Education Reform and Development, 2024, Volume 6, Issue 5
https://ojs.bbwpublisher.com/index.php/ERD
Online ISSN: 2652-5372
Print ISSN: 2652-5364

Analysis of Computer Network Courses Security Precautions Based on Big Data

Weibei Fan*, Dandan Mei, Fu Xiao

Nanjing University of Posts and Telecommunications, Nanjing 210000, China

Corresponding author: Weibei Fan, wbfan@njupt.edu.cn

Abstract: With the advent of the era of big data, computer networks have become one of the indispensable infrastructures in modern society. In this era of information exchange highly dependent on the network, the development and application of wireless network technology are becoming more and more important. However, the problem of network security is becoming more and more prominent, especially in the field of wireless networks. This paper aims to analyze the security precautions of computer wireless networks in the era of big data, discuss its classification, the necessity of application, and the security risks faced, and put forward the corresponding security technology application scheme, to provide reference and guidance for building a more secure and reliable wireless network environment.

Keywords: Big data; Computer; Network security prevention; Measures

Online publication: June 21, 2024

1. Necessity of classification and application of computer wireless network technology in the era of big data

In the era of big data, computer wireless network technology has become an indispensable infrastructure to support the operation of modern society. The necessity of its classification and application is not only related to the innovation and development of information technology but also directly affects national security, economic development, and all aspects of people's lives [1].

From the perspective of classification, computer wireless network technology mainly includes wireless local area network (WLAN), wireless metropolitan area network (WMAN), wireless wide area network (WWAN), and wireless personal local area network (WPAN). Each of these technologies has its characteristics and is suitable for different application scenarios. For example, wireless LAN mainly serves a certain range of fixed user groups, such as campus, and enterprise internal network connection, while wireless wide area networks achieve cross-regional wireless access through the mobile communication network, which has become an important pillar of mobile communication in modern society.

The reason why these technologies have such an important application necessity in the era of big data is mainly derived from the following considerations. First, the information exchange and processing in the

era of big data have extremely high requirements for speed and efficiency. The traditional wired network is limited by physical wiring, and it is difficult to meet the needs of rapid deployment and flexible adjustment. The emergence of wireless network technology has greatly improved the freedom and convenience of data transmission and provided strong technical support for the real-time processing of big data [2]. Second, the popularization and application of wireless network technology have greatly promoted the development of emerging business forms such as mobile offices, telemedicine, and online education. These new forms of business not only enrich people's lifestyles but also promote the transformation and upgrading of the social economy [3]. Third, from the perspective of national security, the development of wireless network technology is of great significance for maintaining national information security and ensuring the stable operation of critical information infrastructure. In the complex and changing international security environment, having an autonomous and controllable wireless network technology is an indispensable part of ensuring national information security [4].

2. Application of computer wireless network security technology in the era of big data

2.1. Change the wireless network settings

In the era of big data, wireless networks have become an indispensable part of people's life and work. However, with the popularity of wireless networks, their security problems are becoming increasingly prominent. Computer network security engineers know that wireless network security is critical to protecting user privacy and corporate data security. Therefore, the proper setting of a wireless network becomes the first line of defense to ensure network security [5].

The service set identifier (SSID) in wireless network settings is the foundation of network security. By default, the SSID of many wireless routers is set to the manufacturer's default name, which undoubtedly provides a convenient attack for hackers. Therefore, changing the SSID becomes a top priority for wireless network settings. They should set the SSID to a name that is not easy to guess, and avoid using content related to personal information to reduce the risk of malicious attacks [6]. On the other hand, the choice of wireless network encryption method is also key. WPA2-PSK (AES) is one of the most secure encryption methods. Compared to WPA and WPA-PSK (TKIP), WPA2-PSK provides higher encryption strength and can effectively prevent man-in-the-middle attacks and brute force cracking. When setting up the wireless network, they should choose the WPA2-PSK encryption method and set a complex and difficult-to-guess password to ensure the security of the wireless network.

In addition to SSID and encryption, MAC address filtering in wireless networks is also an effective means to improve security. By enabling MAC address filtering, they can limit the number of devices that can connect to the wireless network. In this way, even if the wireless network password is cracked, the attacker cannot connect to the network through the illegal device, thus greatly improving the security of the wireless network. In addition, in the era of big data, the security settings of wireless networks also need to take into account the encrypted transmission of data. Enabling WPA2-PSK encryption is just the first step, as they also need to ensure that wireless networks support emerging encryption technologies such as WPA3, which can provide better data protection and prevent data from being stolen or tampered with in transit [7].

2.2. Improve the encryption mechanism

Under the background of the big data era, the security problem of computer wireless networks has become more and more prominent. Because of its convenience and flexibility, the wireless network is widely used in

various scenarios, but it also faces many security risks. Among them, information leakage and illegal intrusion are the two major threats. Therefore, perfecting the encryption mechanism becomes the top priority to ensure the computer's wireless network security.

Encryption mechanism is the core technology to protect data security with self-evident importance. In the process of wireless network communication, data is transmitted in the air in the form of electromagnetic waves. If it is not encrypted, it is like plaintext transmission. Anyone with the appropriate equipment can intercept and interpret this information, resulting in sensitive data leakage. To improve the encryption mechanism is to ensure the confidentiality, integrity, and non-repudiation of data through technical means in every link of data transmission.

First of all, to improve the encryption mechanism, computer technicians should start with the selection of encryption algorithms. At present, the common encryption algorithms include the symmetric encryption algorithm and asymmetric encryption algorithm. Symmetric encryption algorithm encrypts and decrypts using the same key, encryption speed is fast, but key management is difficult. An asymmetric encryption algorithm uses a pair of keys, the public key is used for encryption, and the private key is used for decryption, so the security is higher, but the encryption speed is relatively slow. In practical applications, the encryption algorithm should be reasonably selected according to the real-time requirements and security requirements of data transmission [8]. Secondly, strengthening the key management is also the key to improving the encryption mechanism. The key is the core of the encryption algorithm, and its security is directly related to the security of the whole encryption system. Therefore, a strict key management system should be established, including the generation, storage, distribution, use, and destruction of the key. At the same time, key escrow, key segmentation, and other technical means should be adopted to prevent the key from being lost or illegally obtained. Finally, they need to pay attention to the application of data encryption technology. In wireless network communication, data encryption technology can effectively prevent data from being intercepted and tampered with. For example, the SSL/TLS protocol is used at the transport layer to encrypt and verify data on both sides of the communication to ensure data integrity and authenticity. At the application layer, technical means such as file encryption and database encryption are used to protect the sensitive data stored in the wireless network [9].

2.3. Hiding wireless routes

In the context of the era of big data, the popularity and application of wireless networks have brought great convenience to our lives, but at the same time, it is accompanied by network security risks. Among them, wireless routing is a key hub connecting wired networks and wireless devices, so its security is particularly important. As an effective network security measure, hidden wireless routing can improve the security of wireless networks to a large extent.

First, in the security settings of the wireless network, the wireless router broadcasts its SSID (Service Set Identifier) by default, which is the name of the wireless network. This broadcasting setting enables any wireless device that is nearby to search for and connect to the network. However, it also opens up opportunities for potential attackers, who can easily spot and attempt to crack nearby wireless networks by scanning them. Therefore, the restricted first step is to turn off the SSID broadcast function of the wireless router, making the wireless network invisible and reducing the possibility of being attacked [10]. Second, although the wireless network is no longer broadcast after hiding the SSID, it does not mean that it is completely secure. It is still possible for an attacker to discover the hidden wireless network by other means. Therefore, computer technicians need to take further steps to enhance security. This includes setting complex wireless network

passwords, enabling more advanced encryption methods such as WPA3, and changing passwords regularly. At the same time, it is also necessary to ensure that the firmware version of the wireless router is up to date to prevent potential vulnerabilities from being exploited by attackers [11–12]. Finally, in addition to the above measures, they can also consider physical means to enhance the security of the wireless network. For example, place the wireless router in a location where it can't be seen easily to avoid its exposure to public areas, use wired connections instead of wireless connections, especially when transferring sensitive data, and restrict access to wireless networks to only allow known and trusted devices to connect, among other things [13]. These measures together constitute a complete strategy to hide wireless routes, which can greatly improve the security of wireless networks. In short, by turning off SSID broadcasts, setting complex passwords and encryption methods, keeping firmware updated, and using physical means, they can effectively improve the security of wireless networks and protect users' data and privacy from illegal access and theft.

2.4. Set up non-repudiation mechanism

In the era of big data, the security of computer wireless networks is particularly important. Among them, the non-repudiation mechanism, as a key security technology, aims to ensure that the parties in the network communication cannot deny the operation or transaction they have participated in. This mechanism has a wide application prospect in the fields of e-commerce, e-government, and so on [14].

Suppose there is an online auction platform where buyers and sellers conduct transactions over a wireless network. In this scenario, the role of non-repudiation mechanisms comes into play. Both buyers and sellers need to ensure that their transactions are confirmed to prevent the other party from disputing them later.

First, computer technicians need to establish a trusted third-party authority, such as a certificate authority (CA). This authority is responsible for issuing digital certificates to buyers and sellers that contain their public keys and identity information. The public key is used to encrypt the information, ensuring that only the recipient who has the corresponding private key can decrypt it. Second, during the transaction, buyers and sellers use their private keys to sign the transaction information [15]. Signature is a digital signature technology that ensures the integrity of the message and the identity of the sender. Once the message is signed, it cannot be tampered with or the signature becomes invalid. Buyers and sellers send the signed transaction information to each other and keep a copy for their evidence. At the same time, the buyer and seller are also required to send the transaction information to the CA for filing. The CA will verify the validity of the transaction information and store it in a secure database after confirming that it is correct. This way, even if the communication between the buyer and seller is tampered with or deleted, the CA can still provide proof of the transaction record. Finally, after the transaction is completed, if either party denies its conduct in the transaction, the other party can present as evidence the copy of the signature it has kept and the record of the transaction provided by the CA. This evidence can effectively prove the authenticity of the transaction and the participation of all parties, thus ensuring the legality and fairness of the transaction.

By setting the non-repudiation mechanism, computer technicians can effectively solve the problem of trust in wireless network communication. This mechanism can not only protect the legitimate rights and interests of buyers and sellers but also improve the transparency and fairness of transactions. At the same time, with the continuous development of big data technology, it is undeniable that the mechanism will be applied and promoted in more fields, providing a more solid guarantee for the security and reliability of wireless network communication. In short, under the background of the big data era, setting the non-repudiation mechanism is one of the important measures to ensure the security of computer wireless network communication. Through reasonable mechanism setting and technology application, they can effectively solve the trust problem in

wireless network communication and provide strong support for the development of information technology in various fields.

3. Conclusion

The advent of the era of big data has brought unprecedented opportunities and challenges to the development of computer networks. In the field of wireless networks, it is especially necessary to pay attention to security prevention work, to deal with illegal user access, impersonation attacks, information tampering, and other security risks. By changing the wireless network settings, improving the encryption mechanism, hiding the wireless route, setting the non-repudiation mechanism, and other security technologies, the security and reliability of the wireless network can be effectively improved. It is hoped that the analysis and discussion of this paper can provide certain enlightenment for the research and practice in related fields, and promote the continuous improvement and innovation of computer wireless network security prevention in the era of big data.

Disclosure statement

The author declares no conflict of interest.

Reference

[1] Jiang C, 2023, Analysis of Computer Network Security Measures based on Big Data. Electronic Technology, 52(11): 112–113.

[2] Jin SG, 2023, Research on Computer Network Security and Preventive Measures based on Big Data. Materials for Information Recording, 24(11): 48–50.

[3] Lin BN, 2022, Analysis of Computer Network Security Precautions based on Big Data Technology. Electronic Components and Information Technology, 6(08): 228–232.

[4] Xu BJ, 2022, Research on Computer Network Security Precautions based on Big Data Era. Network Security Technology and Application, 2022(02): 68–69.

[5] Fan DZ, 2021, Discussion on Computer Network Security and Preventive Measures based on Big Data. Journal of Jilin Radio and Television University, 2021(05): 143–145.

[6] Sun LY, 2023, Analysis of Computer Network Security in the Era of Big Data. Digital Technology and Application, 41(07): 237–239.

[7] Zhou HY, 2023, Analysis of Computer Network Security and Countermeasures based on Big Data. Journal of Integrated Circuit Applications, 40(06): 360–362.

[8] Li YJ, 2023, Analysis of Computer Network Security and Countermeasures based on Big Data. Journal of Integrated Circuit Applications, 40(05): 164–165.

[9] Wu LG, Ma SL, 2023, Analysis of Information Security Measures in Big Data and Computer Network. Integrated Circuit Applications, 40(05): 274–276.

[10] Cai Q, 2023, Analysis of Approaches to Computer Network Security in the Era of Big Data. Modern Industrial Economy and Information Technology, 13(04): 69–71.

[11] Mo HG, 2019, Analysis of Computer Network Security and Preventive Measures in the Era of Big Data. Digital Technology and Application, 37(09): 196–198.

[12] Xue KP, 2019, Discussion on Computer Network Security Precautions in the Era of Big Data. Computer Products

and Distribution, 2019(04): 64.

[13] Yue C, 2018, Computer Network Security Precautions in the Context of Big Data. Communications World, 2018(06): 31–32.

[14] Li J, 2018, Computer Network Security Preventive Measures under the Background of Big Data. Legal Review, 2018(04): 240.

[15] Xiong HQ, 2015, Computer Network Security Measures under the Background of Big Data. Computer CD-ROM Software and Application, 18(02): 160–162.