Research and Implementation of Key Technologies of Network Security System Software

Xiang Wang¹, Chenxing Na¹, Benhai Wei¹, Minghui Zhou¹,*

¹China Gridcom Co., Ltd Research and Development Center, Shenzhen, China, 518000

*Corresponding author e-mail: zhouminhui@rdc.grid.org

Abstract. With the continuous development of computer technology, computer technology has been very mature, various industries have widely used computer technology, our life has been inseparable from computer multimedia technology. Computers have become irreplaceable products in our lives. Nowadays, it is also very common for people to use computers to access the Internet. Computers can also store a lot of our information, so network security is very important. We must pay attention to the network security of our computers. There are a lot of necessary information on the network.

Keywords: Computer Network Information Security, Computer Technology, Hackers, Network Environment

In today's society, our work and life have been inseparable from computers, computers have become a necessity of people's lives, a healthy network environment is crucial, only in a healthy network environment, we can make better use of computer technology, we must fully understand the problems of computer network security, building a good computer network security system to ensure the information security of users

1. Security of computer networks

1.1. Virus attack
Nowadays, many network dangerous molecules make computer viruses to threaten the computer network environment [1-3]. This computer virus is also infectious. It can harm computer systems and cause the loss and leakage of files. At the same time, the virus will also cause great damage to computer hardware, seriously affecting the normal use of computers [4-6].

1.2. Muma and malicious program intrusion
Many computers have a common problem is Trojan horse and malicious program, this program will often invade everyone's computer, causing a certain degree of damage to everyone's computer, so where did this intrusion come from? Some computer users will inadvertently browse some unhealthy websites, which contain these malicious programs. The intrusion of Trojans and malicious programs
will seriously threaten the security of computers and bring great inconvenience to computer users. It poses a great threat to users' network information and privacy and many confidential information and personal privacy information are stolen.

1.3. Threats from network sharing and openness
In today's society, computers bring a lot of convenience to people's lives, there are a lot of shared resources on the Internet, there are many hackers to use this trait, computer attacks and malicious destruction. In addition to sharing, computer networks are open. Saboteurs take advantage of this feature to browse the information content of enterprises. They sometimes even disclose personal information to the relevant media or profit from it, and we become victims unconsciously.

1.4. Threats from improper user operations
In addition to the above factors, some bad behavior habits will also have a certain impact on network security. Computer users should have a certain awareness of network security, click or browse some non-formal websites knowing that there is a risk, and even actively register and enter personal real information, which will make it profitable for lawbreakers. Often lend their own accounts, credulous others, these processes are easy to lose effective information.

![Figure 1](image_url)  
Figure 1. Security of computer networks.

2. Construction of computer network and information security system

2.1. Enhanced virus prevention
Why did the computer suffer a virus invasion? The computer itself will contain some vulnerabilities, so we must regularly check the computer, check and repair these vulnerabilities, so as to effectively and timely prevent virus attacks. We only need a good antivirus software to solve this problem. The antivirus software not only has the function of antivirus, but also can monitor the computer in real time. Therefore, the user must install an antivirus software, update the virus library in time, and enhance the ability of computer virus prevention.

2.2. Firewall technology
Firewall technology is a very effective computer protection measure, which can effectively avoid the illegal invasion of computer by external network and improve the security of computer network. It is actually a kind of defense system, which can isolate its computer system from the external system, it
can effectively isolate the connection of the security zone of the risk zone, and it is an efficient network security model. Therefore, users should improve the level of firewalls.

2.3. Enhanced access control technology
Strengthening access control system can also ensure our computer information security, so what is access control system? The access control system can manage the access rights. The access control technology can make the corresponding network access rules. Only the computer can access it, and some networks are forbidden to be accessed. Access control technology can reduce the probability of network being attacked to a certain extent. It improves the security of the network. The development of access control strategy consists of three parts: access control, network authority division and client protection strategy. Access control is the first gateway of the network, which is generally controlled by verifying the user account and password. Therefore, in order to improve the security of computer use, users should try to complicate the account number and password, and make regular changes to prevent others from stealing.

2.4. Establishment of a security implementation defence and recovery system
As we all know, the computer itself has the ability to resist risks, the computer will have a certain ability to control its own vulnerabilities, However, it can not always ensure the security of the computer, so when it is found that the network information is destroyed, A remedy should be made in time to recover and reduce the loss. In order to ensure the security of network system, it is necessary to establish security implementation defense and recovery system, including security detection and early warning mechanism, security response mechanism, intrusion detection mechanism and security recovery mechanism.

2.5. Information encryption and authentication technology
Nowadays, there are many popular e-commerce, which often has the popular e-commerce, which depends on encryption technology as the guarantee. Information encryption can prevent others from maliciously stealing or destroying information, which can effectively protect the confidentiality of information. Authentication technology can ensure the integrity of information and make information changed maliciously by others, which plays an important role in the security defense of open computer network environment. Therefore, in order to ensure that the data, files, passwords and other important information in the computer are not stolen by others, it is necessary to encrypt and authenticate the data to be transmitted in the process of information circulation. There are three common methods of information encryption, namely link encryption, endpoint encryption and node encryption.

3. Key technologies of computer network and information security system

3.1. Set password technology
If we want to further improve the security of the computer, we must encrypt the computer and set the relevant password to the computer, which can guarantee the security of the computer network information. This is also the most basic method. First, encrypt the information to prevent the information from being accessed by unauthorized users. Secondly, the adoption of cryptographic technology makes the network information more protective shell, even if the information is stolen by illegal elements, but it is difficult to crack the content, effectively prevent the leakage of information.

3.2. Access control technology
Access control technology can also effectively improve the security of the computer, protect our computer, access control technology is to control the access rights of the computer, only access rights can be accessed. This technology is mainly to prevent users from using resources ultra vires. When using access control technology, users need to authenticate when using certain network resources to determine whether users have the right to use. The technology is to some extent. It limits the behavior
of accessing the network and reduces the possibility of network information being infringed.

3.3 Virus prevention and firewall technologies
Computer viruses are not all harmful. Sometimes we can also use computer viruses to protect our computers. Installing antivirus software is also a very effective protection measure. In the current development process, there are two kinds of antivirus software: single machine antivirus software and network antivirus software. These two kinds of virus software have different functions and uses. The emphasis of network antivirus software is on the network, which can be checked and killed in time when the virus attacks the network system. But we also need to know that antivirus software is not omnipotent, these software can only prevent some viruses, a small number of viruses can not be prevented. We also need to backup important files of the system and encrypt key information. Firewall is a network protection software, can prevent the network from the outside world. The installation of fire protection software can prevent the network from being infringed by the outside world.

4. Summary
To sum up, computer network security needs us to maintain together, computer users should also master the relevant computer security usage norms, improve the security awareness of computer use, and jointly build a good computer network environment. In the future, computer security will become more and more important. We must pay attention to computer security. When we use computers at ordinary times, we should always pay attention to protecting our privacy. We can set passwords for some important files to ensure the security of files. At the same time, we should also master ways to improve computer security. When viruses are in computers, we should know how to solve these problems. Computer technology is a double-edged sword. Although it has brought great convenience to our life, we should always pay attention to computer security in case of information leakage. It is very important to improve our computer security consciousness, because computer is already a necessity of our life, and we should make rational use of it. In order to ensure their own Internet information security. We usually have some important files to backup, if in the computer virus, our files will not be lost, in peacetime use of the computer to have good habits.

References
[1] Yin Hongbo Network Environment [J].]1 Computer security, 2011(2):68-69.
[2] Wang Yue, Yang Pingli, Li Weijun. Design and Implementation of Information Security Management System for Confidential Computers Computer Engineering and
Design, 2010(18):3964-3967.

[3] Li Weiming. Computer Network Application and Information Security Research [J]. Wireless Interconnection Technology, 2012(2):35.

[4] Bin Li, Shaohai Hu. A practical one-time password authentication implement on Internet[C]. Hangzhou, 2006.

[5] Neil Chou, Robert Ledesma. Client Side defense against web-based identity theft webspoof[EB/OL]. http://crypto.stanford.edu/webspoof, 2008-03-25.

[6] Collin Jackson, Dan Boneh, John Mitchell. Spyware Resistant Web Authentication Using Virtual Machine spyblock[EB/OL] 2008-12-30.