Discussion and Analysis of Computer Information Data Security and Encryption Technology

RongBin Hao
Sichuan Judicial and Police Officers Professional College, Deyang, 618000, Sichuan, China

Abstract: With the continuous development of science and technology, Internet technology has become more and more mature, and the advantages of actual information technology have gradually emerged. In the development of such technologies, it can also provide new opportunities for the promotion of computer network technology. This article summarizes the security threats of computer information data based on previous work experience, and discusses the application form of encryption technology in computer information data includes seven aspects: data encryption technology, key management encryption technology, confirmation encryption technology, storage encryption technology, transmission encryption technology, message digest technology, and integrity authentication technology.

1. Introduction
At this stage, people are increasingly researching computer technology. When people use computer technology to provide convenience for production and life, they also turn their attention to the field of computer network security. How to do the related safety protection work is the content that the staff needs to focus on. In addition to strengthening their own network security performance, various computer companies must also strengthen the audience's security awareness and the protection of personal private data. Only in this way can we build a more harmonious and safe Internet environment.

2. Significance of Computer Data Security Protection

2.1. Technical Level
Up to now, computer information technology has been widely used in people's daily lives. As can be seen from the development of many small and medium-sized enterprises and production institutions, computer information technology plays an irreplaceable role in actual operation and can also improve its work efficiency. From another perspective, if there is a problem with computer information technology, the enterprise will also suffer huge economic losses, and the actual service work cannot be carried out normally. During the operation of an enterprise, if problems occur in the processing of computer information technology and are attacked, at this time, the relevant departments need to formulate management measures for the characteristics of computer information to keep the enterprise in normal operation.

2.2. Production Level
In the current development process of SMEs, many business activities require the support of computer technology. If more serious technical problems arise, the normal development of the enterprise will be
greatly hindered. Therefore, all enterprise organizations should do a good job of computer information
data security protection and strengthen production efficiency.

3. New Features of Computer Network Security

3.1. Identification
With the continuous development of computer technology, people began to pay attention to the
security of their information and data. At the same time, many traditional security measures have been
unable to match the current security requirements. Data leakage and theft have occurred frequently,
and we urgently need to improve them. The emergence of new features of computer network security
has effectively solved the above problems. One of the most important features is identity recognition.
When users operate computers, they need to pass the audit of the computer network system. Only in
this way can information be tampered with and lost, and the probability of network attack problems
can be reduced.

3.2. Computer Network Security System Identification
It can be seen from the operation of the computer network system that most of the information and
data involved are stored in the network space. In order to avoid problems such as data corruption,
people can back up important data. Once the data is found damaged or stolen, it can be restored by
means of a computer network security identification system. Through the backup operation of data
information, the problem of data and information loss can be completely solved, which also makes it
an important content among the security features of computer networks. In order to further meet the
computer data security requirements, the relevant staff can also design corresponding functions in the
operating system, such as saving, sharing and copying. With these functions, users can make better use
of data information and operate more conveniently, enhancing the security performance of the entire
computer network system.

3.3. Encryption of Computer Data and Information
In recent years, China’s computer network technology has achieved better results, prompting more and
more computer application fields and continuous improvement of application strength, which also
makes the maintenance of information and data security more important. For this reason, during the
operation of the computer system, a complete data encryption system needs to be equipped to maintain
the security of all data. At the same time, in order to further strengthen data security, we can combine
laws and regulations to do a good job of reviewing information data and design corresponding
protection systems. Users who want to obtain data should enter the correct password to ensure the
absolute security of information.

4. Computer Information Data Security Threat

4.1. Human Error
The application of computer technology has made social production and life more intelligent, while
also reducing people's work burden and strengthening work efficiency. However, the operator of the
computer itself is a human, and operation errors are unavoidable, which leads to computer failure,
resulting in loss or leakage of information and data. In order to avoid such problems, related
companies need to do a good job in introducing and cultivating computer talents, and systematically
manage them, strengthen their operational capabilities and operating standards, avoid more mistakes,
and set up special supervisors.

4.2. System Error
Computers generally run for a long period of time and are prone to problems such as hardware aging
or damage, which in turn leads to systemic failures and increases the risk of information data loss and
leakage. Therefore, users should regularly upgrade and improve computer hardware facilities, and carry out computer operation and maintenance work. For the maintenance of the computer room, common maintenance measures include filtering decoupling, electromagnetic shielding and electromagnetic isolation to avoid electromagnetic interference problems, keep the computer in a safe and stable operation state, and avoid more failure problems.

4.3. Malicious Intrusion
For the impact of computer data security, human factors dominate, which includes not only the operation errors of internal personnel, but also the malicious intrusion of external personnel. The so-called malicious intrusion mainly refers to the use of computer viruses by criminals to damage computer systems, which in turn leads to the theft and destruction of information and data, and seeks illegitimate benefits from them. For example, in May 2017, the WannaCry ransomware virus broke out, which involved many fields, such as finance, energy, resulting in the computer system not working properly. There are many similar to the above-mentioned incidents. Some criminals steal viruses and steal personal users' information and materials, causing great economic losses to users. To this end, users need to install reliable protection software in the computer system to prevent viruses and Trojans, so as to eliminate hidden dangers in time.

5. Application form of Encryption Technology in Computer Information Data

5.1. Data Encryption Technology
In the actual application of data encryption technology, it is mainly through the use of encryption algorithms to effectively process the data and convert the data into ciphertext form. If a hacker hacks into the computer, the data cannot be tampered with or cracked because it does not have the key, so as to protect the data and strengthen the security of the computer. For example, most of my country's online banks have applied data encryption technology to encrypt the information data involved. This technology has been applied from the client to the server, forming a layer-by-layer encryption protection mechanism. In this way, online banking can be effectively guaranteed, and it can avoid huge economic losses caused by hacking. Generally speaking, the key to the application of data encryption technology is the key. Although the algorithm is relatively easy to determine, it can generate many keys to realize the dense cultural processing of information data and strengthen the degree of information security.

5.2. Key Management Encryption Technology
It can be seen from the actual information security management work execution process that the actual key management technology and confirmation encryption technology can improve information security. Among them, the key management technology mainly relies on key media to strengthen the management of information data, so that the information data is always in a safe state. In addition, the materials of the storage and disk in the key media are semiconductors, which is also the basic structure of the key media, which can make the security management more perfect. In general, the key management technology comes from the cooperation of multiple layers of keys, starting from the aspects of generation and storage, and doing a full range of information management operations. Only in this way can the positive role of key encryption technology be presented.

5.3. Confirm Encryption Technology
Confirm that the main function of encryption technology in the application process is to limit the scope of reading data reasonably, and then to display the role of maintaining information security. In general, confirming data technology skills to maintain the security of stored information can also prevent information from being tampered with and applied, fundamentally express the purpose of protecting information, and strengthen the accuracy of information. At the same time, it is necessary to verify the source of information effectively to highlight the source of counterfeit information to avoid
problems such as information leakage. From another perspective, the confirmation encryption technology can also ensure the data system to confirm the legal identity of the user with the highest efficiency, which is also the root of the digital signature and information confirmation functions. For example, when the online banking system is running, digital signature encryption technology is often applied, and user information verification is done. The process of actual information verification is also the process of decryption.

5.4. Storage Encryption Technology
The improvement of actual storage encryption technology is one of the most important components in encryption technology. The application of this technology can ensure that information data is not subject to any attack and maintain the storage security of information. In general, the most common storage encryption technologies include two types, one of which is to perform information data ciphertext storage for information content, and the other is to perform information data storage control operations for user behavior. In general, when the ciphertext storage technology comes into play, it mainly uses the encryption module to carry out encryption protection work. The actual storage control is also based on the user's reasonable control of data access, to avoid data from being invaded by criminals, and to eliminate access to data. Various misconducts. With the help of the above operations, the security protection effect of computer information data can be better presented, and the protection of information data has become more comprehensive. In order to maintain information security without any impact, people also need to innovate and improve computer storage encryption technology, clarify the latest forms of attacks and viruses, and update preventive measures to keep computer systems in a safe state of operation. For example, Santoku is a python script based on Linux system, which can crack Android 4.4 full encryption. It takes about 30 minutes to brutally crack the 4-digit pin code on Core i7 CPU. Therefore, compared with the bkdf2 scheme, the crypt scheme greatly improves the difficulty of cracking.

5.5. Transmission Encryption Technology
The most common transmission encryption technology mainly involves two types, namely end-to-end encryption and line-to-end encryption, which is also the process of encrypting data. For example, during the implementation of encryption technology between lines, due to the large amount of data, multiple keys are required to perform data processing operations. This way, it is possible to prevent criminals from obtaining all data after stealing a key. For the encryption technology between the ends, the data at the transmitting end can be encapsulated by the encryption operation in advance and sent to the host in the form of a data packet. When the host receives all the data packets, it will automatically perform the decoding operation. The data of the sender is transferred to the receiver, so as to effectively transfer the data information.

For example, in the features of bmc200 series encryption communication gateway products, it can be seen that it can support LTE / 3G / PPPoE / DHCP / static address and other communication modes, wired and wireless backup each other, and also support IPSec VPN, L2TP VPN, PPTP VPN, open VPN. See Figure 1 for details.
5.6. Message Digest Technology

In the actual information transmission process, the message digest can ensure that the user returns the reliable value when transferring the information. Then, with the help of the application of the encryption function, the accurate analysis and budget of the message are realized, which is also the fundamental process of generating the message digest. In the actual data transmission operation, the sender can use the computer key to encrypt the message digest. When the computer user receives the message, it will also perform a key decryption operation to compare the message with the content sent by the sender to see if it is in a consistent state. Only in this way can the security characteristics of information data be presented and perfected Basic functions of computer network. For example, with the help of hash for information digest encryption operation, at this time, the hash value has obvious randomness characteristics, and it is difficult to be attacked. Therefore, during transmission, the staff can keep the hash value and the data value in a one-to-one correspondence state. When the sender performs digest encryption, it can also use the private key to strengthen the use of confidential
technology to check the accuracy and legitimacy of the data to avoid the integrity of the information being affected.

5.7. **Integrity Authentication Technology**

It can be seen from the specific computer application process that information data often has a higher risk of theft during transmission, and is also accompanied by omissions. In order to ensure the completeness of the information, the relevant staff can use the complete identification technology to realize the effective inspection of the data. At this time, if you want to better show the role of authentication technology, the relevant staff can enter specific feature values and data in the message system. Only in this way can we meet specific information security needs, maintain high-quality data transmission, and maintain the integrity of data structures. It is also because of the application of integrity authentication technology that makes computer information data appear more secure.

6. **Conclusion**

In summary, the application of Internet technology has brought about great changes in people's lives and work styles, but it should be noted that there is a huge security risk in computer information data security, and there are many reasons for this type of problem. In order to strengthen the security of network data, the implementation of computer information data security encryption work is particularly important. At the same time, the staff must also make innovations in this technology to avoid the impact of information data security.

**References**

[1] Guo Weitao. Brief analysis of the application of data encryption technology in computer network information security[J]. Network Security Technology and Application, 2020(05):48-49.

[2] Luo Songjie. Application Research of Data Encryption Technology in Computer Network Information Security [J]. Volkswagen Standardization, 2020(08): 211-212.

[3] Yang Mancang. Application of data encryption technology in computer network information security [J]. Science and Technology Information, 2020, 18(11): 8-9.

[4] Zhao Yunpu. Research on Data Encryption Technology in Computer Network Information Security [J]. Communication Power Technology, 2020, 37(06): 113-114.

[5] Wang Yajun. Exploring data encryption technology in computer network information security [J]. Satellite TV and Broadband Multimedia, 2020(05):59-60.

[6] Yang Shuming. Data encryption technology in computer network information security [J]. Computer Knowledge and Technology, 2020, 16(06): 36-37+40.