Journal of Electronic Research and Application, 2024, Volume 8, Issue 5
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Cutting-Edge Challenges in Communication Technology and Computer Network Security

Haikang Gu*

Lanzhou Bowen College of Science and Technology, Lanzhou 730100, China

Corresponding author: Haikang Gu, guhaikang@163.com

Abstract: The rapid development of communication technology and computer networks has brought a lot of convenience to production and life, but it also increases the security problem. Information security has become one of the severe challenges faced by people in the digital age. Currently, the security problems facing the field of communication technology and computer networks in China mainly include the evolution of offensive technology, the risk of large-scale data transmission, the potential vulnerabilities introduced by emerging technology, and the dilemma of user identity verification. This paper analyzes the frontier challenges of communication technology and computer network security, and puts forward corresponding solutions, hoping to provide ideas for coping with the security challenges of communication technology and computer networks.

Keywords: Communication technology; Computer network; Security

Online publication: October 8, 2024

1. Introduction

Under the background of information technology, communication technology and computer networks continue to promote social development, which provides great convenience for production and life, but also brings information security problems. Today, faced with increasingly complex and diversified security threats, the topic of information security has attracted people's attention. To cope with the endless information security problems, people have developed generations of security technologies to provide support for ensuring the security of communication technology and computer networks. This paper analyzes the development trend and frontier challenges of communication technology and computer network security, and puts forward a series of concrete and feasible solutions, hoping to effectively enhance people's awareness of communication and network security, and provide some useful references for ensuring the sustainable development of digital society.

2. Security challenges of communication technology and computing network

2.1. Threats have evolved and become more complex

Security issues are becoming more complex, and cyber threats are constantly evolving, making dealing with

communications technology and cyber security a serious challenge in today's society. With the continuous development of attack techniques and modes, traditional network security models are also constantly changing to cope with new changes and challenges. At present, there are various types of malicious attacks, including viruses, Trojan horses, worms, and so on. This malicious software spread in the communication system and network system, which brings huge challenges to system security maintenance [1]. Driven by the Internet of Things (IoT) and cloud computing, new threats such as physical layer attacks and side-channel attacks have gradually emerged. In recent years, there have also been social software and phishing aimed at personal privacy. Various means of attack continue to emerge, making users have to deal with increasingly hidden and covert threats [2]. This trend of more diverse attack types has made the network security situation more complex, directly affecting the integrity, availability, and confidentiality of information systems, causing major network security accidents, and indirectly or directly causing property losses of enterprises and affecting social stability.

2.2. The risk of data transmission cannot be effectively controlled

Due to the development of information technology, people's communication is increasingly dependent on network information transmission. However, network attacks will also affect the security of network information transmission, resulting in information leakage and other security risks. With the development of cloud storage and edge computing technology, a large number of users and enterprises choose to store data in remote servers or the cloud, which increases the risk of data theft or tampering during data transmission [3]. Especially for transnational and cross-border data transmission, because different countries and regions have different data standards, data tampering has a greater impact on such data transmission. Data interception and eavesdropping have also become a big problem for data security. Interception and theft of data through network attacks or eavesdropping, obtaining commercial secrets and personal privacy, thus posing a serious threat to the security of enterprise and personal property [3]. For large-scale data transmission, once data leaks occur, the impact may be far greater than people expect. A breach of personal privacy can lead to problems such as identity theft and financial fraud. Corporate data leakage may lead to the disclosure of trade secrets, brand reputation damage, and other major consequences.

2.3. Potential vulnerabilities arising from the application of emerging technologies

The continuous application of new technologies has added new potential vulnerabilities to cyber security. Due to the lack of standardization and perfection of new technologies, they may be seized by malicious attackers. The wide application of emerging technologies such as the Internet of Things, artificial intelligence, and blockchain has not only brought a series of security loopholes to the communication and network system but also increased the complexity of the network system, making the network security work more difficult. The components within the system are interrelated, and the attack of one component may lead to the attack of the entire system, causing the entire system to be paralyzed [2]. Hackers and malicious elements carry out more secretive and destructive attacks on the potential vulnerabilities of attacking new technologies. For example, using artificial intelligence to conduct targeted cyber attacks to make them more precise and covert. With the continuous upgrading of attack systems, they may be upgraded automatically, which further increases the difficulty of communication and network systems to cope with security attacks [3]. Some new applications without adequate security verification may cause potential risks in the operation of the system from being discovered and repaired in time.

2.4. User identity verification

User identity authentication has become a major problem faced by the current communication and network systems. With more network users, information access is more intensive. People's requirements for information security are higher and user authentication has become an important means to protect network security. However,

the work of user authentication is facing more severe challenges. The traditional authentication method of user name and password is getting weaker in security performance, and users may suffer from phishing attacks or password leakage that can lead to identity theft. The emergence of biometrics provides a new way to solve this problem [4]. Biometrics improves the accuracy of identity verification, but it also brings another set of challenges. For example, biometrics can be imitated or used fraudulently, exposing user authentication to the risk of being attacked, fraudulently used, or abused. Multi-platform and multi-device user usage scenarios increase the complexity of authentication. How to implement cross-platform authentication of identity information is one of the urgent problems in communication and network security.

3. Communication technology and computing network security problem-solving strategy

3.1. Enhancing network defense and detection capabilities

Improving network defense and detection capabilities has always been an important means of dealing with network system security issues. Network defense requires a comprehensive application of various firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and other technical means to build a multi-level and multi-dimensional network security defense line. The types of network detection include real-time monitoring of network traffic, identification and detection of abnormal behaviors, and detection of threat intelligence [5].

At the defense level, the system uses deep packet detection technology to conduct in-depth analysis of network packets, identify potential threats, and block attacks. Additionally, through network access control, the system restricts access to key systems and information, prohibits unauthorized access, and blocks illegal access and attacks [6]. Encrypting communication data, encrypting data by some encryption method to prevent information from being stolen or tampered with during transmission [8].

At the detection level, the development of artificial intelligence is making detection more efficient. Access behavior is analyzed through a series of intelligent checks to rule out potential threats. The system intelligently identifies network traffic and user access behaviors, and determines them as normal or abnormal activities, thereby improving the accuracy of detection [7]. Moreover, a security information and event management system (SIEM) has been established to centrally monitor, analyze, and respond to network events and behaviors, find potential threats in time, and deal with them promptly. By updating security patches on time, planning the compliance configuration of network devices and systems, and conducting regular assessment and optimization of the network topology to adapt to the evolving cyber threat situation.

3.2. Ensure effective security management of identity verification

Authentication technology can effectively verify the identity of users and prevent unauthorized users from entering. Since most of the identity authentication in the network system is based on static passwords, this also has its own problems. Firstly, it is easy to crack. Users generally choose some common words as passwords, so it is easy to be cracked by deciphering tools. Secondly, password leakage. Due to the frequent turnover of personnel, password leakage may occur, or the same password is used repeatedly. Hackers may intercept the user's password through telephone, network, and other ways, so that it is easy to get the user's key information. Thirdly, after obtaining legal authority, internal personnel fail to use the authority according to relevant norms [9].

To prevent unauthorized or illegal access to communications and network systems by illegal personnel or outsiders, it is necessary for relevant departments to strictly review important content or the identity of users with higher authority. The dynamic password verification method can accurately identify the user's identity information. The dynamic password authentication system consists of an authentication server, a backup server,

and a management workstation. Among them, the authentication server is the core of the whole system. Through connecting with the server, it can comprehensively monitor the network access of Internet users, authenticate their identity information, and provide the permissions and resources matching their identity level. In general, the authentication server mainly includes encryption algorithm software, real-time computing, authentication management, and other aspects. This server has good data security, will encrypt and store all the data, and in the data exchange, will be transmitted through the form of encryption [10]. The management workstation is mainly responsible for the authentication server management interface supply work and will set the operation section between the authentication server and the network administrator, to facilitate the management personnel to carry out a series of work such as user management and system maintenance.

3.3. Strengthen data privacy protection

Data privacy protection is an important part of cyber security, and comprehensive encryption measures can effectively protect data privacy. Data privacy can be effectively protected by encryption during the whole life cycle of data transmission and storage. Advanced encryption algorithms, such as the Advanced Encryption Standard (AES) should be adopted to prevent cracking encryption problems.

In the data processing and storage links, the security of data information can be achieved through differentiated access control permission settings, and different levels of permission control can be adopted for different levels of data. Only by meeting specific conditions can access permission for data be obtained, which can avoid unauthorized information disclosure. Additionally, the security configuration of databases and storage devices is more widely used in practice. By regularly reviewing and updating access rights, data privacy protection can be enhanced to respond more effectively to potential internal and external threats, and data privacy protection can be implemented by introducing technologies such as data anonymization and desensitization. The anonymization of data can reduce the degree of data correlation, thus responding to attacks and information theft, and preventing private information from being leaked. Simultaneously, sensitive data is processed using desensitization to ensure the integrity and availability of data and reduce the sensitivity of data, to effectively protect users' privacy data. Establishing a sound data privacy policy and mechanism is the basic work of data privacy protection, standardizing the operation of the whole process of information collection and processing, clarifying the target and scope of a database application, and effectively protecting the right to know and choose network users [11]. Regularly carry out privacy risk assessment, and timely update privacy policies to improve systematic regulations and standards to improve data processing compliance and protect data privacy [12].

3.4. Applying emerging technologies to promote the upgrading of security protection

When applying new technologies, researchers should consider them from the perspective of safety. In the early stage, the application of new technology may bring about an accurate assessment of the risk, to lay the foundation for the subsequent data security protection work, and improve the security of new technology applications by adopting systematic security analysis methods, such as threat modeling and risk assessment. After the application of new technologies, the relevant staff should strictly follow the work norms and standards. The industry should speed up the construction of safety standards, the development, and application of new technologies to regulate, provide a set of systematic security architecture for the development of new technologies, and promote the continuous improvement of the security level of the entire industry [8].

Strengthening new technology monitoring and vulnerability mining can effectively ensure network security. Researchers can build a global vulnerability-sharing platform to integrate information about vulnerabilities in new technologies and push relevant vendors or research and development teams to provide fixes as soon as possible.

Concurrently, through the cooperation of the security team, the researchers carry out system attack and protection experiments, find out the security risks, and propose the corresponding security protection measures [14–15]. In the application of new technology, the publicity and training of users should be increased to enhance the security awareness and adaptability of users. Furthermore, through regular training courses and information release, users can be aware of the security problems faced by new technologies, and master the corresponding countermeasures to reduce potential security risks. This project aims to promote the cross-research of information security as a whole through the cross-integration of computer science, communication engineering, law, psychology, and other disciplines, and improve the overall grasp of emerging technologies.

4. Conclusion

In the face of the frontier challenges of communication technology and computer network security, it is necessary to take systematic countermeasures, pay attention to the development trend of communication and network system security issues, and innovate security protection paths to ensure the robustness of network communication and the security of user data. The goal of this paper is not only to put forward effective strategies to improve the level of security protection, but also to provide ideas for the development of communication technology and computer network security. Through continuous research and innovation, future research is expected to make greater achievements in the field of communication technology and computer network security, to ensure that information exchange and storage in the digital age can be carried out safely and reliably.

Disclosure statement

The author declares no conflict of interest.

References

[1] Yuan P, 2024, Analysis of Communication Technology in Big Data and Computer Network. Applications of Integrated Circuits, 41(04): 140–141.

[2] Zhao C, Hu Y, 2023, Research on Computer Remote Network Communication Technology Under the Background of Big Data. Information and Computer (Theoretical Edition), 35(15): 199–201.

[3] Qiao X, 2023, Network Security Protocol and Application of Computer Communication System in Cloud Computing Environment. Application of Automation, 64(14): 228–230 + 233.

[4] Liu N, 2022, Fault and Processing Analysis of Computer Network Communication Technology. Wireless Internet Technology, 19(24): 16–18.

[5] Li S, 2022, The Role of Network and Communication Technology in Computer Control. Software, 43(09): 94–96.

[6] Wu H, 2022, Problems and Solutions of Computer Network Communication Technology. Digital Technology and Application, 40(08): 99–101.

[7] Zhang B, 2022, On Practice of Network Remote Control in Computer Communication Technology. Contemporary Agricultural Machinery, 2022(04): 79–80.

[8] Liu W, 2022, Problems and Improvement Strategies in Computer Network Communication Under the New Situation. Network Security Technology and Application, 2022(03): 170–171.

[9] Dai Y, 2021, The Role and Countermeasures of Network Security Protocol in Computer Communication Technology. Yangtze River Information and Communication, 34(10): 122–124.

[10] Hou B, 2021, Application Research of Data Encryption Technology in Computer Network Communication Security.

Computer Programming Skills and Maintenance, 2021(09): 164–165.

[11] Ameti E, 2021, Data encryption in Computer Network Communication. Electronic Technology and Software Engineering, 2021(18): 254–255.

[12] Yuan S, 2021, Research on the Function and Method of Network Security Protocol in Computer Communication Technology. Yangtze River Information and Communication, 34(06): 119–121.

[13] Xu H, 2021, Analysis on Network Interconnection Technology of Computer Communication. Southern Agricultural Machinery, 52(07): 173–174.

[14] Guan D, 2021, Research on Fault Analysis and Treatment of Computer Network Communication Technology. Communication Power Technology, 38(01): 174–176.

[15] Zhao Q, 2021, Analysis on the Integration and Development of Mobile Communication Technology and Computer Communication Technology. Digital Communications World, 2021(01): 181–182.