Exploration and Research on computer network security measures based on Internet of things technology

Li Bin

North Sichuan Medical College, Nanchong, Sichuan, China

Keywords: Internet of things technology; computer; Network security; measures

Abstract: With the rapid development of economy and the continuous innovation of network technology, Internet technology has been widely used in national politics, economy, life and other fields. Internet of things technology is a technical form emerging under the rapid development of Internet technology. With the help of modern technical means, the Internet of things system can be connected to the network system, so as to better realize resource information sharing. Therefore, the network security and control of the Internet of things have also attracted great attention. This paper discusses the network security problems and Countermeasures Based on Internet of things technology.

1. Introduction

Computer network technology has been applied to all aspects of enterprises and daily life. In the Internet of things environment, the normal operation of devices and equipment is inseparable from the support of computer network technology. With the continuous research on computer network technology, it has greatly facilitated people's work and life, such as equipment monitoring, smart home, logistics tracking and other applications, but its potential data value makes many criminals start to steal data information to make huge profits, which has brought huge security risks to people. Computer network security technology is the basis of ensuring the reputation of enterprises. If it is attacked by security, it may lead to the leakage and loss of a large number of customer information, resulting in serious consequences for enterprises. Therefore, in the process of using computer network, we should constantly strengthen the attention and research and development of computer network security technology, so as to improve the level of network security and build a safe network environment for people. The commonly used network security technologies include firewall technology, digital signature technology, anti-virus software and file encryption. Professional network security maintenance personnel use professional computers to carry out real-time and effective monitoring and protection of computer networks, that is, the essence of computer network security technology. With the continuous improvement of computer network security level, they carry out comprehensive security protection on hardware and software to prevent criminals from invading computer networks, To ensure the safety of user information and use data. The application and research and development of computer network security technology provide a strong technical guarantee for people's normal life and the safe operation of enterprises in the Internet of things environment.

There are many classifications of computer network technology. Generally, it can be divided into three types according to the network scope. From large to small, they are wide area network (wal), metropolitan area network (man) and local area network (LAN). LAN belongs to a small-scale network, such as schools and units. The use of LAN can not only meet the needs of users, but also reduce security risks, so it is widely used. The laying of LAN has relatively small coverage, so the laying cost is low, the time is short, and it is easy to establish. In order to establish the Internet of things environment, sensor network is indispensable. Through the intermediate role of sensor network, the dynamic monitoring and data acquisition of computer equipment connected to the network can be realized. Adding sensor technology to computer network technology can not only improve the efficiency of data collection, transmission and processing, but also improve the degree of network security. Computer network virus has great harm and fast transmission speed. If the computer network is unfortunately attacked by network virus, it is likely to cause huge information leakage and

DOI: 10.25236/ichamhe.2022.095

economic losses, resulting in irreversible impact. Therefore, it is very necessary to strengthen the security level of computer network in daily life. Computer network security technology is a powerful guarantee for the security of computer network environment.

Table 1 Classification of computer network technology

Computer network technology	category
	WAL
	MAN
	LAN

2. Security problems of Internet of things computer network

2.1 Internet of things communication security issues

The core of the Internet of things is Internet technology. Therefore, the Internet of things and the Internet are of great significance. While bringing convenience to people in the application process, there are also hidden dangers of information leakage of this person, enterprise and even the country. In many cases, the transmission of the Internet of things is actually wireless transmission. Because the signal is exposed in public during the transmission process, it is easy to be disturbed and stolen, resulting in information leakage. In modern public places, shopping malls, shops, transportation and so on are closely related to the Internet of things. Once the Internet of things is affected by unsafe factors, the consequences are very serious. Nowadays, the economic development of each field depends heavily on computer network technology. According to the different user groups, in order to maximize the use needs of users, the computer operating system presents a diversified development trend. Each industry has different applications of computer network technology, so professional technicians develop specific types of computer operating systems according to the use characteristics and needs of users. However, no matter what kind of computer operating system, even if it meets the use needs of users, there are security risks to a certain extent, which can not be completely eliminated, and the absolute privacy protection of user information and use data can not be fully realized. When users conduct web browsing, file viewing and data transmission on the Internet, they will leave some browsing traces and use data accordingly. Various industries and fields are striving for information transparency and openness, but there are great risks in realizing information openness on the computer network, which will make the user's personal information and relevant use data all open to the public, which may make some criminals use these data to mine all personal information and pose hidden dangers to the user's data security

2.2 Security and privacy issues

In essence, the Internet of things technology comprehensively processes and superimposes the data information through radio frequency identification technology, infrared induction technology and global positioning system, so as to promote the passive acceptance of the items used by people for scanning and tracking, and transform the private data information into a kind of public information. However, due to the lack of effective protection of information, the problem of information loss will occur when the whole system is used.

2.3 Prominent data transmission security issues

The perception layer of the Internet of things system has many ways to realize the transmission of data. However, in the real operation process, the ability of perception nodes is insufficient, which seriously affects the stable operation of the Internet of things system, improves the probability of data information damage, and increases the possibility of security risk of the system. On the other hand, the nodes in the perception layer also have other serious disadvantages, such as imperfect data processing capacity, which will lead to errors in data processing and affect the overall security of the Internet of things system. The realization of computer network security technology depends not only on the optimization and improvement of technology, but also on the strong backing of advanced hardware facilities. High performance computer hardware composition is the premise of giving full play to network security technology. The external factors affecting network security mainly come from the attacks of network hackers. Hackers generally scan the target user's computer system in an all-round way on the network through various technical means such as program data to find the loopholes in the user's computer operating system, which is what we often call bugs, or where security precautions are not in place. If they find loopholes in the computer system, Then hackers can use system vulnerabilities to maliciously attack and destroy the user's computer system, steal the user's information, tamper with passwords, etc., which will pose a great threat to the user's computer network security, and even import network viruses into the computer, and the computer system will be paralyzed or even crash directly. This external risk factor is everywhere, Serious events may cause huge economic losses to society and even the country. In addition, some natural environments will also have an adverse impact on the computer system. For example, when the computer is attacked by lightning, it will cause some damage to the computer hardware and computer system.

2.4 Improper operation of computer users

With the popularity of the Internet, there are a large number of computer users, including some children and the elderly who do not understand the knowledge of computer network. They may not pay attention to the importance of network security in the process of use, and even fail to use the computer correctly due to low education, resulting in potential safety hazards of the computer system. When browsing web pages on the Internet, there will be many pop-up advertisements and virus software. Delayed operation will lead to downloading some monitoring software to the computer system and divulging personal information. Or keep your account information and mobile phone number on the website, leaving potential security risks to the computer network. Even some criminals build false websites, publish false links, cheat users' bank card numbers, payment passwords and other information, or cheat them into direct transfer, and then immediately tamper with these information and illegally transfer users' money, resulting in users' failure to recover in time. Users with high security awareness usually encrypt important information, but if the security level of the password is not high, hackers will still decipher the user's password and steal the information of the computer system

3. Computer network security technology and prevention strategy

3.1 Create a safe computer network environment

Creating a safe computer network environment needs the support of the state. The government will formulate unified standards for the design and construction of server rooms, and issue relevant policies for people's supervision. The construction of the server room is a major project, and it is inevitable that there will be imperfect construction. Therefore, before the server room is officially put into use, it needs to be strictly tested in many aspects by many relevant national departments. Only the server room that meets the high standard can be allowed to be used. The operation of computer network needs strong power support. Therefore, power security is also a key concern in the use environment of computer network. The power supply department should always supervise the safe use of power. The government can also formulate power use norms and systems to increase the standardized supply and use of power. The daily maintenance and detection of computer equipment is also an important measure to maintain the computer network environment. The equipment lines, computer equipment and server room shall be regularly overhauled in terms of radiation prevention, fire prevention and lightning protection. Avoid unsafe computer network environment caused by disrepair or accidents.

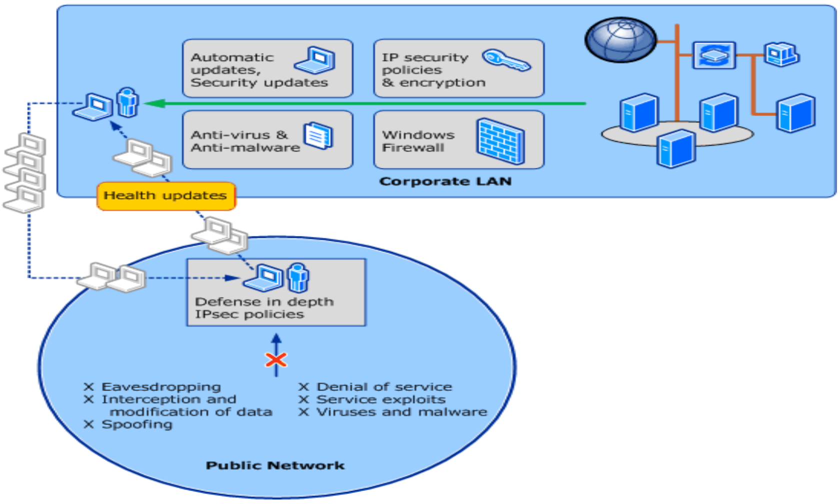
Automatic updates, Security updates
IP security policies & encryption
Anti-virus & Anti-malware
Windows Firewall
Corporate LAN
Health updates
Defense in depth IPsec policies
× Eavesdropping
× Interception and modification of data
× Spoofing
× Denial of service
× Service exploits
× Viruses and malware
Public Network

Figure 1 Computer network environment

3.2 Construction of computer network security defense line

The security of computer network environment largely depends on advanced network security technology. With the progress of science and technology, relevant computer security experts continue to develop virus scanning and isolation technology, data encryption technology, firewall technology and user access technology, The multi-party protection of these powerful technologies can build a solid network security defense line for computer network users and create a secure network environment. Virus scanning and isolation technology can detect malicious software, network viruses, illegal reading of information and other adverse factors in time, and remove and kill them. Data encryption technology can improve the security of users' important data, focusing on the protection of confidential files or private stored data. Firewall technology can establish a barrier between computer and global network, monitor and maintain the security of computer network environment at any time, and "shut out" some risky behaviors. The combined application of these network security technologies builds a security defense line for computer network. When users are using the computer network, the firewall technology will be turned on in the whole process to monitor the network environment in real time. At the same time, it can prevent almost most network viruses from entering, so as to ensure the security of data transmission and storage process of users' computers. If the computer encounters the malicious attack of hackers or the intrusion of hidden network viruses, the firewall system will give a warning in time to remind users that the computer network environment has been damaged. Then the virus scanning technology will quickly scan the intrusion of viruses and kill viruses in time to protect the data security of the computer. Therefore, one of the important research directions of computer network security is to build a stronger and more comprehensive defense line of computer network security.

3.3 Training on improving computer network security awareness

In today's Internet of things environment, the normal operation of enterprise equipment is inseparable from the support of computer network. At the same time, the security of computer network will also seriously affect the economic security of enterprises. The employees of the enterprise should strictly follow the rules and regulations of the local area network at any time, and the employees of the enterprise should also improve their awareness of the safety of the computer network at any time. Enterprises should strengthen the security training of computer staff to make them master advanced security technology and ensure the long-term security of computer network. The government can organize computer professional lecturers to give lectures on the correct use of computers and the protection of network security to social groups, improve the network security awareness of the whole people, help them use computer networks correctly, update formal computer anti-virus software, and ensure that computer fire walls and virus detection and killing software can detect and identify new computer viruses at any time, Establish an advanced computer network security protection system. Network security managers and computer network maintenance personnel should constantly improve their moral quality and professional skills, and strive to create a safe network environment for the whole people

4. Conclusion

The development of computer technology is inseparable from the security of the computer industry, and even the strong support of the information industry. The factors affecting computer network security technology, whether from inside or outside the system, cannot be completely eliminated. Therefore, social groups, enterprise network maintenance specialists and government departments should improve network security awareness, strengthen the research and development of network security technology, and jointly create a safe computer network environment, Make computer technology better promote the development of society.

References

[1] Meng Guiying, Li Nuosha, Gao Lu Research on the reform of classroom teaching mode of art design specialty based on new media technology [J] Daguan, 2021 (11): 109-110.

[2] Liang Jie Innovation and development of art design in new media environment [J] Grand View of art, 2021 (29): 50-51.

[3] Chen Yinan Integration of digital media and contemporary art [J] Grand View of art, 2021 (27): 137-138.