Research on Data Confidentiality and Security Protocol in Computer Network

Yizhi Li\textsuperscript{1,*}

\textsuperscript{1}College of Internet of Things, Jiangxi Teachers College, China, 335000

*Corresponding author e-mail: ytxy2015@163.com

**Abstract.** With the development of society, we are going the Information age. With the Internet, we can improve our work efficiency and management level. Because of the Internet, we can chat with others in a new way. However, because of the particularity in the internet, our computer internet meets too many problems, for example, when we surfing the Internet, user privacy was leaked and the transaction process was peeped. So we need to solve these problems, and the best way to solve these problems is to understand these problems clearly. So to get this target, the article tells the concept of computer network firstly, and then writes the problems in Computer Network Security. On the other hand, the article analyzes the computer network information security and security all. After these things, we will make our Internet better and better.

**Keywords:** Network Security, Encryption, Digital Signature, Security Protocol, Firewall

1. **Introduction**

With the quick development of computer network technology, there are many advantages it has laid a solid foundation under the application of the field. With the computer network technology, our public resources can be used reasonably. Chinese enterprises have established their own computer network systems, these systems make these company better and better. But because of the complexity of the network environment, the computer network is easily interfered by hackers or malicious software. This not only affects the normal operation of the computer network, but also the important information in the enterprise may be leaked and brought to the enterprise, even give the enterprise unnecessary losses. So how to protect data security in computer, is an important problem.

2. **The nature of computer network information**

Why Internet can be wide spread and spread to people's lives in a short time, the reason is: it is inseparable from its own characteristics and the development of the times. We has entered an information age, and the main way for people to communicate is through the network. And Computer networks have the following properties:

2.1. **Reliability**
Enterprises will design computer network software according to their own business model and business philosophy, with these things, the employees can use computers to complete the tasks assigned by enterprises, and enterprises can also monitor the dynamics of employees going to work. Under certain conditions, even if the computer network is disturbed by external conditions, it can enable employees to work normally, and this is also the reason why enterprises choose computer network.[1]

2.2. Security
Computer network can protect users' privacy well, but some software must be opened by user himself. This can effectively place the leakage of user privacy, so that users can have their own private space in the network.[2]

3. Risks of computer network data
Because of its special conditions, computer network will be disturbed by many factors. There are many risks in computer network data. We can analysis it in these aspects.

3.1. Hackers are powerful in technology
In the computer network risk, the hacker attack can directly lose the data in the computer. Especially for large enterprises, there are many important documents in the enterprise computer system. So in order to get the internal documents of the enterprise, many competitive companies will use hackers to attack the enterprise. They input the corresponding instructions and codes into the computer to damage the basic functions of the computer network and spread some data, which affects the normal use of the computer network.[3]

3.2. Virus invasion
Viruses invade computers with a certain latency, and once outcropped, they are extremely destructive. Viruses are the strongest source of network infection, with a wide variety, rapid spread, needless to say, harmfulness and super difficulty in governance. For example, Trojan horses, earthquake nets, flames and other viruses are transmitted through the network, and their controllability is very poor. Once a computer is attacked by a virus, its data and security will be threatened.

There are many rubbish email in our Internet, this is the computer network risk beyond our control. And the virus will also be hidden in these emails. As long as you click, the virus will directly invade your computer. When we browse the web, spam will jump out and occupy your sight at any time, and accidentally clicking will even make the system be jammed. On the one hand, rubbish email will occupy a large memory of the user's computer, on the other hand, rubbish email will threaten computer data.

4. Computer network information security technology
With the development of the times, to prevent data theft, we will use certain security technology. We mainly use physical or chemical protection to prevent data leakage.

4.1. Key management technology
Key management technology is the use of password settings, it uses passwords as a basis for security, and use password settings to ensure data security in computers. Key management technology can set complex passwords, and can also change passwords regularly, only in this way can the password be protected from being easily cracked by others. In addition, when we try the database, we can use different classifications in the database to implement different password protection, so that different types of modules can remain independent. Under such technical protection, only when we match all passwords can we obtain data. Although this method is complicated, it can guarantee a certain degree of security.[4]

Although the use of keys can strengthen our management of related data, the acquisition of keys is also the first step for hackers to steal data, so preventing hackers is something that every one of us must be conscious of when surfing the internet. The most direct way to prevent hackers is to set relevant keys
and provide effective protection reminders through firewalls. For some malicious attacks and damages on the network, we should find professionals to guard against them at the first time to ensure that our personal information will not suffer a greater crisis. (As shown in Figure 1)

![Figure 1. Key management technology](image)

### 4.2. Digital signature technology

Because of the complexity of the key itself, the use of digital signature technology can make our work more convenient and fast. We only need to connect our own digital signature to the relevant files. If we don't have our own signature, we can't open the relevant information. Digital signature can generate a series of key chains in the network and pair them with data. Only the key chains you master can open the data. Therefore, on the whole, digital signature will be more convenient than key, but it will cause trouble if I am absent or when others need data.[5] (As shown in Figure 2)

![Figure 2. Digital signature technology](image)

### 4.3. Use firewall to prevent virus

Firewall is a special router, which separates the internal network from the external network, monitors the incoming and outgoing information, and implements access control. Specifically, it is to forward reliable data packets, discard suspicious data packets, and only let safe and compliant information enter the internal network. The firewall is like a barrier between the internal network and the external network, which prevents unexpected and potential damage from invading the user's network and provides a safe network environment for network users. Logically speaking, firewall is a separator, limiter and analyzer, which can simplify network security management, effectively monitor the activities between intranet and internet, and ensure the security of internal network. From the perspective of implementation, firewalls can be divided into hardware firewalls and software firewalls. Hardware firewalls are realized by combining hardware and software, while software firewalls are realized by pure software. General firewalls can filter out unsafe and illegal services, prevent intruders from approaching the internal network, limit internal users' access to special sites, and provide convenience for monitoring the security of the Internet. If we don't have a firewall, then every host in our whole network will be directly under attack, so the risk to our computer is too big.[6] (As shown in Figure 3)
4.4. Network security protocol

At present, there are a variety of network security protocols to protect the security of network information. The most common IP protocol can encrypt all data in IP datagrams and also provide source authentication services. Among IP security protocols, the two most important protocols are authentication header AH protocol and encapsulation security payload ESP protocol. Among them, AH protocol provides source authentication service to ensure data integrity, while ESP protocol can also provide encryption service. SSL protocol is the foundation of transport layer security protocol TLS, which is not only compatible with common browsers and Internet servers, but also can be applied to IMAP mail access. PGP protocol was put forward in 1995. It is a complete e-mail security software package, including encryption, authentication, electronic signature and compression technology. The function of PEM protocol is similar to PGP protocol, which can encrypt and authenticate e-mail, but its key management mechanism is more perfect than PGP.

4.5. Intrusion detection

Intrusion detection is a technology that discovers and reports unauthorized operations or abnormal phenomena in the system. Intrusion detection is mainly used to monitor violations of security policies in the network, and it can identify all unwanted activities. In addition to ensuring low false alarm rate and false alarm rate, intrusion detection system also needs fault tolerance and good scalability. (As shown in Figure 4)

4.6. Key distribution

Because the cryptographic algorithm is open, the security of the password lies entirely on the protection of the key. Our demand for key protection makes cryptography an important research field, this important field is the distribution of keys. Key distribution is the biggest problem in key management, we must distribute it through a safe passage. With the increase of network users and traffic, the key must be changed frequently. The main method of key distribution is to set up a key distribution centre, which temporarily distributes session keys to secretly communicating network users. At present, the most
effective key distribution protocol is Kerber-os developed by Massachusetts Institute of Technology, which uses AES encryption algorithm which is safer than DES algorithm. (As shown in Figure 5)

![Key distribution diagram](image)

**Figure 5.** Key distribution

**5. Conclusion**

In real life, with the rapid development of new products and technologies, the preventive technologies and safety measures we adopt today may not meet the safety requirements tomorrow. Any prevention technology has limitations, and we can't guarantee absolute safety. The security of computer data is very important for every person, we should vigorously publicize the security of network data, so that every person can enhance their awareness of information protection. We should not arbitrarily publish personal real information in social networking sites, and use keys or digital signatures in computers to install firewalls. Each of us should do these things to ensure our own security in the network.

**References**

[1] Chen Xinwen. Computer network cloud computing technology [J]. Computer knowledge and technology, 2015, 11(31):10-11.

[2] Jia Qianwen. Talking about the idea of enhancing the security and confidentiality of computer database [J]. Reading and Writing Computing (Education and Teaching Research), 2014(17):118-118.

[3] Xie hongda. Application of data encryption technology in the field of computer network security [J]. Digital technology and application, 2013(08):176-176.

[4] Xie Xiren. Computer Network (5th Edition) [M]. Beijing: Electronic Industry Press, 2008, 1.

[5] Matt bishop. Computer security: art and science [m]. Beijing: Tsinghua University Press, 2004, 5 (1st edition).

[6] Dong Xuewen, Niu Wensheng et al. Extension of anonymous formal analysis based on string space [J]. Journal of Communication, 2011, 32 (6):124-131.