NMIMS University

Information Security

Unit -7

Unit 7:

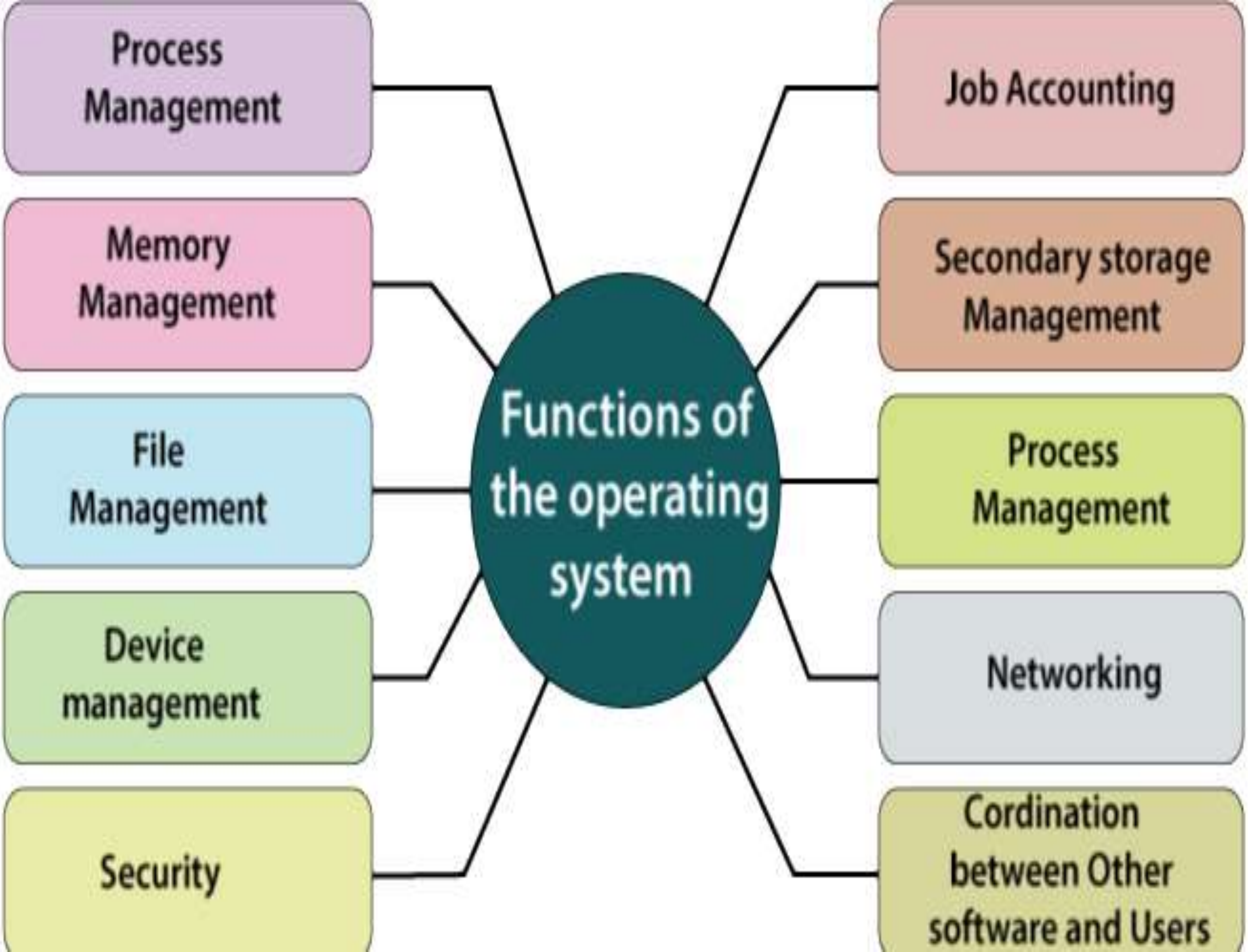
- Operating System Security
- Security architecture
- Analysis of security in windows/linux

Operating system (OS)

- An **operating system** (OS) is **system** software that manages computer hardware, software resources, and provides common services for computer programs.

Function of operating System

- Memory Management.
- Processor Management.
- Device Management.
- File Management.
- Security.



Functions of the operating system

Process Management

Memory Management

File Management

Device management

Security

Job Accounting

Secondary storage Management

Process Management

Networking

Cordination between Other software and Users

Operating system security

- Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.
- OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions.

Protected Objects

- Hardware, software and data.
- Memory.
- Sharable I/O devices.
- Serially reusable I/O devices.
- Sharable programs and sub-procedures.
- Sharable data.

As it assumed responsibility for controlled sharing, the operating system had to protect these objects.

Security Methods

❖Seperation:

- keeping one user’s objects separate from other users’
- Physical Seperation
- Temporal Seperation
- Logical Seperation
- Cryptographic Seperation

❖Granularity of Control

- The larger the level of the object controlled, the easier it is to implement access control.

Memory address protection

- An operating system is the multiprogramming system allowing multiple users to use concurrently.
- Operating system is designed in such a way that one user's computation cannot be intercepted by malicious user.
- For this purpose, operating system has following facilities.

1. Memory protection,
2. File protection,
3. General control on how objects are accessed,
4. User authentication

Memory and Address Protection:

- Memory protection in multiprogramming prevents other programs from interfering to user’s program.
- Hardware is designed to provide memory protection.

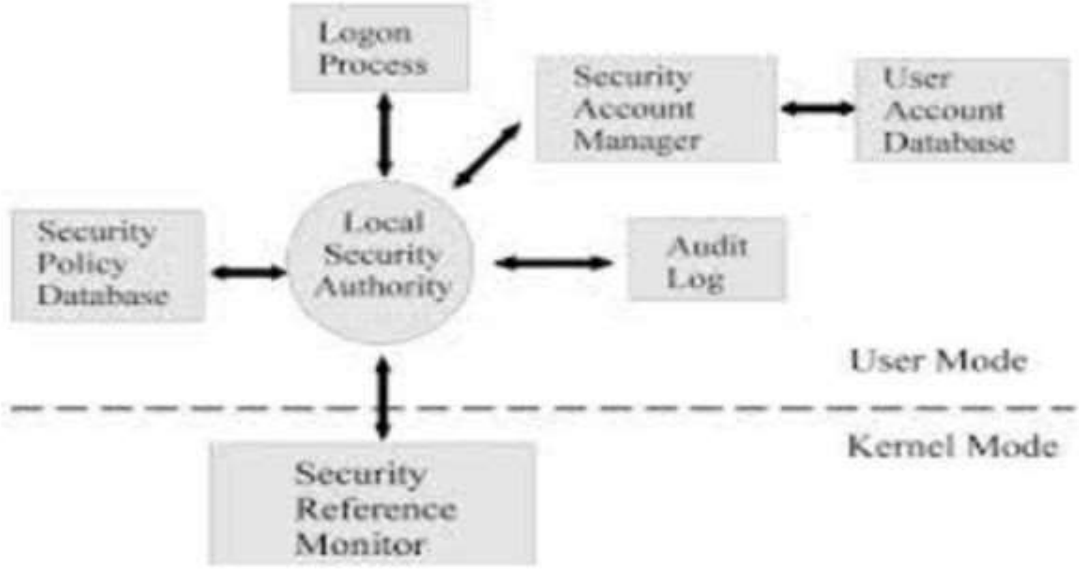
1. Fence
2. Relocation
3. Segmentation
4. Paging

Relocation

- ***Relocatability - the ability to move process around in memory without it affecting its execution***
- Operating systems can manage where each process is stored in memory using a technique called **relocation.**
- With **static relocation**, the process must be put in the same position.
- With **dynamic relocation**, the **OS** finds a new position in memory for the process and updates the **relocation** and limit registers.

Security Architecture of Windows

- Security Reference Monitor(SRM)
- Local Security Authority(LSA)
- Security Account Manager(SAM)



- The Security Architecture of the OSI Reference Model (ISO 7498-2) considers five main classes of security services:

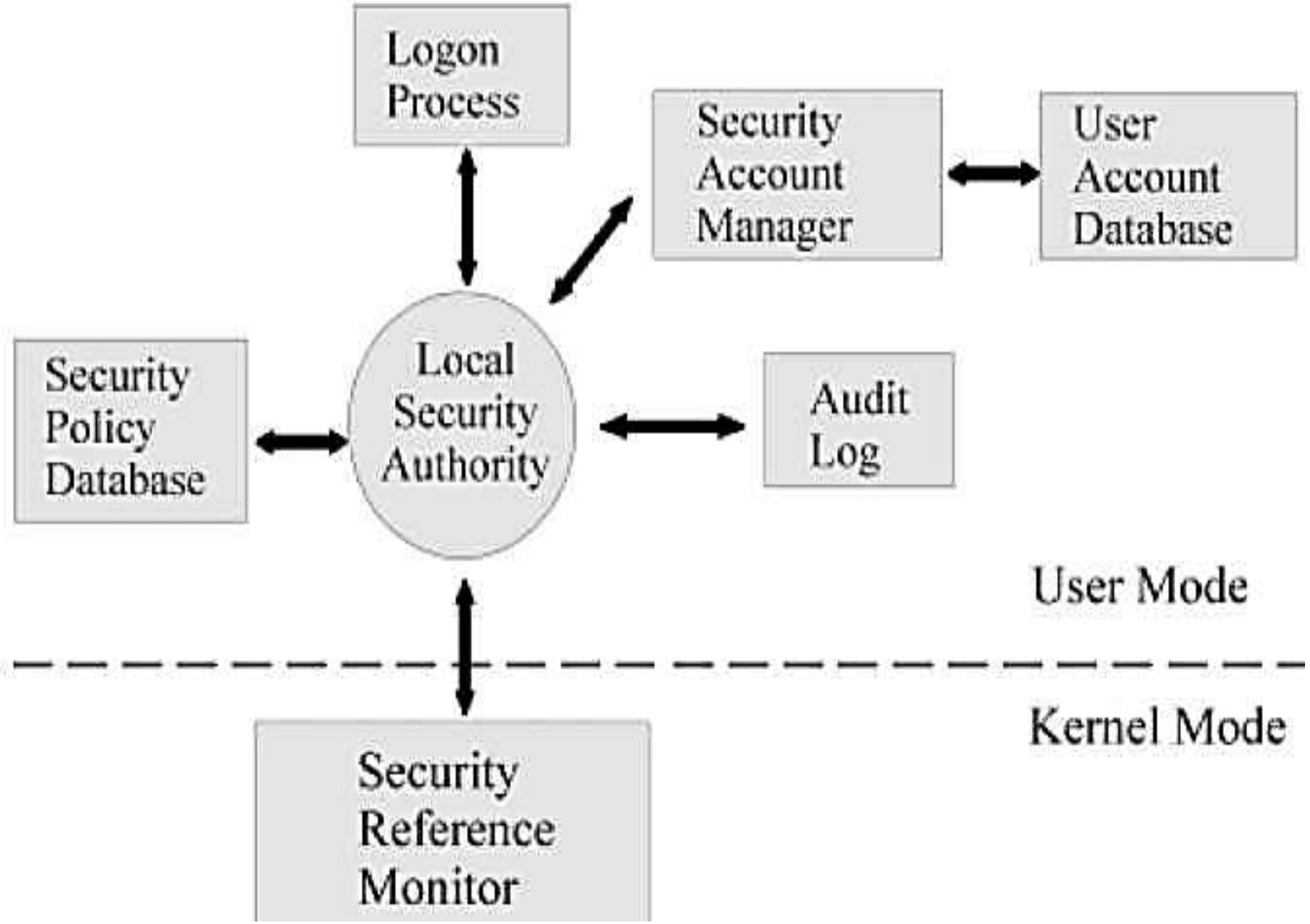
a) **Authentication,**

b) **Access control,**

c) **Confidentiality,**

d) **Integrity**

e) **Non-repudiation**.


Logon Process
Security Account Manager
User Account Database
Security Policy Database
Local Security Authority
Audit Log
User Mode
Kernel Mode
Security Reference Monitor

- The OSI security architecture **focuses on security attacks, mechanisms, and services**.
- These can be defined briefly as follows: Threats and Attacks (RFC 2828) Threat.
- A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

Security in Linux

- The Linux kernel boasts an array of built-in security defenses including **firewalls** that use packet filters in the kernel, the UEFI Secure Boot firmware verification mechanism, the Linux Kernel Lockdown configuration option and the SELinux or AppArmor Mandatory Access Control (MAC) security enhancement systems

Levels of security in Linux

- 3 levels of security in Linux
- For each level of access control (user, group, other), the 3 bits correspond to three permission types.
- For regular files, these 3 bits control **read access, write access, and execute permission**.
- For directories and other file types, the 3 bits have slightly different interpretations.

- These levels are user, group and others.
- Each permission level has three types of permission; **read, write and execute**.

How to secure Linux server

1. Only install required packages.
2. Disable the root login.
3. Configure 2FA.
4. Enforce good password hygiene.
5. Server-side antivirus software.
6. Update regularly or automatically.
7. Enable a firewall.