Research on Security and Protection Strategy of Computer Communication Network

Setlla Bowman[1], **Wendy Jefferson**[2]

[1] Centre of The Mind Research Network, Albuquerque, USA

[2] Communication and Media Research Institute, USA

Abstract: Computer communication network technology makes life colorful and work more efficient. However, computer communication network technology is not omnipotent, it will also produce security problems, security problems will not only make the computer network failure, but also make the communication network system paralyzed. The loss caused by computer network security is fatal. Only by strengthening the security performance of computer communication network can computer communication security problems be better served for us. Starting with the problems existing in the computer communication network, this paper analyzes the security threat factors of the unit network, and puts forward the security of the computer communication network. The purpose of this paper is to provide some reference for improving the security performance of computer communication network.

Keywords: Computer; Communication Network; Security; Protection Strategy

1. Problems in computer communication network

1.1 The core technology of computer network's hardware and software comes from imports

The domestic informatization construction develops slowly in the core technology. For the core CPU of information equipment, it is imported from the United States or Taiwan. The key software of computer network, such as database and gateway software, is produced abroad. In fact, there are some hidden dangers in these systems, such as hidden channels and embedded viruses. Most of the network management equipments used in China are imported, which makes the computer network vulnerable to various foreign network threats, network information eavesdropping, theft accidents occur frequently, and fraud through the network. Cheating cases also happen frequently. In fact, domestic network security is in extremely fragile state.

1.2 Computer communication networks are highly susceptible to virus infection

Modern viruses are ubiquitous, not only spread in the network with the help of files, but also spread greatly when the user opens the web page. It often hides in the computer system after the computer starts up, and destroys the data information through the computer platform, and even destroys the computer hardware equipment. Through continuous self replication, spreading to the entire network will occupy the network system.

Slow down the speed of the network, eventually leading to the paralysis of the entire network system.

1.3 The low reliability of information transmission across the network requires a number of network nodes

In these nodes, each node will increase the risk of information being stolen and modified. For example, by modi-

Copyright © 2018 Setlla Bowman *et al*.

doi: 10.18063/csnt.v1i2.

This is an open-access article distributed under the terms of the Creative Commons Attribution Unported License (http://creativecommons.org/licenses/by-nc/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

fying the information and running the order to close the network, this harm will affect the operation of the entire network[1].

1.4 Internet external and internal threats may cause attacks on the network

All computers in the computer network are threatened by the network, such as planting Trojan Horse virus through the network, and modifying the data on the hard disk. Intruders on the network can disguise as legitimate users, enter the network, modify and steal information, and destroy computer software. When the top-secret information passes through the site, the intruder can intercept the information and read some top-secret information. There are also many lawless elements inside the network. These lawless elements log on to the website as legitimate users, modify the content of the information, and destroy the application system. Some network hackers can also modify the IP address, become legitimate users, escape the security settings of network administrators, and carry out network operations. Invasion.

2. Analysis of network security threat factors

2.1 Natural factors

2.1.1 Threats caused by network devices and links themselves

Network communication equipment and links also belong to an electrical equipment, it will also have some security risks, there will be oxidation, aging problems, will also appear over-voltage, breakdown, over-current and other issues, the most serious, will also occur burnout[2].

2.2.2 The activities of nature and the behaviour of human society can destroy the communication system

The destruction of communication networks by nature and human society is sometimes accidental or frequent. The frequent damage is mostly caused by the electrical characteristics of the line itself. The strong current interference, the lightning damage may cause the line damage, some artificial mechanical damage, the gnawing animals may destroy the line, Wet conditions can also erode roads. These hazards can actually be prevented by artificial dryness, and the damage to the line is not fatal. In previous work, as long as some measures can be adopted to prevent the occurrence of such hazards. There is a kind of sabotage, Most of them come from nature, although they are accidental, but the damage to the line is fatal, such as flood, fire, earthquake, storm and so on. These disasters will completely destroy the line, and the damage is irresistible.

2.2 Computer system factors

2.2.1 Has poor capability in developing software and hardware of network communication system.

There is still a big gap between China and developed countries in the technology of computer system and network communication. For the main hardware of computer, especially CPU and motherboard, most of them rely on imports. For computer software, such as computer operating system and communication software, especially network database, it is mainly imported. In developed countries in Europe and America. These hardware and software are likely to add backdoor programs, bury some network vulnerabilities, bury hidden dangers for network security. There are still some problems in the operation ability and information processing of the CPU independently developed in China, which can not meet the requirements of information processing in the network information society. The hardware and software of the network information technology need to improve the level of autonomy.

2.2.2.2 Long-term risk of viral infection

Virus is everywhere in the network system, the development of virus is also with the development of science and technology to improve their own technology. Some malicious programs can break into networks, such as mail, web pages, files, etc., by means of various means, especially some system vulnerabilities, which provide an intrusive mechanism for viruses, and these malicious programs can be copied and spread in the network. It is especially feared that they also have the function of automatic booting, they are hidden in the system memory and can destroy the computer system at any time. Once the computer system is infected by the virus, it will also become a springboard for virus generation, allowing the virus to pass the calculation. The computer invades the whole communication network and threatens the information security of the network seriously.

2.2.3 Secret-related information in the communication network transmission security very poor Secret-related information in the network with the help of nodes to spread, these

Information is always at risk of being stolen and altered. Some outlaws can attack information by tampering and deceiving the data in any node of the network. It is possible for information to be reissued.

Cause network blockage, serious will cause system crash. Malicious computers in the network can also intercept data, and change the content of the data, to deceive the recipient of data, to achieve network fraud. Computer information may also be leaked by electromagnetic waves, causing information leakage.

2.2.4 Network hardware node defects threaten network security

The problem of network security is becoming more and more prominent. Traditional computer information security only depends on firewall and antivirus software, but with the development of virus and intruder technology, These technologies can not completely guarantee the security of information in network communication. In fact, the firewall has a lot of security holes, its system structure is only a single processor, it can only produce a protective wall to the virus, there is only one layer of security detection mechanism, and these defects of the firewall make it difficult to protect itself. Extremely easy to be breached by the virus, people think that with a firewall, you can ensure the information security while surfing the Internet, in fact, even if there is a firewall Protection, while surfing the Internet, will still be attacked by hackers. There are more than 30% of the network attacks have their own firewall protection of the network. The fragility of firewalls has led the National Security Bureau to propose that physical isolation be used to maintain information security in key departments, but these physical isolation methods, like firewalls, have some drawbacks, such as poor security. Long start-up time, poor reliability, etc.

2.3 Factors of Internet users

In the long run, network builders only focus on network lines and hardware facilities, and often ignore the factors of network users, the management of network users is loose, there is no certain norms. The control of network security is far from enough for network security. Network users can only take extreme methods to close the network when network security problems occur. These methods can not achieve the purpose of solving network security problems at all. Although some legal provisions have been formulated for the security of network system in China, there are many defects in these network operation and management mechanisms. Units generally lack network security management personnel, only to take inadequate security measures for network protection, for network security problems, the lack of solutions. The unit's information security system is insensitive to the rapid response to security issues and is unable to give timely response capability[3]. Network administrators and users of the network lack of safety awareness, and their quality is generally low. With the development of information technology, the number of computer network users has increased exponentially. However, the personal technology of users has not improved, and the computer security problem has not been given enough attention. When the computer intervenes in the network, it brings the danger of information being stolen and rewritten. Especially some key confidential information, users do not have a certain sense of confidentiality, and do not encrypt and backup these data in time, making these top-secret information completely exposed to hackers under the attack. Some units of computer security software has expired, need to be updated long ago, these problems also buried hidden dangers to the security of information.

3. Computer communication network security and protection measures

3.1 Hidden IP address

IP address is the main attack way of computer network by lawless elements and hackers. These illegal elements and hackers use special network monitoring and testing technology to obtain computer host information, and then steal the IP address of the computer. Once the IP address is acquired, it means that the computer system is completely exposed to these criminals, who attack the computer using Floop overflow or DOS attack techniques, so, The computer's

IP address must be hidden, not exposed to illegal elements, there is a best way to hide the IP address In the case of a proxy server, these criminals can only obtain the IP address of the proxy server, but not the real IP address of the computer terminal. Thus, the end of the computer is protected.

3.2 Improving the security technology of computer communication network

Computer communication network security technology can greatly enhance the security of computer communication network, so that the computer network to prevent outside hacking attacks. Common computer network communication technologies include the following:

3.2.1 Encryption technology

Encryption technology is actually a kind of camouflage information technology, which usually uses symmetric encryption and asymmetric encryption. The principle of this technology is to prevent the intrusion of the outside world by setting the cipher.

3.2.2 Firewall

The modern firewall technology provides the first defense barrier for the computer. It filters and restricts the virus by identifying the external data. The application gateway and proxy technology actually belong to the scope of the firewall.

3.2.3 Identification technique

Authentication technology can make the exchange process of information in the network more reasonable and effective. Through the authentication technology, the network information becomes more real. Through the authentication technology, the security performance of the network is greatly enhanced.

3.2.4 Internal protocol of computer communication network

The internal protocol of the computer communication network is a kind of authentication behavior to the information data. If it is used with the encryption technology, the security performance of the computer communication network can be greatly improved.

3.2.5 Intrusion detection technology

Intrusion detection technology can identify the virus in time and provide alarm service. It can remind the network manager to deal with the virus in time.

3.3 Improving the performance of computer communication network system

By strengthening the difficulty of keeping computer communication network data confidential, we can strengthen the security of computer network itself. Through security grade identification, we can enhance the confidentiality of computer network data. The vulnerability of computer communication network system is greatly reduced, so as to prevent the invasion of virus. Therefore, enhancing the performance of computer network is the most important task to enhance the security of computer communication network.

3.4 Strengthening security education of computer communication network

The security of computer communication network must be supported by qualified personnel. It is necessary to strengthen the security protection consciousness of communication network personnel so as to make use of the network technicians who have been trained professionally. To strengthen the re-education of computer communication network technicians and cultivate a group of network technicians with high quality to maintain the network security.

3.5 Perfect network security strategy should be established

3.5.1 Set user access rights

To provide network users with passwords, passwords and other identification threshold, access to address only for specific users, if visitors do not have a password, can not log into the network, do not have access to the user, can not connect to the network.

3.5.2 Authorization mechanism

The network administrator provides the license book for the user as the key to log on to the network, and the unauthorized user can not make use of the network resources at will.

3.5.3 Encryption mechanism

Encryption mechanism allows unauthorized users not to read network information.

References

1. Liu MY. Computer network security problems and their countermeasures [J] .Electronic Technology and Software Engineering 2017; (22).
2. Wang L. Analysis of Network Security Technology [J] .Science and Technology Innovation and Application 2015; (27).
3. Xiao Y. Analysis and study of network virus and network security maintenance path [J] .Heilongjiang Science and Technology Information 2016; (10)
4. Tanenbaum AS, Wetherall DJ. Computer network[M].5th ed.Beijing:China Machine Press, 2011; China Internet Information Center. 30th China Internet Development Statistics Report [EB/OL]. http://www.cnnic.cn/research/bgxz/tjbg/20120719_32247.html, 2012-7-19.
5. Wang SB, Li XN, Chen LW. Computer Network Experiment Course System Based on Network Technology [J]. Laboratory Research and Exploration 2010; 29(4): 49-51, 111.
6. Shi YB. Exploration of Computer Network Course Experiment Course in Independent College [J]. Office Automation (Comprehensive Monthly) 2010; (8): 63-64.
7. Xue Q. Computer Network Simulation Experiment Teaching Based on Packet Tracer [J].Laboratory Research and Exploration 2010; 29(2): 62-64.
8. Xie H, Nie F.Computer Network Simulation Experiment Teaching Research Based on Boson Netsim[J].Experimental Technology and Management 2007; 24(5): 89-91.
9. Boson NetSim.Network simulator &amp; router simulator [EB/OL]. http://www.boson.com/AboutNetSim.html, Boson Holdings 2010; LLC.
10. He LJ, Zhai YB, Li CT, *et al*. Project-based experimental teaching mode and its feasibility evaluation method [J].Laboratory Research and Exploration 2010; 29(2): 94-96.
11. Wang Y. Practical Exploration of Project-based Teaching Method in the Basic Course of Electronic Technology [J].China Market 2007; (12): 193.