Sri Lanka Institute of Information Technology

Securing Operating Systems: A Comprehensive Approach to Security with Best Practices and Techniques

Secure Operating Systems (IE2032)

Year 2 Semester 1 - 2025

Group Members Details

- **Topic :** Securing Operating Systems: A Comprehensive Approach to Security with Best Practices and Techniques
- **Course code:** IE2032
- **Batch:** Y2.S1.WD.CS

IT Number	Name
IT23822412	H.M.S.T. Karunarathna (Group Leader)
IT23834088	Raksha Mariyanesan
IT23833920	Rachana Mariyanesan
IT20625566	D.S.W. Weerakoon

- # Introduction

In modern computing, operating systems (OS) serve as the vital bridge between user applications and underlying hardware. With the escalating dependence on interconnected digital environments, safeguarding operating systems has become a matter of paramount importance. In 2024, a research article named ‘A Critical Analysis of “Securing Operating Systems: A Comprehensive Approach to Security with Best Practices and Techniques” by Zarif Bin Akthar, published in the International Journal of Advanced Network Monitoring and Controls, presents a comprehensive investigation into OS security challenges, methods, and best practices. The work not only draws from a vast pool of literature but also employs empirical testing, case studies, and experimental designs to provide a full-spectrum view of the security landscape for operating systems.

• Research Scope and Objectives

The research establishes multiple objectives. firstly, to delineate the theoretical foundations of OS security. Secondly, to investigate real-world threats and vulnerabilities. Thirdly, to evaluate security solutions through verifiable evidence, and finally, to provide strategic guidance for improving system security.

The approach by author was multi-disciplinary, considering aspects such as human factors, system architecture, encryption techniques, and policy frameworks. His focus on integrating real-world practices with academic high standards makes the paper accessible yet deeply analytical.

• Methodological Strength

Research methodology by the author was commendably robust, combining:

- **Theoretical review:** Analyzing existing frameworks, architectures, and historical evolution.
- **Empirical data:** Extracted from threat reports, advisories, and system logs.
- **Case studies:** Including historical incidents such as the Morris worm.
- **Experimental testbeds:** Evaluating malware impact, buffer overflows, and intrusion detection systems (IDS).
- **Comparative analyses:** Benchmarks across different operating systems and tools.
- **Qualitative input:** Gathered from forums and expert interviews.

This triangulation allows for cross-validation of findings and reinforces the credibility of the conclusions.

Core Principles of OS Security

The author grounds his discussion in the CIA triad (Confidentiality, Integrity, and Availability), which serves as a framework for identifying vulnerabilities and designing countermeasures.

He distinguishes protection mechanisms (resource control within the system) from security mechanisms (defense from external threats), asserting that both are necessary for robust system integrity. Foundational tools such as passwords, file permissions, and encryption are positioned as the first line of defense

Threat Categorization

The paper provides an effective breakdown of threats under the categories of program threats, system/network threats, and authentication/cryptographic weaknesses:

- **Program threats:** Logic bombs, trapdoors, Trojan horses, and buffer overflow attacks. Stack overflow diagrams clearly depict how return addresses can be hijacked to inject malicious code.
- **System threats:** Including port scanning, worms (e.g., Morris Worm), and Denial-of-Service (DoS) attacks, which can cripple systems by overwhelming resources.
- **Authentication threats:** Exploiting weak passwords, shoulder surfing, or social engineering to gain unauthorized access.

These threats are explained using real scenarios and technical illustrations that help even non-specialist readers grasp their implications.

Security Techniques and Controls

Author discusses various methods and techniques used to counter the outlined threats:

- **Access Control:** Using discretionary (DAC), mandatory (MAC), and role-based access control (RBAC) models.
- **Encryption:** Describes symmetric (AES, DES) and asymmetric (RSA) encryption with implementation illustrations
- **Authentication**: Covers static and one-time passwords (OTPs), as well as biometric methods such as fingerprint or retinal scans.
- **IDS and Firewalls:** Akhtar elaborates on anomaly-based vs. signature-based IDS, application proxy firewalls, XML firewalls, and personal firewalls. He explains the use of DMZs for isolating internal networks from public-facing services.

His discussion of Tripwire, a file integrity monitoring tool, is particularly insightful, emphasizing the need to detect unauthorized file changes after breaches have occurred.

Cryptographic Mechanisms

Author explores the use of cryptography as a safeguard against data breaches, especially over public or untrusted networks:

- **Encryption:** Highlights the role of block ciphers and stream ciphers, including modern algorithms like AES and Twofish.
- **Hashing:** Uses SHA or MD5 to ensure data integrity.
- **Digital Signatures and Certificates**: He underscores the role of public key infrastructures (PKIs) in enabling secure key exchanges and verifying authenticity.

His explanation of asymmetric encryption with public and private key pairs, including man-in-the-middle (MITM) vulnerabilities, demonstrates a deep understanding of modern cryptographic issues.

Human-Centric Vulnerabilities

One of the most valuable sections of the paper addresses human vulnerabilities, often overlooked in technical security discussions:

- **Social Engineering:** Through phishing and manipulation.
- **Poor password practices:** Reuse, weak passwords, and lack of MFA.
- **Insider threats:** Disgruntled or careless employees.

The author suggests enhanced training, routine policy enforcement, and the deployment of multi-factor authentication (MFA) to mitigate these risks.

Logging, Auditing, and Monitoring

The paper emphasizes logging and auditing as critical tools for real-time monitoring and forensic analysis. Logs can reveal patterns, intrusion attempts, and misuse. However, Akhtar notes that performance overheads are a trade-off, and administrators must carefully balance granularity and system impact.

Security Classifications

The paper references the Trusted Computer System Evaluation Criteria (TCSEC), commonly known as the Orange Book, to classify OS security levels:

- **D-class:** No protection.
- **C1/C2-class:** Basic discretionary access and auditing (e.g., traditional UNIX systems).
- **B-class:** Enhanced labeling and object sensitivity.
- **A-class:** Mathematically verifiable system integrity using formal methods.

The author places emphasis on Class C2 and B1 systems, noting that many enterprise systems strive to meet these standards for regulatory compliance.

• Emerging Technologies and Trends

The discussion section provides insights into how the OS security domain is evolving with new technologies:

- **Cloud Computing:** Introduces new layers of complexity with shared resources and virtual machines.
- **Containers and Virtualization:** Present both advantages (isolation) and challenges (shared kernel vulnerabilities).
- **Internet of Things (IoT):** Raises concerns due to minimal OS footprints and lack of regular patching.
- **AI in Cybersecurity:** Highlights promising tools for behavioral analysis, anomaly detection, and automation in patching.

The author argues that as systems grow more complex, security approaches must become proactive, leveraging machine learning and real-time analytics.

• Policy Recommendations

To complement the technical measures, Akhtar offers policy-level best practices:

- **Security Awareness Training:** Educating users about phishing, social engineering, and safe computing habits.
- **Patch Management:** Emphasizing the timely application of OS and application updates.
- **Incident Response Planning:** Recommending structured response protocols for breaches.
- **Compliance Audits:** Aligning systems with standards like ISO 27001 or NIST 800-53.

These guidelines reflect a well-rounded view that spans technology, governance, and culture.

Strengths of the Research

Several attributes make this paper a standout contribution to the field:

- **Interdisciplinary Approach:** Technical, behavioral, and policy aspects are all covered.
- **Visual Illustrations:** Diagrams enhance comprehension of complex topics.
- **Empirical Validity:** The use of case studies and experimental data grounds the theory in practice.
- **Forward-Looking:** The inclusion of AI, IoT, and cloud security reflects contemporary relevance.

Areas for Further Enhancement

Despite its strengths, there are areas where the paper could expand:

- **Quantitative Metrics:** Performance benchmarks and threat frequency data would solidify the analysis.
- **Cross-industry Comparisons**: Different sectors (e.g., healthcare vs. fintech) face unique security requirements.
- **Cost Considerations:** Economic implications of security implementations are not discussed.
- **Usability vs. Security:** The balance between user convenience and stringent access control is not fully explored.

These additions could broaden the applicability of the findings to a wider audience.

- ## Conclusion

The research paper wrote by Zarif Bin Akthar was a significant contribution to the field of cybersecurity. Its strength lies in its exhaustive scope, ranging from foundational OS security theories to cutting-edge technological implications. By integrating theoretical, empirical, and qualitative perspectives, the author crafts a narrative that is not only informative but actionable.

In a digital world fraught with evolving threats, Akhtar provides both a technical blueprint and a strategic roadmap for organizations, developers, and policymakers to safeguard operating systems against current and future risks. The paper successfully bridges the gap between academia and real-world application, establishing itself as essential reading for anyone involved in cybersecurity or IT infrastructure management.

References

Akhtar, Z. B. (2024). Securing Operating Systems (OS): A Comprehensive Approach to Security with Best Practices and Techniques. International Journal of Advanced Network Monitoring and Controls, 09(01), 100–111. DOI: 10.2478/ijanmc-2024-0010