LGURJCSIT
Volume No. 1, Issue No. 3 (July- September), pp. 39-49

Performance Analysis of Hardware Protection & System Security in Different Operating Systems

[1]Ayesha Nasir, [2]Muhammad Adnan Khan, [3]Muhammad Nadeem Ali, [4]Saqib Aslam Malik, [5] Umer Farooq

[1, 2, 3,4.5]Lahore Garrison University, Lahore, Pakistan
[1]ayeshanasir@lgu.edu.pk, [2]madnankhan@lgu.edu.pk ,[3]mnadeemali@lgu.edu.pk ,[4]saqibaslam@lgu.edu.pk,[5]umerfarooq@lgu.edu.pk

Abstract: The intention of article is to protect the hardware, which includes protecting CPU, I/O, and Memory. This article portrays and relates the security in different operating systems. Therefore, helping us to choose the best. We can evaluate the security in different operating system like Windows, UNIX, Linux secure our all data to unauthorized users.

1. Introduction:

Computer hardware is the group of physical peripherals that makes up computer system. The term hardware security is defined as the protection of physical system from unauthorized access or person.

Protection means mechanisms and policies to save program and user from opening or altering material. Computer linked to internet are not fully secured from hackers. Unauthorized person can find the computer and can alter information.

The main purpose of hardware security is to lessen the risk of illegal access. Therefore, confirming the effective use of resources.

2. Literature Review:

Any tangible part of computer is known as its hardware. Tangible means touchable component or any component whose existence can be felt.

Categories of computer hardware are enlisted as: [1]

1. Processor
2. Memory
3. Input and Output
4. Storage

Central processing unit is another name for computer processor. It is an electronic circuit board which is responsible for carrying out some instructions given by any computer program by performing some basic operations. These basic operations include arithmetic operations, logical operations, some control operations and basic input output operations. In other words, the main function of processor is to process the data. Processing is defined as converting useless data into useful information. This conversion is involves two components of hardware.

1. Processor
2. Memory

Instructions coming from user or any software are organized and carried out by processor. [1][2]

Without interaction computer is a useless machine. So certain devices are required to interact with computer. These devices will receive instructions as well as gives the result

of instructions. These interacting devices are input output devices.

Input device receive data or instructions from the user, or from some other computer system. After performing desired operations, the processed data is returned to user by output devices.

Some common types of input devices are: [3][4]

1. Keyboard.
2. Mouse.
3. Microphone.

Some common types of output devices are:

4. Monitor
5. Printer
6. Speakers

3. Protection:

Protection means securing your system from unauthorized access or hackers. Making your data inaccessible to any unofficial person. Protecting something means act of preserving public freedoms and rights [5][6].

3.1. Hardware Protection:

Hardware protection means protecting many things, like, protection of hard disk drives, protecting memory, trapping unauthorized system call.

Three types of hardware protection are as follows:

1. I/O Protection
2. CPU protection
3. Memory protection [2][4]

3.2. I/O Protection:

I/O protection is to avoid illegal use of the I/O. I/O system should protect against any wrong I/O.

I/O protection has several steps including; I/O instruction must define to be privileged, I/O must be performed in system call.

In user mode, user program cannot control computer and is unable to perform input output operations. [9] While when in kernel mode, all input output requests are performed. In addition, user program can send request to OS for accessing input output.

Privileged Instructions: Privilege instructions are those, which only run in kernel mode.

Non-Privileged Instructions: non-privileged instructions are those which run in both user modes as well as in kernel mode [4].

3.2.1 Dual Mode Operation:

In dual mode operation, user defined and system defined codes are distinguished. Bit mode, which is added to computer hardware, indicates the current mode [1][2].

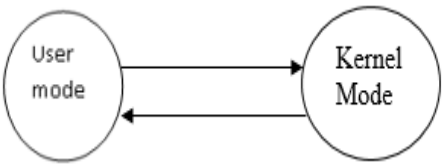

Figure 1: Dual Mode

User Mode: In User mode, the program has cannot directly access hardware or any memory. Mode bit defined for kernel mode is 1.

Kernel Mode: In Kernel mode, the program has complete access to the hardware. Mode bit defined for kernel mode is 0 [6].

3.3 CPU Protection:

CPU protection is to avoid illegal use of CPU. Multiple processors can execute the multiple instructions, that is why time

problem can occur. To solve that problem, we can introduce two types of counters [4][6].

1. Fix counter
2. Variable counter

3.3.1 Fix Counter:

In this counter value of counter is fix, and the time processor can move on other tasks. For example, two users can operate instructions but the fix counter operates both instructions at equal time. When time is complete than processor can move on next instruction. Suppose all processors contain two mints. After two mints processor moves on next one [16] [17].

3.3.2 Variable Counter:

In this counter value of counter is not fix it can be change if task contain maximum time. In this way, variable counter depends upon task. For example, two users can operate

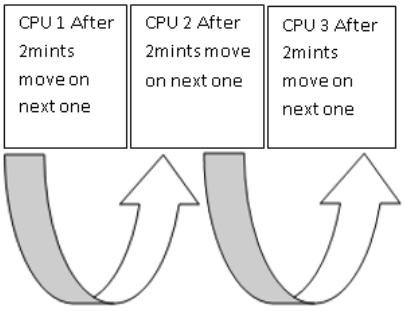

Figure 2: Fix Counter

instructions but if there are different sizes first user contain two mints to complete the task and second one is to complete in five mints. In this way, variable counter depends on task [7][8].

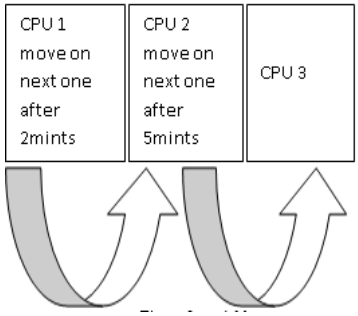

Figure 3: Variable Counter

3.4 Memory Protection:

Avoiding illegal use of memory is called memory protection [8] [9].

The internal storage area of the computer is referred to as memory of computer.

There are two types of memory. Usually know as:

1. Main memory
2. Secondary memory

3.4.1 Main Memory:

Main memory in computer is the area that contains current data. It is a temporary storage area [9] [10].

Some common types of main memory are as follows:

1. RAM
2. ROM
3. EPROM
4. EEPROM

3.4.2 Secondary Memory:

It is the external storage or additional storage area. This area contains data permanently [8][9].

Examples of secondary storage:

1. Magnetic tape
2. Floppy disk
3. Hard disk

4. Optical disk
5. Flash drive

Memory protection must be providing. Two registers that determine the range of legal addresses the program can access are added in memory protection [10].

It consists of two registers:

1. Base Register
2. Limit Register

Base Registers: A process's smallest legal physical address or starting address of process is stored in base register.

Limit register: Process size resides in limit register [10].

3.4.3 Use of Base and Limit Register:

Here base and limit registers where monitor is the system area and the jobs are the user areas jobs assign to different users. System area exists in the operating system and user area exists in the job pool [11][12].

3.4.4 Hardware Protection:

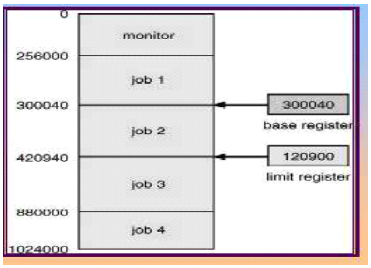

Figure 4: limit register

3.4.5 Memory Protection: -

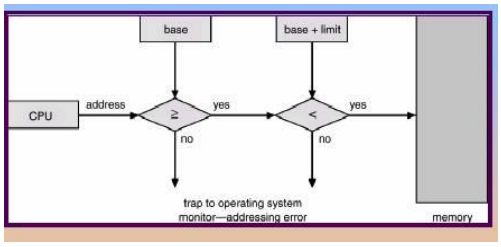

Figure 5: Memory protection

CPU register is greater than or equal to base limit.

If (256000>300400)

If it not greater than it will illegal & otherwise it will trap system.

If (520942 >=300400)

If it is not greater than it will legal it will not trap. [13]

4. System Security:

Before attempting to make your system, secure following things should be considered. You should determine threat level, risk you should take or should not take and susceptibility of your system [13] [14].

Risk is the measure to check possibility that an unauthorized person is successful in accessing your system.

Threat is the motivation to gain unauthorized access to your network or computer [14].

Susceptibility portrays how well−protected your PC is from another system, and the potential for somebody to increase unapproved get to [15] [16].

Security in different operating systems:

1. Window
2. LINUX
3. UNIX

4.1.Window:

In OCTOBER 2001, WINDOW XP was discharged as both a refresh to the WINDOW 2000 desktop working framework and trade for WINDOWS 95/98. Windows XP refreshes the graphical UI (GUI) with a visual outline. Window XP is a multiuser working framework, supporting all the while access through dispersed framework. There are two

desktop forms of Windows XP; Window XP expert and Window XP [17][18].

Window XP security objectives required something other than adherence to plan norms that empowered Window NT 4.0 to get C-2 security arrangement that US government. Presence code recipient and testing were joined with advanced programmed examination devices to distinguish and venture potential imperfections that may speak to security obligations [18].

1. Visit the Microsoft Update site and introduce the most recent administration packs and basic updates. A few updates must be introduced alone, and will require a reboot. Visit Microsoft Update the same number of times as important to introduce every single basic refresh. Allude to the Microsoft Windows XP Service Pack Installation and Deployment Guide for nitty gritty data about how to physically introduce benefit packs, uninstall benefit packs, and add them to an introduce catalog [17][18].
2. Arrange Automatic Updates to consequently advise you of the accessibility of new security fixes. On the off chance that conceivable, arrange Automatic Updates to consequently download refreshes and introduce them without manual intercession. For more control over updates, utilize Microsoft Software Update Services, Microsoft Systems Management Server, or a comparable answer for decrease the work related with sending patches. [19]
3. Understanding the new security features of Windows XP Professional.
4. Enabling Internet Connection Firewall.
5. Enable EFS for files and folders that contain private information, as documented in Microsoft Knowledge Base articles 307877 and 308989.
6. Keep the latest security hot fixes by using the Security Bulletins Search
7. Follow the Microsoft Windows XP Professional Baseline Security Checklist.
8. Familiarize yourself with these best Practices in Enterprise Security.
9. Update your anti-virus tools and signature files from viruses.[19] Check out the Virus Alerts regularly.
10. Use the Baseline Security Analyzer to scan and evaluate the security of your system.

4.2 Linux:

Linux is created by vast group of software engineers and is open source. Linux is frequently regarded as an exceptionally secure working framework, however it too has numerous security blemishes [4]. What's more, these security blemishes enable outer programmers to get into your framework to pulverize or change your critical information. Since there are different methods by which these blemishes can be expelled. [20]

4.2.1 Securing BIOS System:

An Operating System needs a security from its booting up to closing down. In the event

that an assailant approaches the BIOS, nothing will stay safe. [20] The BIOS is the most minimal level of programming that keeps up the equipment. LILO and other Linux boot strategies get to the BIOS to decide how to boot up Linux machine. [20] [21] We can set BIOS secret key to keep from unapproved get to and to forestall changes to BIOS Settings. We can likewise secure LILO by setting secret word.

4.2.2 Network Security:

4.2.2.1 Securing NFS:

NFS is an acronym for network file system. NFS share whole records with countless hosts. Be that as it may, easily of utilization comes an assortment of potential security issues. With these taking after strides we can limit the NFS security chance.

- **Host access:** NFS control who can mount its file. Host must be given rights to mount its file.

- **File permission:** After the NFS record framework is mounted, the main insurance each common document has is its authorizations [21].

4.2.2.2 Securing NIS:

NIS is network information system. It disperses sensitive data like secret word, username and so forth to any PC asserting to be inside its domain [21] [22]. Because NIS ignores delicate data the system, it is critical to run the administrations behind a firewall.

4.2.3 File Security:

In Linux, a solitary client on that framework claims every record and each directory. Each record and directory additionally has a security group related with it that approaches rights to the document or catalog. In the event that a client is not the directory or record proprietor nor appointed to the security bunch for the document, that client is named other may at present have certain rights to get to the document [20][23].

All file access categories i.e. owner, group and other have a set of three access permissions. These are read, write, and execute permissions. With these file system is secured.

Here are some examples of typical file permissions and their appropriate numeric equivalent [22][23].

- Owner can read, write, and execute. Group can read and execute. Others can read only.

Chmod 754 ABC

rwx rx r ABC

- Owner can read and write. Group can read and write. Others can read only.

Chmod 664 ABC

rw rw r ABC

- Owner can read, write, and execute. Group can read and execute. Others can read and execute.

Chmod 755 ABC

rwx rx rx ABC

- Owner can read and write. Group can read only. Others have no access.

Chmod 640 ABC

Rw r _ _ _ ABC

4.2.4 Kernel Security:

The Linux kernel is the very important in all Linux systems. If any virus controls or damages any part of the kernel, then the system can get severely damaged. Clearly, it is in the user's best interest to keep the kernel secure. Linux is a very secure system because of the kernel and its security [23]. There are less Linux viruses than Windows viruses even in proportion to the number of users, and Linux users get less viruses than Windows users. There are several modules to protect Linux kernel. Without these features Linux cannot become secure OS. App Armor (Application Armor), Security-Enhanced Linux, Smack, TOMOYO, Yamas, Linux Intrusion Detection System (LIDS), Systrace [19][20].

4.3 Unix:

UNIX has fundamental design that can support most technological advances. Moreover, it permits individuals to do large portions distinctive things regardless of director does not have any desire them with would. At that happens, security is broken. For today's progressively electronic society, security breaches have those possibilities about being genuine [23] [24].

UNIX system security can be divided into three main areas of concern

1. Account security
2. File system security
3. Network security

4.3.1 Account Security:

The primarily concern of account security is to keep unauthorized users from gaining access to the system [23][24].

All privileged accounts and SSH keys must be completely detected.

By real-time checking and recording of privileged sessions security can be increased and preserving the native command line experience that UNIX users prefer.

UNIX framework permits to diminish an aggressor's window of chance on basic UNIX frameworks with ongoing location and alarming of abnormal favored record movement. Productivity of UNIX record organization can be enhanced by associating UNIX records to AD for incorporated confirmation and provisioning [24][25].

These UNIX security capabilities make all privileged accounts secure. [25]

4.3.2 Network Security:

Most UNIX frameworks have an expansive number of system administrations empowered, enabling remote people to interface with the framework and increase different levels of get to. Any of these administrations can contain a powerlessness that is recently holding up to be discovered

and exploited [25].

Therefore, to counteract unapproved get to, extraordinary care must be taken to limit the quantity of system administrations running on the machine and confine access to administrations that are running on the framework. Likewise, a considerable lot of the system benefits that accompanied UNIX are not secure and ought to be supplanted with secure options, for example, SSH [25][26].

4.3.3 UNIX Files Security:

In UNIX file system, each file has owner and group. Each process has three Ids; owner, group, other. Permissions are set by owner. Permission includes Read, write, execute. Only owner, root can change permissions [24] [26].

4.3.3.1 Owner: Each record and directory (an exceptional kind of document) has a "proprietor." This is the client account that has essential control over the record, enabling it to do things like change the record's consents. The proprietor is communicated as a client record, for example, root or your own client account, or even some "client" account consequently made for the utilization of a bit of programming you have introduced. [23] [27]

4.3.3.2 Group: Notwithstanding the owner, each document has a gathering account related with it. This gathering, similar to the client account that is the record's proprietor has its own particular arrangement of get to consents to the document. While making a record, the gathering is set to the default gathering of the client account used to make the document, however documents can be reassigned to an alternate gathering. For example, for the root account, this for the most part implies that the document's gathering owner is the wheel assemble on BSD Unix frameworks [25] [26].

4.3.3.3. Other: It is the last permission category and covers “everyone else” [26].

The basic level security on UNIX can be achieved by keeping the file permissions as restrictive as possible, without preventing the system from doing what it needs to do, and without preventing yourself from accessing the files [26][27].

5. Comparison:

	Window	Linux	UNIX
Efficient	×		
Secure	×		
Convenient	✓	×	×
Availability	×		
Stable	×		

From above comparison, it can be concluded that:
In terms of efficiency and security, LINUX and UNIX are more efficient and secure than Window. But Windows are more convenient as compare to Linux and Unix. Linux and Unix are more stable than Window.

6. Conclusion:

This research explores the hardware protection and security in Linux, UNIX and Windows. After investigating the results, it is concluded that UNIX and Linux are perfect choice as compared to Windows.

References

[1]. Tanenbaum, Andrew S. "Distributed operating systems". Pearson Education India, 1995.

[2]. H.M.Dietel, P.J.Dietel, D.R.choffnes, "Operating system and Networks", 3 edition,

[3]. Tanenbaum, Andrew S., and Herbert Bos. Modern operating systems. Prentice Hall Press, 2014

[4]. Galvin.S, Galvin.p.b, "operating system concept", 6th edition, ISBN: 0-471-41743-2.

[5]. Crowley, Charles. "The design and implementation of a new UNIX kernel." Proceedings of the May 4-7, 1981, national computer conference. ACM, 1981.

[6]. Gary.J.Nut, "Operating system modern perspective".

[7]. Dhamdhere, Dhananjay M. Operating Systems: A Concept-based Approach, 2E. Tata McGraw-Hill Education, 2006.".

[8]. Hansen, Per Brinch, ed. Classic operating systems: from batch processing to distributed systems. Springer Science & Business Media, 2013.

[9]. Kifer, Michael, and Scott Smolka. Introduction to operating system design and implementation: the OSP 2 approach. Springer Science & Business Media, 2007.

[10]. Comer, Douglas. Operating system design: the Xinu approach, Linksys version. CRC Press, 2011.

[11]. Tanenbaum, Andrew S., et al. "Experiences with the Amoeba distributed operating system." Communications of the ACM 33.12 (1990): 46-63.

[12]. Leonard, Ozgur, Andrew Tucker, and Andrei Dorofeev. "Multi-level computing resource scheduling control for operating system partitions." U.S. Patent Application No. 10/771,827.

[13]. Tanenbaum, Andrew S., Jorrit N. Herder, and Herbert Bos. "Can we make operating systems reliable and secure?." Computer 39.5 (2006): 44-51.

[14]. Dhamija, Ashutosh, Robin Walia, and Vidhu Rawal. "Demographics of Linux And Windows." International Journal of Technology Enhancements and Emerging Engineering Research 1.5 (2012): 36-38..

[15]. Engler, Dawson R., and M. Frans Kaashoek. Exokernel: An operating system architecture for application-level resource management. Vol. 29. No. 5. ACM, 1995.

[16]. Stallings, William. Cryptography and network security: principles and practices. Pearson Education India, 2006..

[17]. Shirisha, B., M. Tech, and K. Sumalatha. "SWAS-SOFTWARE AND WEB APPLICATIONS SECURITY."

[18]. Solomon, David A., Mark E. Russinovich, and Alex Ionescu. Windows internals. Microsoft Press, 2009..

[19]. Economides, Nicholas, and Evan Katsamakas. "Linux vs. Windows: A Comparison of Innovation Incentives and a Case Study." (2005). [20]. Nemeth, Evi, Garth Snyder, and Trent R. Hein. Linux administration handbook. Addison-Wesley Professional, 2006.".

[21]. Narayan, Shaneel, Kris Brooking, and Simon de Vere. "Network performance analysis of vpn protocols: An empirical comparison on different operating systems." Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on. Vol. 1. IEEE, 2009.

[22]. Nagy, Benedek, and László Szegedi. "Membrane Computing and Graphical Operating Systems." J. UCS 12.9 (2006): 1312-1331.

[23]. Stallings, William. Operating Systems: Internals and Design Principles—Edition: 5. Pearson, 2005.

[24]. Bach, Maurice J. The design of the UNIX operating system. Vol. 1. Englewood Cliffs, NJ: Prentice-Hall, 1986.

[25]. Chou, Andy, et al. "An empirical study of operating systems errors." ACM SIGOPS Operating Systems Review. Vol. 35. No. 5. ACM, 2001.

[26]. Venkateshmurthy, M. G. Introduction to Unix and Shell Programming. Pearson Education India, 2009.

[27]. Schimmel, "UNIX system of architecture", 2008.

[28]. Bach, Maurice J. The design of the UNIX operating system. Vol. 1. Englewood Cliffs, NJ: Prentice-Hall, 1986.