Engineering Technology Trends Vol 2 Issue 4 2024

Original Research Article

Open Access

Omniscient Pte.Ltd.

Analysing Computer System Security and Computer Network Security

Guo-Liang Zhang*

Guangzhou Institute of Commerce and Industry, Foshan, Guangdong, 258137, China

***Correspondence to:** Guo-Liang Zhang, Guangzhou Institute of Commerce and Industry, Foshan, Guangdong, 258137, China, E-mail: 9986807@qq.com

Abstract: Computer system security and computer network security are the key areas to guarantee the security of data and information assets in the era of information technology. Computer system security focuses on protecting hardware, software and data from internal and external threats to ensure stable and reliable operation of the system. Computer network security, on the other hand, focuses on the protection of data transmission and storage security in the network, and effectively defends against network attacks and data leakage by means of access control, data encryption, network isolation and other means. The two are interdependent, and together they build a secure and trustworthy computing environment.

Keywords: Computer; system security; network security

Introduction

With the rapid progress of information technology, computer system security and network security are increasingly highlighting their importance. System security concerns the integrity and confidentiality of hardware, software and data to ensure stable system operation; network security focuses on the security of network data transmission and storage. The two are intertwined to build a fortress of information security, which has an irreplaceable role in the protection of personal privacy, stability of business operations and even national security. Therefore, an in-depth understanding and strengthening of computer system and network security is crucial.

1. The Importance of Computer System Security and Computer Network Security

Computer system security and computer network security in today's information society has a pivotal position, the importance of which can not be ignored. With the rapid development of science and technology, computer networks have become an indispensable part of people's daily life, work and study. However, along with this is the increasing number of network security threats, which makes computer system security and computer network security become particularly important. First, the importance of computer system security lies in the fact that it protects the security of computer hardware, software and data resources. Once a computer system is attacked or damaged, it may not only lead to the damage of hardware equipment, but also to the collapse of software systems and the loss

of important data. These losses may be the leakage of personal information for individuals, and may involve the loss of important assets such as business secrets and intellectual property rights for enterprises and organizations. Therefore, ensuring computer system security is a basic safeguard for maintaining the interests of individuals and organizations. Second, the importance of computer network security lies in the fact that it protects the security of network communications. In the digital era, people carry out activities such as information transfer, communication and transaction through the network. Network attackers may use various means to steal, tamper with, or destroy data in the network, thus bringing serious losses to individuals and organizations[1]. Strengthening computer network security protection to ensure the confidentiality, integrity and availability of network communications is of great significance for maintaining social stability and promoting economic development. Third, computer system security and computer network security are also closely related to national security. With the wide application of information technology, network security has become an important part of national security. Once a country's computer system or network is attacked, it may lead to serious consequences such as the leakage of national secrets and the paralysis of infrastructure, posing a serious threat to national security. Therefore, strengthening computer system security and computer network security plays a crucial role in maintaining national security. Fourthly, the importance of computer system security and computer network security is self-evident. We should fully understand their importance and strengthen security measures to ensure the security and stability of computer systems and networks, so as to provide a strong guarantee for the healthy development of an information-based society.

2. Computer System Security Analysis

2.1 Operational Security

Operational security as the core of computer system security, the key is to ensure that the system in the face of external threats and internal failures, can maintain a stable operating state, continue to provide reliable services, so as to effectively protect the integrity and availability of system data. Specifically, operational security involves the following aspects: (1) system stability: to ensure the stable operation of the computer system to prevent system collapse or data loss due to software defects or hardware failure. (2) Data protection: to ensure that the data in the system is not subject to unauthorized access, modification or deletion, whether stored on the hard drive or transmitted over the network. (3) Resource management: Reasonably allocate system resources to prevent service denial attacks caused by resource competition or resource exhaustion. (4) User Behaviour Monitoring: Monitor user behaviour in the system to identify and stop potential malicious behaviour or misuse in a timely manner. (5) Emergency Response: Establish an emergency response mechanism, so that once a security incident occurs, measures can be taken quickly to minimize losses. In order to achieve the above goals, a series of technical and management strategies are required. Technically, tools for real-time monitoring of system status, such as Intrusion Detection Systems (IDS) and data encryption, as well as regular system updates and patch management to fix known vulnerabilities, can be used. Management-wise, strict operating procedures and access control policies are formulated, and regular security training is provided to users to improve their security awareness.

2.2 Information Security

In the analysis of computer system security, the central position of information security is self-evident. Information security is not only about the confidentiality of data to ensure that sensitive information is not illegally accessed; it is also about the integrity of data to prevent data from being tampered with during transmission or storage; and more importantly, it is about the availability of data to ensure that the data can be normally accessed and used by authorized users when needed. In a complex network environment, every aspect of a computer system - from data generation to transmission, storage and use -- requires tight information security protection to ensure data security and reliability. Data confidentiality requires that information can only be accessed and used by authorized users, which requires the system to have strong authentication and access control mechanisms to ensure that only authenticated users can access specific data resources. Data integrity requires that information is not tampered with or destroyed during storage and transmission, which relies on the system's ability to

detect and recover data integrity, as well as to respond to and stop illegal tampering in a timely manner. The availability of data requires that information can be accessed and used normally when needed, which requires the system to have high reliability and fault tolerance, and to be able to quickly recover data and services in the event of failure to ensure business continuity[2]. In order to ensure information security, computer systems need to adopt a series of security measures, such as data encryption, security auditing, intrusion detection and so on. At the same time, it is also necessary to strengthen the security awareness and training of users to improve the security protection of the entire system.

2.3 Management Security

Management security is a crucial part of computer system security, involving the responsibility, supervision, planning and execution of managers and administrators in system security. Throughout the life cycle of a computer system's operation, management security runs through the design, deployment, operation and maintenance phases of the system to ensure that the system continues to maintain a high level of security. (1) Responsibility and Oversight: In managing security, managers and administrators assume an important role of oversight and responsibility. They should ensure that system security policies are developed, implemented and monitored, and are responsible for ensuring system compliance and integrity. Administrators should have professional security knowledge and skills, review and update system security measures on a regular basis, and address identified security vulnerabilities and issues in a timely manner. (2) Security Training and Awareness Enhancement: Managing security also includes security training and awareness enhancement for system users and related personnel. Through regular security training and education activities, users' awareness of security issues is enhanced, and their ability to deal with security threats and risks is strengthened. Only if users have good security awareness and behaviour, the overall security of the computer system can be guaranteed. (3) Security Audit and Monitoring: Management of security in the security audit and monitoring is an important safeguard for system security. Through the implementation of comprehensive security audits and daily monitoring, security vulnerabilities and abnormal behaviour can be detected in a timely manner, and take appropriate measures to address. Security auditing and monitoring help assess system security and respond to potential security threats in a timely manner. (4) Improvement and refinement: Managing security should also include a mechanism for continuous improvement and refinement of system security. Managers and administrators need to continuously optimize security strategies and countermeasures based on problems and lessons learned during system operation, and improve the system's ability to cope with risks and threats, so as to ensure that system security can be continuously improved.

3. Computer Network Security Analysis

3.1 Access Control

Access control is a crucial aspect in computer network security analysis. Access control aims to ensure that network resources are only accessed by authorized users or systems, thus protecting the confidentiality, integrity and availability of data. The core of access control is the implementation of authentication and privilege management. Authentication is the process of verifying a user's identity, usually by means of a username and password, biometric technology or digital certificates. Once the user's identity is confirmed, the system assigns the appropriate access rights to the user based on a preset rights management policy. Privilege management policies define what resources a user or system can access and what operations they can perform. These policies are usually based on factors such as roles, responsibilities, tasks, or data sensitivity. For example, administrators may have full access to system configuration and management, while regular users may only have access to data and applications relevant to their work. There are also several key points to keep in mind when implementing access control: (1) Least Privilege Principle: Assign each user or system the least amount of privilege needed to complete a task to reduce potential security risks. (2) Regular auditing and updating: Regularly review and update privilege management policies to ensure they still meet the organization's business needs and security requirements. (3) Monitoring and logging: Monitor user and system access activities to resources and log them for later auditing and analysis.

3.2 Data Encryption Protection

In the field of computer network security, data encryption protection plays a crucial role. By adopting advanced encryption algorithms and technologies, data encryption protection can ensure that data is not illegally intercepted and parsed during transmission, and at the same time prevent unauthorized access to or tampering with the data when it is being stored, thus greatly enhancing the security and confidentiality of information in the network environment. Data encryption prevents data from being illegally stolen or tampered with by applying specific algorithms and keys to convert the original data (plaintext) into a form that is difficult to be understood by unauthorized persons (ciphertext). The importance of data encryption protection cannot be overstated. During data transmission, data may be transmitted over public or untrusted networks, which puts it at risk of interception and theft. With data encryption, even if data is intercepted, unauthorized persons cannot decrypt and read its contents, thus safeguarding the confidentiality of the data. Data encryption also protects the integrity of data. During data transmission, malicious attackers may try to tamper with the data to compromise its integrity and availability. By using encryption, even if the data is tampered with, the receiver is able to detect and reject the tampered data by verifying the integrity of the data, thus ensuring the integrity and availability of the data. Data encryption protection is implemented in a variety of ways, including symmetric encryption, asymmetric encryption, and hash functions. Symmetric encryption uses the same key for encryption and decryption, and is suitable for scenarios that require efficient encryption of a large amount of data; asymmetric encryption uses a pair of keys (public and private keys), with the public key used to encrypt the data and the private key used to decrypt the data, and is suitable for scenarios that require the verification of the identity of the sender of the data; and the hash function verifies the integrity of the data by calculating the data's digest value.

3.3 Network Isolation Protection

In computer network security analysis, network isolation protection is an important strategy aimed at dividing the network into different security zones by physical or logical means to prevent potential network attacks from spreading or affecting the security of the entire network. Network Isolation Protection plays a vital role in protecting critical systems and data. Network Isolation Protection can effectively restrict unauthorized access. By dividing the network into different security zones, such as internal network, external network, DMZ (quarantine zone), etc., and setting up strict access control policies, it can ensure that only authorized users or systems can access specific network resources. This greatly reduces the risk of unauthorized access and potential attacks. Network isolation protection helps prevent attacks from spreading; once a security zone is attacked, network isolation protection can limit the attacker's ability to further access other zones, thus preventing attacks from spreading throughout the network[3]. This isolation mechanism ensures that critical systems and data are protected from attacks, ensuring business continuity and stability. Network isolation protection can also improve the manageability and security of the network, and by dividing the network into different security zones, network management can be simplified and management costs can be reduced. At the same time, different security policies can be set between the various regions to adapt to different security needs and improve the security of the entire network. There are various methods to achieve network isolation and protection, including physical isolation (e.g., using different network equipment, lines or physical space) and logical isolation (e.g., using VLANs, firewalls, intrusion detection systems, etc.). According to the specific network environment and security needs, you can choose the appropriate isolation methods and strategies to achieve network isolation protection.

Conclusion

In the era of information technology, the challenges in the field of security are becoming increasingly severe, and we must constantly increase our efforts in research and investment in it. Through continuous technological innovation and perfect security strategies, we can actively respond to various security threats and challenges to ensure the security and stability of the digital world. At the same time, we should also be committed to popularizing information security awareness, so that everyone can become the guardian of digital security. Let's work together to build a

safe, stable and reliable digital environment, lay a solid foundation for the continuous progress and development of society, and move towards a more secure and reliable future.

References

[1] Zhang Pingping. Analysis of Common Security Problems and Optimization Strategies in Computer Network Engineering [J]. China New Communication, 2021, 23(08):132-133.

[2] Hu Cheng. On the analysis of computer system security and computer network security[J]. Popular Standardization, 2021(02):159-160.

[3] Cheng Yang. Research on Computer System Security and Computer Network Security[J]. Computer knowledge and technology, 2020, 16(12):29+35.