



OPERATING SYSTEMS- SECURITY



Presented by-

45 Vanshika Khatri
53 Prem Narayani
54 Hitesh Nihalani
55 Drishti Ochani

Introduction

- **Definition of OS Security:** Operating system security encompasses measures to protect data integrity, confidentiality, and accessibility in systems.
- **Importance of Data Protection:** Effective OS security safeguards sensitive information from unauthorized access, ensuring user trust and regulatory compliance.
- **Maintaining System Functionality:** Robust security mechanisms are essential for delivering consistent system performance while mitigating potential vulnerabilities.





What is Encryption?

- **Encryption Definition:** Encryption transforms data into unreadable code, ensuring only authorized users can access sensitive information.
- **Data Protection Mechanism:** Employing encryption prevents unauthorized access, safeguarding user data against breaches and malicious entities.
- **Role in OS Security:** Integral to operating systems, encryption maintains data integrity, confidentiality, and security within digital environments.



Types of Encryption

- **Symmetric encryption:** Utilizes a single key for both encryption and decryption, ensuring fast processing and performance.
- **Asymmetric encryption:** Employs a pair of keys (public and private) to enhance security, facilitating secure communications.



How operating systems use encryption ?

- **File System Encryption:** Employs encryption to protect individual files, ensuring unauthorized users cannot access sensitive data.
- **Full Disk Encryption:** Encrypts the entire disk, safeguarding all stored data against unauthorized access and physical theft.
- **Securing Network Communications:** Utilizes encryption protocols to secure data during transmission, protecting against interception and eavesdropping.

Challenges of Encryption

- **Performance Overhead:** Encryption often incurs processing delays, impacting system performance and affecting user experience during operations.
- **Key Management Complexities:** Effective encryption relies on robust key management practices, which can be operationally challenging and resource-intensive.
- **Balancing Security and Speed:** Achieving optimal encryption levels requires balancing security needs with the system speed and performance capabilities.



Identity Management in OS

- **Authentication Importance:** Establishing users' identities through robust authentication methods is crucial for securing access to systems.
- **Access Permissions:** Authorization determines user permissions, ensuring that only authorized individuals have access to specific resources.
- **Action Auditing:** Comprehensive auditing mechanisms track user actions, providing accountability and facilitating forensic analysis when necessary.



Technologies Used in Identity Management

- **Single Sign-On (SSO):** SSO allows users to authenticate once, gaining access to multiple applications without repeated logins.
- **Directory Services:** Directory services manage user data and permissions, streamlining authentication processes across networked resources.
- **Pluggable Authentication Modules (PAM):** PAM enables flexible authentication mechanisms, allowing systems to integrate various authentication methods seamlessly.



Advanced Security Mechanisms in OS

- **Mandatory Access Control (MAC):** MAC enforces strict access policies based on security labels, limiting user control over resources.
- **Role-Based Access Control (RBAC):** RBAC assigns permissions according to user roles, enhancing security by streamlining access management processes.
- **Sandboxing Applications:** Sandboxing isolates applications within controlled environments, minimizing risks from malicious software and unauthorized access.

Threats and Vulnerabilities in OS Security

- **Malware Threats:** Malware can compromise operating systems, leading to data theft, system damage, and unauthorized access.
- **Privilege Escalation:** Attackers exploit vulnerabilities to gain elevated access, potentially compromising sensitive system resources and security.
- **Insider Threats:** Internal actors with legitimate access may intentionally or accidentally compromise system security, endangering data integrity.

How to Protect Against OS Security Threats

- **Timely Updates:** Regular updates patch vulnerabilities, enhancing security by mitigating risks from emerging threats and exploits.
- **Intrusion Detection Systems:** IDS monitor network activity, identifying and responding to potential security breaches in real-time efficiently.
- **Secure Coding Practices:** Implementing secure coding reduces vulnerabilities, ensuring software robustness and safeguarding against code injection attacks.



Emerging Trends in OS Security

- **Zero Trust Architecture:** Adopting a Zero Trust model mandates strict identity verification, reducing risks of unauthorized access and breaches.
- **Hardware-Based Solutions:** Utilizing hardware-based security, like TPM, enhances encryption key protection and safeguards against physical attacks.
- **AI in Security:** AI applications bolster security by enabling adaptive threat detection, predicting vulnerabilities, and automating response mechanisms.



Case Studies: Security in Windows, Linux, Mac OS

- **BitLocker in Windows:** BitLocker provides full disk encryption, protecting sensitive data on Windows devices from unauthorized access.
- **SELinux in Linux:** SELinux enhances security by enforcing mandatory access controls, limiting application access to system resources.
- **FileVault in macOS:** FileVault encrypts the entire startup disk, ensuring data protection on macOS devices against unauthorized access.

Best Practices for OS Security

- **Regular Updates:** Consistently applying software updates mitigates vulnerabilities, enhancing the overall security posture of operating systems.
- **Least Privilege Access:** Implementing least privilege ensures users have only necessary permissions, reducing risks of unauthorized actions significantly.
- **User Education:** Educating users on security best practices fosters a security-aware culture, minimizing human-related vulnerabilities in systems.



Conclusion

- **Key Takeaway:** Operating system security is pivotal for safeguarding sensitive data and ensuring operational reliability across environments.
- **Importance of Robust Mechanisms:** Advanced security measures, including encryption and identity management, critically defend sensitive information from potential threats.
- **Ongoing Education:** Continuous education on security practices empowers users, promoting diligence in maintaining system integrity and privacy.



References

- **ResearchGate Resource:** The 'Operating System Security' article on ResearchGate provides valuable insights into various OS security practices.
- **IEEE Articles:** IEEE offers numerous articles addressing critical OS security issues, essential for contemporary research and understanding.
- **IJCRT Study:** IJCRT's study on Windows OS security explores specific vulnerabilities and proposes effective mitigation strategies.



THANK YOU!