

OPERATING SYSTEM SECURITY

Subject Code: CS34213CS	Subject Type: Core
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 2-0-2

Pre-Requisites: Operating Systems, Computer Networks, Data Structures and Algorithms, Database Management Systems, Programming (C/Python/Java), Computer Architecture, Basic Knowledge of Computer Security and Virtualization

Course Objective:

1. To understand the core concepts, architecture, and services of modern operating systems.
2. To analyze process, memory, file, and resource management mechanisms in operating systems.
3. To study security models, protection mechanisms, and trusted operating system design principles.
4. To understand security implementation in UNIX/Linux and Windows operating systems.
5. To evaluate operating system vulnerabilities, attacks, and mitigation techniques for secure computing environments.

Course Outcomes: At the end of the course, the student will be able to

CO-1	Analyze the architecture, services, and process management mechanisms of operating systems.
CO-2	Evaluate memory management, storage systems, and file system implementation techniques.
CO-3	Analyze operating system security models, access control mechanisms, and trusted system design principles.
CO-4	Evaluate modern operating system security implementations, vulnerabilities, and protection techniques in real-world computing environments.

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	2	2	-	-	-
CO-2	3	3	2	1	1	1
CO-3	3	3	3	2	2	-
CO-4	3	3	2	2	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Operating System Fundamentals and Process Management

Introduction to operating systems, Operating system structures and services, System calls and kernel architecture, Process concept and process states, Threads and multithreading models, CPU

scheduling algorithms, Inter-process communication, Synchronization mechanisms, Deadlocks and deadlock handling techniques, Distributed operating systems overview

Unit-2: Memory, Storage, and File System Management

Memory hierarchy and management techniques, Contiguous and non-contiguous memory allocation, Paging and segmentation, Virtual memory and demand paging, Page replacement algorithms, Thrashing and working set model, File system architecture and implementation, File allocation methods, Free space management, Disk scheduling algorithms, I/O systems and storage management

Unit-3: Operating System Protection and Security Models

Security goals and trusted systems, Protection mechanisms and access control, Authentication and authorization models, Reference monitor concept, Information flow security, Bell-LaPadula confidentiality model, Biba integrity model, Clark-Wilson model, Denning's lattice model, Secure kernel architecture, Security policies and assurance techniques

Unit-4: Security in Modern Operating Systems and Emerging Trends

UNIX/Linux security architecture, Windows security architecture and protection mechanisms, User authentication and privilege management, Malware and privilege escalation attacks, Address Space Layout Randomization (ASLR), Secure boot and trusted execution, Logging and auditing mechanisms, Operating system hardening techniques, Virtualization and container security, Cloud and distributed operating system security, Mobile and IoT operating system security, Zero-trust systems, AI-assisted threat detection, Case studies on recent operating system vulnerabilities and mitigation techniques

Learning Resources:

Text Books:

1. Abraham Silberschatz, Peter B. Galvin, Greg Gagne, *Operating System Concepts*, Wiley, 10th Edition.
2. William Stallings, *Operating Systems: Internals and Design Principles*, Pearson.
3. Trent Jaeger, *Operating System Security*, Morgan & Claypool Publishers.

Reference Books:

1. Andrew S. Tanenbaum, Herbert Bos, *Modern Operating Systems*, Pearson.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger, *Security in Computing*, Pearson.
3. Avi Silberschatz, Greg Gagne, Peter Baer Galvin, *Applied Operating System Concepts*, Wiley.
4. Michael Palmer, *Guide to Operating Systems Security*, Cengage Learning.
5. Gerardus Blokdyk, *Security Focused Operating System – A Complete Guide*, 5STARCook.