Research on Key Technology of Computer Network Defense

Yong He1,*

1School of Preschool Education, Jiangxi Teachers College, China, 335000

*Corresponding author e-mail: hy15731555@163.com

Abstract. Computer network technology has been widely used in all walks of life in China under the acceleration of scientific and technological upgrading. In all aspects of social production and people's lives, we can see the use of the computer network scenarios. A good computer network environment can ensure that citizens' personal information will not be leaked for no reason and the health of computers themselves. At the same time, there is a trend of diversified development of computer network attack means. So as to improve computer network’s security, we need to explore and analyze the key technologies of computer network defense so as to prepare for the loss or leakage of information and data in computer network. Based on today's information situation, this paper analyzes today's network environment, points out the necessity of network defense technology for us, and hopes that China's information defense technology will be strengthened day by day.

Keywords: Network Security Computer, Computer Network, Key Technology, Moving Target

1. The necessity and present situation of computer network defense

At present, China is in an information society. Xi Dada pointed out: "Without network security, there will be no nationwide safety. Without informationization, there will be no aggiornamento, and there will be no stable economic and social operation, and the interests of the broad masses of the people will be difficult to be guaranteed." Thus, computer network defence is significant in national growth. Therefore, comprehensive defense of computer networks can effectively protect individual data safety and the maintenance of citizens’ legal entitlements in cyberspace. With the continuous improvement of science and technology, the functionality of computer networks is slowly enhanced, and the probability of computer networks being attacked is also greatly increased. The leakage of network information poses great challenges and dangers to individuals, enterprises, society and the country. Cyber fraud occurs from time to time, and harmful information such as online rumors is repeatedly prohibited, seriously endangering national security and harming people's interests.

1.1. The importance of computer network defense
As far as China's current network information environment is concerned, the comprehensive defense of computer network can create a strong network security atmosphere, further build China's information infrastructure and contribute to the all-round growth of China's information economy. In the information society, the proficiency of data distribution has been significantly improved, and the probability of information loss has also increased greatly. Information resources have become an indispensable valuable asset for the people. Computer network defense can effectively ensure the safety of people's information, avoid the loss of information and maintain people's normal living conditions. Therefore, it is urgent to carry out high-strength computer internet protection.

1.2. Computer network defense status

At the present stage, people still stay in the use stage of computer network, and ignore the application of key technologies of network defense to varying degrees, so the key technologies of computer network defense are difficult to play their due role. The application effect of key technologies of computer network is an important factor that affects the level of computer network defense. At the same time, the application of key technologies of network defense depends on a sound network security management system. However, there are still some defects in the current network security management system, which makes it difficult to create a good application environment for key technologies of network defense. The design of firewall is unreasonable, which makes it difficult to fully coordinate computer functions and security protection. Therefore, the application of key technologies of computer network defense has also been affected to some extent. All at once, the scanning function of the key technology of computer internet defense has some deficiencies, which makes it difficult to fully identify the hidden dangers in the computer.

2. Several key technologies for computer network defence

Computer network defense diagram: as shown in Figure 1 and Figure 2.

![Figure 1](image_url)
2.1. Firewall technology

In recent years, China has heeded the function of computer internet defence, and the key technologies of computer internet defence have brought into full play, which is a comprehensive combination of technological advantages such as computer science, internet technology, communication technology, password technology and data safety. A firewall is a set of components or a system between two networks. At present, firewall is one of the main systems in computer network defence function. So as to further protect human information security and maintain a good information environment, the design of firewall must be comprehensively optimized. Researchers should base themselves on the current application situation, application level and application characteristics of key technologies in computer network defence, fully clarify the application conflicts between firewall and key technologies in computer network defence, and establish a cooperative processing mechanism between firewall system and key technologies in computer network defence system to achieve effective maintenance of network security.

The defence functions that an ideal firewall should have include:

(1) virus scanning and anti-virus function: for example, scanning ZIP and DOC files attached to e-mail, FTP uploading and downloading the contents of files, and discovering the dangerous information possibly contained therein.

(2) Defense of Denial of Service Attack: Denial of Service Attack means that attackers occupy shared resources too much, resulting in consumption of bandwidth, suspension of some services and even host crash, thus preventing other users from sharing resources or accessing servers. The firewall can prevent or mitigate DOS attacks to a certain extent by adopting reasonable control mechanism, detection mechanism and alarm mechanism.

(3) Intercept ActiveX, Java, cookies, java-script and other ways to filter HTTP content: some HTTP pages are included in malicious code, the firewall should be able to detect dangerous code or viruses from PHP, ASP and Script code, as well as from HTTP page stripped of Applet, ActiveX, Java and other programs, and to the browser user alarm.

2.2. Data encryption technology
Data encryption technology is separated into four aspects: information stowage, information spread, information integrity identification and secret key management technology. Among them, the encryption technology of data storage is to avoid the loss or leakage of confidential data in the field of storage, can be classified as encrypted storage and access control two kinds, data encryption technology is the data flow in transit encryption methods, port encryption and line encryption are two commonly used methods. Data encryption is mainly through the network data encryption to provide the network security and reliability, can effectively prevent the loss and disclosure of confidential information. In addition, it is widely used in information identification, digital certificate and other technologies to prevent electronic fraud, in the information processing system security plays an important role.

2.3. Virtual special technology

Tunnelling is the underlying supporting technology of VPN (Virtual Private Network). Tunnel technology is comparable to point-to-point link technology, which establishes a data channel on the public network, which is used to transmit the internal network data of an enterprise, similar to a tunnel passing through the public network. The specific content of tunnelling technology is that, at both ends of a tunnel, other types of protocol packets (such as IP protocol packets) are loaded data, repackaged by the source node, a new IP package is obtained, and then sent to the Internet for transmission. When the target node receives the packet, it will be used for public network transmission and removed by the IP header added by the source node. On non-IP networks, this technology can also be reversed, i.e. IP packages are encapsulated by other protocols to create tunnels for data transmission.4]

Tunnel protocol is the core of tunnel technology, and VPNs based on different tunnelling protocols are different. Tunnelling technology can be based on a second or third-tier tunnel protocol. The above layering is based on the reference model of open system interconnection (OSI). The data link layer in the OSI model corresponding to the second-layer tunnel ingon protocol uses frames as data exchange units.

2.4. Web report system

Nowadays, there is a large distance between China and developed countries in the computer network defence level. In order to build a network power in an all-round way, China must take the initiative in key technologies of computer network defense and upgrade its scientific and technological level. On this basis, comprehensive improvement of anti-virus technology is the prerequisite for promoting the application of key technologies of computer network defense. Anti-virus technology can fully identify potential viruses in current computer network systems. It can also comprehensively resist viruses that attempt to steal internal information resources in the external network of computers. Thus, anti-virus technology and key technologies of computer network defense have the same purpose. However, in practical application, because anti-virus technology has a high degree of recognition, it will mistakenly treat the key technologies of computer network defense as viruses, which inhibits the function of key technologies of network defense. Therefore, relevant personnel should combine the application advantages of anti-virus technology and key technologies of network defense to fully improve anti-virus technology, so as to build a collaborative application pattern of anti-virus technology and key technologies of network defense in computer network system.(As shown in Figure 3)
2.5. Network scanning technology

Improving the defence function of computer network in multifaceted approach will effectively improve the degree of information security protection in our country, which is the key to mastering the core technology of the Internet, and can help our country to occupy the scientific and technological highland of Internet development, and comprehensively guarantee Internet security and national security. Now, it is true to lag in the application of key technologies for computer network defence, which is mainly due to the lack of coverage of scanning functions of key technologies of computer network defence. It is difficult for scanning functions to fully discover viruses and other risk factors of information leakage in computer network systems. Therefore, in order to further strengthen the application effect of key technologies of computer network defence, the scanning functions of key technologies of computer network defence must be fully strengthened. Optimize online scanning, server scanning selection and workstation scanning functions, solve the problem that the scanning system occupies part of system resources and reduces system performance, improve the compatibility between scanning functions and other software (especially operating systems), and fully strengthen network defence functions. [7]

3. Conclusion

To sum up, computer network has penetrated into all levels and fields of society, and its security performance has become the first key problem. In order to effectively prevent various attacks, computer network needs to construct a perfect computer network defence system, and adopt key technologies of computer network defence strategy to sure the safe control of computer internet system and fully strengthen the computer network defence function, which is the key to ensure China's information security and maintain China's information environment stability. In the use process of key technologies of computer internet defence, it is necessary to comprehensively apply many technologies, coordinate and bring into full play characteristics and benefits of various technologies. At the same time, it is necessary to fully optimize the application process and application environment of technologies, and highly penetrate the awareness of security protection, so as to promote the construction process of China's socialist modernization power and help China become a world network power.
References

[1] Bennett Kevin B,Bryant Adam,Sushereba Christen.Ecological Interface Design for Computer Network Defense.[J].Human factors,2018.,18720818769233.

[2] Kevin B. Bennett,Adam Bryant,Christen Sushereba.Ecological Interface Design for Computer Network Defense[J].Human Factors: The Journal of Human Factors and Ergonomics Society,2018,60(5),610-625.Bouvrie J. Notes on Convolutional Neural Networks[J]. NeuralNets, 2006.

[3] Chen Chen,Ray Surette,Mubarak Shah.Automated monitoring for security camera networks: promise from computer vision labs[J].Security Journal,2020,(prepublish),1-21.Lowe D G. Distinctive image features from scale-invariant keypoints[J]. International journal of computer vision, 2004, 60(2): 91-110.

[4] Min Xiao,Mei Guo.Computer Network Security and Preventive Measures in the Age of Big Data[J].Procedia Computer Science,2020,166,438-442.

[5] Mingsheng Li. Application of Computer Network Security Technology in E-Commerce[J].International Journal of Computational and Engineering,2020,5(1).

[6] XiaoJing Wang.Research on Computer Network Security Policy of Cloud Computing[J].Journal of Physics: Conference Series,2020,1533(3).

[7] Chen Chen,Zhang Hui.Computer Network System Security Management and Maintenance Strategy[J].Journal of Physics: Conference Series,2020,1533(2).