Parul® University
Vadodara, Gujarat

NAAC GRADE A++

Information and Communication Technology

Introduction to Operating Systems & Security Concept

Prof. Khushal Bhoyar
Department of CSE (Cyber Security)
PIET, Parul University

1.1 Core Concepts and Functions of Operating Systems

- An Operating System (OS) serves as an intermediary between computer hardware and users.
- It manages hardware resources and provides services for applications.
- Primary functions include:
- Process management.
- Memory allocation.
- File system organization.
- Device coordination.
- Security enforcement.
- Operating systems implement abstraction layers that hide hardware complexity.
- This abstraction enables applications to run across different hardware configurations.
- They provide consistent interfaces through system calls.

-cont

- System calls allow user programs to request services while maintaining system stability and security.
- Modern operating systems support concurrent execution of multiple processes.
- This is achieved through sophisticated scheduling algorithms and resource management techniques.

1.2 Types of Operating Systems

- **Batch processing systems** were the earliest OS type.
- They executed jobs in groups without user interaction.
- **Multiprogramming systems** improved CPU utilization.
- They kept multiple programs in memory simultaneously.
- The OS switched execution when one program waited for I/O.
- **Multiprocessing systems** utilize multiple CPUs.
- They execute several processes concurrently.
- This significantly enhances computational power.
- **Real-time operating systems (RTOS)** guarantee response within strict time constraints.
- They are essential for industrial control, medical devices, and aerospace applications.
- **Distributed operating systems** manage collections of independent computers as a single coherent system.
- They provide transparency of location and failure.

-cont

- **Cloud-based operating systems** represent the latest evolution.
- They are designed specifically for virtualized cloud environments.
- Key features include elastic resource allocation and multi-tenancy support.

1.3 OS Services and System Calls

- Operating systems provide essential services through well-defined interfaces.
- **Program execution services:** Load programs into memory and run them with proper resource allocation.
- **I/O operations:** Handle communication between devices and applications through standardized interfaces.
- **File system manipulation:** Enables creation, deletion, reading, and writing of files with appropriate permissions.
- **Communication services:** Facilitate data exchange between processes on the same system or across networks.
- **Error detection and response:** Identify and handle hardware/software malfunctions to prevent system failures.

-cont

- **System calls** serve as the programming interface to these services.
- They are typically implemented through software interrupts or special processor instructions.
- System calls transition the system from user mode to kernel mode while maintaining security boundaries.

1.4 Operating System Structures

- **Monolithic kernels** integrate all OS services in kernel space.
- They provide excellent performance but have reduced modularity and reliability.
- **Layered architectures** organize the OS into hierarchical levels.
- Each layer uses services of lower layers and provides services to higher ones.
- This enhances modularity at the cost of some performance.
- **Microkernels** minimize kernel functionality.
- Most services run as user-space servers.
- This improves reliability and security but may reduce performance due to increased inter-process communication.
- **Hybrid kernels** combine aspects of monolithic and microkernel designs.
- They keep critical components in kernel space while moving others to user space.

.

-cont

- **Modular kernels** use dynamically loadable modules.
- Modules can be added or removed as needed.

This offers flexibility while maintaining the performance advantages of monolithic designs

1.5 Virtual Machines and Virtualization

- Virtualization technology enables multiple operating systems to run simultaneously on a single physical machine.
- It works by abstracting hardware resources.
- **Type 1 hypervisors (bare-metal)** run directly on hardware.
- They offer superior performance for server virtualization.
- **Type 2 hypervisors** run as applications on a host OS.
- They are commonly used for desktop virtualization.
- **Virtual machines (VMs)** provide complete isolation between guest systems.
- Each VM has its own virtual CPU, memory, storage, and network interfaces.

-cont

- **Containerization** offers lightweight virtualization at the OS level.
- Containers share the host kernel while providing isolated user spaces.
- Virtualization enables:
- Server consolidation.
- Sandboxing for security testing.
- Legacy system support.
- Forms the foundation of cloud computing infrastructures.

1.6 Platform Security Fundamentals

Platform security encompasses hardware, firmware, and software mechanisms that protect computing systems.
The **CIA triad** forms the foundation:
Confidentiality: Ensures information accessibility only to authorized entities.
Integrity: Maintains data accuracy and consistency.
Availability: Guarantees reliable access to information for authorized users.
Attack surfaces represent all points where an attacker can try to enter or extract data from a system.
Examples include network interfaces, user inputs, APIs, physical ports, and peripheral devices.
Modern platforms implement **defense-in-depth** strategies.
This involves multiple security layers.
It requires attackers to breach several independent defenses to compromise the system.

Table: Comparison of OS Security Mechanisms

Security Mechanism	Implementation Level	Primary Protection	Performance Impact
User Account Control	Application/OS	Unauthorized privilege escalation	Low
Address Space Layout Randomization	Memory Management	Buffer overflow attacks	Minimal
Data Execution Prevention	CPU/Memory	Code injection attacks	Low
Secure Boot	Firmware/BIOS	Boot-time malware	None during runtime
Full Disk Encryption	Storage System	Data theft from lost/stolen devices	Medium
Mandatory Access Control	Kernel	Process isolation and containment	Low to Medium

1. https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs

2. https://www.konverge.co.in/virtualization-in-cloud-computing-need-types-and-importance/

3. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-application-security/

Parul® University

NAAC GRADE A++

https://paruluniversity.ac.in/