Exploration and Implementation of Computer System Data Security Management System

Isyaku Uba Haruna[1], Ang Ching Wen[2]
[1]Taraba State University, Federal University Dutse, Nigeria.
[2]School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Pulau Pinang, Malaysia.

Article Info

Article history:

Received Jan 17, 2025
Revised Feb 29, 2025
Accepted Mar 5, 2025

Keywords:

A computer network
System security
Safety management
Intrusion Prevention
Mechanisms
Network Management

ABSTRACT

Most system security policies for computers are written relatively loosely. This is designed in many respects to provide easy access to all the features of the computer network. However, without the need to access many of the network features, so much leeway gives users the ability to perform functions that might damage the infrastructure or have access to information they do not necessary to look at. The intrusion prevention mechanisms, firewalls, and other protective equipment ensure the secure functioning of the system, but inside increasingly widespread use of networks, malware, hackers as well as extra safety accidents, these safety measures devices can deliver tens of thousands of alerts in a very small time, rendering it impossible for network management staff to locate valuable information. With this in mind, this paper deals with a look at computer system security. This paper deals with computer misuse and detection, and the exploration and application of a control of safety system. Detection of misuse includes at least two elements. Audit elimination and profiling capacity are these. Huge files can be set up when audit functions are allowed in the operating system. The automatic audit features can easily search audit files by setting staff user profiles, checking for usage that falls below what is determined to be usual, alerting administrators, and removing old audit data.

Corresponding Author:

Isyaku Uba Haruna,
Taraba State University, Federal University Dutse, Nigeria.

1. INTRODUCTION

It is not trivial to describe “computer security”. The challenge lies in creating a concept that, independent of the structure being defined, is broad enough to be accurate, and precise enough to explain what security is. Security is ‘safety from harm or threat’ in a general sense. In the framework Privacy in the field of computing is the avoidance of, or defense from, Links to data by unapproved receivers, and Deliberate but illegal loss or modification of the record.

"Security is the capacity of a system with regards to confidentiality and honesty to secure information and system properties." Note that, in addition to information, this second idea's scope includes system resources, such as CPUs, disks, and applications. A crucial part of maintaining a computer system's stability. It is a means of ensuring the confidentiality and integrity of the OS. Although no system can provide complete protection against numerous harmful threats and unauthorized usage, it is considered protected if its features are used and accessible as intended under all circumstances [1,3].

A system's security can be threatened by two breaches: Threat: Software that can inflict significant device harm. Attack: A security breach attempt and unauthorized use of a resource.It is possible to categorize vulnerability breaches impacting the device as intentional and unintended. As the name proposes, malicious threats are a kind of dangerous programming code or web script intended to build device vulnerabilities that

lead to backdoors and breaches of protection. Accidental threats are relatively easier to defend from. For instance: Denial of Service DDoS attack [2].

2. BASIC ELEMENTS OF COMPUTER SYSTEM SECURITY

The protection of Privacy, accessibility, and reliability are essential for computers. They all have different meanings depending on the context in which they occur. Understanding a certain element in a certain context is based on the customs, laws, and preferences of the relevant body [4].

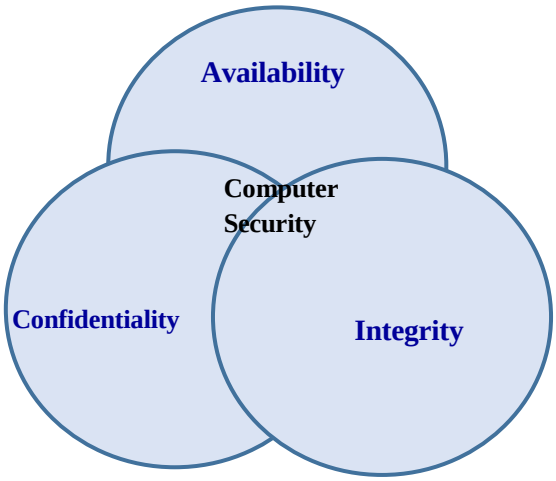

Figure 1. Elements of Computer System Security

Confidentiality

Confidentiality is the dissimulation of data or resources. In sensitive areas such as government and manufacturing, the need to keep knowledge confidential emerges from the use of computers. In the government, for example, military and civilian agencies frequently limit access to information to those who require it [5].

The soldiers' effort to introduce measures to impose a ‘need to know’ theory inspired the initial systematic work on information security. This theory also extends to manufacturing businesses that maintain their patented designs secret enough that their rivals cannot threaten to copy the designs. In another instance, employee records are kept confidential by every kind of organization. Access management system promotes confidentiality. Cryptography, which scrambles data to render it unintelligible, is one access management tool for maintaining secrecy. Entry to unscrambled information is managed by a cryptographic key, but even the cryptographic key itself becomes another data to be secured. Other system-dependent mechanisms can avoid the unauthorized access of information by systems. However, unlike enciphered data, where the controls malfunction or are bypassed, data controlled only by these controls can be accessed. Then a similar downside balances their advantage.

Another major part of secrecy is resource hiding. Sites also want to mask their setup and what systems they use; companies do not want others to know about specific facilities, and a service provider renting services from a corporation may not want others to recognize what tools it uses. Mechanisms for access regulation have these abilities too. Both secrecy compliance systems include the system's support facilities. The presumption is that the kernel and other agents can be counted on by the security services to provide accurate data.

Integrity

Integrity refers to data or service’s trustworthiness, and it is generally articulated in terms of avoiding illegal or unwanted alteration. Integrity requires the integrity of records and integrity of roots (the information source, then identified authentication). The information source can be based on its authenticity and credibility and the confidence put in the information by individuals.

Integrity systems fall into two groups: Mechanism for avoidance and mechanisms for identification. Avoidance systems aim to protect the data's privacy by preventing any illegal efforts to modify the

information or any striving to alter the information in ways that are not allowed. It is vital to differentiate between these two forms of attempts. The former happens when a person wants to modify facts that she has no power to alter. The latter happens when a person who is allowed to apply such modifications to the data, must alter the specifics in some manner. Assume, for example, that a computer is running a system for bookkeeping. In an attempt to alter the accounts, someone breaks into the system records.

Detection protocols do not aim to stop integrity violations; they merely announce that the integrity of the Data is no longer trustworthy. To detect issues, detection mechanisms can evaluate device events (client or system events) or (more usually) examine the data itself to observe whether there are still appropriate or anticipated restrictions. It is different to work with honesty than to work with secrecy. The information is either tainted with secrecy or not, but honesty requires both the correctness and the trustworthiness of the information.

Availability

Availability describes the right to use the requested knowledge or asset. It is a significant feature of both reliability and system architecture, as a system that is not usable at least is worse than having nothing at all. One security-related aspect of accessibility is that someone can intentionally set up a system to deny access to information or services by making it inaccessible. Device architectures typically assume a statistical model to evaluate anticipated usage trends, and when the statistical model holds, structures ensure availability. Someone could be able to modify use such that the mathematical model's predictions are no longer accurate. This implies that in a setting for which they were not planned, the structures for maintaining the resource or data accessible work. They would also collapse as a result.

3. THREATS CLASSIFICATION

The threats can be classified into program threats and system threats. A code prepared by a cracker to steal the protection or alter the usual process actions. The threats include the misuse of resources in the scheme. They aim to generate a condition where tools of the operating system and client documents are misused. They are also utilized as an intermediate for initiating threats to the program [6].

3.1 Program threats types:

✦ Virus: A well-known and most frequently recognized hazard. It is a self-reflecting and destructive thread that connects itself to system data and then reproduces itself easily, altering and deleting important files that contribute to a system crash. Besides, computer threats can be briefly summarized as follows:

- Data/parasitic- joins to a file itself
- Boot/memory- affects the boot segment
- Macro- drafted in a foremost language such as VB and impacts MS Office documents
- Source code- looks for and changes source codes
- Polymorphic- alterations in copying at any time
- Encrypted- encrypted virus and code decryption

✦ Trojan Horse: The code section that mistreats the situation is called the Trojan Horse. They appear to be an enticing and safe cover plan, but they are a secret, very dangerous program that can be utilized as the bearer of the virus. Users are deceived into entering their private login information on an application of one of the Trojan versions. These data are hijacked by the login simulator and can also be utilized as a means of breaching the records. An additional difference is Spyware, which supports an application that the user has selected to set up and download advertisements to view on the user's device, generating pop-up browser windows and, while those pages are accessed by the user, collecting necessary messages and sending it to the remote server. These threats are further classified as covert networks.

✦ **The Door of Trap:**

The developer of a program or computer will leave a void in the software that can only be used, and the Trap Door operates on similar concepts. It is very difficult to locate trap doors when they have to be analyzed, one needs to go through all the device's components' source code.

✦ **Logical Bomb:**

A software that begins a safety attack just in a particular condition.

3.2 System threats types:

In addition to the program threats, numerous system threats often threaten our system stability:

✦ **Computer Worm:**

Bug software that travels through networks. Dissimilar to viruses, they primarily target LANs. A worm-affected computer concentrates the objective structure and marks a short "hook" code to it. This hook is also utilized to copy the warm to the target system. This mechanism replicates recursively, and entire LAN networks will soon be affected. It uses the spawning function to replicate itself. The worm spawns use the bulk of machine energy and also lock out all other operations.

✦ **Scanning Port:**

In the scanning port, the cracker determines the flaws of the attack method. It is an automatic procedure that includes establishing a TCP/IP link to a particular point.

✦ **Denial of Services:**

These attacks are not meant for gathering information or deleting machine data. Instead, they are utilized to interrupt the legal exploit of a device or service. These intrusions are usually based on a network. They go down into the following two categories: Attacks in this primary group consume so many machine possessions that no valuable work can be completed.

3.3 Protection Measures Taken

Protection precautions should be taken in the following steps to secure the system [7]:

Physical:

Sites holding information infrastructure must be physically defended from equipped and hostile intruders. Workstations ought to be carefully secured.

Human:

Only suitable users must be allowed to use the device. Phishing (collection of sensitive data) and Dumpster Diving (collection of essential data to obtain illegal contact) should be stopped.

Operational system:

The device must defend itself from unintended or deliberate violation of security.

A Framework of Networking:

Almost every piece of data is exchanged over a network of various networks. Intercepting this data may be almost as dangerous as hacking into a device. The network should be adequately protected against such attacks from now on.

Typically, anti- Malware tools are utilized to regularly find out and uninstall certain viruses and attacks. Also, a firewall is sometimes used to defend the system from network attacks.

4. DATA SECURITY MANAGEMENT SYSTEM

A Computer data security management system also called information technology (IT) security system, is a developing domain used by both government organizations and private companies. Confidential company information can be handled effectively and securely with the help of a Data Security Management System (DSMS). The area of safety control systems is fairly broad and usually encompasses anything from tracking safety with the installation of sophisticated protection control systems in shopping centers and institutions that are typically designed to secure the information of the company [8].

Data security management system Characteristic [9]: Buildings, people, and products are all physically safe as part of security management. It is the acknowledgment of the company's qualities. Generally, the Data Security Management System is given to any organization that uses security management and procedures such as data classification, risk evaluation, and risk analysis to detect risks, categorize assets, and rank.

4.1 Data Security Management System Importance

Some significant aspects of security management are usually offered to every organization and are mentioned below [10]:

Intellectual Property:

There are fundamental explanations for the company to formalize an innovation strategy policy to achieve a strategic advantage in competition. While the initial phases of ideation are available to everyone, a lot of effort goes into creating and improving certain concepts, and that refinement is always the difference

between the gradual concept and the transformational one and the organizations do not secure those later stages of refining operations, because they could risk the strategic advantage they achieve from building up an invention management scheme in the first place.

The Integrity of Data:

Data Security Management systems have confidence in a lot of data to help prioritize and verify programs, and usually, we should talk about votes and feedback on ideas, ROI data, and more. If data security management systems are not reliable, this data may be stripped or tampered with. It'll be easy to make the concept or initiative look more popular or desirable if the device can be played.

Personal Identifying Information:

Those who join in the protection management software share a minimum of their personal data to access the system, where confidentiality is crucial. Programs for security management are offered to keep all users safe. as a matter of nature.

Interconnectivity of the system:

Security control software typically integrates with some other programs, such as project management, social software, and beyond. The fragility of one system will Contribute to the fragility of others, which is why every data security management system must be equivalent to the systems with which it communicates.

Table 1. Facts about Computer Security Management

Qualified certification	The Certified Information Systems Security Professional (CISSP) credential is provided by $(ISC)^2$
Key skills	Intelligence, logic, decision making, management, analytic skills
Workplace	Mostly for business/financial organizations, consultancy agencies, or computer enterprises; usually full-time and often over forty hours a week.
Same profession	IT accountant, IT manager, security engineer, IT/Computer/Networking specialist, computer network programmer, database controller
Average earnings	$111,266 (information systems managers); $72 (information security analysts)
Job perspective (2015-2025)	12 percent- computer and information system managers; 28 percent- computer and information system managers; information security investigator

4.2 Implementation

Security management deals with ensuring the safety of the infrastructure is preserved in the face of man-made challenges and hazards, whether deliberate or accidental. Intentional human- These hazards includes computer infections, hacking, and spying. Among the unintended hazards are those caused by wounds or individuals who are not aware of the repercussions of their behavior. The procedures involved in managing security and the elements that contribute to its success are explained in the following section [11].

Figure 2. Importance of Data Security Management System

1. Decide & Evaluate assets of IT

Physical, information, and people are the There are three categories of resources that need to be identified.

Physical:

- Capital for hardware and applications
- Construction services
- Tools used to house classified assets or to process sensitive information

Information:

The details group contains classified details related to the activities, plans, and policies of the organization.

People:

The group of persons comprises important individuals occupying key positions whose incapacity or absence would affect the enterprise.

2. Risk Analysis

Any efficient data security management system represents a wary estimation of how much safety is required. Very less protection ensures that the device may be hacked deliberately or accidentally. Excess protection will make the machine impossible to work or humiliate its use inappropriately. Protection is inversely proportional to usefulness—if a user needs the device to be 100 percent safe, don't allow anyone uses it. Systems will often be at risk, but sometimes these threats are embraced if they change the system more influential or easy to work.

3. Establish Security Practices

Define the following main areas of security monitoring in detail:

Asset categorization Performance: recommendations for the concept of protection standards as discussed above Hazard evaluation and acceptance: as mentioned above Asset Ownership: assigning of positions to handle critical properties.

Asset Management Duties: The activities and processes to be followed by organizations managing the asset, as identified above.

Strategies on abuse security properties

Why security breaches are identified and responded to Threat alertness practices: outreach initiatives and asset marking.

Compliance audits: Unannounced security safeguards placed to assess if they are in service.

4. Implement Security Standards

• Implement protection measures as specified at this stage of the previous step. To make the transfer to the fresh workplace easier for everyone, you must accomplish this in phases climate.

• By agency, beginning with the most fragile properties. The IT department will be the obvious first option.

• Company feature or operation, beginning with those that rely on (or create) the most vulnerable properties.

• By venue, particularly if the priority critical assets are more physical. This strategy is the simplest to incorporate.

• Women, beginning with core members of the organization.

5. Monitor Activity

• Successful security management discipline relies on proper supervision of compliance. If security procedures are not monitored and addressed, inadvertent or deliberate security practice violations increase in frequency and severity. A programmer for computers who escapes punishment for first device infiltration will come back again and again if he thinks that no one will track his activities.

6. Reevaluation

• Security monitoring is a practice that never sits on it. Large changes that would require a reassessment of security policy procedures include:

• Security breaches are rampant.

• Changes in corporate structure or composition.

• The corporate climate is evolving.

• Changes in technology.

• Fund funding is decreasing.

[12] A mistake or flaw in network security is one that a malevolent attacker could exploit to carry out unlawful actions on a computer system. Any software designed to harm computers, documents, or people is known as malware, or harmful software. Trojan horses, spyware, the threat of ransom spyware, worms, file-less malware, computer infections, and hybrid attacks are examples of malware kinds. Since the advent of artificial intelligence and tailored spear-phishing emails, risks associated with ransomware have evolved.

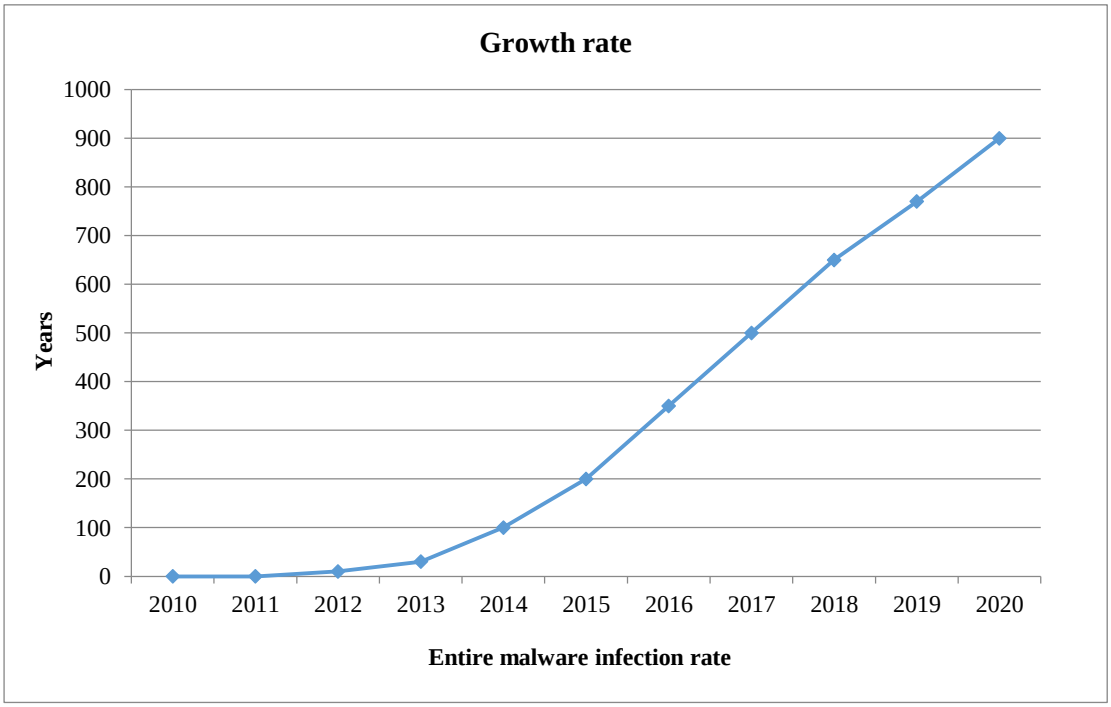

Figure 3. Malware Statistics

Over the past ten years, the total number of infections with malware has increased. Which is shown in Figure 3.

5. CONCLUSION

As the variety and significance of technological advances continue to grow, it is crucial to protect mission-critical computer systems that carry out the most crucial business tasks and procedures. Data protection helps to protect the secrecy, fairness, and compatibility of computing devices and their components. Three key sections of the computer system are subject to attack: hardware, software, and records. All three, and interactions between them, are vulnerable to computer security vulnerabilities. In contrast, certain individuals and programs that are involved in breaching the mechanism will formulate attacks that target vulnerabilities. Network safety affects social harmony, national security and autonomy, and national cultural heritage and, hence, it is an important topic to raise awareness of the security of society as a whole, and to increase the technological standard of Security of computer networks, [13] and encouraging innovation in networking security, bolstering network security for computers has become an urgent issue at the moment.

REFERENCES

[1] Dictionary of Computing, Fourth Ed. (Oxford: Oxford University Press, (1996).
[2] J. Anderson, "Computer Security Threat Monitoring and Surveillance," James P. Anderson Co., Fort Washington, PA (1980).
[3] Computer Security: A Practical Definition. http://www.albion.com/security/intro-4.html
[4] Matt Bishop, "Introduction to Computer Security", 2004. http://www.uoitc.edu.iq/images/documents/informatics-institute/exam_materials/Introduction%20to%20Compute r%20Security%20pdf%20DONE.pdf
[5] G. Serrao, "Rating Network Components," Proceedings of the 18th National Information Systems Security Conference, pp. 344–355 (Oct. 1995).
[6] System Security, 2019. https://www.geeksforgeeks.org/system-security/
[7] R. Conway, W. Maxwell, and H. Morgan, "On the Implementation of Security Measures in Information Systems," Communications of the ACM 15 (4), pp. 211–220 (Apr. 1972).
[8] M. Bishop and D. Klein, "Improving System Security via Proactive Password Checking," Computers and Security 14 (3), pp. 233–249 (Apr. 1995).
[9] Security Management System, 2019, https://www.geeksforgeeks.org/security-management- system/
[10] D. Bailey, "A Philosophy of Security Management," in Information Security: An integrated Collection of Essays [6], pp. 98–110.
[11] Harris Kern**, "**Implement security management with these six steps", Security. 2003. https://www.techrepublic.com/article/implement-security- management-with-these-six-steps/
[12] 2020 Cyber Security Statistics The Ultimate List https://purplesec.us/resources/cyber-security-statistics/ Ma xiaojuan, "Research and Implementation of Computer Data Security Management System", Procedia Engineering 174 (2017) 1371 – 1379. doi: 10.1016/j.proeng.2017.01.290