Detailed Analysis of Security in in Operating Systems

1st Author

1st author's affiliation
1st line of address
2nd line of address
Telephone number, incl. country code

1st author's E-mail address

2nd Author

2nd author's affiliation
1st line of address
2nd line of address
Telephone number, incl. country code

2nd E-mail

3rd Author

3rd author's affiliation
1st line of address
2nd line of address
Telephone number, incl. country code

3rd E-mail

**ABSTRACT**

The paper is intended to cover a Detailed analysis of Security in Operating Systems. It will involve explanations of different types of operating systems including bash, time sharing, distributed and network operating systems and cover central criterions which are required to meet including user accounts management, account policies, file systems and security of network services. It will also explain how to avoid threats due to inadequate operating system security, which are based only on user identity information and require to achieve kernel level security. The paper will extensively cover possible security issues using conventional operating systems with details of various security levels, including D, C1, C2, and B2, until A1, which is considered as the most secure level, where most operating systems are secure up to C2 or below. Recent cases study that provide secure operating system controls on kernel level will also be discussed.

**Keywords**

Security of Operating System; Kernel Level

# INTRODUCTION

**1.1 Operating System**

Operating system is a low-level software that works as an interface to link the computer user and hardware of a computer. It manages all tasks relating to software and hardware like scheduling tasks and managing peripherals. The operating system acts like a ‘manager’ to provide memory, central processing unit and storage to multiple programs running simultaneously.



Figure 1-General Operating System [8]

**1.2 Operating system security**

Operating system security (OS Security) is a vital process to ensure the availability, discretion and integrity of an operating system. OS security includes a set of measures which shield the OS from distant hacker attacks, malware invasions, warms, viruses and threats. OS Security is established in multiple ways which include:

# LITERATURE REVIEW

The first operating system was introduced in early 1950s. In [2], the complete background of operating systems ranging from batch processing system in 1950s to the distributed system in 1990s is described. With time, new operating system is introduced according to market needs.

However, there are six operating systems worth mentioning hat altered the concept of user’s access to computer. These include simple batch system, open shop, multiprogramming, distributed system, personal computing, and time-sharing operating systems. Earlier, there was no methodology to lessen the computer idle time to tackle that issue. Therefore, the batch system was introduced. Batch system used the swift tape stations and small-sized satellites computers. [2] The batch systems required user to submit a program on a card and the operator would pit multiple programs on the input devices without interaction between the user and the computer system.

A time-sharing OS lets multiple users access resources of the computer at same time. The main objective is to reduce the response time by letting multiple programs utilize resources in their specified time slots [3]. It can be described through an example of a mainframe computer, where numerous users are logged in simultaneously.

Networking operating systems are based on internet and computer networking. The Networking Operating system uses stack protocols in their architecture so as to provide means to computer networking [5]. Networking OS is fundamentally designed facilitate personal computer systems, workstations, and sometimes older terminals, connected on any local area network (LAN).

There is not only research conducted on Distributed Operating System but also, they are available for commercial use. The selection of machine in Distributed OS is automated [7]. The main purpose to develop a better operating system is to make low-cost and efficient microprocessor.

## Criteria

In case at any time, operating system becomes defenseless, the application security is compromised as the operating system provides the environment to any application to run. There exists security policies and criteria for operating systems.

One of them is user Account policy which defines actions of a user for better security [13]. The number of users is limited on a server computer to Avoid system complexity and vulnerability. It also decreases the amount of time required on administration. Limiting number of administrators can also help make process easier.

Another policy that can be adopted is Network Services, which gives the least number of essential services on that main server computer. It decreases the permission to access for users and makes sure that users with access to web, cannot access the shell functions. [11]

File system permits to set permission and examination setting for folders and files etc. [4] It allows users read-only access to essential directories (except those who obtains exclusively), so even when the attackers gain access, they only have permission of a user for that application. In this way, it guards the assets that were neglected by the administrator. [11]

Account policies promote OS security by developing and managing code or password policies, for example, strength and complexity of password rule and routinely password changing practice, at most number of failed log in tries etc. [8,7]

# METHOD

## Security threats

A risk which can possibly harm the data or the computer system is called a security threat to a computer. This harm can be physical like stealing device which has important information or virtual like a virus or hack. Today, there are several serious threats to computers and data due to political, or social reasons.

## Level of Security

There are four level of security to determine how safe a computer system is. Following is the classification of these levels.

* **Type A**: It is the highest level and uses proper design instructions and authentication practices.
* **Type B**: It offers compulsory protection system. Its properties are same as that of a C2 system. It assigns a sensitivity label to every object. It is divided further in three types.
	+ **B1** –The security label which decides about access control is well-preserved.
	+ **B2** – System resource like storage objects receive sensitivity labels, review of events and provisions covert channels.
	+ **B3** – permits to generating lists or user groups for giving control or cancel access to a named object.
* **Type C:** it facilitates in protection and user liability using audit aptitudes. Its types are as follows:
	+ C1 −For protecting data from deletion or reading by other users and protecting isolated information, C1 integrates controls.
	+ C2 − It has individual user access control is added to competences of a Cl level system.
* **Type D**: It is the minimum level of security.

## Kernel level Security:

Kernel Security level is used for the trusted and lowest level functions of OS. In this mode, the execution of code is completed and it restricts access to embedded hardware. It has control to execute any of CPU instructions and also can refer to any memory address.



Figure 2-Protection ring[12]

The model of protection ring gives an idea of different levels of security for an operating system.

## 3.4 Ways to avoid security Issues:

To avoid security issues in conventional operating systems, security policies related to who can access the system, must be appropriately implemented. The use of firewall, even with internet connected, the ensures local security and only authorized traffic passes. Another way to keep system and data safe is to utilize encryption technique. It is used when data is sent over Internet with risk of being exposed to others. The message I encoded and the key of encryption is only with authorized receiver. Setting password is another way to keep the log in secure.

# FINDINGS

It is clear that the security system for present conventional OS is not sufficient to sustain its integrity and discretion.

## 4.1 Case Study:

In such conditions, Mandatory Access Control (MAC) is required to meet the needs. However, due to shortcomings including scalability, complexity, cost, maintenance etc., it cannot be applied to conventional OS.

The National Security Agency (NSA) has collaborated with Secure Computing Corporation (SCC) and developed accommodating MAC architecture which is termed as Flask. It will overcome shortcomings of conventional MAC. They implemented it in Linux OS to generate a prototype called Security-Enhanced Linux (SELinux). In addition to this, NAI labs presented a sample policy outline to determine and showcase the advantages of MAC architecture. This will serve as foundation for other to implement [6].

# DISCUSSION

It is observed that steps are taken to makes this innovative technology accessible to a widespread public and to aid more research in safe OS. Threats can enter a computer system through web simply or a peripheral device when connected to it. If hacker accesses the physical access to a server, no matter how secure web is, the system becomes vulnerable to the attacker. OS Security comprehends every precautionary step that will guard the data on computer that can be removed, modified, and stolen in case OS security is in jeopardy. Any system is built on these four levels of security, according to its sensitivity.

# FUTURE ASPECTS

Every day, new threats emerge and new ways to combat them are needed. It is a given that the security has to be improved. To keep devices secure, Multi factor Authentication (MFA) has been practiced for quite a while. It requires password, as well as biometric scan and sometime any specific information. However, it is observed that now a days, username or password are not sufficient.

 Evidently, a further protected system for verification is required. Intel has begun place new validation solution in sixth-generation Core vPro processor, which has capacity to combine multiple factors of hardware simultaneously to authenticate. Deep learning is an upcoming technology and Deep learning merged with operating systems structure can open up new path to technological advancement.

# CONCLUSION

In conclusion, the security of an operating system is an inevitable phenomenon which needs maximum attention. Operating system security guarantees safe environment to run applications and perform tasks. There is no safety parameter that can alone protect the entire operating system. An appropriate mechanism has to be developed in order to achieve system security. [10] It is to be noted that an extremely safe security system will not be enough until it has application dedicated security mechanism.

# REFERENCES

[1] Michael Burtscher. 2007. System and method for kernel-level pestware management. Retrieved November 11, 2019 from https://patents.google.com/patent/US20070094496A1/en

[2] Per Brinch Hansen. 2013. Classic Operating Systems: From Batch Processing to Distributed Systems. Springer Science & Business Media.

[3] Rohit Khurana. Operating System (WBUT). Vikas Publishing House.

[4] Sakari Kouti and Mika Seitsonen. 2002. Inside Active Directory: A System Administrator’s Guide. Addison-Wesley Professional.

[5] Yukun Liu, Yong Yue, and Liwei Guo. 2011. UNIX Operating System: The Development Tutorial via UNIX Kernel Services. Springer Science & Business Media.

[6] Anthony Pell. Integrating Flexible Support for Security Policies into the Linux Operating System - Linux Security Server Security. Linux Security. Retrieved November 11, 2019 from https://linuxsecurity.com/news/server-security/integrating-flexible-support-for-security-policies-into-the-linux-operating-system-3499

[7] PRADEEP K. SINHA. 1998. DISTRIBUTED OPERATING SYSTEMS: CONCEPTS AND DESIGN. PHI Learning Pvt. Ltd.

[8] Steven Hand. Operating Systems. Retrieved November 11, 2019 from https://www.cl.cam.ac.uk/teaching/1011/OpSystems/os1a-slides.pdf

[9] Yepeng Yao, Liya Su, Chen Zhang, Zhigang Lu, and Baoxu Liu. 2019. Marrying Graph Kernel with Deep Neural Network: A Case Study for Network Anomaly Detection. In Computational Science – ICCS 2019, João M. F. Rodrigues, Pedro J. S. Cardoso, Jânio Monteiro, Roberto Lam, Valeria V. Krzhizhanovskaya, Michael H. Lees, Jack J. Dongarra and Peter M.A. Sloot (eds.). Springer International Publishing, Cham, 102–115. DOI:https://doi.org/10.1007/978-3-030-22741-8\_8

[10] 1998. 21st National Information Systems Security Conference: Building the Information Security Bridge to the 21st Century : October 5-8, 1998, Hyatt Regency Crystal City, Arlington, Va. National Institute of Standards and Technology.

[11] 2014. Techniques for Securing the Operating System. Retrieved November 11, 2019 from www.ibm.com/support/knowledgecenter/en/ssep7j\_10.1.1/com.ibm.swg.ba.cognos.crn\_arch.10.1.1.doc/c\_securing\_the\_operating\_system.html

[12] 2016. CISSP Security Mechanisms. ASM , Rockville , Maryland. Retrieved November 11, 2019 from https://asmed.com/cissp-security-mechanisms/

[13] Computer Security - Policies - Tutorialspoint. Retrieved November 11, 2019 from https://www.tutorialspoint.com/computer\_security/computer\_security\_policies.htm