Journal of Information Systems & Information Technology (JISIT)
ISSN: 2478-0677; Vol. 7 No.1 2022; [Pages 19 - 25]

Security Issues and Challenges in Windows OS Level

Uthuma Lebbe Muhammed Rijah
MS21900686
Department of Graduate Studies and Research
Sri Lanka Institute of Information and Technology
ms21900686@my.sliit.lk

U.U. Samantha Rajapaksha
Senior Lecturer
Department of Graduate Studies and Research
Sri Lanka Institute of Information and Technology
samantha.r@sliit.lk

ABSTRACT

An operating system is a software that controls and communicates with the computer's hardware and offers the most fundamental services to other applications. The operating system is a very important component of the system software of a computer system, functioning as a channel between users and hardware. Today's commercial operating systems contain bugs and security flaws. The objective of any operating system manufacturing company is to provide a reliable operating system that can resist attacks and offer a secure computing environment to safeguard a computer's valuable assets. Windows is a Microsoft Corporation personal computer operating system part of the Windows NT family. The various security issues of the Microsoft Windows Operating System are deeply analyzed in this paper.

Key Words: OS Security

INTRODUCTION

Software is a set of instructions or programs that instruct the computer to perform specified tasks. The three kinds of commonly used software are application software, system software, and programming software. Operating systems (OS) and other programs that support application software are called system software. Computer hardware and software resources are managed by an operating system, providing standard functionality for computer-based applications. The latest version of the Microsoft operating system, Windows 11, was launched on October 5, 2021, replacing Windows 10. Most likely, it is the most secure Windows version to date. The most recent version of the Windows operating system, Windows 11, is the most secure it has ever been against malicious software. Compared to older versions of Windows, Windows 11 has several built-in defensive methods to protect the system's privacy, security, and availability [1].

Initially, when a computer boots up, the OS controls everything. This makes it the most important part of system software. Users run their application programs through an OS, allowing them to communicate with computer hardware. It also manages processes, allocating main memory to various applications, threads, data storage, hosting device drivers, and input and output devices, and offers a multi-level secure processing architecture [2].

As computers and networks have rapidly increased, protecting sensitive data has become an urgent issue for IT administrators. Further, the security of the operating system (OS) plays a significant role in the safety of the computer network. [3]. Therefore, analyzing OS security is very important for information security and OS research. This research investigates the windows operating system's security threats, cyber threats, and some security mechanisms.

OPERATING SYSTEM'S FUNCTIONS

The OS works as a gateway between computer hardware and users, and OS is responsible for the following fundamental actions or tasks [4].

- *Processor Management*- The OS controls the processor's workflow and monitors the processor's multiple tasks.
- *Memory Management*-The system's memory management is also handled by the OS It allocates memory to various tasks and ensures that the system's memory is effectively used.
- *Storage Management*- The operating system also monitors storage networks and devices.
- *Booting*- Booting involves turning on the computer's operating system and placing it to use. The computer is checked and prepared for use.
- *Data Security*- Data is a crucial component of a computer system. The operating system safeguards the data on the computer against unauthorized access, alteration, or deletion.
- *File Management*- A computer's OS controls how files are created, deleted, accessed, copied, and saved. It also manipulates programs and data by sending and receiving data, transferring and saving it.
- *Device controlling* - The OS also manages all computer-connected devices. Hardware devices are controlled by software known as device drivers.

SECURITY

Security is a primary issue for operating system developers. In general, operating system security includes the protection of the operating system against unauthorized users and the protection of the file system. The multiple processes should be kept separate from one another when a computer system has no users and allows for the execution of multiple processes simultaneously. In other words, security refers to a technique for limiting program access. As a result, the security system prevents unauthorized access to the system and verifies malicious data removal. Additionally, it refers to system users' authentication to protect the system's data's integrity [3].

Authentication attacks are at the bottom of the priority list regarding operating system security. The primary issues include Trojan Horses, buggy software, and Login spoofing threats. Program Threats are also a source of concern when it comes to security. Processes and the operating system's kernel carry out the given job as specified earlier. When these processes are created by a user application and are used to carry out malicious tasks, they are referred to as Program Threats [5].

A. Cyber threats

Windows is the most widely used operating system in the world, and hackers often target it to carry out attacks. There are a lot of cyberattacks performed on the internet. These cyberattacks are done by a cybercriminal who wants to make money. Some of the most common cyber threats that impact Windows are discussed in the following sections.

- *Malware:* Software and applications which aren't secure to use are called Malware. It generally causes system damage and interferes with the regular operation of computing devices. Cybercriminals can use Malware to obtain access to and use system resources illegally, shut down a computer, claim payment, steal passwords and attack the system with malware. Hackers are often motivated by financial gain and will take sensitive information that may be sold or used to extort money from victims. However, there are many types of malware. This research focuses on the most popular ones that have affected Windows security in the past. Rootkits, phishing, and ransomware are the most popular malware attacks.
    - *Rootkits*- Rootkits are a kind of malware that operates in kernel mode and has the same privileges as the operating system.

Rootkits can hide for as long as they want in a system. A device's information about itself after a rootkit attack is no longer reliable. Below are four different forms of rootkits. The following are four different types of rootkits.

- *Firmware Rootkits*-It simply rewrites the firmware of the computer for these rootkits to start up before Windows begins

- *Bootkits*-These are rootkits that have the basic capabilities of a rootkit as well as the power to attack the Master Boot Record. Individuals create bootkits so they can run from the system's master boot record and stay active during its use.

- *Kernel Rootkits*- To take total control of a computer, an attacker must get access to the kernel of the operating system. A section of the kernel is replaced by these rootkits, allowing them to run as soon as the system starts up.

- Driver Rootkits Almost all drivers work in" kernel mode," which means they have access to all of the important files in the system. It uses them as one of the trusted drivers that Windows can use to communicate to hardware on your computer [6].

- *Phishing*- Phishing attacks use emails, text messages, website and other types of electronic connection from reputed company or person to steal private information. There are many crimes that can be done with the in- formation that was stolen, like hacking, taking money from a bank or credit card, and so on. Some of the most common phishing techniques are listed here.
  - *Similar spoofing*- Cybercriminals spend more time and resources creating websites that seem just like the official ones. The phishing site's URL and the legitimate site's URL will be similar, and the user will be misled.

  - *Invoice Phishing*-An attacker sends an email to users claiming that they have an overdue invoice from a well-known vendor or firm, with a link to see it and pay the invoice.
  - *Payment/ Delivery Scam*-A credit card number and

personal information are given to a well-known company to keep the user's payment information with them.

- *Downloads*- Another common phishing technique is sending a fake email asking the recipient to open or download a document, usually asking the recipient to sign in [7].

- *Ransomware*-Files and directories are encrypted by this kind of malware, making it unavailable to everyone except the malware attacker. Its goal is to steal money from users in return for the decryption key, which is generally in the form of cryptocurrency. Ransomware is recognized for evolving malware behavior, shown by the usage of vulnerabilities and other attack routes, making older systems more sensitive to ransomware attacks. The most common ways of ransomware attacks are random email messages with attachments that try to install ransomware and malicious websites that attempt to install ransomware by exploiting weaknesses and vulnerabilities in browsers and other software browsers and other software. When a system is infected with ransomware, its data is automatically encrypted using RSA or RC4. The most popular ransomware techniques are WannaCry, Spora, and Petya [8].

B. *Countermeasures to Cyber Threats*

Windows OS provides the following safeguards to prevent the cyber threats mentioned above. There are some Countermeasures to Cyber Threats are offered in the literature [6] [7] [8].

- *Secure Boot UEFI*- The integrity of each boot process component is checked before the operating system is loaded. Only trusted OS bootloaders can be loaded on computers with UEFI firmware and a Trusted Platform Module (TPM).

- *Updates*- The most recent operating system updates should be installed.

- *Data Backup*-This can help prevent delay, data loss, and financial loss in case of a cyber-attack.

- *Exchange Online Protection*- It utilizes many levels of spam filtering and provides a variety of spam filtering features, including bulk mail and international spam. It assists in protecting email, files, and internet storage against viruses.

- *Limited Access to Folders*- It protects ransomware from encrypting data and keeps users for ransom by limiting file and folder access.
- *Awareness*
- *Regular OS patch updates*
- *Monitor network traffic via a firewall.*
- *Enforcement of secure access via least privileges and user restrictions*

C. *Security Methods*

Many security methods to protect windows OS are discussed in the literature [3] [4] [9], which we discuss in this section.

- *Identification and authentication:* It is necessary to identify and authenticate users. The system requires the user's identity for identification. Authentication is the process of associating a user's identity with the user.
- *Access Control:* Access control is the key tool for computer system security. There are three stages to it. The first step is authorization, followed by access permission, and finally, by imposing access permission.
- *Least Privilege:* Allow users to have just the permissions necessary to perform the job.
- *Trusted Channel:* In most computers, the interface between the operating system and the user occurs via a middle application layer, which is insecure. As a result, the operating system must ensure that a Trojan horse cannot take data during transmission.
- *Virus protection:* Protecting our computer system against viruses in the real world is challenging. A virus protection mechanism will generally be used to secure particular functions.

CONCLUSION

Operating systems research is a broad area because the hardware is growing more powerful and complicated by the day. Therefore, there is

competition for the operating systems to sustain. The purpose of this article is to discuss the security issues and challenges in Windows OS security is a challenging task to achieve. OS are responsible for coordinating all other systems in a computer system. Because of this, security is the primary and serious issue. This research analyzed several aspects such as windows security, cyber threats, and windows security methods. We explored some past research and proposed some countermeasures for cyber threats. Complete security is considered impossible to achieve, and no operating system is completely safe against attacks and weaknesses. But, the OS's designers and developers may aim to maximize security in all possible ways and must meet the demands of the end users.

REFERENCES

[1] R. Zahilah, F. Tahir, A. Zainal, A. H. Abdullah, and A. S. Ismail, "Unified approach for operating system comparisons with windows os case study," in 2017 IEEE Conference on Application, Information and Network Security (AINS), 2017, pp. 91–96.
[2] K. Chen, C. Du, J. Chen, and Z. Yuan, "Real-time extension technologies on the windows operation system," in 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2019, pp. 789–793.
[3] G. J. Ruiz, M. M. Chowdhury, and S. Latif, "A comparative study of os security," in 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 2021, pp. 01–06.
[4] M. Xin, "On computer operating system and its development," in International Conference on Application of Intelligent Systems in Multimodal Information Analytics. Springer, 2019, pp. 1385–1390.
[5] H. A. Noman, Q. Al-Maatouk, and S. A. Noman, "Design and imple- mentation of a security analysis tool that detects and eliminates code caves in windows applications," in 2021 International Conference on Data Analytics for Business and Industry (ICDABI), 2021, pp. 694–698.
[6] K. Thakur, M. Qiu, K. Gai, and M. L. Ali, "An investigation on cyber security threats and security models," in 2015 IEEE 2nd international conference on cyber security and cloud computing. IEEE, 2015, pp. 307–311.
[7] G. J. W. Kathrine, P. M. Praise, A. A. Rose, and E. C. Kalaivani, "Variants of phishing attacks and their detection techniques," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 255–259.
[8] H. Turaev, P. Zavarsky, and B. Swar, "Prevention of ransomware execu- tion in enterprise environment on windows os: Assessment of application whitelisting solutions," in 2018 1st International Conference on Data Intelligence and Security (ICDIS), 2018, pp. 110–118.
[9] J. Barath, "Optimizing windows 10 logging to detect network security threats," in 2017 Communication and Information Technologies (KIT), 2017, pp. 1–4.