International Journal of Computing and Mathematics
Vol. 1, Issue. 3, Sep 2024, pp. 31~35

Security Control for Computer System in the Real World

Emmanuel O.C. Mkpojiogu[1], Ahmed Al-Athwari[2]
[1]Department of Computer and Information Technology, Veritas University, Abuja, Nigeria
[2]School of Computing, Universiti Utara Malaysia, Sintok, Kedah, Malaysia

Article Info

Article history:

Received Jun 10, 2024
Revised Jul 22, 2024
Accepted Aug 18, 2024

Keywords:

Computer privacy and security
Data integrity and security
Security technologies

ABSTRACT

The combination of computer system security into existing Computer Science undergraduate education is a critical and convoluted errand. With the expanding danger of computer intrusion, PC violations, and data wars, Computer Science instructors bear the duty of developing another age of graduates who know of computer security-related issues and are outfitted with appropriate information and skills to tackle the issues. The errand of incorporating PC security into existing Computer Science programs, in any case, is confounded because of the way most faculty individuals do not have the forte information in this field. Computer system security contracts with the administrative process and technical protection applied to computer software, hardware, and information to guarantee against unintentional illegal permission to computer system information. This paper introduces the system security technologies including validation, data encryption technology, firewall technique, antivirus technology, intrusion detection system, and VPN (a virtual private network).

Corresponding Author:

Emmanuel O.C. Mkpojiogu,
Department of Computer and Information Technology, Veritas University, Abuja, Nigeria

1. INTRODUCTION

Computer system security has been familiar among people for more than thirty years [1]. The subject/object access framework paradigm, access control records, public-key cryptography [2], cryptographic protocols, and astounding security using information streams and the defining property are only a few of its many academic achievements. Notwithstanding these victories, the protection of a vast majority of transmitted computer systems remains appalling. On the overwhelming majority of these frameworks, the majority of the data might be taken or destroyed by a determined and skilled attacker. Even worse, the attacker could instantly do this to a significant amount of architectures [3].

The Internet has made computer security substantially extra troublesome. A few years back, a PC framework had multiple clients, all things considered, and all individuals from a similar association. Many of those who reside on the planet today are connected to the web. Anyone can attack your system. When a company is sold off, it might subsequently tarnish others. You face potentially threatening code that originates from a wide range of sources, frequently without your insight. Your PC faces an antagonistic physical condition. In the unlikely event that you possess drugs and must sell them, you will encounter intimidating hosts. Since you may need to run code from anywhere or impart data to anyone, you cannot just separate yourself.

Certain vulnerabilities—worms and infections—welcome defacement. They also make it much easier to attack a specific target, either to steal information or to corrupt it.

Then again, the damage these assaults cause is restricted, however expanding. Unfortunately, precise data regarding the cost of system security failures is unavailable: Most are never revealed because of a paranoid fear of embarrassment, but when a public incident occurs, security experts and vendors have an incentive to exaggerate its costs. The experience of the previous hard years affirms this investigation. Due to the increase in infection attacks, people are now required to buy firewall software and antivirus software and install fixes that address security flaws. At some cost to client comfort and reverse similarity, companies are making their systems safer. Be that as it May, the progressions have not been sensational [4].

Many people have suggested that technology monoculture exacerbates security problems and that more reasonable variation would enhance security, however, this is far too simple. The evidence shows that when the majority of platforms have the same flaws, criminals can achieve greater success. However, if an association presents multiple structures that all approach the same fundamental knowledge, as they probably will, then a concentrated attack only needs to find a flaw in one of them to succeed.

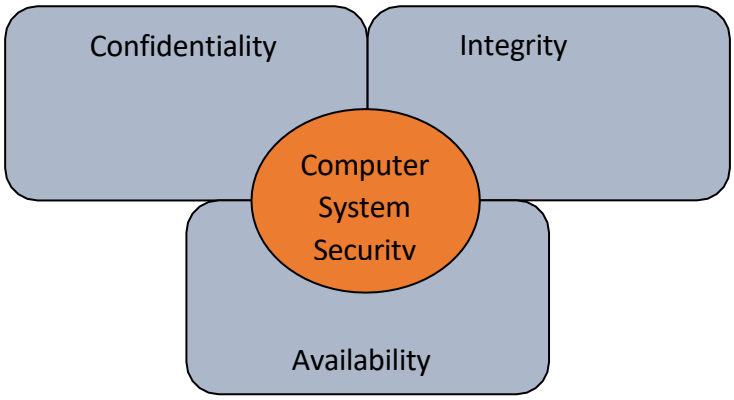

Figure 1. Computer System Security

2. OVERVIEW OF COMPUTER SECURITY

Most of the real-world schemes are not secure by the complete standard. Security on computers is merely a software component that is inexpensive to create, externally placed, and impenetrable by any means. This makes it easy to get sucked into the notion that electronic security can be perfect. Assurance is vital for security since the model needs to withstand hostile attacks rather than normal usage.

Identifying Security:

Companies and persons that utilize PC can explain their requirements for data safety under four main headings [5]:

Privacy: managing who can access and review data. Integrity: managing the transformation of data or the use of resources. Availability: providing prompt access to assets and data. Accountability: limiting access to information or assets. They are assisting in protecting certain resources from potential threats. Data or money are the sources. The most frequent risks include data loss, service interruption, financial loss, privacy invasion, and sabotage that ruins data. Users of PCs have to decide how much safety signifies for them.

Security Implementing Mechanism:

The code and the configuration are the two components of a safety architecture. The purpose of security implantation is to guard against threats. These come in three varieties: spoofing communications, thoughtless bad agents, and malicious programs (hostile or bugged).

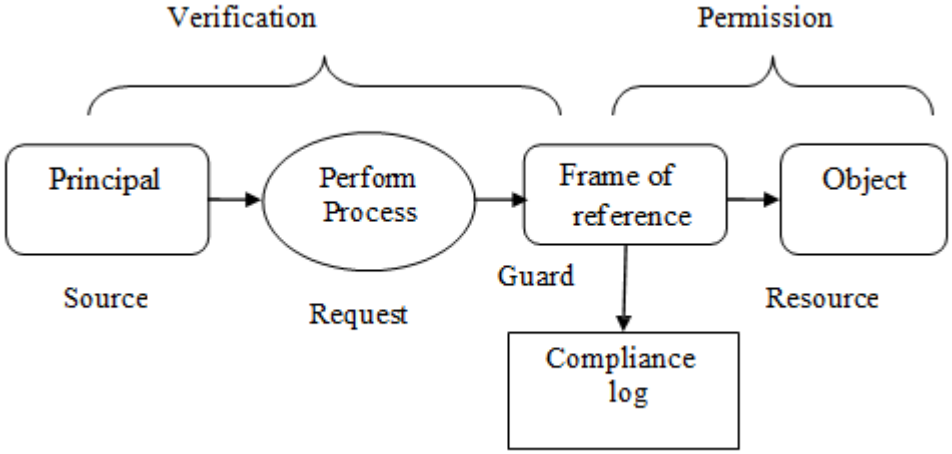

Figure 2. Access Control Representation

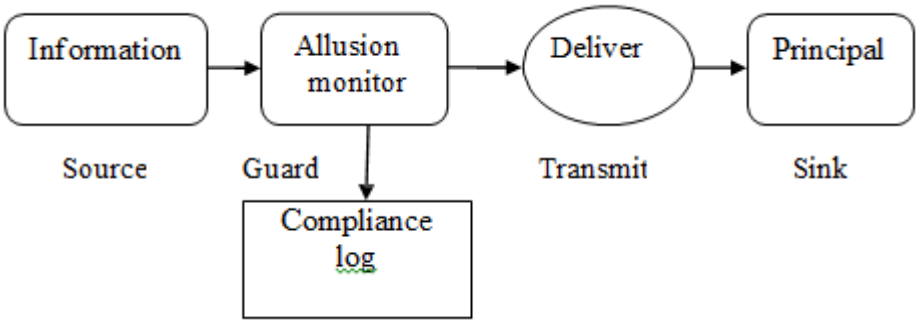

Figure 3. The Data Flow Representation

Extensively, there are five guarded procedures:

Coarse: Separate—keep everyone out. It gives the finest safety, yet it shields you from utilizing data or services from others, and from giving them to other people.
This is unrealistic for everything except for a couple of utilizations.
Medium: Eliminate—remain the trouble makers out. It's OK for programs within this safeguard to be guileless.

1) Fine: Control—Let the trouble makers in, yet keep them from harm. Sandboxing does this, regardless of whether the traditional kind is provided by a functional framework measure or the sophisticated type of a Oracle computer.
2) Recover—Undo the harm. Reinforcement frameworks and re-establish focuses are models. This does not help with mystery, but it does help greatly with legitimacy and availability.
3) Discipline the troublemakers by arresting them. Reviewing and cops do this.

Making Security Procedure:

The basic approach for clarifying the security protocol is described below:

If the only security strategy for machines on a LAN is to allow them to access the Web but not other computer authorities and no internal access will be allowed, then the TCB is simply a router (equipment, programming, and configuration) that allows active port 80 TCP connections but no other traffic. On the off chance that the strategy likewise says that no product gathered from the Internet should run, at that point, the TCB additionally incorporates the program code and settings that incapacitate Java and other programming downloads [6,7].

If a the Unix operating system framework's safety policy allows clients to browse guidelines indexes as well as browse and compose their home registries, the TCB is typically the device, the Unix component, and every application that can create a framework record (including any that runs within the super client).

This is a significant amount of programming. It also includes /etc/password and the permissions on the foundation and personal directories [8, 9].

3. EVALUATION OF SECURITY MANAGEMENT SYSTEM

With the growth of the World Wide Web and PC innovation, the PC has become an important tool in people's lives and at work. And yet, the PC infection assaults the PC and the network develops step by step, and the annihilation is not kidding step by step. An infectious attack has the potential to alter information, obliterate papers, impact exhibitions, or impact memory [10].

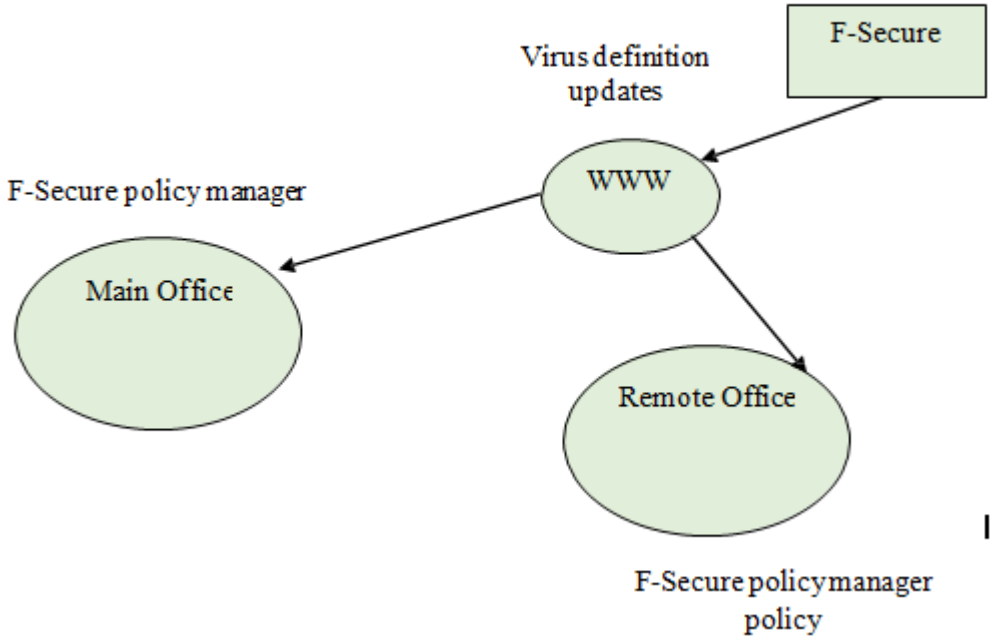

Figure 4. Experimental Representation of Antivirus Architecture

Computer malware can cause genuine or irreversible harm to PC users. To successfully keep the infection from hurt, the solution is to distinguish the infection early, and its disposal. There are two different ways to recognize and take out the PC infection. One is the physical strategy; the two are the programmed technique. This strategy needs the administrator to be well-known with the framework, and the activity is unpredictable and inclined to blunder, there is a sure danger when the activity will prompt unforeseen outcomes. This strategy is regularly used to dispense with the new infection which can't be wiped out by the programmed technique. Programmed recognition and end of a specific sort of infection or an assortment of infections utilizing specific enemies of infection programming or hostile to infection cards naturally recognize and dispense with the infection. This technique doesn't demolish the framework information, the activity is simple, the running rate is swift, is one sort of comparable ideal, and it is also more common to Identify and eliminate the infection using the technique [11].

The organization's works are the focal point of the PC organization, and it is the foundation of the organization. Organizational loss of motion is a significant image of the organization worker. When an organization worker is hit, the resulting damage is catastrophic, difficult to recover from, and impossible to evaluate. Currently, the majority of techniques to prevent and treat infection based on workers include the malware load module (NLM), which can provide the ability to identify the infection continually.

3.1 To Strengthen the Computer Network Management

The Protection and prevention of PC connection infection, fundamentally require innovation is ludicrous to effectively dispose of and forestall its propagation; only the specialized ways and the broad instrument carefully together, raise folks' awareness of avoidance, can secure.

The encrypted operation of the administrative framework in a broad sense. At the moment, the critical situation in the business's infection prevention and management innovation is an inactive guard; nonetheless, the management should be active. Most significantly, aside from the physical gear and developing framework maintenance, the executives, administration, and other parts of dangerous norms and rules, strengthen trustworthy instructions and employment ethical instruction on the network that framework head and client, operating methods, and standard performing methodology, reject the system, and individuals to participate in criminal activities [12].

Furthermore, if the individual is responsible for specific issues, infection side effects, an ideal review A system, new issues, and a new circumstance report, do infection discovery on a group of work stations, within the main door control organization. Notwithstanding the utilization of hostile to infection instruments on the worker has, yet additionally normally check the infection with the infection programming to check the worker. In particular, we ought to define exacting the board framework and organization

framework, improve their enemy of infection mindfulness; the advancement of following organization infection counteraction innovation, beyond what many would consider possible the utilization of new advancements and new successful methods, set up hostile to slaughter blend, to forestall the fundamental, assistant, delicate and difficult to murder one another, handling the issue "the best network infection protected mode [13,14].

4. CONCLUSION

The basic ideas of computer system security have been outlined in this paper: confidentiality, integrity, and availability. We have put forth the key concepts of PC privacy: privacy, honesty, and accessibility, which are implemented through access control based on the greatest level of quality of verification, approval, and inspection. We investigated the reasons why it does not perform well in practice.

- Emphasis on anticipation rather than identification and penalty.
- Difficulty with the coding and security arrangements, causing clients and directors to feel overwhelmed.

To reduce the complexity of this situation, we used a variety of phrases. Principals with many-leveled names are especially important. A parent can allocate for all of their children. Setting up namespaces in keys eliminates the need for a universally trusted root. Network security entails public security and influence, social strength, and public culture legacy, and conveys the significant issue; in this manner, to upgrade the security attention to the entire community, to improve the specialized degree of PC network safety, and to advance the progress of PC network protection, improve the protection of PC networks has become a pulling matter continuing apart from all other things.

REFERENCES

[1] Butler W. Lampson, “Computer Security in the Real World”, 6.826—Principles of Computer Systems, 1-14, 2004.
[2] B. Lampson,“Protection,” ACM Operating Systems Rev., vol. 8, no. 1, 1974, pp.18-24.
[3] J.H. Saltzer, “Protection and the Control of Information Sharing in Multics,” Comm. ACM, July 1974, pp. 388-402
[4] D.E. Denning, “A Lattice Model of Secure Information Flow,” Comm. ACM, May 1976, pp. 236-243.
[5] National Research Council, Computers at Risk: Safe Computing in the Information Age. National Academy Press, Washington D.C., 1991, books.nap.edu/catalog/1581.html
[6] CERT Coordination Center, CERT advisory CA-2000-04 Love Letter Worm, www.cert.org/advisories/CA-2000-04.html
[7] Clark and Wilson, A comparison of commercial and military computer security policies. IEEE Symp. Security and Privacy (April 1987), 184-194.
[8] B. Lampson et al., “Authentication in Distributed Systems: Theory and Practice,” ACM Trans. Computer Systems, vol. 10, no. 4, ACM Press, 1992, pp.265-310; www.acm.org/pubs/citations/journals/tocs/1992 -10-4/p265-lampson.
[9] P. England et al., “A Trusted Open Platform,” Computer, July 2003, pp. 55-62.
[10] Ma xiaojuan, “Research and Implementation of Computer Data Security Management System”, Procedia Engineering 174 (2017) 1371 – 1379.
[11] Wang Jie, easy to Jiang. Power enterprise information network security analysis and Countermeasures [J]. Electric power information. 2008 (10).
[12] Song hangs, Yuchi Kevin. [J]. science and technology achievements performance tuning method of Java EE based on the research aspect. 2008 (04).
[13] Wang Weiping, Liu Renyong. Research on enterprise information security management [J]. Information security and communication security. 2007 (06).
[14] Wang Yingxin, Niu Dongxiao. Electric power enterprise network information security management research [J]. China management information system (integrated version). 2007 (03).