Discussion on Importance of Communication Network Security and Technical Maintenance Measures

Saibei Han

Network Center, Changchun Normal University, Changchun, 130032, China

Keywords: Communication network; Security; Technical maintenance

Abstract. With the continuous development of information technology level, the communication technology is continuously improved and the scale of communication network is increasingly expanded, which proposes higher requirement for communication network security. Through analysis on the importance and current situation of communication network, this paper proposes corresponding technical maintenance measures for safe network for professional personnel's reference.

Introduction

With continuous progress of communication network technology and larger and large influence on people's life, the communication network becomes an essential part of people's communication and improves people's working efficiency. With the deep development of communication network, the security problem attracts higher and higher attention, and to adopt the technical maintenance measures to maintenance a safe development of communication network has become a hot issue.

Importance and current situation of communication network

Importance of communication network information security

With the continuous development of internet technology, the new generation of communication technology has been gradually applied in people's life, such as interconnection and interworking, and cross-regional cooperation of mobile 3G, 4G, WLAN, and WI MAX, which gradually forms an open and flexible generalized network platform; however, while the network technology is widely applied and changes people's life, the communication network security problem is increasingly prominent. The communication network security refers to the security problems caused by accident factor, deliberate action, virus intrusion, overload of application service, and loopholes of operating system, etc.[1] As a kind of main tool for information delivery, the communication network is applied in various aspects of people's life, thus it is not only related to personal information security, but also related to China's business information security, and even related to national security. Once the communication network security issue happens, the data information will be disclosed, which will cause serious damage on country, threaten national security, and bring imponderable economic loss to the society.

Current situation of communication network security

Due to the unique openness, interactivity, and dispersibility of communication network, it is widely applied in various industries and involves various aspects of people's life while it makes people realize information sharing and information exchange. However, those features also cause the situation that partial security threat can't be avoided well; the computer virus, and hacker intrusion cause the threat on communication network security; most of commercial software have open source codes and source program, which causes frequent occurrence of software security problem; the enterprises also use communication network as the media of information delivery and lack of certain safe maintenance technology, thus the information can be easily stolen. Through analysis on current situation of communication network, the main hidden dangers existing in communication network security include: hidden danger in communication network operation software facilities, safety loophole in the process of communication network information and data delivery, and the hidden

danger with respect to communication network supervision mechanism and management mechanism. ① Hidden danger in communication network operation software facilities: in the application process of communication network, there exists certain loophole in using software facilities to carry out operation, control, and management on communication equipments, which will bring opportunity for hacker intrusion. Besides, the operation management personnel's improper operation may also cause disclosure of information and data. ② Safety loophole in the process of communication network information and data delivery: Due to network virtualization, the virtual storage is also applied for information, data, and application storage; in the process of information delivery, certain electromagnetic radiation will happen, but the comprehensive shielding is not adopted for the radiation in special transmission channels, which increases the possibility of hacker intrusion. ③ Hidden danger with respect to communication network supervision mechanism and management mechanism: due to imperfect communication network supervision mechanism and management mechanism in China at present as well as insufficient supervision made by relevant departments and personnel on communication network, there is no uniform supervision and control standard on communication network information and data application, which brings great safety loophole on communication network.

Technical maintenance measures for communication network security

Introduction of advanced communication network equipments

In order to improve communication network security, we shall firstly start from hardware equipments, greatly introduce advanced communication network equipments, and replace and apply advanced communication network software facilities; the high-quality communication network equipments and facilities have high network security technology index, thus it is hard to change and destroy them. Then, we shall greatly introduce advanced communication network security technology, such as firewall security protection technology, hacker intrusion prevention technology, technology related to communication network security encryption and maintenance, user and management personnel authority authentication technology, VPN technology, and automatic detection on loopholes and virus technology. [2]

Anti-hacker measure

In the process of communication network information and data delivery, we will often meet the hacker intrusion, and the attacking means used by hackers include diverting attention from the quarter where the real attack is to be made, "true and false Li Kui", going straight to the heart of the matter, and beating around the bush, etc.[3] In order to realize supervision, anti-counterfeiting, review, and tracking on illegal intrusion, and avoid the situation that the information is tampered, replaced or destroyed, it is able to adopt password entry, identity authentication and other methods. While the password entry is adopted, the password shall be set as complicated and long as possible; it is able to combine English letters with figures to reduce hacker's decoding possibility and avoid hacker intrusion. Besides, the users shall reduce the use of same password in multiple systems, and use diversified passwords as much as possible to avoid the situation that the security of other systems is affected due to occurrence of security problem in individual system. The identity authentication is used to realize dual authentication on user and access network; while the identity authentication is used, it is required to issue the letter of access permission to the terminal through network authorization to avoid secondary users' access to network and network resource, which can play certain protection function on network.

Anti-virus measure

The computer virus also can cause threat on communication network security at any time; the virus can damage and even destroy computer data, and tamper or disclose computer information data through viral transmission.[4] By use of ways of network connection, it is able to spread the virus on one computer to another computer. While the data file can't be opened or is damaged, the computer is halted or restarted for no reason, the operation speed suddenly slows down, the usable space of disk suddenly decreases, and the abnormality appears in network service, it is very likely that the virus is

hidden. In order to avoid the occurrence of above situations in computer, the users shall carry out regular virus detection on computer, insert the hard disk or download software after safe scanning to reduce the possibility of occurrence of virus. Meanwhile, while downloading the required software, the software shall be downloaded from official and professional website; as for the links on QQ, e-mails and annexes, it is required to not easily click and open them to avoid the situation that the virus extracts the list of e-mails through infected network, and then transmits to other users via e-mails attached with virus, which then causes communication network paralysis.

Application of communication network security technology

Firewall technology. The firewall technology is an important link in communication network security, and it is generally applied in external interface of network for convenience of carrying out access control to network layer. Through verifying, limiting, and changing the data flow which spans across firewall, it is not only able to prevent hacker's access to our network to maximum degree, but also able to prevent network hackers from arbitrarily tampering, changing, deleting and destroying network important information and data. In this way, the firewall can play a role of protective layer for network security and effectively prevent the intrusion of unsafe factors on the internet and extension to LAN.[4] Generally speaking, the firewall software installed in computer includes Rising, and Kingsoft, etc., which can carry out real-time supervision and virus checking and killing on computer.

Intrusion detection technology. The firewall technology can protect the internal network to certain degree so that it is hard for external network to intrude into internal network; however, it can't supervise the internal network, can't effectively control illegal activities of internal network, and can't handle virus or malicious codes such as Trojan Horse, thus we need a technology which can make up firewall. The intrusion detection technology is short for IDS; through its combination with firewall technology, it is able to provide strong protection for external and internal attack, and even provide protection for security problem caused by improper operation. IDS will carry out effective interception on intrusion before the network system is damaged so as to further improve information security.

Network encryption technology. The network encryption technology is a kind of technology applied to prevent hackers from utilizing network to intercept and steal public or private information. Through encryption and sealing handling on IP package transmitted in public network, this technology can realize more complete data transmission and make the transmission become more confidential. The application of network encryption technology not only can ensure the security of data transmission under public network, but also can ensure remote users' security while they make an access to internal network.

Authentication technology. The authentication technology includes static password authentication, IC card authentication, short-message password authentication, dynamic password authentication, USBKEY authentication, digital signature authentication, and biological recognition authentication, etc. This technology can be applied in various kinds of authentication mechanism, and it can effectively guarantee information integrity, ensure confidentiality of information data, improve information security, and protect the information from being stolen.

VPN technology. VPN technology refers to making use of public network such as internet to establish a safe temporary network connection through which the remote users, corporate branches, and corporate business personnel are connected with corporate internet network to form a corporate expansion network on the basis of original network. Due to the fact that this network is virtual, the network host will be not aware of the existence of other public network except for this network, thus this network will be not easily affected by external public network, which ensures network security.

Vulnerability scanning technology. The network is under continuous change and it has certain complexity, and thus it is insufficient to merely depend on network administrators' technology and experience to look for the vulnerabilities in communication network technology; through full use of network security scanning tool, it is able to eliminate hidden danger to maximum degree. The network security scanning tool can carry out optimal configuration on system, timely compensate the security holes in the system, and reduce the occurrence of potential danger; meanwhile, it can also

make use of various kinds of hacker tools to carry out network simulated attack on security degree of communication network so as to make the network vulnerabilities exposed in the process of simulating hacker attack and reduce the occurrence of potential danger in use process.

Perfection of communication network safety management mechanism

The communication network safety is not only related to personal information security, but also related to China's business information security, and even related to national security.[5-6] Once the communication network security issue happens, the data information will be disclosed, which will cause serious damage on country, threaten national security, and bring imponderable economic loss to the society. Therefore, the relevant departments shall pay enough attention to the communication network security problem, continuously perfect communication network security management mechanism, combine with actual application situation to improve communication network management mechanism, continuously improve communication network supervision mechanism and management mechanism, formulate uniform supervision standard for information data and application of communication network, and formulate scientific network restraint mechanism and uniform behavior norms to enhance communication network safety management mechanism. Meanwhile, the relevant department shall greatly propagandize the importance of communication network security to make people be aware of the important significance for individuals and country, improve people's awareness of security protection, and reduce occurrence of communication network security problem.

Enhancing of system security

The communication network users shall strive to enhance the security of network system. In the process of computer use, the users shall timely remove the unnecessary files or picture resource, and set the files or pictures which can't be deleted as forbidden form to prevent the occurrence of network security problem.[7] Meanwhile, in the communication network equipments, the users shall configure default user name and password access, limit the access of anonymous account, carry out regular scanning on network system, often carry out checking and scanning on internal storage, boot sector of disk, system resource, and file data, timely handle abnormal problems which have been found, not easily click and open the links on QQ, e-mails, and annexes to avoid the situation that the virus extracts the list of e-mails through infected network, and then transmits to other users via e-mails attached with virus, which then causes communication network paralysis. The users shall enhance their knowledge of communication network security and reduce the safety danger of communication network to maximum degree.

Enhancing of self-protection awareness of communication network

The communication network users shall make an access to safe sites such as 360 Safe, Rising, and Kingsoft on an irregular basis, and operate the recent security data to effectively avoid virus intrusion, as well as timely pay attention to safe hotspots of communication network and relevant communication network information, not arbitrarily open the unknown e-mails and website links, set password with high degree of security to prevent hacker intrusion, and also establish high self-protection awareness to enhance communication network security.

Conclusion

In conclusion, as the main passer of information and data, the communication network has been widely applied in various fields; it has brought great convenience for people's life and also has become one of quick and effective ways of communication. Through continuously introducing advanced network equipments and facilities and advanced science and technology, enhancing the use of network security technology, perfecting communication network security mechanism, enhancing the self-protection awareness of communication network, it is able to effectively improve the communication network security problem.

Acknowledgments

This paper is a phased research result of key project of Jilin Provincial Department of Education "Twelfth Five-year" science and technology research, and the project name is Research on Reusable RJ45 Connector (J.J.K.H.Z.[2013]No.245).

References

[1] Wang Xiaoduan, Gao Kun. Internet Information Security Knowledge and Prevention Measures, *Technology Trend*, 2014 (24): 163-165.

[2] Zeng Yan. Computer Network Information Security and Protection Measures, *Theory Herald*, 2013 (16): 132-133.

[3] Liu Jian. Network Information Security Problem and Guarantee Measures, *Computer Programming Technology & Maintenance*, 2013 (03): 167-168.

[4] Xu Yeling. Discussion on How to Enhance Network Information Security Protection, *China's New Technology and New Product*, 2012 (22): 103-105.

[5] Wang Nan. An Algorithm Realizing Transformation of Web Data to XML Document, *Journal of Dalian Maritime University (Natural Science Edition)*, 2010, 36 (3): 76-78.

[6] Dong Xuewen, Ma Jianfeng, et al.. Ad Hoc Security Routing Protocol Attack Analysis Model Based on Strand Space, *Journal of Software*, 2011, 22 (7): 1641-1651.

[7] Fan Zhenghe, Wang Li, Li Yan. Risk Management of Information Security, *Information Technology & Informatization*, 2011 (06): 119-120.