Research on Data Confidentiality and Security of Computer Network Password

Hanyu Liang1,*

1Public Basic Teaching Department, Hezhou University, Guangxi, Hezhou, China, 542899

*Corresponding author e-mail: liang_hy@163.com

Abstract. In the wave of computers and the Internet, people's production and lifestyle have been significantly changed, and many traditional offline economic activities have been gradually replaced by convenient online technologies. However, due to the particularity and complexity of the Internet structure, a variety of network security problems emerge in endlessly, among which the leakage of network password is the most serious. The security of network password is related to people's information security and property security, so it is particularly urgent to explore efficient and reliable measures to protect network password. Therefore, this paper analyses the current network password security problems, and explores the feasible measures of network password data encryption and protection, which provides a new thinking direction for the research of network password security.

Keywords: Network Password, Data Encryption, Security

1. Introduction

The 21st century is an era dominated by computer and Internet. People enjoy the convenience brought by the Internet all the time. Computer network is not only an important source of information, but also an important platform for communication, entertainment and consumption. Many economic activities, such as online shopping, the hotel reservation, contract signing and so on, have moved from offline to online in large scale. With the gradual deepening of people's dependence on computer network, the security problem of computer network password has become increasingly prominent. If the network password can-not be effectively protected, then people will face a huge threat when using the computer network. Therefore, the scientific community and Internet enterprises should fully realize the importance of network password and flexibly use various security technologies to protect network password, so as to create a healthy and safe computer network environment.
2. Security problems of computer network password

2.1. Security problems caused by the improper configuration of the computer system
The system configuration of the computer has a great influence on the security of the user's network password. In some computer systems, the firewall configuration is too low, anti-virus software and other security measures are not in place, which will produce great data security problems [1]. Especially for some computers, due to the low version and configuration of firewall and anti-virus software, the overall performance of the computer can not meet the requirements of its own system configuration. In addition, there are many loopholes in the computer operating system, such as computer communication protocol, web browser, super user use, etc. Once the user operates carelessly, it will easily lead to the leakage of network password when using the computer.

2.2. Security problems caused by computer virus invasion
When users use the computer, if they do not operate properly, the computer is vulnerable to virus invasion and attack, which has become one of the most important security issues of computer network password disclosure. There are many kinds of computer viruses. For most computer viruses, they not only spread rapidly, but also spread in various ways [2]. Most importantly, the virus is very harmful. If the computer is invaded by the virus due to network protection problems or human operation problems, it is easy to make the user's information data leak or lose, which brings great threat and damage to the user's information and data security, and even brings the user's economic loss that cannot be ignored.

2.3. Security problems caused by hacker attacks
In addition to the configuration of computer systems and virus problems, in the current network environment, the most worrying and frightening thing for users is the security problems brought by hacker attacks. In the current network environment, there are some criminals who use superb computer technology to maliciously attack other people's computers, causing problems such as system failures in others' computers. Some hackers may even attack other people's computers to obtain information and data in other people's computers, or modify and misappropriate information in other people's computers. Some hackers will attack other people's computers at will, causing trouble to others. The actions of these hackers not only bring serious information and data security threats to other users, but also may cause serious economic losses.

3. Encryption and protection technology of computer network password

3.1. The principle of network password encryption and protection
Data encryption technology refers to the use of the computer system for network transmission information reorganization to ensure the security of information transmission [3]. Data encryption technology can reduce the probability of data being stolen and tampered, ensure that all data can be transmitted timely, safely and accurately, so as to protect the security of the user's personal data and property. In essence, data encryption refers to encrypting the data transmitted in the network through algorithmic ciphertext. The data receiver can extract the data through the private key, so as to ensure the security of data transmission. The specific principle of data encryption is shown in Figure 1.
3.2. **End-to-end encryption technology**

End-to-end encryption is an encryption and decryption process during the transmission of data from the source point to the end point, and the security of the message is not affected by the situation of the intermediate node [4]. It should be implemented at the transport layer or higher, if you choose to encrypt at the transport layer, the security measures can be transparent to the user. When implementing in the application layer, users can choose the encryption algorithm according to their own situation. In end-to-end encryption, in order to ensure that the intermediate nodes can correctly select the route, the control information part of the protocol data unit cannot be encrypted. In summary, this method is easy to receive traffic analysis attacks.

3.3. **Node encryption technology**

Node encryption technology refers to the use of links as the carrier of technology to encrypt and decrypt the information data to be transmitted through each node [5]. However, although there will be a relatively secure area at the communication node, and the information data is also transmitted in the form of ciphertext, the process of data encryption and decryption is carried out in their respective security areas, which is relatively too simple, easy to be cracked by others, and obtain the information data behind the ciphertext.

3.4. **Digital signature technology**

The current application frequency of digital signature authentication technology is relatively high. For example, digital signature technology is used in the business processing activities of banks. This technology verifies the user's identity information through various authentication methods to ensure the safety of user information [6]. This technology is more intuitive, because neither the sender nor the receiver of information can tamper with the information, which not only ensures the convenience of information transmission, but also ensures the security of transmission.

4. **Security protection measures of computer network password**

4.1. **Implementing key management technology**

The key management technology is to use the password as the basis of network password security protection. In order to ensure the security of the data in the computer, users can use this technology to
set complex passwords, and regularly change the password, so as to ensure that the password is not easily cracked by others. When trying out the database, the key management technology can use different classifications in the database to implement different password protection, so that different types of modules can remain independent, and data can only be obtained when all passwords are entered correctly. Although this method is more complicated, it can guarantee certain security.

4.2. Standardize and rationalize the operation of computers
In order to better solve the security problem of computer network password, it is necessary to ensure that users can use the computer reasonably. Now our common computer system is the Windows series of operating systems, this system itself has certain security risks, so users need to install patches to strengthen and repair the system, thereby further enhancing the stability of the operating system. Users need to regularly check the security of the computer operating system, install patches in a timely manner, and upgrade the computer operating system accordingly to reduce the network password security problems caused by the computer system.

4.3. Strengthen the detection and investigation of computer virus
Now our country has a relatively advanced computer virus detection technology, we need to continuously strengthen the detection and prevention of virus based on this, so as to better solve the virus problem. Computer users can install anti-virus software to regularly check and kill the computer virus. This anti-virus software can integrate the corresponding monitoring technology. When the user uses the computer, it can prevent the possible virus problems, and automatically process and clear some relatively small destructive viruses, so as to effectively ensure the security of the user's network password.

4.4. The combination of static password and dynamic password
At present, computer network users generally use the mode of static passwords to protect the security of network information. To strengthen the security level of this cryptographic technology, an encryption method in which static passwords and dynamic passwords are integrated can be used, as shown in Figure 2. The user can set the dynamic password according to the prompted information, and the data information can be updated by the verification method at the next entry, so that the problem of the static password can be effectively solved.

![Diagram](image)

**Figure 2.** Combination of static password and dynamic password

5. Conclusion
The data security of the computer network password is a key obstacle that computer technology must overcome. This paper discusses several kinds of encryption technology of computer network password, and puts forward the feasible protection measures of computer network password security. However, any technology and measure has its limitations, and the current protection measures may lose their effect
in the near future. Therefore, people must be aware of the severe challenges faced by the security of computer network password, and constantly explore the encryption and protection measures of computer network password, so as to ensure the benign development of computer network.

References

[1] Zeyu Jiang. On cryptography and its role in computer network security [J]. Value engineering, 2020,39 (16): 189-191.

[2] Xiaohu Ge. Application and development of cryptography technology in network information security [J]. Electronic technology and software engineering, 2020 (06): 236-237.

[3] Jianfeng Wang, Yinghui Zhang, Hua Ma. On cryptography and information security [J]. Journal of Xi’an University of Arts and Science (Natural Science Edition), 2020, 23(01): 34-36.

[4] Xiaolong Huang. Discussion on Password Protection in Internet [J]. Engineering Technology Research, 2017(04): 255-256.

[5] Di Li. How to protect passwords in the Internet [J]. China new communications, 2017, 19 (08): 68-69.

[6] Mingbei Jie, Qinglan Ru. Data confidentiality and security in computer networks [J]. Information communications, 2012 (03): 162-163.