# Research on hidden dangers and control measures of computer network security

**Xiong Chuixiang**

Hankou University, Wuhan City, Hubei Province, 430212, China

**Keywords:** computer network; security risks; control measures

**Abstract:** Under the background of the rapid development of information technology, the rapid spread and popularization of computer network has penetrated into all aspects of people's lives and work, and has a great role in promoting social development. However, while the computer network brings many conveniences to people, there are also many network security problems, which threaten the privacy security of network users, and are not conducive to the long-term and stable development of computer networks. For this reason, starting from the current situation of computer network security, this paper analyses in detail the hidden dangers of computer network security, and puts forward some suggestions on this basis, aiming at improving the security of computer network.

## 1. Introduction

After entering the 21st century, the information network technology represented by the Internet has penetrated deeply into all fields of society, and information globalization has become an inevitable trend. However, the Internet itself has the characteristics of freedom, openness and internationalization, which not only provides convenience for people to exchange information, but also leaves a lot of security risks, which brings great losses to people's lives and production. Therefore, it is very necessary to strengthen the computer network security management and control. Only in this way can we better guarantee the network information exchange security and smooth, and promote social development to a higher level. However, because the development of computer network in China is relatively short, and then all aspects are not perfect enough, resulting in many security risks. Therefore, it is necessary and significant to strengthen the study of computer network security risks and control measures.

## 2. Current Situation of Computer Network Security

Internet application technology came into being in the 1960s, then began to grow in the 1990s, and occupies a very important position in people's daily life and work. With the continuous development of information technology, the problem of computer network security is born, and more and more prominent. As far as the current situation is concerned, computer system damage and virus infection are still serious. Although the state has introduced a series of laws, regulations and policies, and has achieved some results, but driven by interests, some hackers still ignore them. For example, the panda incense burning in 2007 and extortion virus in 2017 have brought great harm to society[1]. For the latter, it is considered to be the most serious extortion virus incident so far, involving 150 countries, more than 300,000 users recruited, with losses of up to $8 billion. This shows the harmfulness of computer network security risks.

In this context, our country also attaches great importance to, and has taken a series of important measures to strengthen the development of network security and information technology. President Xi Jinping has repeatedly mentioned that “without cyber security, there can be no national security.” This shows the importance of network security. In “Some Opinions of the State Council on Promoting Information Consumption and Expanding Domestic Demand”, it is emphasized that the construction of information infrastructure should be strengthened, the optimization and upgrading of information industry should be promoted, and the ability of information network security should be enhanced. To this end, all sectors of society should also respond positively and pay more attention to the management and control of hidden dangers of computer network security, so as to

  DOI: 10.25236/scmc.2019.053

make illegal elements inorganic.

## 3. Hidden dangers of computer network security

As far as the current situation is concerned, computer network security risks include the lack of user network security awareness, network viruses and hackers. See Figure 1:

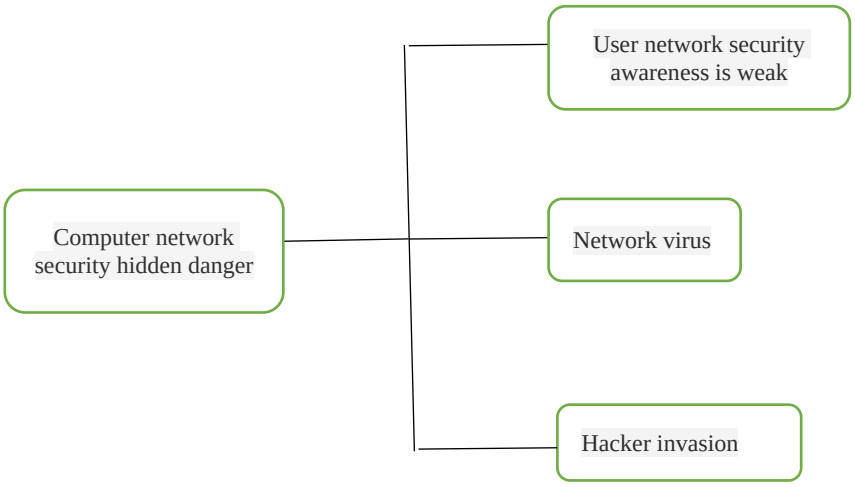


Figure 1 Computer network security risks

### 3.1 User's weak awareness of network security

In recent years, computer network security issues emerge in an endless stream, paper media, radio and television for network security issues exposure rate is also increasing. However, as a whole, many people still do not attach much importance to the computer network security issues, the awareness of network security is very weak, and the understanding of computer network security is not deep and thorough enough, which makes the network security level a lot of hidden dangers. Some users only use computer networks for entertainment, so they feel that they are far away from network security issues, and then more casual in network security, mostly relying on anti-virus software. Even in some units, the computer network has not been regularly checked in terms of security, and various security control measures have not been implemented in place. When many computer network users use computers, they will not set the privileges and passwords of programs or files. They have no protection consciousness at all, which makes the protection barrier of files and programs very fragile, or no barrier at all [2]. Because of this, the overall level of computer network security in China is not high, and the potential security risks are large.

### 3.2 Network virus

Computer viruses are infectious, destructive, and reproducible. The most important mode of transmission is network communication. Network virus is one of the important factors affecting computer network security. In the application of computer operation, if we fail to do a good job in virus detection and killing management and virus anti-intrusion protection measures, it will very likely lead to the leakage of user's personal data and privacy, and may also lead to the slowdown of computer operation ability and serious damage to it. Computer application system. Usually, network viruses are attached to applications and files. If users download programs or files with network viruses in computer applications, network viruses will invade computer systems. For example, the panda incense burning virus in 2007 was mainly transmitted through downloaded files. With the continuous development of network information technology, network viruses are gradually upgraded, which is more and more destructive and harmful to computers.

### 3.3 Network hackers

Network hackers mainly refer to people who illegally infringe on personal information of network users, destroy computer systems and implant network viruses by means of computer networks. Intrusion by network hackers will not only destroy computer systems, but also lead to property loss and privacy disclosure of computer users. Simply put, network hackers have a strong ability to operate and invade computers. They have a deep understanding of computer programs and systems. They first select the intrusion target, then test the protection capability of the target computer, at the same time formulate the intrusion method, and finally attack the target computer defense system, in order to achieve the purpose of stealing important information, personal privacy and data of computer users. For example, in February 2018, the Pingchang Winter Olympic Games in South Korea was attacked by hackers because they were afraid that hackers would take the next step. The organizers chose to shut down the server and the official network was down for 12 hours, which made the ticket printing impossible and the media center system malfunctioned. MsAfee reported that many micro-event infrastructure service providers had been attacked by hackers long before the event. Their main purpose was to steal financial data and sensitive information. The hacker intrusion not only caused great economic losses to the organizers of the Pingchang Winter Olympic Games in South Korea, but also had a great negative social impact.

## 4. Computer Network Security Management and Control Measures

### 4.1 Strengthening user network security awareness

In order to effectively improve the security of computer network applications, the most critical thing is the user's own security awareness. If computer users can pay more attention to computer network security issues, and actively build defense in the application, it will greatly enhance computer network security. Therefore, it is necessary to strengthen the network security awareness of computer users. Specifically, we can start from the following aspects: First, strengthen the training of computer professionals. The development of computer network can not be separated from the support of talents. In the face of network security problems, only high-quality and professional talents can effectively deal with them. To this end, the relevant departments should pay more attention to the training of high-quality and high-professional personnel, and invest funds to enable them to learn more advanced technology, so that they become the backbone of computer network security maintenance [3]. At the same time, cooperation with schools can be strengthened to encourage schools to increase the design of computer network security courses; secondly, through broadcasting, network, Street brochures and other forms to enhance the awareness of ordinary users of computer network security, and regular or irregular lectures in community organizations to instill network security threats for the broad masses of the people. Serious consequences, let them realize that once intruded, but privacy exposure, may also cause great economic losses, so they will consciously enhance their awareness of network security. In this way, hackers and viruses can be cut off, and no chance can be given to them to build a strong network security wall.

### 4.2 Rational application of antivirus software and construction of firewalls

In view of the current situation of the network virus rampant, we can deal with it through anti-virus software, building firewall and other measures. First, anti-virus software, such as Kingsoft Antivirus, 360 security guards and computer housekeepers, can well prevent the invasion of network viruses, and is also simple and easy to operate, which is very practical for some ordinary users. However, with the continuous development of network technology, network viruses have also developed rapidly, such as Trojan horse virus, worm virus, etc. It can be said that the prevention is insurmountable, ordinary anti-virus software is difficult to prevent. To this end, users need to actively maintain and upgrade anti-virus software to ensure that anti-virus software has been in the best state; second, standardize the application of hard disks and excellent disks, do not open unknown websites casually, so as to prevent virus intrusion; third, build a firewall. In addition to the basic computer hardware and software architecture, updating network protocols and enhancing

personnel security awareness, firewall technology is one of the important ways to manage and control network security risks. Common types of firewalls include: judging the type of network application layer and circuit of security type by handshake detection between client and server; judging whether to let data packet filter type through IP datagram port, starting address in data packet, etc. [4]. Of course, we must clearly recognize that everything has two sides. While firewalls bring security to people, they also lead to network delays caused by data entry and exit rules, especially when large amounts of data are accessed. Through these ways, it is bound to solve the problem of virus intrusion well, so that the vast number of computer users can rest assured to go to work.

### 4.3 Perfecting Network Security Access Mechanism

On the one hand, in the perfection of computer network security, we need to strengthen the construction of network security mechanism, in order to effectively guarantee computer security and prevent hackers from intruding. Specifically, it is to build an identity authentication mechanism. When users access resource data and application computer systems, it is necessary to set up user authentication to ensure the authenticity and legitimacy of visitors. Secondly, it is necessary to build an access control mechanism, which includes mandatory access control and autonomous access control. For mandatory access control, the main purpose is to set different security levels for different subjects and objects, and determine whether users have access rights according to the level. Autonomous access control mainly refers to the determination of whether the object has access rights according to the subject setting. Simply speaking, the resource owner can determine whether the resource demander has access rights. In this way, it is bound to effectively enhance the computer network security factor, and further optimize the operating environment.

The other is to optimize system access control to build a robust protection platform for computer networks. The first is to establish access control to the network, refine the location and time of the network, and build the first layer of protection for network security. Secondly, establish network server security control measures, set network management personnel access to the system directory, and eliminate the application of other personnel. And set up the server so that it can only be installed from the system directory; again establish a two-tier mechanism, the inner layer mechanism is used for blocking, and the outer layer is responsible for filtering. Moreover, a separate area should be vacated between the internal and external, which provides space and assistance for the internal firewall function. See Figure 2 below. Finally, encrypt important files, block the hacker's access to information and intrusion, and maximize the computer. Network resource security.

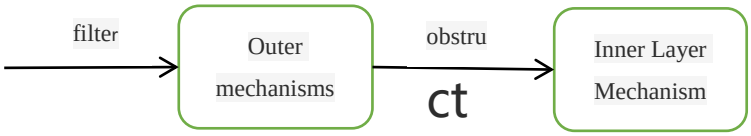


Figure 2 Two-tier mechanism

## 5. Conclusion

The continuous popularization of computer network technology has brought great convenience to people's life and work. However, due to the influence of some factors and the improper operation of computer networks, some network security risks are caused. From this perspective, we can start from the aspects of strengthening user network security awareness, vigorously promoting anti-virus

software and setting network access rights, and formulating effective security management measures to effectively improve the security and stability of computer networks and provide a network for the majority of Internet users. The high-quality network environment has pushed the development of computer networks to a higher level.

## References

[1] Wang Mu. Hidden dangers and Countermeasures of computer network security under the background of “Internet +” [J]. China new communications, 2019,21 (13): 138.

[2] Chen Wenyang. Research on the hidden dangers of network information security of government agencies in the Internet+ era and countermeasures [J].China New Communications, 2019, 21(12):144.

[3] Wang Zhiwei, Fan Wei. On the hidden dangers of computer network information security and suggested countermeasures [J]. Electronic World, 2019 (11): 62-63.

[4] Li Xuesong. Research on hidden dangers and management of computer network security [J]. Wireless Internet Technology, 2019, 16 (11): 28-29+42.