Research on Network Security Issues in the Era of Big Data

Chunxiao Li

Xi'An International University, Institute of Technology, Xi 'An, 710077, China

Keywords: Big data, Cyber security issues

Abstract: Although the wide application of big data technology in various industries has achieved good application results, it also makes people highly dependent on various types of data and information. Once a network security accident causes important data and information to be lost or leaked, It will inevitably cause very serious consequences. Based on this, this article combines various network security incidents in recent years to summarize and analyze the network security issues in the era of big data. At the same time, it discusses various effective technical means to solve network security issues, hoping to be a new era. Effective control of network security risks helps.

1. Introduction

In the era of big data, both individual network users and various enterprises and units will inevitably face various network security problems. Once network security is neglected, property losses are prone to occur, or It brings a lot of trouble to daily life and work. To solve these network security problems and provide adequate guarantees for the security of various important data information, it is necessary to accurately grasp the characteristics of the big data era and conduct various network security prevention techniques. Flexible application.

2. Cybersecurity Issues in the Era of Big Data

2.1 Information Access Permissions Are Confusing

From the perspective of network resource management, the access rights of various information systems and network platforms are basically controlled by the administrator. Only after being granted access rights by the administrator, can outsiders gain access to the system and platform. The security of data information resources can basically be guaranteed. However, in the era of big data, due to the explosive growth trend of all kinds of data information, it is difficult for administrators to manage all access behaviors in detail. Therefore, the access authority management of many information systems and network platforms is gradually weakened. The definition of the access authority of the information source has also become more confusing, and the security of the internal data and information resources of the system and the platform has been directly affected. For example, after some companies have established information systems, they often adopt an extensive management mode due to the excessive workload of operation and maintenance management, directly distributing the authorization function of access rights to various subsystems and devices, relying on the authorization of the device and the operating system. Function to manage access rights, which not only provides opportunities for hackers to obtain authorization or illegal access, but also it is difficult to adapt to business management requirements.

2.2 Mobile Payment Security is Difficult to Guarantee

With the rapid popularity of smart phones, mobile payment has gradually become the most important payment method for people in recent years. Although this has brought a lot of convenience to people's daily life, many mobile phone applications need to obtain users in the era of big data. Mobile payment needs to be completed with the help of various mobile phone applications. Therefore, the security of mobile payment is also difficult to guarantee when the user's awareness of network security is insufficient [1]. For example, some small and medium-sized

  DOI: 10.25236/icited.2021.078

application software operators have insufficient network security protection capabilities. After completing user information collection, they will often be maliciously attacked by hackers and cause the leakage of important information such as registered user account passwords, contact information, and mobile payment passwords. Users may suffer economic losses as a result, or affect their normal life.

2.3 Industrial Control System Faces Security Threats

For a long period of time, although network security issues will have a serious impact, their scope of influence is limited to the Internet field. However, with the promotion of various advanced technologies such as computer technology, network communication technology, and big data technology in recent years Application, the scope of influence of network security problems has begun to show a trend of further expansion, and gradually penetrate into the industrial field, bringing a series of security threats to the industrial control system. Generally speaking, because the engineering station and operation station of the industrial control system are all established on the Windows platform, at the same time, to ensure the independence of the system operation, patches are rarely installed, so during the use process, the system will inevitably expose Various vulnerabilities, once these vulnerabilities are discovered and used by others, it is very likely that the industrial control system will be attacked by malicious networks, infected with network viruses, etc., which will directly affect the normal operation of the entire system. It even leads to a complete paralysis of the industrial control system. For example, the Stuxnet virus attack in Iran’s nuclear facility in 2010 was due to the fact that professional technicians discovered vulnerabilities in the Siemens industrial control system and the Windows system. Afterwards, they wrote virus programs for these vulnerabilities and inserted them through artificial U disks. The virus was implanted into the industrial control system, and ultimately paralyzed the industrial control system of Iran's nuclear facilities, which has a high level of security.

2.4 Smart Devices Have Security Vulnerabilities

Since smart devices have been widely used, various security risks derived from smart devices have also been exposed, and have become another emerging network security issue in the era of big data. From the perspective of the Internet of Things, many important smart devices usually need to be managed by special application software. Only when users log in to the application software and complete related operations can they control the smart device, but due to the different smart device control software Network security levels vary greatly. Therefore, once the application software that controls the smart device has high-risk vulnerabilities and is discovered and applied by others, then the control authority of the smart device will be obtained by other people, which will bring to the user of the smart device. The safety hazard is very large [2]. For example, in 2015, a hacker conducted a live demonstration of cracking the intelligent furniture control system. If this kind of intelligent device security vulnerabilities appear in the fields of pacemakers, driverless cars, and intelligent access control systems, people’s lives, The safety of property is obviously facing huge threats.

2.5 There Are Many Hidden Dangers in Mobile Terminal Security

The popularization and development of various mobile terminals has not only brought about various mobile payment security problems, but also many hidden security risks derived from mobile terminals have gradually emerged. For example, some criminals will use host computers and laptops to establish pseudo base stations, and then collect relevant information about surrounding mobile terminal devices, and then pretend to be operator base stations to send fraudulent information to these mobile terminal devices, so as to use the identity of the operator. Gain people's trust and complete various telecom fraud activities. Some hackers will use the characteristics of mobile terminal application software to call the server interface to install various software on the mobile terminal, and then complete the decompilation and modification when the software calls the server interface to achieve in-depth understanding of the business logic of the application software system. In this way, the hacker can directly retrieve various data from the server, and the hacker can

use this to complete the decompilation and modification of the data related to the server interface. The app is equivalent to installing a set of software on the user's mobile phone. This software cannot be self-contained One, the interface of the server must be called to obtain data, and other users who install the software will face the risk of privacy information leakage.

3. Effective Technical Means to Solve Network Security Problems in the Era of Big Data

3.1 Data Encryption Technology

Although network security issues in the era of big data are very diverse, in essence, most network security issues actually come from the leakage of important data and information, and data encryption technology is an effective measure to solve such network security issues. . Generally speaking, the application of data encryption technology is realized with the help of encryption functions and encryption keys. Before people want to transmit important data information, they can use encryption functions and encryption keys to perform data encryption processing. It can be converted into ciphertext with no logic and unrecognizable meaning. After the data information is transmitted, the data receiver who has the decryption key and decryption function will decrypt it, so that the ciphertext can be converted to the plaintext again. In this way, both parties can realize the normal transmission of data and information, and at the same time, the security of the data and information transmission can be fully guaranteed. Even if a criminal receives the data and information during the transmission process, they can only obtain unidentified and unidentified data. Meaningless ciphertexts will not cause data leakage problems [3].

3.2 Data Backup Technology

Because the value of data information in the era of big data is very high, even if a lot of important data information is not obtained by others, if it is lost due to hacker attacks, network viruses and other network security issues, it will also cause serious losses. Therefore, In order to effectively reduce the impact of network security issues, various data backup technologies can also be widely used. Data backup technology usually refers to copying the data in the hard disk of the application host and storing it in other storage media, so that after important data information is lost, the lost data information can be extracted again from the backup storage medium, and then the data can be restored. The rapid recovery of data information can be divided into several technical methods such as cloud backup, database backup, remote mirror backup, network data backup, etc., which can effectively avoid the hidden danger of important data information loss in practical applications [4]. Take the cloud backup technology as an example. Through the application of this data backup technology, after the cloud backup is established, the user can simply download the relevant backup software to the computer device or mobile terminal, and then use the software to realize the massive data information. Effective backup not only has a very large storage capacity, but at the same time, the security of data information transmission can also be fully guaranteed without the involvement of physical media.

3.3 Firewall Technology

As one of the most common network security protection technologies, firewall technology can also play a very good role in solving various network security problems. Generally speaking, since network users often need to transmit data with external networks when completing various activities with the help of computers and internal networks, in order to prohibit various illegal access behaviors, it is completely possible to set up a firewall between the computer, internal network and external network , And screen all access behaviors through custom standards. Once you find that the access behavior from a certain IP address is abnormal, you can directly prohibit the access of the IP address and filter out the packets sent from the host. When all dangerous access behaviors are restricted, whether it is a hacker attack or a network virus intrusion, it will be difficult to achieve, and the security of computers and internal networks will naturally be greatly improved.

3.4 Network Isolation Technology

For network security problems caused by network attacks, network isolation technology can also be used to effectively prevent data exchanges outside the trusted network while ensuring the internal information security of the trusted network. It can be seen that various network isolation techniques still have certain shortcomings, but their role in data information security is unquestionable. For example, when using dual-machine dual-network isolation technology, you can prepare two computers to establish a connection between the internal network and the external network. If you need to transfer data from the internal network to the external network, you can transfer the data stored in the internal network from Export from the computer, and then use the mobile storage device to transfer the data to the computer connected to the external network to complete the data interaction [5]. Although this data interaction method is not efficient in terms of efficiency, as long as the security of the mobile storage device can be ensured, the security of the data can also be guaranteed.

3.5 Obfuscation Technique

For some application software that uses Java language for programming, operators can completely reorganize and process Class files by obfuscating technology, and modify various strings or illegal characters in classes, variables, methods, packages, etc. in the program code. Add some irrelevant instruction codes, so that when the criminals decompile again, they will not only not be able to understand the operating logic of the software system from the code, but will also cause the decompiled software to crash due to the execution of the irrelevant instruction codes, and the application software users will be private. The security of information can also be guaranteed.

4. Conclusion

All in all, in the era of big data, network security issues have gradually spread to mobile payments, smart devices, industrial control systems and many other fields, and have greatly threatened people’s property and life safety. The reasons for network security problems, while the rational application of advanced technology such as network isolation technology, firewall technology, and data backup technology, these network security issues can still be effectively resolved.

References

[1] Xiao Huimin, Zhu Xiaomeng. Research on social network security issues and countermeasures based on big data. Information System Engineering, 2018, (2): 79-81.

[2] Wang Lei. Analysis of network security situation based on big data. Information and Communication, 2020, (10): 151-153.

[3] Yin Hang. Research on network security strategy for big data. Information Recording Materials, 2020, 21(6): 39-40.

[4] Wang Ronghan, Peng Tianhuan. Analyze the opportunities and challenges of big data-driven network security. Electronic Testing, 2020, (20): 126-127, 135.

[5] Yu Fang. Research on network security problems and countermeasures in the era of big data. Computer Knowledge and Technology, 2017, 13(17): 8-9, 11.