Computer network information security and its protection countermeasures

Wu Weiwei

Zhejiang Yuying College of Vocational Technology, Hangzhou, Zhejiang, China

Keywords: computer network, information security, threats, risks, protective countermeasures

Abstract: With the rapid development of information technology, computer network has become an indispensable part of people's daily life and work. However, the problem of computer network information security is also becoming more and more prominent, network attacks, information leakage, system crash and other security problems have brought serious losses to individuals and enterprises. Therefore, this paper discusses the basic concepts of computer network information security, threats and risks, and protection countermeasures.

1. Introduction

With the rapid development of information technology, computer networks have become an indispensable part of people's daily life and work. While computer networks bring convenience to people, they also face more and more security threats. Network attacks, information leakage, system crashes and other security problems have brought serious losses to individuals and enterprises. Therefore, computer network information security has become an important research field. This paper aims to discuss computer network information security and its protection countermeasures. Firstly, the basic concepts of computer network information security are introduced, including the definition, objectives and basic principles of information security. Secondly, the threats and risks faced by computer networks are analyzed. Next, protection countermeasures for computer network information security are discussed, including network security policy, access control, encryption technology, security audit and emergency response plan. Finally, the importance of computer network information security is summarized and some future research directions are proposed.

2. Basic concepts and threats and risks of computer network information security

2.1 The basic concept of computer network information security

Information security is a series of measures and principles to protect the confidentiality, integrity and availability of information and information systems in computer networks. It ensures that only authorized people can access information, that the integrity of information is maintained, and that information and information systems are available when needed. It is very important to secure information in a computer network, and here are a few basic principles. First is the principle of least privilege, according to the principle of least privilege, users and systems should only be given the minimum privileges needed to do their jobs. This means that users should only have access to the resources and data they need, and systems should only perform the operations they need. By limiting permissions, potential security vulnerabilities can be reduced. Next is the shortest path principle. The shortest path principle refers to restricting security traffic in the network to the shortest possible path, minimizing the opportunity for attackers to enter the network. This can be accomplished through the use of technologies such as firewalls, intrusion detection systems, and network isolation. Once again, there is the weakest link principle, which emphasizes the holistic nature of network security, i.e., the security of the entire network depends on the weakest link. Attackers usually choose to utilize the weakest link in the network for invasion, therefore, strengthening the security of the weakest link is crucial for the security of the entire network. Finally, there is the principle of comprehensive auditing, which emphasizes comprehensive monitoring and auditing of information and operations in the network. By recording key events and user behaviors, abnormal activities can be detected in a timely manner and the source of the event can be traced. Security auditing can also help improve security

  DOI: 10.25236/iceieis.2023.011

measures and address future security threats.

2.2 Threats and Risks to Computer Networks

Threats and risks faced by computer networks mainly include network attacks, information leakage, and system crashes. All these risks can lead to losses such as data loss, malware infections and service interruptions. Here, we will delve into the specific threats posed by each of these risks. Cyber-attacks are one of the most common and significant risks that cause disruption or damage to computer networks and their internal resources. One of these is a denial-of-service attack (DDoS), which paralyzes a server or network by making the services of the target system unavailable. An attacker can launch a DDoS attack by exploiting a network vulnerability and make network transmissions abnormally slow or crash completely. There is also the risk of eavesdropping, where attackers listen in on transmissions to gain access to keys or sensitive information, which can lead to confidential data leaks. Information leakage is another common risk that can lead to personal privacy breaches or loss of trade secrets. One example is information tampering, where an attacker may modify or delete data or files that have been stored, making the information unavailable or inaccurate. Another possible threat is malware infection, where attackers often use spoofing, phishing, or social engineering to trick users into installing malware to infect their computers. In addition, hackers can use vulnerabilities to break through network security defenses to gain access to sensitive data. System crashes are another risk to computer networks; system crashes can cause computer applications to fail to function properly or even cause computer systems to crash. One such threat is virus infection, which is a type of malware that damages computer systems by modifying or deleting files and data. Another threat is malware, which can contain many types of computer viruses, Trojan horses, spyware, etc., causing system and data security hazards.

3. Protection Countermeasures for Computer Network Information Security

3.1 Network security strategy

Network security strategies are a series of measures taken to protect the security of information and information systems in computer networks. The goal of these strategies is to prevent unauthorized access, data leakage, network attacks, and other potential threats, and to ensure the availability, integrity and confidentiality of the network. Some common network security strategies are described in detail below. First, network access control is an important security policy. By implementing an access control policy, you can restrict access to network resources and allow only authenticated and authorized users to use the system. This can be achieved by using techniques such as strong passwords, multi-factor authentication, access lists, and access control lists (ACLs). Second, network isolation is a strategy for separating networks to mitigate the ability of an attacker to propagate within the network. Network isolation is achieved by dividing the network into different security zones and using techniques such as firewalls and virtual private networks (VPNs). This way, even if an attack occurs, its impact on other network resources can be minimized. Network traffic monitoring and filtering is another important network security strategy. Monitoring network traffic can help identify abnormal behavior and potential attacks so that timely action can be taken. Traffic filtering allows network traffic to be inspected and filtered according to pre-defined rules, blocking potentially malicious traffic from entering the network system. In addition, regular vulnerability assessment and security patch management is a key network security strategy. By regularly checking for vulnerabilities in the network system and quickly deploying vendor-supplied security patches, the chances of attackers exploiting known vulnerabilities can be reduced and the security of the system can be improved[1].

3.2 Access Control

Access control is an important part of the computer network security system, which aims to ensure that only authenticated and authorized users can access computer systems and network resources to protect the security of information and information systems. Access control involves three main aspects: authentication, authorization and auditing. Authentication is the first step in access control,

which is used to verify that the user's declared identity is consistent with his or her true identity. Authentication can be done through passwords, digital certificates, biometrics, etc., of which the most common is authentication using a username and password. In addition, there are some advanced authentication techniques, such as multi-factor authentication, which requires the simultaneous use of passwords, hardware tokens, cell phone authentication codes and other authentication factors to confirm the user's identity. Authorization is the second step of access control, which determines the privileges that a user has in the system and the ability to access resources. Authorization can be managed by means of access control lists (ACLs) and role-based access control (RBAC), etc. An ACL is a table that stores the relationship between an empowered user and an authorized object. RBAC, on the other hand, manages the permissions of users by assigning them to different roles. when a user is assigned to a role, he or she automatically has the permissions associated with that role. Auditing is the third step of access control, which records users' access behaviors and events in the system, including logging in, accessing, operating, and logging out. Auditing can help administrators detect abnormal behavior and take timely action to prevent and combat security threats. At the same time, auditing can also provide system administrators with tracking and analysis of security events, thus strengthening the reliability and stability of the entire network security system[2].

3.3 Encryption Technology

Encryption technology is an important means of information security protection, which transforms the original information into a special form through mathematical algorithms to ensure the confidentiality and integrity of the information in the transmission and storage process. Commonly used encryption techniques include symmetric encryption, asymmetric encryption and hash function. Symmetric encryption is an encryption algorithm that uses the same key for encryption and decryption. The sender uses the key to convert plaintext to ciphertext and sends the ciphertext to the receiver. The receiver decrypts the ciphertext to plaintext using the same key. Common symmetric encryption algorithms are DES, AES and RC4. Symmetric encryption has the advantage of being efficient and fast, but key management and distribution is a challenge because the sender and receiver must share the key in advance. Asymmetric encryption, also known as public key encryption, uses a pair of keys, public and private, for encryption and decryption operations. The sender encrypts the plaintext using the receiver's public key, while the receiver decrypts the ciphertext using his own private key. Since the private key of the receiver is unique, it ensures the confidentiality of the message. Common asymmetric encryption algorithms are RSA and Elliptic Curve Cryptography (ECC). Asymmetric encryption provides high security but has higher computational complexity as compared to symmetric encryption. A hash function is a one-way hash function that converts an input message of arbitrary length into an output of fixed length, called a hash value. The hash function has characteristics: the same input always produces the same hash value, and different inputs are almost impossible to produce the same hash value. Hash function is often used to verify the integrity and consistency of information. For example, in the file transfer process, the file can be hashed, the sender and receiver respectively calculate the hash value of the file and compare it to verify whether the file has been tampered with.

3.4 Security Audit

Security audit refers to a series of inspection, monitoring and analysis activities carried out to prevent and respond to the security risks of information systems, aiming at discovering security vulnerabilities and misconduct. Security auditing can help organizations or enterprises to discover and solve security problems in a timely manner and reduce losses caused by security threats. Security auditing usually includes analyzing logs and configuration files of operating systems, network devices, databases, and other systems, as well as detecting and responding to security events, detecting anomalies, and alerting the police in a timely manner. In addition, security auditing can also assess and improve the security performance of the system according to relevant security standards and specifications. Through security auditing, network security awareness can be improved, security management can be strengthened, security technology level can be improved, and various security threats can be effectively prevented and responded to[3].

3.5 Emergency Response Program

Emergency response plan is a series of emergency measures formulated and implemented when a security incident occurs in a computer network, aiming at rapidly identifying, isolating and resolving security threats and minimizing security losses. An emergency response plan usually includes categorizing security events and taking appropriate emergency measures according to different types of events. For example, security incidents such as network intrusions, malware infections or data breaches may require different response strategies and processes. An emergency response plan should also include a clear incident response process to ensure that the appropriate response procedures can be initiated in a quick and orderly manner in the event of a security incident. This may involve a series of steps such as notifying relevant personnel, isolating affected systems, gathering evidence, fixing vulnerabilities and restoring compromised services. In addition, the emergency response plan should also provide detailed guidelines for handling security incidents, including the responsibilities and authorities of involved personnel, contact information, communication channels and tools, etc., to ensure that the response team can work together efficiently.

4. Conclusion

This paper discusses the basic concepts, threats and risks, and protective countermeasures of computer network information security. Computer network information security is very important for both individuals and organizations. A series of protective countermeasures can be taken, including network security policy, access control, encryption technology, security auditing, and emergency response plan. These measures aim to protect the security of information and information systems in computer networks.

References

[1] Zhang Ke. Research on computer network information security and its protection countermeasures[J]. Office Automation, 2023, 28 (14): 19-21.

[2] Ma Yuehuan. Discussion on computer network information security and its protection countermeasures[J]. Modern Information Technology, 2022, 6 (19): 116-119.

[3] Wei Zhongqing. Analysis of information security protection countermeasures of computer network[J]. Electronic Technology, 2022, 51 (05): 270-271.