

Analysis and Protection of Computer Network Security Issues

Ju Jinquan*, Mohammed Abdulhakim Al-Absi*, Ahmed Abdulhakim Al-Absi**, Hoon Jae Lee***

*Department of Computer Engineering, Dongseo University, 47 Jurye-ro, Sasang-gu, Busan 47011, Republic of Korea

**Department of Smart Computing, Kyungdong University 46 4-gil, Bongpo, Gosung, Gangwon-do, 24764,
Republic of Korea

***Division of Information and Communication Engineering, Dongseo University, 47 Jurye-ro, Sasang-gu, Busan 47011,
Republic of Korea

Jujinquan351939917@gmail.com, mohammed.a.absi@gmail.com, absiahmed@kduniv.ac.kr, hjlee@dongseo.ac.kr

Abstract— with the rapid development of information technology, the influence of network on human way of life is greatly enhanced, and network technology is rapidly popularized in all fields of society, which makes the security of computer network become an urgent problem to be solved. How to ensure the rapid and healthy development of the network has become the focus of attention of scholars, and has a very prominent realistic background and extremely important theoretical significance. In this paper, the research background of computer network security, the significance of this paper, the related research status at home and abroad and the research methods used in this paper are summarized. Then the theory of network security technology is advanced. This paper summarizes the connotation of network security, the research content of network security, the framework of network security information and the dynamic model of network security. In the third part, the problems of computer network security are analyzed, and the network security problems are studied from four aspects: network hardware, network software, network managers and network users, and the possible network security problems and their causes are analyzed. In the fourth part, the network security protection measures are put forward, and the security measures of hardware system, system security loophole, application software and manager are put forward respectively.

Keywords—computer; network security, protective measures, Security, Computer Network

I. INTRODUCTION

The requirements of the International Organization for Standardization (ISO) for computer system security are: to protect the technology established and adopted by data processing systems and the security of management, to protect computer hardware, software and data from being damaged, altered and accidentally and maliciously. Give way. At present, a standard definition has not yet been formed for network security. Integrating various viewpoints, network security should refer to the use of various network management, control, and technical measures to protect the data resources of the network system hardware, software, and its systems. These resources are not destroyed, altered, or leaked due to some unfavorable factors, ensuring that the network system operates continuously, reliably, and safely[1,2]. Network security is a

comprehensive discipline involving computer technology, network technology, communication technology, cryptography, information security technology, applied mathematics, number theory, and information theory.

II. ANALYSIS OF COMPUTER NETWORK SECURITY ISSUES

- Security issues in network hardware

There are design flaws in the development process. The design principle of the network system is mainly based on the fact that once the central system fails and cannot operate normally, the rest can still continue to work without being affected, thus ensuring accurate transmission of various information. Under such general principles, network systems tend to be more practical and ignore security. The Internet was originally an environment developed by computer researchers [3]. It is not a means of information transmission for profit. Generally speaking, the Internet has not included factors such as network security into consideration. The premise of the establishment of the network protocol is to assume an absolutely trusted environment [4]. The security of the mode of this connection has serious flaws and cannot be sustained. This will inevitably be subject to various cyber terror from outside, such as scanning attacks, intercepting attacks, spoofing attacks, and denial of service. Both network communication systems and application system protocols have different design flaws, which are used to attack network systems.

Hardware in the network system often has different levels of security design vulnerabilities. For example, the reliability of network applications is poor, and many key parts of network technology have security risks. The setting of system parameters needs further verification. Whether the application of products such as firewalls can meet expectations. The effect, whether the operation itself is complete, whether the parameters are vulnerable or not. In the Windows desktop, Unix operating system, NT operating system and network software, there are different degrees of defects and deficiencies in the application itself. Currently, the widely used operating system itself cannot fully guarantee the safe operation of the network. If the setting of the firewall cannot meet the standard, then this setting will not only play a role, but also cause other harm to the network. When the firewall is connected with the

network, it is likely to become a breakthrough point of attack [5].

- Security issues in network software

Network intrusion: Network intrusion can gain access, write and storage permissions for using computer network systems; it can also pave the way for access to other systems or deeper systems; destructive attacks on computer network systems, making them lose all services And the ability to execute.

Backdoors and Trojans: After the rise of the Internet, computer network hackers developed a "backdoor" technology that allowed them to break into other network systems again and again. Trojan technology is a special backdoor technology [6]. The program mainly uses remote control and other means to conduct a covert attack on the Internet. Therefore, it has become a network intrusion tool that hackers often use.

Computer viruses and worms: In the process of writing a computer program, a network processing method that can damage the computer function and destroy the corresponding program is implanted into a computer virus. Computer viruses not only make the computer unusable, but also automatically copy code and programs related to the computer network. The worm is a new type of computer virus, which is mainly used to find the vulnerability of the operating system or program for spontaneous attacks while the computer is running, and can use the network to spread the malicious virus quickly and widely.

Denial of service attacks: Attacks on DOS systems are simple and easy, but at the same time the offensive effect is very significant, there is almost no effective way to deal with this attack. A denial of service attack destroys the normal operation of the system by denying the access request of the service, thereby destroying the link between the Internet and the local area network system, thereby causing the system to lose its service function.

Attack on encryption method: This attack method is mainly for all kinds of files with passwords. The cracker can choose to attack the known cipher text, attack the known plaintext, and selectively attack the cipher text. And a variety of attacks, such as selectively attacking plaintext.

Port scanning: This method mainly uses a method that can actively obtain core network information [7]. Using the port scanning method to scan the network information, not only can the number of ports be inferred in the main system, but also the serial number corresponding to each port can be calculated, and the running mode and operation method of the main system can be inferred. The other scan results are matched to finally get the composition of the entire Internet.

- Network administrators have security issues

Most networks nowadays pay more attention to the overall scale of the network and often ignore security construction. Many network managers mainly focus on the construction of the capacity and scale of the network. The network security awareness is not enough, and no network security defense system is established. Lack of technical personnel related to network security management [8]. At present, most network managers in China have insufficient network security knowledge and security management experience, which is difficult to cope with the increasingly complex and versatile

network security situation. A small number of network administrators pay insufficient attention to network security, and do not want to spend time studying network prevention technology, and lack of security management methods.

- Security issues with network users

Most network users now have a weak awareness of cyber security. Except for some computer professionals who have some knowledge of cyber security, most people lack sufficient network security capabilities [9]. They generally believe that network maintenance is a matter for relevant managers. It has nothing to do with it, which creates a network security risk.

Whether it is a network of enterprises or colleges, IP technology is generally used as the main application method to reorganize the framework of the system. This system itself is in danger of being attacked. The security strategy adopted by the network management technicians also has the disadvantages of single defense, poor initiative, lack of early warning mechanism and lack of flexibility. It is impossible to fundamentally manage the network facilities, and it is not able to cope with the rapid development of network technologies. The complex network environment is adapted.

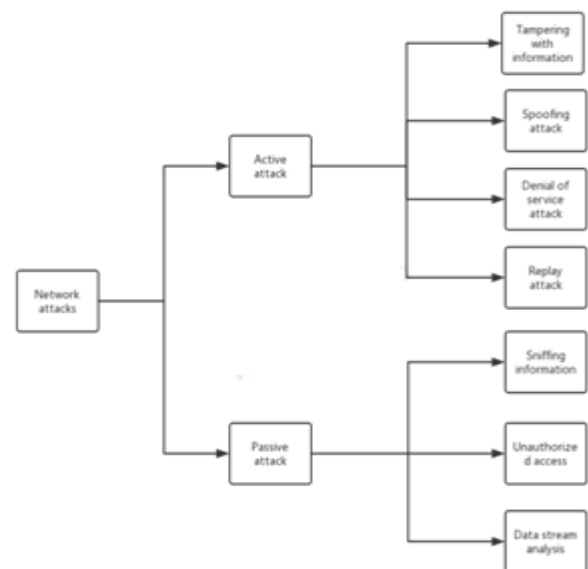


Fig. 1 Principle of network attack

III. RESEARCH ON COMPUTER NETWORK SECURITY PROTECTION MEASURES

In this paper, the network security protection of colleges and universities is taken as an example to study the preventive measures of campus network security. The operation level of the university campus network is directly related to the quality of school teaching management, which is the top priority of the school development. As the core network management center of the campus network, whether it can operate safely and reliably is directly related to the overall operation level of the campus network. Therefore, it is important to say that the security and stability of the network center is essential.

- Strengthen system security vulnerability prevention

Firewall technology: As a security guarantee in the network environment, the firewall can prevent insecure factors from entering the system. Its role is to prevent external network users from entering the system without authorization. Firewall technology combines software and hardware to create a secure gateway between the Internets to prevent unauthorized internal network attacks (Fig. 1).

In the campus network of colleges and universities, the method of shielding the host gateway or subnet firewall can be implemented, and it is very important to improve the anti-attack capability of the firewall [10]. The design scheme of the shielded subnet in the above scheme has the most advantages. The design method is as follows: Between the Internet and the intranet, two routers that can be filtered separate the subnets from them. These two routers are set at the end of the subnet, so that the subnet is buffered. One router controls the Internet data stream, and the other is responsible for the intranet data stream. Both streams can be accessed with the subnet. Data transfer. It is also possible to set up the bastion host in the subnet as required, and it can provide proxy support for the intranet to access the external network, and in this process, it is subjected to analysis and inspection by the filtering router. In this way, internal and external users can also access the externally exposed servers on the Internet through an Internet server [11].

Network intrusion detection technology: Network intrusion detection technology can be used to detect internal and external attacks. It mainly uses active monitoring to detect unauthorized behavior of users and detect intrusion of illegal intruders into the network. Network intrusion technology can effectively make up for loopholes in firewall technology [12].

Data Encryption Technology: Data encryption technology is a commonly used network security technology. By reconstructing data, it ensures that recipients accept information security. This technology improves the security and confidentiality of the network and is an important technical means to protect information security. Data encryption is a means of actively protecting information [13]. The information encrypted by the data can guarantee the security during transmission and reception, and ensure that it is not intercepted by others.

Anti-virus technology: Anti-virus technology mainly includes virus detection, scanning, analysis, protection, killing, repairing, etc. It is an important security technology essential to protect network systems. The destruction of computer viruses is the biggest hidden danger of network security. Nowadays, various viruses are emerging one after another, which seriously threatens the security of the network. The virus is rampant in e-mail, FTP, and instant messaging tools, spreading rapidly, and most college networks suffer. Because the virus has the characteristics of diversification and complexity, the anti-virus work of the campus network must form a three-dimensional and hierarchical anti-virus system. Specifically, anti-virus software must be installed on the Internet gateway, and anti-virus software must be installed on the server. Train relevant management personnel on anti-virus knowledge to improve their anti-virus level (Fig. 2).



Fig. 2 Vulnerability management life cycle

User Authorized Access Control Technology: User-authorized access control technology includes both authorization and access control. Authorization refers to the right to give visitors access to resources, that is, users can only access system resources according to their own access rights, and they must not access them. Access control technology is a policy based on access control and refers to the technology that the subject grants or restricts access to the client's access capabilities and scope [14]. Its main purpose is to protect system resources from damage caused by illegal access.

- Strengthen the security management of application software

To improve the security of campus application software, on the one hand, to improve software security awareness, it is necessary to put forward the importance of security in all aspects of application software, such as the proponent of software requirements, software design participants, users of software systems and software. Safe maintainers, etc. In view of the above reasons, it is necessary to fundamentally solve the situation that the software security awareness is separated from the information construction speed and the security measures are not timely, and comprehensively carry out safety awareness training, strengthen the management of the security system, and improve the sense of responsibility of all employees.

- Improve network administrators' awareness of network security

Most of the network security problems that appear on campus are due to the fact that internal technical workers do not have the relevant network maintenance technology and network security common sense, so that intruders have the opportunity to attack the computer and achieve the purpose of destroying the computer system [15], [16]. It can be seen that all colleges and universities must consciously enhance the manager's sense of responsibility and cyber security awareness, carry out network moral propaganda for all members, popularize common knowledge of network legal system, establish correct network values and network security concept, and establish a relationship from the personnel's mind. "Firewall" fundamentally protects against attacks on the campus network.

I. CONCLUSION

Network security plays an extremely crucial role in the development of the Internet. It is not only the key to ensuring the operation of computer systems, but also a necessary condition for maintaining national information construction. With the gradual expansion of the application of information technology in society, more and more people will come to the convenience of information technology, and begin to recognize the network more, relying more on the network in learning, work and life. Therefore, ensuring the security application of the network and maintaining the normal operation of the system are the first problems to be solved in the network application process. Computer network security is mainly based on security technologies such as firewall, data encryption, authorized access control, and intrusion detection. It is a constantly updated and improved detection and monitoring system. As the saying goes, there is no absolutely secure computer network in the world. In the face of increasingly complex computer networks, we should recognize the vulnerabilities and inherent defects of the network itself. While making full use of computer network security technology to protect the system in a stable and secure manner, we should also enhance our awareness of security and prevention. Only in this way can we fully enjoy the great convenience and experience brought by computer networks.

ACKNOWLEDGMENT

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (grant number: NRF2016R1D1A1B01011908). And it was also supported by the Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00245).

REFERENCES

- [1] Shi Peipei, Liu Yushu. Research on the Trends and Problems of the US Cyber Security Strategy [J]. Strategic Decision Research, 2018, 9 (01): 3-24+105.
- [2] Jiang Wenjun. Discussion on computer network information security under the era of big data[J]. Network Security Technology and Application, 2018(02): 69+73.
- [3] Tan Guanfu. Network Security from the Perspective of WTO National Security Exception [J]. Social Sciences in Chinese Universities, 2018(02): 63-74+159.
- [4] Wu Shenkuo, Luo Yuyu. Legal Governance of Artificial Intelligence Security: A Review of System Security[J]. Journal of Xinjiang Normal University (Philosophy and Social Sciences), 2018, 39(04): 109-117.
- [5] Zhang Wei, Long Tao. A preliminary study on information security, network security and cyberspace security [J]. Modern Information Technology, 2018, 2 (05): 155-156+158.
- [6] Pan Zhilin, Jia Yanyu. Discussion on Information Network Security in the Age of Cloud Computing[J]. Computer Programming Skills and Maintenance, 2018(05): 174-176.
- [7] Zhang Qiping. Analysis and Discussion of Computer Network Security Problems [J]. Computer Knowledge and Technology, 2018, 14 (13): 59-61.

- [8] Zhang Lei, Cui Yong, Liu Jing. Application of machine learning in cyberspace security research[J]. Chinese Journal of Computers, 2018, 41(09): 1943-1975.
- [9] Liu Enjun. Analysis of Network Security Defense Technology Based on Cloud Computing[J]. Network Security Technology and Application, 2018(09): 77-78.
- [10] Long Wei, Yan Jiyan. Talking about Computer Network Security Problems and Countermeasures[J]. Wireless Interconnect Technology, 2016, 12: 48-50.
- [11] Wang Yan. Research and design of linux-based intrusion detection system and firewall and its collaborative work [D]. Inner Mongolia University, 2017.
- [12] Huang Hui. Preventive measures against hacker attack network [J]. Network Security Technology and Application, 2018(1): 29-29.
- [13] MA Yubing. Security Threats and Preventive Measures Faced by Enterprise Computer Network[J]. Journal of Zhengzhou University of Technology, 2003(3): 18-19.
- [14] Yang Xiangyun. Design of Sichuan Post Integrated Network Security System [D]. University of Electronic Science and Technology, 2019.
- [15] Shu Hao. Types of Cyber Crime and Prevention Strategies[J]. Journal of Party and Government Cadres, 2017(6): 26-28.
- [16] J Jinquan, M Abdulhakim Al-Absi, H Jae Lee. Network Repair Algorithms for Wireless Sensors and Actuators Based on Graph Theory. Advance in material and manufacturing engineering (ICAMME), March, 15-17, 2019.



Ju Jinquan received his BS degree in mechanical and electrical engineering from Dongseo University-South Korea in 2017. Currently, he is a master candidate student in the Department of Information and Communication Engineering at Dongseo University, Korea. His research interests include network security and wireless sensor networks.



Mohammed Abdulhakim Alabsi received his BS degree in Computer Application from Bangalore University in India. He earned his (MS) degree at Dongseo University- South Korea in 2018. Currently, he is a Ph.D. student in the Department of Information and Communication Engineering at Dongseo University, Korea. His research interests include IoT, VANET, UAV, AI, Cryptology, Network Security, Computer Networks and Digital Communications.



Ahmed Abdulhakim Al-Absi is an assistant professor and head of smart computing department at Kyungdong University - Global Campus in South Korea. He earned his Ph.D. degree in ubiquitous computing at Dongseo University- South Korea in 2016. His research interests include Database Systems, Big Data, Hadoop, Cloud computing, Distributed systems, Parallel computing, High-performance computing, VANET, and bioinformatics. He received a Master of Science (MS) degree in information technology at University Utara Malaysia- Malaysia in 2011, and a Bachelor of Science (BS) degree in computer applications at Bangalore University- India in 2008.



HoonJae Lee received his BS, MS, and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, Rep. of Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information Communication Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include Password Theory, Network Security, Side-Channel Attack, and Information Communication/Information Network.