Proceedings of the 2nd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/76/20240594

Analysis of problems and countermeasures in computer network engineering security

Xinyi Feng

Information Technology & Business Management Department, Chengdu Neusoft University, Chengdu City, China

1411570178@qq.com

Abstract. This paper analyzes the existing security issues in computer network engineering and proposes a series of countermeasures. To address the problems of hacker attacks and information leakage, it is recommended to strengthen network monitoring and the application of encryption technology. For the issues of malware and virus dissemination, it is advised to regularly update antivirus software and enhance employee security awareness training. Regarding network data leakage and privacy breaches, the use of secure transmission protocols and multi-factor authentication technology is advocated. For network security management and maintenance issues, establishing a sound security management system and emergency response plans is recommended to ensure the stable operation of network systems. Through the implementation of the above measures, the security level of computer network engineering can be effectively improved, ensuring the normal operation of network systems and the security of information.

Keywords: Computer Network Engineering Security, Security Risks, Network Attacks.

1. Introduction

1.1. Research Background

Computer network engineering security is an indispensable area in today's societal development. With the widespread adoption of the internet and the acceleration of the information age, security issues in computer network engineering have become a pressing problem to be addressed [1]. Currently, computer network engineering faces numerous security risks and challenges, such as cyber attacks, malicious software, and data breaches, posing serious threats to the network security of individuals, businesses, and even nations.

Cyber attacks have become one of the major problems in computer network engineering security. Hackers infiltrate network systems through various means, steal personal privacy information, disrupt normal network operations, and even use the network for terrorist attacks. The forms of network attacks are diverse, including viruses, Trojans, DDoS attacks, etc., posing significant threats to network security. With the development of emerging technologies such as the Internet of Things, cloud computing, and big data, methods of network attacks have become more complex and covert, presenting even greater challenges to network security.

With the rapid development of information technology, network security threats are escalating, posing greater challenges to network engineering security. Issues such as data breaches, privacy leaks,

DOI: 10.54254/2755-2721/76/20240594

and online fraud are emerging one after another, severely affecting the information security of individuals and businesses. Especially in fields like finance, e-commerce, and government affairs, network security issues have even impacted the safety and stability of the entire society. Therefore, strengthening research on computer network engineering security and improving the level of network security have become crucial problems that need urgent resolution.

By conducting in-depth research on computer network engineering security issues, the level of network security protection can be effectively enhanced, safeguarding the information security of individuals and businesses. In response to current security issues, a series of measures can be taken, such as strengthening research on network security technology, raising awareness of network security, and establishing comprehensive network security management systems. Moreover, the government, businesses, and individuals need to pay more attention to network security and work together to build a safe, stable, and harmonious network environment.

With the rapid development of information technology, network security has become a global hot topic. The frequency and scale of network attacks are increasing, and the network security situation is severe. To effectively safeguard personal privacy and critical information, attention and investment in network security need to be strengthened in all fields. In this context, researching computer network engineering security issues is one of the key problems that urgently need to be addressed [2].

Currently, network security faces various threats from both external and internal sources. Hackers continuously carry out network attacks using vulnerabilities and technical means in an attempt to obtain others' confidential information and data. Improper operations by employees can also lead to data leakage and information breaches. Therefore, improving the level of network security is urgent.

To effectively counter network security threats, ongoing enhancement of technical research and innovation is required. Security measures such as encryption technology, firewalls, and intrusion detection systems need to be continuously upgraded and refined to adapt to the changing network environment. At the same time, strengthening education on network security awareness is crucial. Only by making every network user aware of the importance of network security can a societal atmosphere of collective maintenance of network security be formed.

Beyond technical means and awareness education, establishing a comprehensive network security management system is also a vital component. The government should increase investment in network security, enact stricter network security laws and policies to ensure a stable and secure network environment. Businesses and individuals should actively participate in network security efforts, do their part in information protection, and together create a harmonious and secure network space.

1.2. Research Purpose

This paper aims to explore the problems existing in computer network engineering security and propose corresponding countermeasure analyses [3]. With the rapid development of information technology, network security issues have become increasingly prominent, with various network attacks emerging one after another. In computer network engineering, security issues are of utmost importance, concerning the confidentiality, integrity, and availability of information. Therefore, it is crucial to conduct in-depth research on computer network engineering security issues and establish and improve security assurance mechanisms.

The problems existing in computer network engineering security mainly include the risk of network data leakage, the risk of network virus dissemination, and the risk of network intrusion. Network data leakage can lead to the theft of important information, causing irreparable losses; the spread of network viruses often paralyzes the entire network system, affecting the normal order of work; network intrusion is an act of directly invading network servers, posing a serious threat to network security.

In response to these problems, we propose several countermeasure analyses. Strengthen network security awareness education, enhance users' attention to network security, strengthen password management, and protect network-sensitive information. Establish a comprehensive network security technical system, employ technical means such as firewalls and intrusion detection systems, and timely

DOI: 10.54254/2755-2721/76/20240594

detect and prevent network attacks. Update network systems and software in a timely manner, repair system vulnerabilities, and improve network security performance.

Strengthen network security awareness education to fundamentally enhance the security awareness of the majority of network users and avoid risks to network systems due to personal negligence. At the same time, establish a comprehensive network security management system, clarify the responsibilities and duties of network security management, and ensure timely handling and tracking of network security incidents. Through regular network security checks and assessments, discover potential security hidden dangers and take effective measures to address them in a timely manner.

Strengthen the publicity and implementation of network security regulations and policies, forming a nationwide awareness of network security protection. Only with the active participation of the whole society in network security work and joint maintenance of network security can a secure and stable network environment be built, ensuring the safe transmission and communication of information.

It is hoped that the research analysis of this paper will attract more attention to the problems of computer network engineering security. With continuous effort and cooperation, it is expected to jointly promote the development and improvement of the network security field, thereby advancing the progress and perfection of network security affairs.

In the current context of the rapidly evolving information technology, computer network engineering security issues are increasingly highlighted. In response to network security performance degradation caused by system vulnerabilities, it is necessary to further strengthen the construction of network security awareness and technical systems. Continuously perfecting the network security mechanism, introducing advanced information security technologies and tools, timely detecting and repairing system vulnerabilities, and ensuring the secure operation of network systems.

2. Analysis of Computer Network Engineering Security Issues

2.1. Security Threat Analysis

2.1.1. Types of Network Attack

In the field of computer network engineering, there exist multiple security threats and types of attacks, among which the most common include Distributed Denial of Service (DDoS) attacks, malicious software, phishing, and data breaches. DDoS attacks inundate the target server with massive amounts of malicious traffic, causing the server to overload and become unable to provide normal services. Such attacks can not only crash the target server but also prevent legitimate users from accessing the website, posing a serious inconvenience to network operations.

Malicious software refers to harmful programs that attack computer systems through the implantation of viruses, trojans, or worms. Malicious software can lead to data breaches, system crashes, and theft of information, posing a severe threat to the information security of businesses and users. Phishing exploits fake websites and emails to trick users into entering their personal sensitive information, such as bank card numbers and passwords, thereby obtaining user information or committing theft.

These types of network attacks pose a severe harm to network security. Network attacks can lead to unstable network operations, decreased service quality, or even total network paralysis, causing immeasurable losses to users; they can result in the leakage of user privacy and loss of critical data, leading to severe financial losses and crises of trust for users; they can also weaken a company's competitiveness and market image, plunging businesses into economic difficulties.

To counter the threats posed by network attacks, we can take some measures to strengthen network security. Establishing a comprehensive network security protection system, including firewalls, intrusion detection systems, anti-virus software, etc., can enhance network security defenses; enhancing users' security awareness training to raise users' awareness of network security and prevent the casual disclosure of personal sensitive information; strengthening the application of data encryption technology to ensure the security of data transmission and storage and prevent data breaches.

DOI: 10.54254/2755-2721/76/20240594

In summary, the threat of network attacks to network security has become a reality. To better protect network security, we can also take some additional measures. For example, strengthening network monitoring and auditing to timely detect and respond to network anomalies; establishing a network security incident response mechanism to handle and respond to network security incidents; enhancing cooperation with relevant government departments to jointly maintain the security and stability of cyberspace. Actively participating in international cybersecurity cooperation to jointly address challenges such as transnational cybercrime and cyberterrorism, building a secure, harmonious international network environment. The ultimate goal is to establish a comprehensive, multi-level network security system to ensure the stable operation of networks and promote the healthy development of the information society.

The challenges to network security are multifaceted, requiring us to maintain a high level of vigilance and responsiveness. In today's increasingly severe network security situation, we should work together to continuously improve network security technologies and management methods, jointly guarding the "last mile" of network security, and contributing to the development of network security endeavors. Let us join hands to build a more secure, stable network space, injecting more positive energy into the global process of informatization.

2.2. Security Vulnerability Analysis

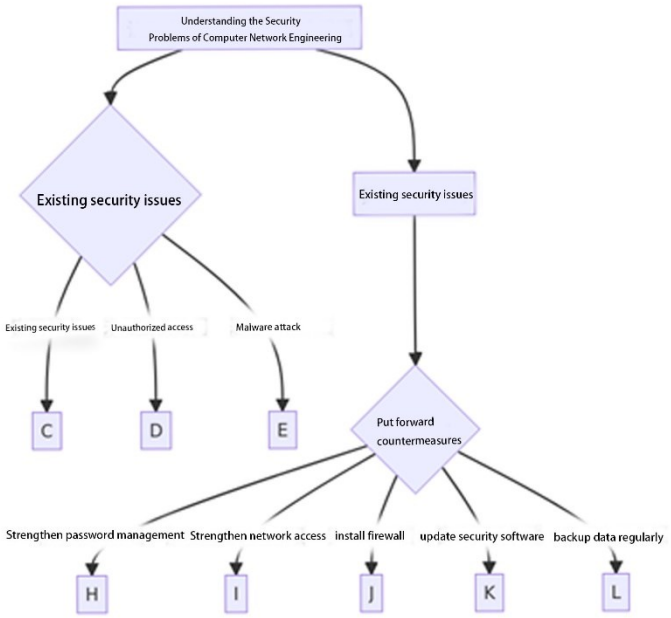

Figure 1. Analysis of Security Issues in Computer Network Engineering and Countermeasures

In computer network engineering, security has always been a topic of considerable attention. With the continuous development and popularization of network technology, network security issues have become increasingly prominent. This paper conducts an in-depth analysis of the security issues present in computer network engineering and proposes corresponding countermeasures [4].

It's crucial to recognize the security vulnerabilities that exist within computer network engineering. With the widespread application of the internet, network attack methods are emerging endlessly, with hackers exploiting various vulnerabilities for attacks and intrusions. Common security issues include weak passwords, unauthorized access, and attacks by malicious software. These security vulnerabilities pose serious threats to the security of network engineering.

DOI: 10.54254/2755-2721/76/20240594

In response to these security issues, we propose several countermeasures: strengthening password management by using complex passwords and changing them regularly can effectively prevent password cracking; enhancing the management of network access permissions and limiting users' access scope and permissions can reduce the risks brought by unauthorized access; installing firewalls, security update software, and regular data backups are important measures to ensure network security.

Many security issues exist in computer network engineering, which requires our utmost attention and effective countermeasures [5]. Only by continuously enhancing network security awareness, strengthening management, and applying technical measures can we better protect the security of computer network engineering, ensuring the normal operation of the network and the security of information.

3. Computer Network Engineering Security Countermeasures Discussion

3.1. Security Protection Technology

3.1.1. Firewall Technology

Table 1. Analysis of Security Issues in Computer Network Engineering and Countermeasures

Existing problems	countermeasures
Unauthorized access	Restrict external network access to internal network
Network Attacks	Monitor network traffic and respond in a timely manner
Insufficient Access Control	Setting Access Control Policies

The security of computer network engineering has always been a topic of great concern. With the continuous development of network technology, network security issues have become increasingly prominent. This paper mainly analyzes the existing problems and countermeasures of computer network engineering security, among which firewall technology is one important solution [6]. As a network security device, firewall technology is mainly used to control network traffic, monitor data packet transmission, and assist network administrators in protecting network security.

The role of firewall technology is mainly reflected in the following aspects: Firewalls can help network administrators limit external network access to the internal network, preventing unauthorized access and improving network security; they can monitor network traffic, detect network attacks and respond in a timely manner, effectively protecting network data security; they can also help network administrators set access control policies, restricting access for different users and applications to prevent unauthorized access.

It is worth noting that while firewall technology has its unique advantages in protecting network security, it also has some limitations. For example, firewalls cannot completely stop attacks within the internal network and need to be combined with other security measures to enhance the overall security of the network. As network technology continues to evolve, hacker techniques are also progressing, posing increasingly severe challenges to firewalls. Therefore, network administrators need to continuously update and perfect firewall technology to ensure network security.

Firewall technology, as an important network security device, plays a crucial role in the security of computer network engineering [7]. However, network security issues are a continuous challenge, and network administrators need to stay informed and respond to network security threats promptly, continuously improving network security levels to protect the network and data security.

3.2. Security Management Measures

3.2.1. Authentication and Access Control

In computer network engineering, security issues have always been a topic of great concern. Among them, authentication and access control are crucial components. Authentication verifies a user's identity

DOI: 10.54254/2755-2721/76/20240594

information, while access control determines whether a user has permission to enter a system or access resources.

In networks, the following formula is commonly used to represent the decision-making process of access control:

$$decision = f(identity, permission)$$

Here, $identity$ represents the user's identity information, and $permission$ represents the permissions requested by the user. Through a decision function f, the system can determine whether the user has sufficient permissions to carry out the corresponding operations.

In practice, the decision function f for access control can be implemented using various algorithms and techniques, such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC). By reasonably selecting and designing access control policies, the security of computer networks can be effectively protected, preventing unauthorized user intrusion and malicious operations.

4. Conclusion and Outlook

Computer network engineering security is an indispensable field in today's societal development. With the proliferation of the Internet and the acceleration of the informatization process, security issues in computer network engineering have become pressing challenges to address. Security risks and challenges such as network attacks, malicious codes, and data breaches pose serious threats to the network security of individuals, enterprises, and even nations. The current security issues primarily include network attacks, data leaks, malicious software, and phishing. To tackle these issues, we have proposed a series of countermeasures, such as strengthening research on network security technologies, enhancing network security awareness, and establishing comprehensive network security management systems. Only by continuously strengthening research and innovation to collectively respond to security threats can we ensure network security, information security, and societal stability. Through the research and analysis in this paper, it is hoped to draw more attention to computer network engineering security and promote the development and progress of the network security industry.

The importance of computer network engineering security is self-evident. Society has entered an era of informatization, and network security issues have become a focal point of concern. With the continuous advancement of technology, network attack methods are becoming more diverse and covert, posing serious threats to the network security of individuals, enterprises, and even nations.

In the process of responding to network security challenges, it is even more necessary to continuously strengthen research and innovation, and promote the ongoing development and progress of network security technologies. Only through the continual advancement and refinement of technology can we better ensure network security, information security, and societal stability. It is hoped that through the efforts of each of us, we can collectively address security threats, jointly maintain network security, and collectively promote the development and progress of the network security industry. The network security industry has a long way to go. Let's join hands and move forward towards a more secure and harmonious cyberspace.

References

[1] Dai, L.J., & Peng, T. (2022). Analysis of computer network security issues and research on protection strategies. Wireless Internet Technology, 19(22), 160-162.

[2] Wan, W.W. (2022). Research on computer network information security issues and solutions. Software, 43(08), 147-149.

[3] Zhao, X.B. (2022). Discussion on the influencing factors and prevention strategies of computer network security technology. Journal of Chifeng University (Natural Science Edition), 38(09), 44-47.

[4] Tang, Q. (2022). Analysis of computer network security and preventive measures. Wireless Internet Technology, 19(03), 27-29.

[5] Fu, S. (2022). On computer network security issues and their preventive measures. Software, 43(06), 124-126.

DOI: 10.54254/2755-2721/76/20240594

[6] Yang, N.N., & Jin, J.X. (2022). Computer network security issues and their countermeasures. Journal of Kaifeng Institute of Cultural Arts, 42(05), 114-116.
[7] Ge, G.W. (2022). Exploration of the influencing factors and prevention strategies of computer network security technology. Network Security Technology and Application, (06), 157-158.