Operating System

Security

Abstract

The software that controls computer hardware resources and offers some fundamental functions to computer programs is known as an operating system (OS). An essential part of the system software in a computer system is the operating system. Simply put, the operating system serves as a conduit between the user and the hardware. The operating system today is crucial for processing the system. Depending on the business you operate in, you can implement a variety of operating system (OS) security rules and procedures. An OS security policy, in basic terms, is one that details the procedures for ensuring that the OS maintains a particular level of integrity, confidentiality, and availability. OS security guards against threats, including viruses, worms, malware, ransomware, invasions through backdoors, and more, for systems and data. All preventative steps and methods used to ensure the safety of an OS, the network it connects to, and the data that can be lost, altered, or destroyed are covered by security policies. With the advancement of hardware and operating system technology for mobile phones, security is becoming a major challenge. Android currently has the most market share of all smartphone operating systems. As these phones' capabilities and functionalities develop, so does their susceptibility, making them more susceptible to security risks.

Keywords: security, operating system, security policy, android security

Introduction

Operating system (OS) security refers to procedures and controls that can guarantee the privacy, availability, and confidentiality (CIA) of operating systems. The purpose of OS security is to defend the OS against a variety of dangers, such as misconfigurations, remote intrusions, and malicious software like worms, trojan horses, and other viruses. The adoption of control strategies that can shield your assets against unwanted addition, deletion, and theft is often part of OS security. The use of antivirus software and other endpoint protection tools, routine OS patch updates, a firewall for observing network traffic, and enforcement of secure access through least privileges and user controls are among the most often used methods for protecting operating systems.

Operating system security in Android [1]

With the advancement of hardware and operating system technology for mobile phones, security is becoming a major challenge. Android currently has the most market share of all smartphone

operating systems. As these phones' capabilities and functionalities develop, so does their susceptibility, making them more susceptible to security risks. The Android operating system has a permission-based approach that enables Android applications to access system data, device data, user data, and external resources on a smartphone. The permissions in an Android application must be declared by the developer. The user must agree to certain permissions in order for an Android application to install correctly.

There are some security attacks in android operating system and some of the issues includes:

- Spyware
- Permission Escalation Attack
- Information Leakage
- Colluding
- Denial of Service Attack
- Repackaging Apps

These issues can be fixed using both static and dynamic methods like Riskmon, Kirin, Paranoid Android, Driodscope. Android is the most popular smartphone operating system. Android has a few sophisticated functions. However, this platform does contain risks and attacks like malware programs. due to the threats that malware on the Android platform poses. The security of an Android operating system is crucial for preserving user privacy and personal data. This article has studied security flaws and attacks on the Android operating system. There are several ways to address security breaches and other problems with the Android operating system.

Linux Operating System security [2]

Linux is utilized in a wide range of settings, including corporations that store customer data on servers and private residences using personal computers. Although this operating system is frequently seen as being more safe than Windows or Mac OS X, there are still security issues that might arise when using it. Attackers can use a network to break easy passwords, vulnerabilities can be taken advantage of if firewalls do not close enough ports, and Linux systems can be infected with malware. Additionally, if the right permissions are not established on the files or folders containing sensitive information, it may be possible for someone to access it physically or online. Since the development of the Linux kernel, Linux has become more widely used in numerous

contexts. Linux has frequently taken the place of expensive Windows software [3]. Because of this, free Linux distributions are quite appealing. Additionally, Linux performs admirably as a server operating system, thus many companies might employ it for this. Linux distributions, like other operating systems, have constrained security out of the box. It is vital to adopt additional security features and procedures to safeguard the data on the machine in order to stop malicious hackers from obtaining access to another machine and potentially stealing confidential information.

There are some methods for creating linux OS secure like

- Security through Repositories
- Use of antivirus: ClamAV
- Precautions using Linux compatibility layer: Wine
- Updating Software
- Firewalls
- Passwords management
- File access Permission

Maintaining an updated system, utilizing an antivirus program, a secure firewall, creating complex passwords, and setting strict file permissions can stop the majority of attacks against Linux computers. Linux systems can be protected from viruses and hackers by installing firewalls, modifying file permissions, and searching for vulnerabilities in specific packages and files. Since Linux can be used for a wide range of purposes, from business PCs and servers to private use in homes, it's critical to apply sound security practices to guard against data loss or theft. For instance, configuring firewalls to stop users from connecting to a Linux computer on the same network and configuring suitable permissions and strong passwords to prevent other users on a Linux machine from accessing files they shouldn't have access to. Additionally, downloading software from reputable sources, such as a distribution's repository, and running antivirus software checks on downloaded software from the internet might stop malware from being installed on the system, especially when Windows malware can be executed on a Linux system via Wine. Users who are familiar with the various Linux security measures can utilize their Linux machines in a more secure manner. Given that these systems have the capacity to store a significant amount of customer data, it may also benefit enterprises who employ these distributions in some way.

Conclusion

The physical setting in which your application operates is determined by the operating system. The security of the program could be jeopardized by any operating system flaw. You can stabilize the environment, manage resource access, and manage external access to the environment by safeguarding the operating system. The system's physical security is crucial. Threats might come from a physical terminal as well as the Internet. Even though the Web access is extremely secure, breaking into a system is significantly simpler if an attacker has physical access to a server. Review your operating system's security guidelines and regulations. The upcoming security best practices should be used.

References

1. Mohamed Razeed Mohamed Nowfeek. *A review of Android Operating System Security issues*. https://www.researchgate.net/publication/358425896_A_Review_of_Android_operating_system_security_issues
2. Md. Minhaz Chowdhury, & Matthew R. Yaswinski. (2019, May). Linux Security: A Survey. DOI:10.1109/EIT.2019.8834112 Retrieved October 31, 2022, from https://www.researchgate.net/publication/335795125_Linux_Security_A_Survey
3. Hadeel Tariq Al-Rayes *Studying the main difference between Linux & Windows OS.* https://www.researchgate.net/publication/328125275_Studying_Main_Differences_Between_Linux