Pisco Med Publishing

*Original Research Article*

# Data and Information Security Technology in Network Communication

**Mengqi Li***

Network Security Technology Research Co., Ltd. E-mail: mq@163.com

***Abstract:*** With the continuous innovation of science and technology, data and information security technology is widely used in various industries. The application of this technology can obviously enhance the security of network communication. This article discusses the significance and insecurity of network information security, and puts forward some measures for protecting data and information security for the reference.

***Keywords:*** Network Communication; Data and Information Security; Security Technology

## 1. Introduction

The computer network system under the network environment is not only easily affected by internal systems and hardware, but also by external environment, human factors, hacker attacks, virus intrusion and other factors, which makes it difficult to ensure its communication security. Moreover, the opening of the network environment and the complexity of network information give birth to more network security problems, which is not conducive to the establishment and maintenance of computer network communication security environment. Based on this, this article introduces the concept of computer network communication security, analyzes the causes of security problems, and puts forward further preventive methods to ensure the security of computer network communication under the network background.

## 2. The concept of computer network communication security

Under the background of network, the security of computer network communication is not controlled or affected by a single factor. The realization of computer network communication security must rely on the joint action of many factors such as technology, system, software and management. In short, the computer network system is an interconnected whole, containing a large amount of private information of users, network information, service items of different network operators, etc., which form a huge public database[1]. Therefore, in order to ensure the security of computer network communication, it is necessary to ensure the security and reliability of each internal connection component. Then a perfect computer network communication security prevention scheme can be formulated to ensure the normal and safe operation of the computer network system.

## 3. The main reasons of security problems in computer network communication


doi: 10.18282/jnt.v2i2.1102

### 3.1 Instability of the computer network system

At the era of network, computer network has become a part of people's work and life, and whatever they do cannot be separated from the support and help of computer network. However, the occurrence of security problems in computer network communication brings about doubt on the stability of computer network system. One of the reasons for the potential safety hazards of computer network communication is the lack of virus prevention and key protection measures, which brings opportunities for hacker attacks, virus intrusion and power failure accidents. The fundamental reason for the instability of the computer network system is the lack of stability of the computer system[2].

### 3.2 Hacker attacks

In history, there have been many computer security incidents caused by hacker attacks. It is widely known that the impact of hacker attacks is usually devastating, which is often difficult to reverse and change[3]. The computer system attacked by hackers can not only run according to the user's consciousness, but also face the danger of breakdown. Because the operation mode of hacker technology is relatively hidden, it is more likely to be the target of attack when the computer system has no security protection. Users may be attacked by hackers when receiving emails every day, causing breakdown of the computer system.

### 3.3 Network viruses

Generally speaking, the invasion of computer network system by network viruses is of obvious extensive characteristics. Once infected by viruses, the computer network is difficult to operate normally, and cannot be connected to the network. The target of computer viruses is wide and in a large range. Once infected with a network virus, the internal system of the computer and the network environment will be severely damaged, and it will spread very fast in a short time, which will bring serious faults to the computer system.

## 4. The strategy of applying data and information security technology in network communication

### 4.1 The application strategy of network authentication technology

At present, in the process of logging into the network platform to carry out various network activities, network users need authentication in most cases. The most commonly used authentication methods consist of user names and login passwords. From the perspective of the structure of this network authentication technology, the user's name and password are separated from each other, with no connection. Therefore, it can be avoided to the greatest extent that the user loses the password[2]. In addition, for the convenience of users, a one-time login interface will be provided in the network communication platform, which can only play a role in a short time. Once the time limit is exceeded, users will be forced to quit the communication platform. This is also a very important way to assist in verifying the identity of users at this stage.

In addition, with the development of network communication technology, fingerprint and face authentication is increasingly applied to the development of network authentication activities. The basic principle of this authentication method is to verify the identity of users by taking advantage of their own particularity. Essentially, as people's fingerprints and faces cannot be forged, this authentication method not only has higher security, but also has higher authenticity, which can greatly reduce the probability of users' information being stolen. In the process of transmitting fingerprint information to the network, it is usually necessary to do a good job of marking and encrypting related information. On this basis, it can effectively prevent the users' network information from being attacked by criminals. While encrypting this kind of information, it is necessary to ensure that the person receiving the relevant information is the designated one. The important information needs to be transmitted in the encrypted form in the network environment. On this basis, the information security can be guaranteed to the maximum extent. That is to say, it can effectively avoid attack to the user network system by criminals and prevent the user network information from being stolen.

At present, the authentication method of user name and password has been widely used in major network commu-

nication platforms, which can guarantee the information security of users to a certain extent. However, there are still some defects in daily application, including a high probability of users' related information being stolen. So, this kind of authentication method is often used to protect non-important information. With the development of mobile payment technology, more and more users are used to mobile payment in the process of participating in commercial activities. In order to ensure the security of users' property information, fingerprint authentication and face authentication are widely used. These two types of information are non-replicable. Therefore, the information security of users can be guaranteed to the maximum extent, and the probability of users' information being stolen can be reduced. In general, face authentication technology and fingerprint authentication technology are often used to protect important information, which has very important practical significance for users' information security.

## 4.2 Application strategy of network encryption technology

During the development of network communication activities, the application of network encryption technology is becoming more and more extensive, which includes not only the contents of password setting in daily life, but also the operations of information encryption. When applying network encryption technology to ensure the security of network data and information, usually, the network encryption method needs to be selected according to the actual situation. Among them, the most commonly used one is the link encryption technology. The physical layer processing method is the most commonly used in the actual process of processing link layer data, which can effectively solve the problem that only single data can be encrypted in the previous application process of network encryption technology. It can realize the simultaneous encryption of data at both ends, thus protecting the data information of users.

In the actual process of information transmission, in order to ensure information security, it is a prerequisite to do a good job of information encryption. Encryption processing of information needs to be carried out according to the actual information transmission needs, including select proper processing methods. On this basis, it is ensured that the information to be transmitted can reach the predetermined position. Usually, the arrangement work needs to be carried out according to the corresponding data blocks when arranging data information. While building data information blocks for the first group, other data block information also needs to actively participate. Based on this, data blocks with their own personality can be gradually formed. The application of this technology can effectively avoid the tampering of user' network data information and maintain the security of users' network information.

From the present situation, apart from data information being stolen, another problem that affects users' network information security is information being tampered. Once information is tampered, individual users can't log into the network communication platform, while criminals may publish some illegal information by logging into it, which brings serious troubles to users' personal life. As for enterprises and government users, when the relevant data and information are tampered, the development of government and enterprise-related work will be affected accordingly, even causing greater losses in serious cases, which is very unfavorable to the maintenance of social stability.

## 4.3 Application strategy of IP address protection technology

It is necessary to strengthen the management of network switches, and do a good job of management and control. On this basis, the effectiveness of information transmission in the tree network should be improved. In the process of actually transmitting data information, the switch is usually set at the second layer of the IP structure to effectively protect the user's IP address. In addition, in order to effectively ensure the safety of data and information in network communication activities, it is also a very important aspect to protect routers, though which access addresses can be made clear. Then it can effectively reduce the occurrence of criminals attacking users' IP.

To protect users' IP security, the physical layer is the most basic breakthrough point. A clear network information control standard should be established on the premise of users' need to transmit network information. During network communication transmission activities, the influence of natural factors and human factors cannot be ignored, especially in the process of collecting network information, it is necessary to make clear the method of installing network control chip. Based on this, rationally set data information, and do a good job in optimizing the configuration of data collection

and data information transmission. Information transmission in physical layer and network layer is often carried out by the means of traffic control or data detection in most cases. Then, the security of link layer information in network system can be guaranteed. The processing and replying error data is mainly carried out in the transport layer so that the authenticity and accuracy of data information transmission are effectively improved.

In practice, IP protection technology is the most basic means to protect users' related data and information, as it can accurately identify users' identities. If the common IP addresses are changed when user carry out communication, it can remind them, so that users can find risks at the first time and deal with them in time to avoid greater losses.

# 5. Conclusion

To sum up, data security is a key issue that technicians need to pay attention to in network communication activities. Once a user's data and information is in danger, it will cause great losses to enterprise users and government users, while it will cause many troubles to individual users. Therefore, it is necessary to apply data information security technology reasonably to ensure the data security of users, so that the convenience of network communication technology can be brought into full play and its adverse effects can be avoided.

# References


1. Li L. Analysis of data and information security technology in network communication (in Chinese). Network Security Technology and Application 2019; (8): 76-78.
2. Han X. Analysis of data information security technology in network communication (in Chinese). Science and Technology Wind 2019; 369(1): 188.
3. Wang J. Brief introduction of data and information security technology in network communication (in Chinese). Digital Users 2019; 25(10): 173.
4. Gao C. Research on data and information security technology in network communication (in Chinese). China New Communications 2019; 21(9): 170.
5. Liu J. Research on network communication technology and information security (in Chinese). Digital Communication World 2017; (8): 157.