DEPARTMENT OF CYBER SECURITY

U23CBT44/ OPERATING SYSTEMS AND SECURITY

PART B

UNIT I OPERATING SYSTEM OVERVIEW

1. Explain the components of a computer system and their interaction during program execution.
2. Explain the different types of computer architectures (e.g., single-core, multi-core, RISC, CISC) and their impact on operating system design.
3. Discuss the challenges of resource management in a distributed computing environment.
4. How do modern operating systems handle user authentication and authorization to enhance security?
5. Explain the architecture of a distributed system and the challenges associated with its implementation.
6. What are kernel data structures, and how are they used to manage operating system functionalities?
7. Explain the structure of system calls and their role as an interface between user applications and the kernel.
8. Outline the steps involved in building and booting an operating system.

UNIT II PROCESS MANAGEMENT

1. Discuss different methods of Inter-Process Communication (IPC), including message passing and shared memory. Highlight their advantages and disadvantages.
2. Explain and compare the following scheduling algorithms with examples:

- First-Come, First-Served (FCFS)
- Shortest Job Next (SJN)
- Priority Scheduling
- Round-Robin (RR)

3. What is the critical-section problem? Discuss the three requirements (mutual exclusion, progress, and bounded waiting) for a solution to the critical-section problem.
4. Explain the concept of mutex locks and their role in process synchronization.

5. Describe semaphores as a synchronization tool. Differentiate between binary semaphores and counting semaphores with examples.
6. Discuss the banker's algorithm as a deadlock avoidance strategy. Provide a step-by-step explanation of how it works.
7. Compare deadlock prevention, avoidance, and detection in terms of their applicability and system overhead.

UNIT III MEMORY MANAGEMENT AND FILE SYSTEMS

1. Explain the structure of main memory and the challenges associated with managing it in a multitasking environment.

2. Compare and contrast contiguous memory allocation with paging and segmentation. Discuss their advantages and disadvantages.
3. Describe the structure and role of a page table in paging. How does the Translation Lookaside Buffer (TLB) improve paging performance?
4. Explain segmentation as a memory management technique. How does it differ from paging in terms of implementation and usage?
5. Define virtual memory and explain how it allows programs to run larger than physical memory.
6. What is demand paging? Describe the steps involved in handling a page fault.
7. Compare and contrast the following page replacement algorithms with examples:

- First-In-First-Out (FIFO)
- Least Recently Used (LRU)
- Optimal Page Replacement

8. Explain the role of free space management in file systems. Why is it crucial for efficient storage utilization?

UNIT IV SECURE SYSTEMS AND VERIFIABLE SECURITY GOALS

1. Explain the concept of trust in a computing system. How does a trust model help in defining security policies?
2. Discuss the different types of access control mechanisms (e.g., discretionary access control, mandatory access control, role-based access control). Provide examples of each.
3. Define a protection system in the context of operating systems. Discuss the relationship between access control and protection.
4. What constitutes a secure operating system? Discuss the essential features and functionalities it must possess.
5. Explain the concept of information flow in a secure system. How does controlling information flow contribute to system security?
6. What are information flow secrecy models, and why are they important in secure system design?

7. Explain Denning's lattice model of secure information flow. How does it enforce security policies in multi-level systems?
8. Describe the Bell-LaPadula (BLP) model. How does it ensure confidentiality in a multi-level security system?

UNIT V SECURITY IN OPERATING SYSTEMS

1. Explain the design principles behind UNIX security. How do file permissions, user roles, and groups contribute to the overall security of the system?
2. Discuss the UNIX protection system in detail, focusing on mechanisms like access control lists (ACLs) and Secure Shell (SSH). How do they ensure secure operations?
3. Describe the process of user authorization in UNIX. How are user and group permissions managed effectively?
4. Identify the most common vulnerabilities in UNIX systems. Discuss real-world examples of UNIX-based exploits and the countermeasures implemented to address them.
5. Analyze the Windows security model. Explain how User Account Control (UAC), NTFS permissions, and Windows Defender contribute to securing the operating system.
6. Explain the role of Active Directory in Windows authorization. How does it integrate with Kerberos and LDAP for secure authentication and authorization?
7. Identify common vulnerabilities in Windows systems. Discuss high-profile incidents involving these vulnerabilities and how they were addressed.