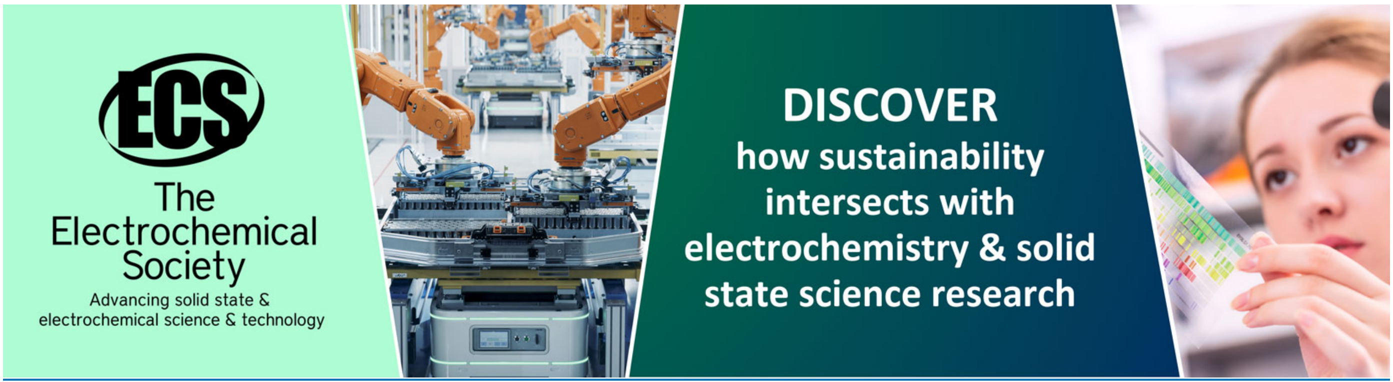
IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Research on Computer Network Security Vulnerabilities and Preventive Measures Based on Multi-Platform

To cite this article: Wenchao Xing 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **740** 012127

View the article online for updates and enhancements.



Research on Computer Network Security Vulnerabilities and Preventive Measures Based on Multi-Platform

Wenchao Xing

Jining University, Qufu, Shandong, 273100, China

Abstract. The protection of computer network security vulnerabilities has always been the focus of people's attention. It is necessary to analyze the causes of network security vulnerabilities in order to effectively protect and control them. In the operation of computer networks, there are some hidden risks, such as viruses, Trojan horses and hackers. For the information storage and transmission security has formed a huge threat, we need to do a good job in computer network security vulnerability analysis and prevention. Therefore, it is very important to strengthen the research of computer network security loopholes and preventive measures. This paper analyzes and discusses the types of computer network security vulnerabilities, the causes of computer network security vulnerabilities and the prevention measures of computer network security vulnerabilities based on multiple platforms.

1. Introduction

With the use of communication technology and computer technology in the network, the rapid development of network technology has been promoted. However, the problems faced by network security also have diversified phenomena. Network security vulnerabilities such as network virus invasion and hacker number theft affect people's use of the network, and also pose a serious threat to people's information security and affect information exchange among people [1]. Computer information and resources are also easily attacked by hackers, even with very serious consequences. Therefore, network and information security technologies are receiving more and more attention. As an important way for computer system to be attacked, it is not conducive to the preservation and confidentiality of user information, and people pay more and more attention to it [2]. In the construction of computer network, there are some security loopholes. Through the analysis of these security loopholes, we can find out the causes of the loopholes, and then take effective preventive measures to achieve the control of computer network security and ensure the normal operation of the network [3]. This paper takes the overview of multi-platform computer network security vulnerabilities as the starting point of this article, and expounds the important significance of developing computer network security work in detail.

2. Analysis on Types of Computer Network Security Vulnerabilities

2.1 System Vulnerabilities

System vulnerabilities are common problems in computer network security. Because computer network system itself has the characteristics of resource sharing and interaction, in order to effectively improve the communication and interaction between users, it is necessary to continuously expand the functions of computer system [4]. The computer system belongs to an interactive platform for unified users, which itself needs to support multiple functions to meet the personalized needs of users. The more functions, the more vulnerabilities will be, the greater the possibility of attack, the longer the operating system service time, the greater the probability of vulnerability exposure [5]. This requires network management personnel to install software patches in time and carefully avoid being attacked due to negligence. However, for some units, they do not know that the confidential information in the mobile media can be recovered even if it is deleted, so when the mobile media is lent or lost, the unit information will be exposed [6]. Based on the multi-functional system environment of the computer network, the hacker network will attack the newly developed functional vulnerabilities to obtain user information in a larger range. At the same time, the longer the operation cycle of the computer network, the easier the vulnerabilities will be developed, and the more likely the hacker is to attack the network [7]. When the link in the system receives the network file interaction, it will inevitably encounter the attack of file or hidden vulnerability in the system, such as protocol vulnerability, physical vulnerability, etc., resulting in data loss and system type vulnerability.

2.2 Protocol Loophole

The protocol vulnerability is mainly divided by the communication protocol of the computer network communication system. The computer network mainly communicates on the basis of the TCP / IP protocol. Due to the vulnerability caused by the TCP / IP defect, the security performance of the computer network is defective, which is divided into protocol vulnerability. Therefore, TCP / IP vulnerabilities are frequently attacked. For example, to meet the special requirements of TCP / IP protocol, such as communication and sharing, the corresponding ports need to be opened, and the speed of information exchange at the ports is very fast, resulting in security vulnerabilities, providing a way for hacker attacks [8]. In other words, the place where the IP address was generated cannot be confirmed in time. Hackers can also hijack the data by interception, infer the serial number from the data, and tamper with the routing address. Therefore, cracking passwords is also an important method for attackers to attack. Attackers can set the network interface to monitoring mode, and use network monitoring tools to intercept the information spreading in the network [9]. TCP/IP protocol is the information channel of computer network and an important factor to ensure network communication. Hackers enter the computer system through the port in the way of analysis and implement malicious tampering or control. China's ability to prevent protocol vulnerabilities is relatively weak. So it is easy to affect the safe use of the computer in the later period because of the lack of maintenance and handling of the security vulnerabilities caused by the long use of the computer operating system.

3. Cause Analysis of Computer Network Security Vulnerabilities

The most fundamental reason for security vulnerabilities is the imperfect computer, and there are many reasons for security vulnerabilities, but the main factors are generally concentrated in DOS and network intrusion [10]. If the user needs to modify the permissions, the resource program will be divided due to the permission resources must be allocated, which cannot guarantee that all resources can be effectively utilized by DOS. The divided resource department branch will be converted into invalid files, causing security vulnerabilities [11]. For example, hackers can use virus writing to enter the metropolitan network system without system authorization, start system files, obtain permission information, cause the system to lose service ability and protection function, and even cause system running confusion. Attackers can send a large number of forged requests to the target host, which may block system resources, making the system unable to continue to provide services for other normal requests, resulting in a denial of service attack effect.

In order to make users have a better use experience, software developers will carry out software testing of the process shown in **Figure 1** after the software is written. Its purpose is to reduce the deficiencies and defects of users in the process of using the software as much as possible so that users can have a better experience in the process of using the software.

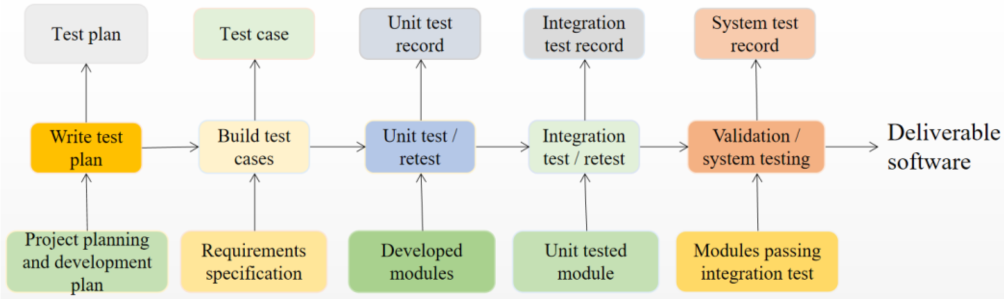


Figure 1 Computer Software Testing Process

DOS security management can not effectively manage all the resources of port communication. The divided resources will be converted into invalid files, which will be used by hackers and viruses, and then lead to network security vulnerabilities. If the computer network is invaded, serious security vulnerabilities will be formed, which will not only reduce the ability of the computer network to protect itself, but also cause system operation chaos. The protected data is in an unprotected state, increasing the risk probability.

4. The Importance of Computer Network Security

In the era of rapid development of information, people have to deal with a large amount of data and information every day. The traditional manual work mode can no longer meet the development needs of the times. However, the huge advantages of computers make them popular with people. Its advantages are mainly reflected in large capacity and fast speed. Computer network systems are more vulnerable to security vulnerabilities and are subject to varying degrees of risk threats [12]. There are various manifestations of network security vulnerabilities. China has made remarkable achievements in network construction, e-commerce has been widely used in thousands of households, and computer networks have also extended to national economy, culture, national defense and other fields. Due to the software design loopholes or the proliferation of malicious software (such as Trojan horse virus, worm virus, etc.), coupled with the limited recognition ability of computer operators and the lack of timely application software for upgrading and maintenance, some application software has loopholes and information security risks, which often become an important driver of network security and a tool for network attacks to be implemented. If the computer software is downloaded with a virus, it will bring great security risks to the use of the computer after the software is installed. Network security vulnerabilities can be said to be inevitable, and only timely repair can be found at any time. However, while the new version of the system corrects the vulnerabilities in the old version, it will also introduce some new vulnerabilities and errors. If the user network is attacked maliciously and no effective preventive measures are taken, it may cause economic losses and is not conducive to the construction of a harmonious social atmosphere. Therefore, to carry out computer network security prevention work is an important channel to meet the development needs of the times, to protect the interests of the people and to build a harmonious socialist society.

5. Research on Prevention Strategies of Computer Network Security Vulnerabilities

5.1 Firewall Technology

The main function of firewall technology is to isolate virus data in the network, thus protecting network security and improving network system security. With the help of routers, vulnerability protection can be used to filter access behavior, but it is impossible to reliably analyze hidden addresses and filter hidden addresses. Therefore, such technologies can only play a simple preventive role and cannot fully realize network protection. In the process of testing software using multiple platforms, the problem that needs to be paid attention to is the coordination among several platforms. Due to the differences in development companies of different testing platforms, human-computer interaction interfaces and usage habits, etc., there are certain differences. Platform selection should not be underestimated. Proper platform selection can greatly improve the accuracy and efficiency of software testing. Through the oil leak to filter the access behavior of network data, to isolate the illegal data, but the use of firewall can not filter the hidden address, some hidden attacks can not be effectively protected. Thus, it can complete the effective control of external access, record protection data, generate encrypted information, and provide convenience for management. The application of proxy technology requires a special server, and the protected object must be within the scope of server influence, so it is impossible to achieve a wide range of protection. Using the firewall to restrict user access, the firewall can identify security users, maintain login permissions, and use passwords or passwords. Restrict users from logging in, protect file data in computers, and prevent criminals from maliciously stealing related files.

5.2 Vulnerability Scanning Technology

The basic principle of vulnerability scanning technology is to simulate vulnerability attacks and cooperate with detection methods to analyze whether there is unreasonable information in the computer system under the premise of simulating vulnerability attacks so as to discover hidden vulnerabilities. Analyze whether there is unreasonable information in the computer system, and implement vulnerability detection by wrong registration method. For example, build a scan path at the host port, issue a request to scan for vulnerabilities, analyze the essence of security vulnerabilities according to information feedback from the computer host, and then simulate vulnerability attacks. In this way, the test effect can be improved to a certain extent. After the test is completed on one platform, the found vulnerabilities and errors should be repaired immediately. Then the test will continue on this platform until no software problems are detected, and then another platform will be selected for testing. At the same time of completing vulnerability scanning of local computer network system, it can also realize remote scanning. Considering that the server and port in the computer network system need to contact with the network environment frequently, which is easy to appear loopholes, we must focus on scanning. On the other hand, anti-virus software is necessary for computer security. Antivirus software can reduce the invasion of virus to the computer and the damage to the computer. In addition, the computer antivirus software should be updated and upgraded in time, so as to avoid the damage caused by computer virus to the computer to the greatest extent.

5.3 Virus Prevention Measures

Viruses have a very strong attack on security vulnerabilities. Computer viruses have the characteristics of dependency and variability. Once viruses appear in the computer network, they can quickly discover system vulnerabilities and enter the system to complete system interference and destruction with the aid of weak defense capability of security vulnerabilities. Therefore, in the network system, anti-virus software can be used to improve the security of the computer and the network system. To build a multi-layer protection system in the computer system: First of all, the corresponding antivirus software should be installed in the computer. Through software to complete the defense and killing of common viruses, regularly scan the computer network environment, and timely repair the existing security vulnerabilities; A large part of the current computer software needs to be connected to the Internet so that the software can run normally. Therefore, to test the performance of these functions. Different test platforms will have different test results. It can be seen that if a test platform is used to test the software, although some vulnerabilities and errors can be detected, the number of detected vulnerabilities and errors is limited. Because computer virus is a constantly changing process, and the ability of virus mutation is very strong, so we need to do a good job of upgrading the computer virus database to prevent the virus from invading into the computer. Finally, cut off the way of virus invasion, use software without virus risk, avoid malicious plug-ins entering the computer system, build a nest for virus, optimize the security environment of network use, and reflect the role of virus prevention.

5.4 Port Parsing Technology

Port mainly refers to the USB interface of computer network communication, generally the external information interface of computer system. In computer system, the security of USB interface is also protected, but in the process of work, there may be security holes. Install and configure a firewall for the system, update the virus library in time, close useless services and ports, delete unused software packages, and do not set default routes. Therefore, the computer should strengthen the protection of computer information in the actual use process, and minimize the loss of computer information by encrypting computer information. When the USB port is connected to the equipment, the system will analyze its communication port and feed back information to the user in time. Once a virus occurs, the system will give an alarm in time. Therefore, when selecting computer application software, the regularity of its source, the credibility of the software provider and the updating and maintenance measures of the application software should be fully considered so as to know fairly well the safety of the installed application software. Implanted into the computer network system. If Trojan virus disintegrates and reproduces in large quantities, it will cause system paralysis. Therefore, when using USB, we should strengthen the prevention awareness of security vulnerabilities.

5.5 Data Backup

A complete security system must have the ability to back up and restore data. Threats to data are usually more difficult to prevent. Once these threats become a reality, they will not only destroy the data, but also the systems accessing the data. A complete security system must have the ability to back up and restore data when working, which can effectively prevent the computer's data threats. Data backup is relatively boring compared with other network jobs. Lack of creative work. But it plays an important role in the network security. It can prevent the trouble before it happens and greatly reduce the loss of users. In practical work, it may not help users, but once the user's computer security problems, data backup can play a proactive role. To a certain extent, it reduces the loss of users and improves the security performance of data.

5.6 Intrusion Detection

Although network security preventive measures are in use, most network security preventive measures have the weakness of passive prevention, and the performance of active defense is poor. Some belong to the negligence of staff, which often leads to serious consequences. The application of intrusion detection technology can make it possible to detect intrusion attacks before invading data attacks the system. And use alarm and protection system to prevent intrusion attack. In the process of intrusion attack, it can reduce the loss caused by intrusion attack. Then use the alarm and protection system to remind the staff, in the process of intrusion detection, it can effectively reduce the property loss caused by the intrusion attack, enhance the performance of the system security protection, and help to enhance the stability of the network.

5.7 Enhance the Information Security Awareness of Computer Application Personnel

We should start from two aspects: strengthening the safe operation level of the personnel and preventing the malicious destruction of the computer system by the application personnel. First, we should strengthen the training of the computer application personnel and improve the encryption strength of the computer operation password to avoid the risk of weak password by encrypting the important data. On the one hand, the user login restriction is adopted, and the user needs to pass password authentication to enter the computer program when using the computer; on the other hand, the internal information of the computer should also be encrypted. In the process of using computer network, users encrypt the data transmission to improve the confidentiality of these data and ensure that the data can not be tampered and stolen in the process of transmission. It is imperative to actively carry out network security management. Through the formulation of complete network management methods and the exertion of legal effects, the network security management will be strengthened, the publicity of network security work will be intensified, the cognitive level of users on relevant knowledge will be improved, and the scientization, rationalization and legalization of online behavior will be ensured. Secondly, information network security problems caused by malicious destruction of computer systems by computer application personnel should be eliminated. Relevant personnel should be trained in ideology in due time to prevent security problems. For those personnel who seriously disrupt computer network security and cause losses to others or public information security, their legal responsibilities should be severely investigated.

6. Summary

The development of computer network technology has led to the extensive use of computer network, which has brought great convenience to our life and work. However, due to the security vulnerabilities in the computer network, people's lives and the development of enterprises are also affected to varying degrees. The computer network security vulnerabilities are mainly caused by the following aspects: the computer operating system itself security vulnerabilities, the current network protocol itself security vulnerabilities, computer application software caused security vulnerabilities, computer operators caused security vulnerabilities and computer network security due to malicious attacks. It is necessary to strengthen the security protection of network environment to ensure the security of computer network operation. In our country, we deeply analyze the causes of network security vulnerabilities and put forward scientific preventive measures. In the specific protection process, we need to comprehensively use the firewall technology, vulnerability scanning technology, intrusion detection technology, anti-virus software control technology and other network security protection. Scientific and reasonable development of network security protection measures can effectively improve the security of computer network system.

References

[1] Li Chenjie, Zhu Lina. Computer Network Security Vulnerabilities and Preventive Measures [J]. Information and Computer (Theoretical Edition), 2018, No.407(13):215-216+219.

[2] Jin Mingmorrow, Liang Xia, Ma Chunyan. On computer network security vulnerabilities and preventive measures [J]. Chinese strategic emerging industries, 2017(16):97.

[3] Liu Sihan. On the computer network security issues and preventive measures [J]. Science and Technology Vision, 2017(11):211-211.

[4] Huang Zhicheng. Research on Computer Network Security Vulnerabilities and Preventive Measures [J]. Science and Technology Information, 2018, v.16; No.503(02):8-9.

[5] Wang lihua. Computer Network Security Vulnerability Analysis and Preventive Measures [J]. Information System Engineering, 2018, No.293(05):66.

[6] Huang Feng. Brief Discussion on Computer Network Security Vulnerabilities and Preventive Measures [J]. Digital Technology and Application, 2017(3):218-219.

[7] Guo Haizhi, Guo Liang. Computer Network Security Problems and Preventive Measures [J]. Information Records, 2018, v.19(01):60-62.

[8] Li Zhuorong. Computer network information security problems and protection countermeasures [J]. Computer fans, 2019, 01(01):74.

[9] Wei Chuwen. Computer Network Security and Preventive Measures [J]. Science and Technology Communication, 2018, v.10; No.202(01):152-154.

[10] Shao kepu, Peng lei. computer network security precautions [J]. digital world, 2017(2):98-98.

[11] Sielis. Computer Network Security Issues and Preventive Measures [J]. Digital World, 2017(6):137-137.

[12] Zhou Feng, Feng Xiaoping. Computer Network Security Issues and Preventive Measures [J]. Science and Technology Wind, 2017(9):100-100.