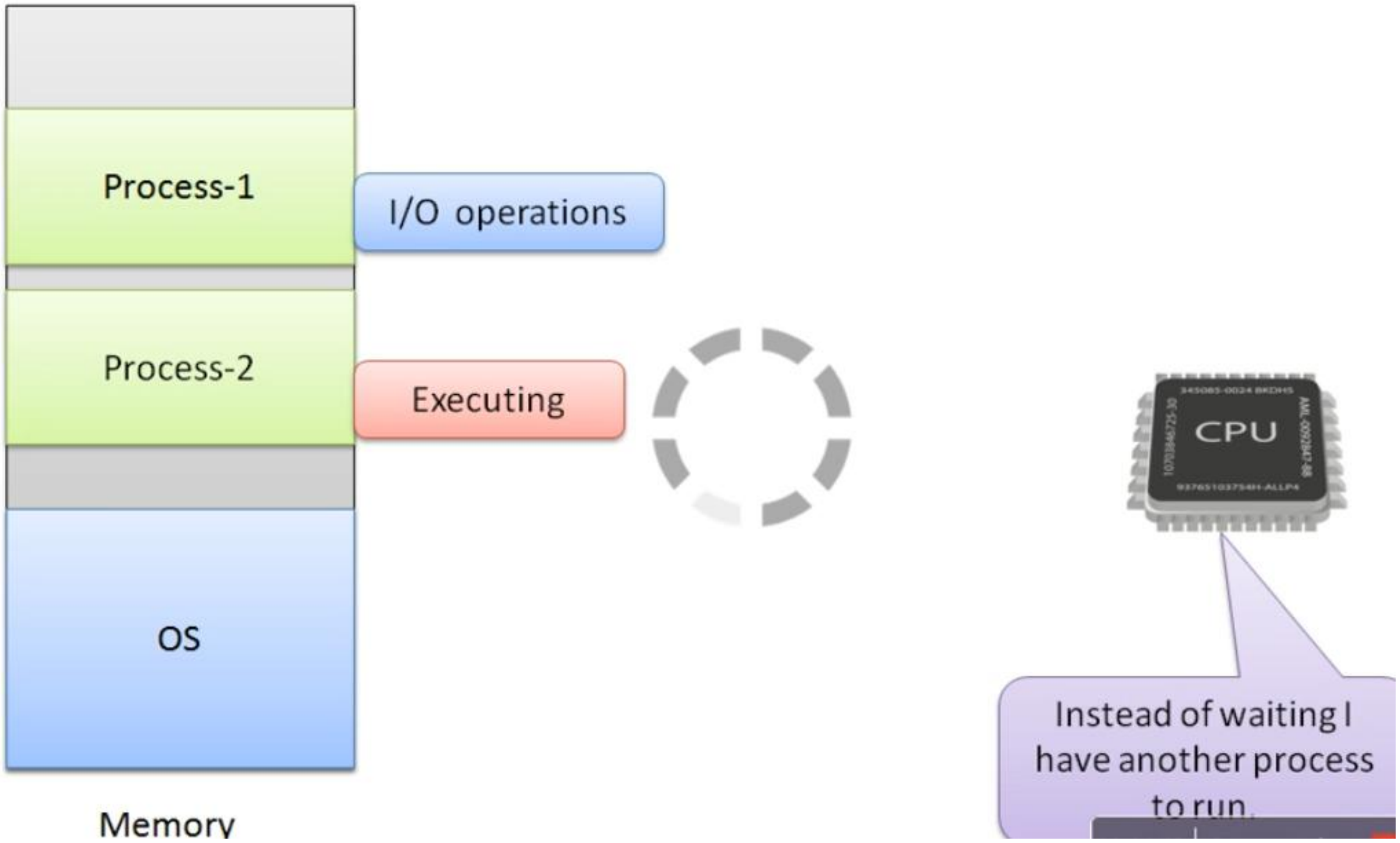


Single-process CPU



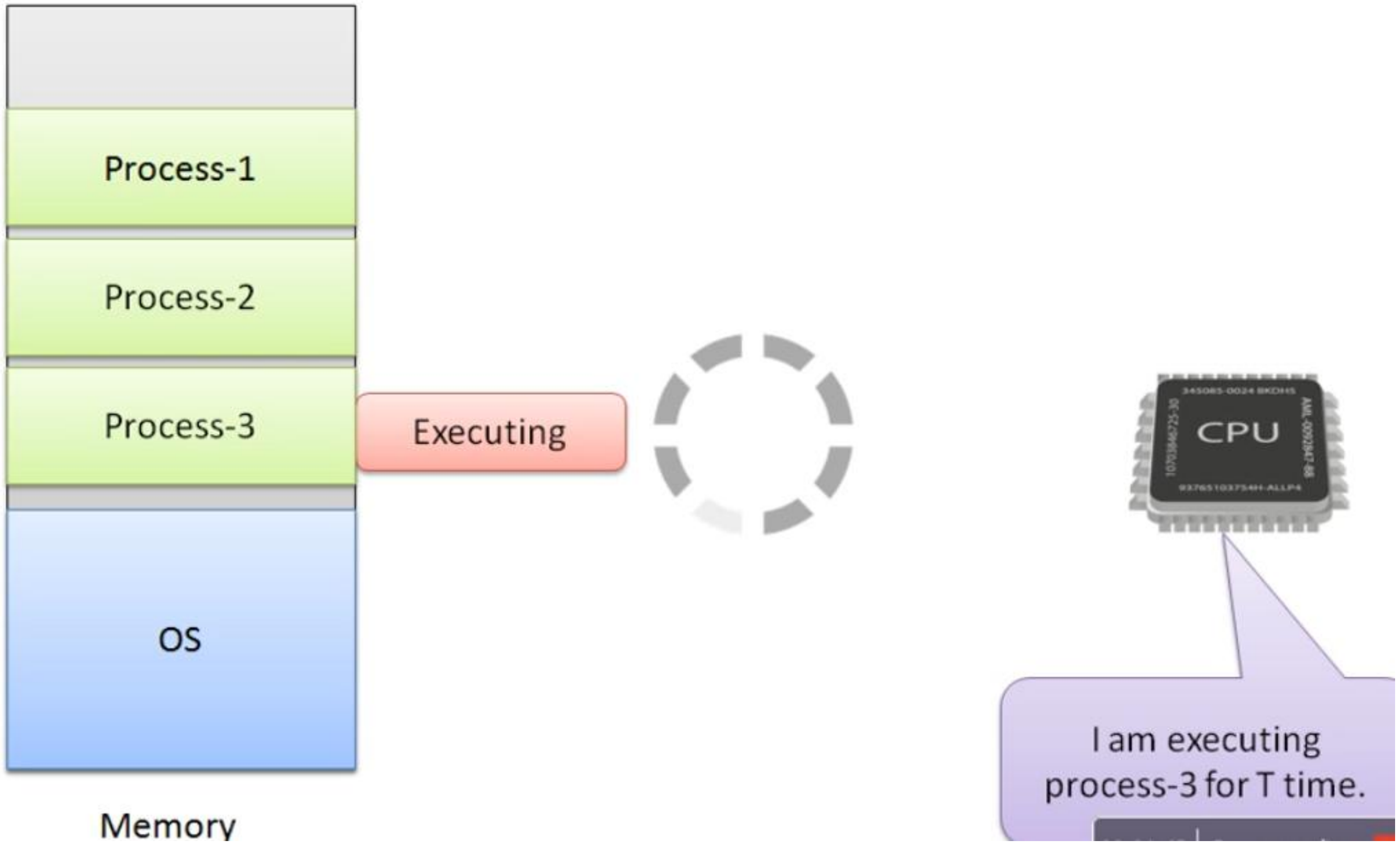


Multi-programming CPU – Operating System



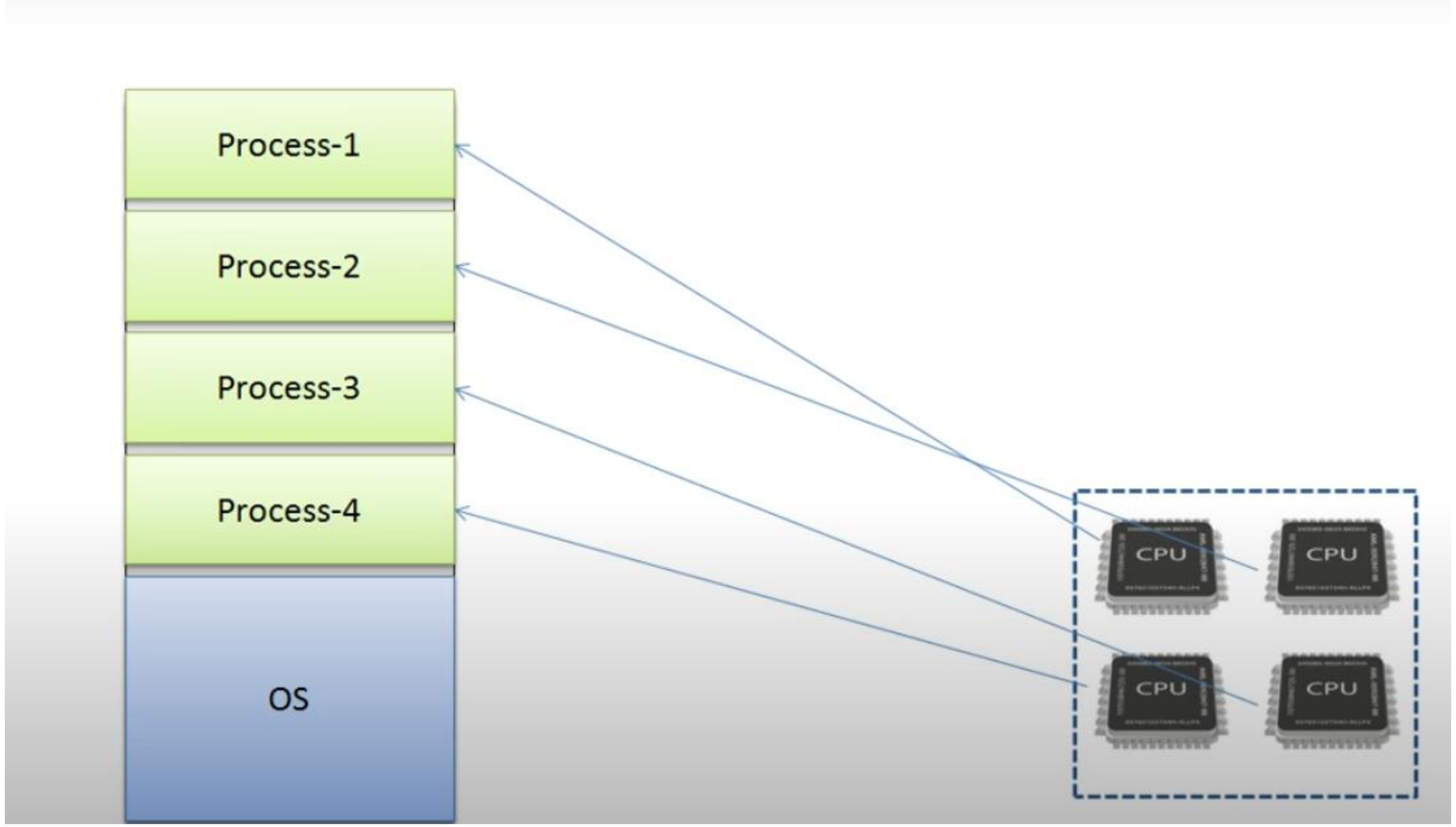
As and when CPU is free, the processors are allotted to CPU by OS.
Starvation (long wait) in case the process is long.

Multi-tasking CPU-

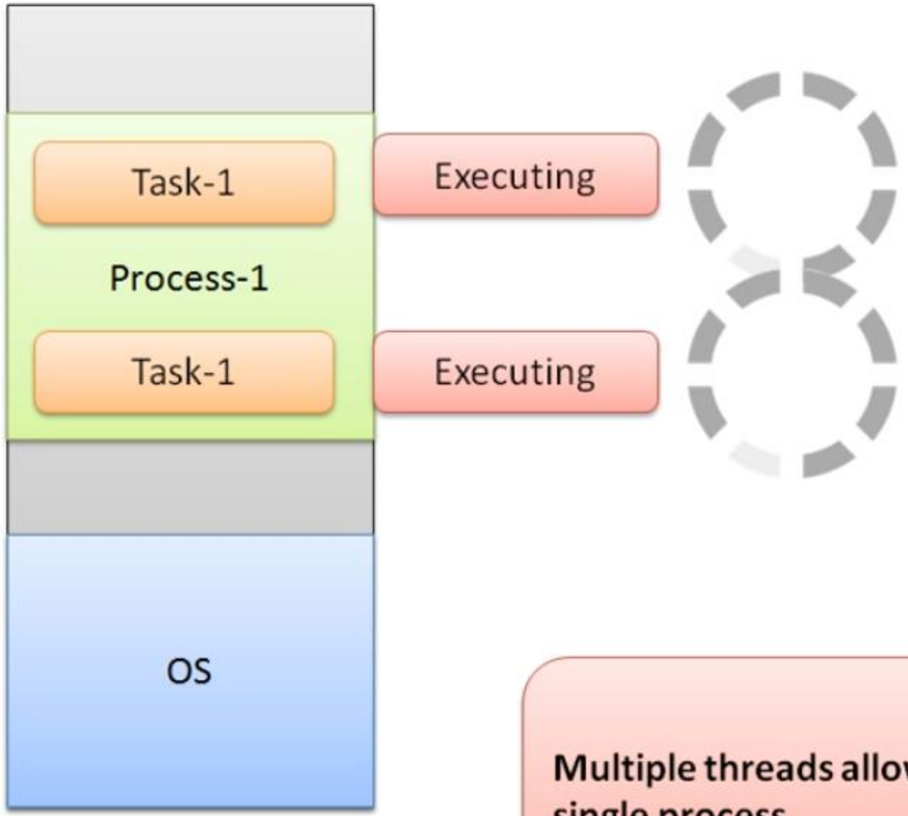


Time-based allotment to processes

Multi-processing

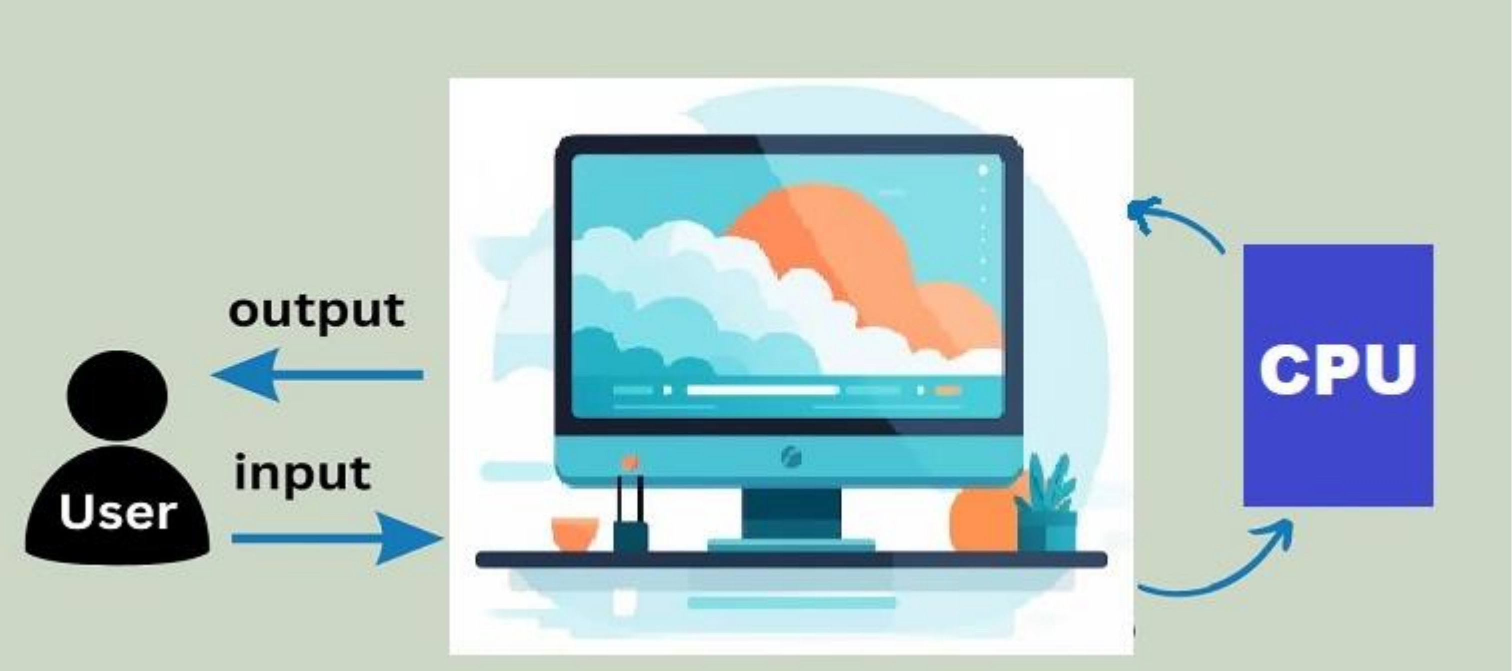


Multi-threading

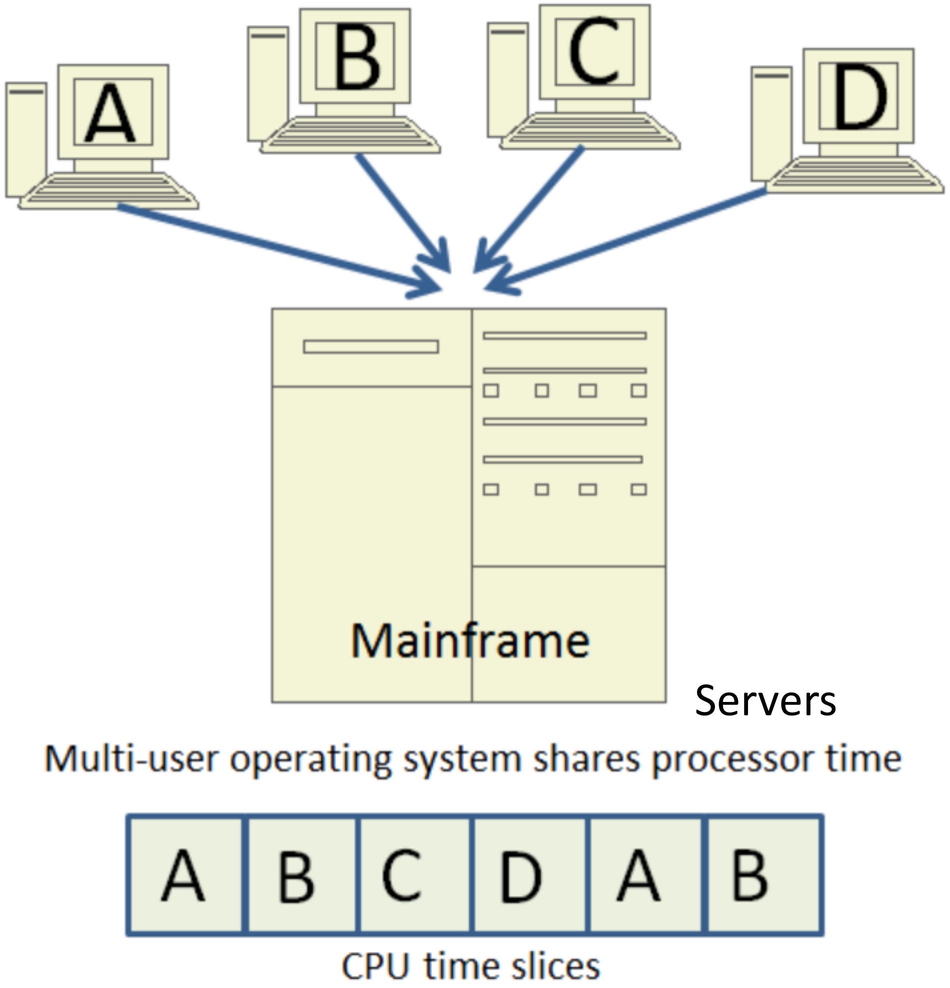


Multiple threads allows execution of multiple tasks in single process.

Single-user operating system



Multiuser Operating System



Servers

Multi-user operating system shares processor time

A	B	C	D	A	B

CPU time slices

Real-time OS

- A real-time operating system processes data and executes tasks within strict time constraints and with a high degree of reliability and precision.
- An RTOS can be critical in situations where delays could lead to operational or safety hazards, and industrial systems, automotive controls, and medical devices commonly use RTOSs.

- FreeRTOS: Used in IoT devices, embedded systems, and industrial control systems
- VxWorks: A high-performance RTOS for embedded systems that are critical, safe, and secure
- Nucleus: A popular RTOS from Mentor Graphics

Applications

Some common use cases for a real time operating system across industries are:

- Automotive Systems: RTOS is used in modern vehicles for managing real-time tasks like engine control units (ECUs), adaptive cruise control, and infotainment systems.
- Medical Devices: In devices like pacemakers and medical monitoring systems, RTOS ensures quick and accurate responses for patient safety.
- Aerospace: RTOS helps manage flight control systems, radar processing, and guidance systems, where timing and reliability are critical.
- Industrial Automation: RTOS powers robotic control systems, assembly lines, and process monitoring, ensuring real-time task handling in manufacturing environments.

Virus

A computer virus is a type of malicious software program (“malware“) that, when executed, replicates itself by modifying other computer programs and inserting its code.

When this replication succeeds, the affected areas are then said to be “infected“.

Viruses can spread to other computers and files when the software or documents they are attached to are transferred from one computer to another using a network, a disk, file-sharing methods, or through infected email attachments.

How a virus spreads

- *Scans your computer for network connections*; copies itself to other hosts on the network
  - Requires programming skill

OR

- Reads *your* e-mail address book *and email* itself to everyone in *your* address book
  - Requires less programming skill
    - *Scripts are available on the web*

Virus Types

- Macro: Activates by running a program capable of executing macros, often found in documents like spreadsheets
  - **macro code** attached to some **data file**
  - interpreted by program using file
    - eg Word/Excel macros
    - esp. using auto command & command macros
- Multi-Partite : attack the computer in multiple ways for example, boot virus infecting the boot sector of the hard disk
- Armored: any virus that tries to prevent analysis of its code. It can use one of many methods to do this: for instance disassembling, compressed code, etc.

Virus Types (Cont.)

- Memory Resident : Installs itself and then remains in RAM from the time the computer is booted up to when it is shut down: infects files opened by user or OS)
- Sparse Infector: Attempts to elude detection by performing its malicious activities only sporadically.
  - The user will see symptoms for a short period, then no symptoms for a time
  - By reducing the frequency of attack, the chances for detection are reduced
- Polymorphic: Literally changes its form from time to time to avoid detection by antivirus software
  - A more advanced form of this is called the Metamorphic virus; it can completely change itself

Virus Examples

- Rombertik – Wreaked havoc in 2015. This malware uses the browser to read user credentials and other sensitive information for exfiltration to an attacker controlled server
  - Over 97% of the file is unnecessary code or data meant to overwhelm analysts
  - Overwrites the Master Boot Record making the machine unbootable, or begin encrypting files in the user's home directory
- Gameover ZeuS - Creates a peer-to-peer botnet. Essentially, it establishes encrypted communication between infected computers and the command and control computer, allowing the attacker to control the various infected computers: DDoS, stealing of data, sending spams, etc,
- FakeAV - July 2012. It affected Windows systems ranging from Windows 95 to Windows 7 and Windows server 2003. This was a fake antivirus that would pop up fake virus warnings. This was not the first such fake antivirus malware, but it was one of the more recent ones

Anti-virus

Typically by one or more of the following functions:

prevention - block virus infection mechanism

detection - of viruses in infected system

reaction - restoring system to clean state

Avast, McAfee, Norton, Microsoft Defender

Anti-virus

- **first-generation**
  - scanner uses virus signature to identify virus
  - or change in length of programs
- **second-generation**
  - uses heuristic rules to spot viral infection
  - or uses program checksums to spot changes
- **third-generation**
  - memory-resident programs identify virus by actions
- **fourth-generation**
  - packages with a variety of antivirus techniques
  - eg scanning & activity traps, access-controls

Advanced Anti-Virus Techniques

- generic decryption
  - use CPU simulator to check program signature & behavior before actually running it
- digital immune system (IBM)
  - general purpose emulation & virus detection
  - any virus entering org is captured, analyzed, detection/shielding created for it, removed