PAPER • OPEN ACCESS

Research on Computer Network Security Problems and Countermeasures

Research on Computer Network Security Problems and Countermeasures

* development of internet, people cannot live without
computers and networks. However, in the process of using network, there are often a lot of security problems. This reduces the user's sense of experience and threatens the security of users' personal information. This study discusses the importance of computer network security, the specific types of security problems and several effective countermeasures. This provides a basis for the development of computer network security.

Keywords: Network Security, Internet, Problems and Countermeasures

1. Computer network security *1.1. The definition of computer Network Security*

The International Organization for Standardization gives the computer network security a definition. It is a kind of security preservation of the technology established and used for some processing systems for protecting computer data of the software and hardware from destruction and leakage due to some unexpected and spiteful reasons. The definition of computer security includes physical security and logical security [1].

Network security is the preservation of the integrity and availability of information on the internet. Integrity, that is, to ensure that unauthorized operations cannot modify data. Effectiveness, that is, to ensure that unauthorized operations cannot destroy information or computer resources.

Therefore, to put it simply, network system security includes network security and information security. Network security refers to the security of physical lines and connections caused by network operation and interconnection between networks, operating system security, personnel management security and so on. Information security refers to the security of data, such as confidentiality, authenticity, availability and controllability.

Figure 1. Network security and defense technologies.

1.2. The importance of computer network security

With the large utilization of computer technology in various fields and the promotion of automation system in work, the traditional working mode is increasingly challenged. Modern office work is gradually developing in the direction of "paperless" and "network". Especially after the commercialization of the Internet, the Internet industry has made great progress [2].

The internationalization, openness and personalization of the information network not only provide people with "information sharing", but also bring high efficiency of work and high quality of life. As the transmission of information will not be limited by time and space, more and more computers are connected into the network, and the government and individuals gradually rely on the network environment and network resources.

However, the security problem of network system is becoming more and more prominent and getting more and more attention. The leakage, tampering and counterfeiting of online information, the spread of viruses and the spread of bad information provide a very damaging threat to the network. So, it is imminent to solve the problem of computer network security.

2. The main types of computer network security problems

There are mainly two kinds of computer security problems: 1) threats to information in the system; 2) threats to equipment in the system [3].

There are many factors that affect the computer system, some of which may be intentional, or network communication can be unintentional, man-made, non-man-made or caused by the natural environment. Generally speaking, the threats to the security of computer systems are as follows:

2.1. Data theft

The security loopholes caused by inexact security configuration of operators, low security awareness of users or users lending or sharing their accounts with othersat will form a threat to network security. It leads to a lot of data loss. The loss caused by data loss is immeasurable. The confidentiality and availability can be menaced at random [4].

2.2. Trojan horse virus

Although the browsers used by many users have greatly improved their ability to block ads, the statistics of some antivirus software websites once again reflect the fragility of browsers.

Trojan horse is a kind of hacker tool based on remote control, which has the characteristics of concealment and non-authorization. Concealment means that the designer of the Trojan horse will take a variety of measures to hide the Trojan horse in order to prevent the Trojan horse from being discovered. Even if the user finds that the Trojan horse is infected, it is not easy to determine its specific location. Non-authorization means that once the control side is connected with the server (the

attacked side), the control side can steal most of the operation rights of the server through the Trojan program. This includes modifying files, modifying the registry, running programs, and so on.

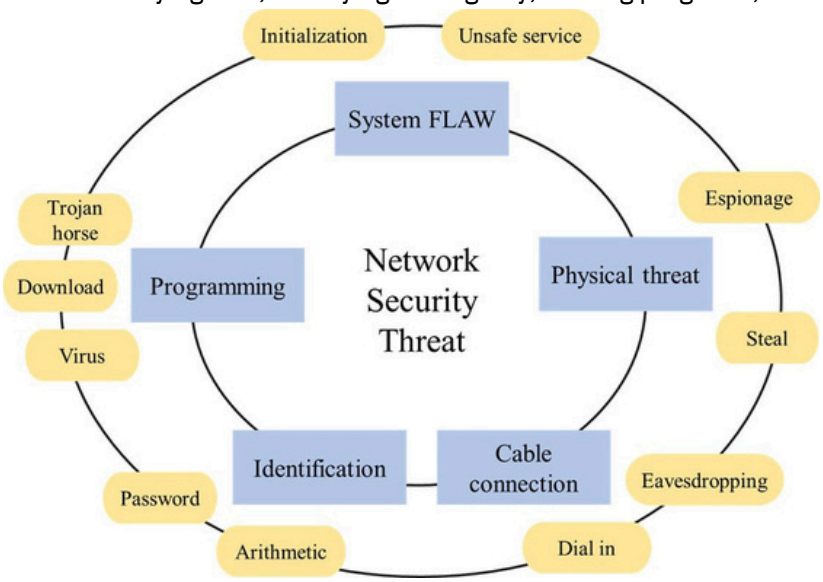

Figure 2. Types of network security threats.

2.3. Vulnerabilities

Many network systems have loopholes of one kind or another. These vulnerabilities may belong to the system. Also, it has the possibility be formed by the negligence of the management. These vulnerabilities can be used by hackers to do various attacks, including the password detection. In addition, software attack is a common method among them. Hackers have ability to gain the super-user rights of the computer illegally and control over it completely. Besides the operations of files, it can also capture images on the desktop, acquire the passwords of lots of applications and some other operations. Client -side and server -side are the two types of those software. When hackers attack, they will log in using client-side programs.

2.4. Mobile threat

Smartphone viruses pose a threat to corporate networks and personal information. From the perspective of today's network development trend, any electronic product may be connected to the network, and the fact that the network is everywhere shows that attacks are also everywhere. In addition, there will be loopholes in hardware, operating system, network access equipment and application system. Using the storage space of mobile devices, the living space and incubation period of malicious code will be unpredictable.

2.5. Electromagnetic interference

High-voltage wires, radio wave transmitting antennas, microwave line high-frequency electronic equipment and so on, will produce electromagnetic interference signals. These electromagnetic interference signals will destroy the information on the computer magnetic medium, thus affecting the network security. 3. Preventive measures and techniques for the formation of computer network security problems

Any network service will lead to security risks. the problem is how to minimize the risk. At present, the network security protectioncountermeasures are as follows:

3.1. Create a secure environment of network

It is very significant to create a secure network environment, including monitoring users, setting user permissions, using access control, identification, monitoring routers and so on.

3.2. Computer virus prevention.

Computer viruses are written artificially by exploiting loopholes in computer software. Due to the fast development of computer and the emergence of new viruses, the speed of transmission becomes faster and faster. Also, the harm is becoming more and more serious. The most commonly used preventive measure against computer viruses is to install antivirus software to check and kill files infected with the virus.

There are also the following measures to prevent the virus:

1) Do not use programs and data of unknown origin.
2) Do not download files from unknown websites at will.
3) After downloading the file, disinfect the virus before using it.
4) Do not easily open the e-mail of the store address of unknown origin (attachment).
5) Often do a good backup of important data and so on.
6) Update system patches should be installed frequently to reduce the number of viruses that exploit system vulnerabilities to attack and destroy.

3.3. Firewall technology

Firewall is a system used to protect the network security of different hosts, users or subnets.

The main function of thefirewall is to implement and enforce secure access policies between different subnets [5]. The firewall divides the user network into different subnets according to the function and security level, and carries on the access control through the firewall.

The intranet is the trust network. It can access external networks, such as Internet, through firewalls. It can alsoaccess the network that provides services through the firewall, that is, the shared security subnet. It can be seen that through the firewall, we can control the access between subnets of different security levels and prevent malicious or unauthorized access [6].

3.4. Data encryption

Because network hackers may invade the system, steal data or eavesdrop on data in the network. Data encryption can make the stolen data will not be simply opened, thus reducing the loss a little. At present, the encryption technology has been relatively mature, and there are two kinds of encryption technologies commonly used: 1) symmetric key encryption technology, and 2) public key encryption technology.

3.5. Digital signature

The digital signature is able to be utilized to verify that the message was given by the sender. Moreover, when a digital signature is used to store data or a program, it can be utilized to prove the integrality of the data or program. Like ordinary handwritten signatures, it has the ability be used to verify the authenticity of information.

3.6. Digital certificate

Compared with the online ID card, the digital certificate uses the digital signature to authenticate the identity on the Internet through the third-party authoritative authentication, which has the function of authenticity. Digital certificates are secure, confidential, tamper-proof and effectively protect enterprise information.

4. Conclusion

People put more and more attention on the security of computer network. Under the situation of the fast development of the network security industry and the acceleration of the information process, a

variety of new technologies will continue to apply. Network security has immeasurable opportunities, which becomes a hot area for researchers to explore, its development is of great strategic significance, and the future network security technology will make more considerable progress. Researchers should completely realize the safety factors to establish reasonable objectives and relevant laws and regulations.

References

[1] Yang Guang, Li Feifei, Yang Yang; Analysis of computer network security measures [J]; Science & Technology Information; 2011.

[2] Yang Shuxin; Research on Computer Network Safety Technology [J]; Journal of Hebei Energy Institute of Vocation and Technology; 2008.

[3] Ren Xingzhou; The Analysis and Solutions to Computer Net Security [J]; Computer Knowledge and Technology; 2005.

[4] U Zhang Suying; An Inquiry into Hidden Danger in Network Safety and the Safety Precautions [J]; The Science Education Article Collects; 2012.

[5] Xiong Fangfang; A brief discussion on the problems of computer Network Security and its Countermeasures [J]; Electronics World; 2012.

[6] Wang Tian, Xiao Hui; Defense Technology of Network Safetyand It's Development [J]; Journal of Anhui Vocational College of Metallurgy and Technology; 2007.