IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

OPERATING SYSTEMS SECURITY – A REVIEW

Shravani Kharade, Samruddhi Takawale,
Akshada Kumbhar, Mrs Mayuri Bapat
Mohammadwadi Pune, Hadapsar Pune, chikli, Pune
Science and computer science department

MIT Arts, Commerce & Science College alandi, Pune, India

Abstract— Security is a primary concern in the modern world. The main focus of this paper is the security of our information and its supporting infrastructure. With good cause, there has been significant effort over the past decade by operating system developers focused on improving the security of operating systems. This has resulted in regular patching, various security- oriented operating system. By keeping the computer system secure we can provide the security to the computer information. In order to have a secure operating system it must be supported by the suitable computer architecture. There is a strong interrelationship between security and privacy even though they are distinct domains, and the aspects of each are often confused. In this paper, I will study the differences between security and privacy as it relates to operating systems and report on developments, contrasts and future improvements. operating system security is a critical area of research and development, pivotal to save guarding information technology systems from unauthorized accesses, data bridges and other cyber threads.

INTRODUCTION:

In general, the concern of security in operating systems is with the problem of controlling access to computer systems and the information stored in them. There have been identified four types of overall protection policies of increasing order of difficulty [6]:

1.No sharing: processes are completely isolated from each other, and each process has exclusive control over the resources statically or dynamically assigned to it. In this case, processes often share a program or data file by making a copy of it and transferring the copy into their own virtual memory.

2.Sharing originals of program or data files: with the use of reentrant code, a single physical realization of a program can appear in multiple virtual address spaces, as can read-only data files. To prevent simultaneous users from interfering with each other, special locking mechanisms are required for the sharing of writable data files.

3. Confined, or memory-less, subsystems: In this case, processes are grouped into subsystems to enforce a particular protection policy. For example, a client process calls a server process to perform some task on data. The server is to be protected against the client discovering the algorithm by which it performs the task, while the client is to be protected against the server's retaining any information about the task being performed.

4.Controlled information dissemination: In some systems, security classes are defined to enforce a particular dissemination policy.Users and applications are given security clearances of a certain level, while data and other resources are given security classifications. The security policy enforces restrictions concerning which users have access to which classifications. This model is useful not only in the military context but commercial applications as well.

The work in security and protection as it relates to operating systems can be grouped into three categories.

1.Access control: concerned with regulating user access to the total system, sub systems, and data, and regulating process access to various resources and objects within the system.

2.Information flow control: regulates the flow of data within the system and its delivery to users.

3.Certification: relates to proving that access and flow control mechanisms per form according to their specifications and that they enforce desired protection and security policies.

cia triad

Principles of operating system Security:

Operating System (OS) Security is built on a set of fundamental principles designed to protect the integrity, confidentiality, and availability of computing systems. Understanding these principles is crucial for anyone involved in the development, administration, or use of operating systems.

1.Least Privilege:The principle of least privilege dictates that users and programs should operate using the least amount of privilege necessary to complete a task. This limits the potential damage from accidents or malicious actions by reducing the access and permissions to the minimum required.

2. Defense in Depth: Défense in depth is a strategy that employs multiple layers of security controls and defenses throughout the system. If one layer fails, others still stand, providing a comprehensive approach to security that addresses potential physical, technical, and administrative vulnerabilities.

3. Fail-Safe Defaults: Systems should be designed to default to a state of security if they fail. Access decisions should deny by default, and permissions should not be granted unless explicitly allowed. This ensures that if a failure occurs, the system remains secure.

4. Economy of Mechanism: The design of security mechanisms should be as simple and small as possible. Complex systems are harder to secure because they potentially have more vulnerabilities. Simplification aids in the verification and validation of security properties.

5. Complete Mediation:

Every access to every resource must be checked for authorization. This principle ensures that attackers cannot bypass security controls to access sensitive resources. It requires the system to verify permission for an action each time that action is attempted.

Requirements for operating system:

An understanding the types of threats to OS security that exist requires a definition of security requirements. OS security addresses four requirements:

1.Confidentiality: requires that the information in a computer system be accessible only for reading by authorized parties. This type of access includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object. 2.Integrity: requires that only authorized parties can modify computer system assets. Modification includes writing, changing, changing status, deleting, and creating.

3.Availability: requires that computer system assets are available to authorized parties.

4.Authenticity: requires that a computer system be able to verify the identity of a user

Methods to Ensure Protection and Security in Operating System:

Keep a Data Backup: It is a safe option in case of data corruption due to problems in protection and security, you can always require it from the Backup. Beware of suspicious emails and links: When we visit some malicious link over the internet, it can cause a serious issue by acquiring user access. Secure Authentication and Authorization: OS should provide secure authentication and authorization for access to resources and also users should keep the credentials safe to avoid illegal access to resources

Use Secure Wi-Fi Only: Sometimes using free Wi-Fi or insecure Wi-Fi may cause security issues, because attackers can transmit harmful programs over the network or record the activity etc., which could cause a big problem in the worst case.

Install anti-virus and malware protection: It helps to remove and avoid viruses and malware from the system.

Manage access wisely: The access should be provided to apps and software by thorough analysis because no software can harm our system until it acquires access. So, we can ensure to provide suitable access to software and we can always keep an eye on software to see what resources and access it is using.

Firewalls Utilities: It enables us to monitor and filter network traffic.We can use firewalls to ensure that only authorized users are allowed to access or transfer data.

Encryption and Decryption Based transfer: The data content must be transferred according to an encryption algorithm that can only be reversed with the appropriate decryption key. This process protects your data from unauthorized access over the internet, also even if data is stolen it would always remain unreadable.

Be cautious when sharing personal information: The personal information and credentials must be shared only with trusted and safe sources by not doing so attackers can use this information for their intent which could be harmful to the system's security.

Operating system security tools:

Operating system security tools encompass a range of software designed to protect the operating system from various threats Antivirus/Anti-malware software:

Detects and removes viruses,worms, Trojans, and other malicious software.

Firewall: Monitors and controls incoming and outgoing network traffic based on predetermined security rules. Intrusion Detection Systems (IDS) and Intrusion

Prevention Systems (IPS) : Detect and prevent unauthorized access to computer networks or systems. File Integrity Checkers: Monitor and detect unauthorized changes to critical system files.

Encryption Tools: Encrypt sensitive data to prevent unauthorized access. Patch Management Software: Ensures that operating system and application software are up-to-date with the latest security patches.

Vulnerability Scanners Identify weaknesses in the operating system or installed software that could be exploited by attackers. Log Management and Analysis Tools: Collect, store, and analyse log data to detect and investigate security incidents.

Authentication Tools: Manage user authentication and access control mechanisms to ensure only authorized users can access the system.These tools can vary incomplexity and functionality, and their effectiveness depends on proper configuration, maintenance, and integration within the overall security posture of an organization.

MODEL OF SECURITY:

In an access control based security model, there are two sets-a set of objects and a set of subjects, which can itself be an object. Each object and subject has a corresponding security attribute or label or clearance, and a defined set of control rule or security policy. This determines which subject is authorized to access which object.

For example, in military security model, a security label consists of two components: a security level with one of the four ratings: unclassified, confidential, secret, and top secret, where unclassified < confidential < secret < top secret, and " NUCLEAR might mean information about cryptographic algorithms, and nuclear. related technology. Given two security labels, (X, S1) and (Y, S2), (X, S1) is defined as being "at least as sensitive as" (Y, S2) iff X • Y and

S2 S1. For example, (TOP SECRET, {CRYPTO, NUCLEAR})> (SECRET,{CRYPTO}) where">" means "more sensitive than". In general, security labels are partially ordered. That is, it is possible for two labels to be incomparable, in the sense that neither is more sensitive than the other. For example, neither of the following is comparable to each other: (TOP SECRET, {CRYPTO}) (SECRET, {NUCLEAR}).A more generalized hierarchy of security classes (or levels) with a mathematical basis was presented by Bell and La Padula in 1973.

Conclusion:

In this paper we listed the primitive security services that are provided in general by operating systems. The services are: memory protection, file protection, general object access protection and user authentication. If those services are provided in a consistent andefficient way, the system in considered being trusted which means that the system meets the security requirements, is of high enough quality and justifies the user's confidence in that quality. [7] The underpinnings of a trusted operating system are: policy, model, design and trust.

References:

[1]https://ijirt.org/master/pub lished paper/IJIRT100350_PAPE R.pdf

[2]"Flask: Flux Advanced security Kernel",

https://wwwold.cs.utah.edu/flux/fluke/h tml/fl ask.html

[3]Issues of Operating Systems Security
https://www.researchgate.net/publication/228409741_Issueo f_Operating_Systems_Secur ity

[4]Tipton, H., Krause, M. -Information Security Auerbach, 2002;
Charlie Kaufman, Radia Perlman, and Mike Speciner,"Network Security: Private Communication in a Public World", PTR Prentice Hall, Englewood Cliffs, New Jersey, 1995.

[6]Tipton, H., Krause, M. -Information Security Auerbach, 200

[7]Pfleeger, C. - Security in Computing, Ed. Prentice Hall, 2003