Research on Application of Data Encryption Technology in Computer Security

Che Liu, Yunpeng Wu

School of Information Engineering, Zhengzhou University, Zhengzhou, Henan, China

Keywords: Data encryption technology, Computer security, Application study

Abstract: With the continuous development and progress of science and technology, computer technology and Internet technology have gradually become popular, and computer network technology has become an indispensable part of people's lives. In people's daily life, work, and students' learning It plays a crucial role, not only bringing a lot of convenience to people's lives, but also bringing great help to people's work. In recent years, computer technology has been widely used in various industries. While computers have brought us convenience, they have also brought great security risks to our information and data. With people's emphasis on computer security and the increasing role of computers, the application of data encryption technology in computer security has attracted attention and attention from all walks of life. At present, there are many professional articles on the application of data encryption technology in computer security. Therefore, this paper makes an in-depth analysis of the application effect of data encryption technology in computer security.

1. Introduction

With the innovation of computer technology, the level of network communication security requirements has risen. At the same time, various types of network information theft and destruction have also made the demand for computer security in various fields of society increasingly strong. In general, computer information security includes two levels of requirements: on the one hand, the storage security requirements for computer information; on the other hand, the communication security requirements for computer networks. In the threat to computer security, human factors have a much greater impact than non-human factors. Human security threats are divided into passive attacks and active attacks. Among them, passive attacks mainly affect the confidentiality of computer data. There are six commonly used methods: one is the theft and interception of information transmitted on communication lines; the second is the data analysis of the theft and interception; the third is impersonating the identity of the user; the fourth is against The information transmitted on the network is tampered with; five is refusal to confirm the information sent; six is other means.

2. Overview and Algorithm of New Data Encryption Technology

If you want to meet the information security needs of all computer workers, you must grasp the nature of data encryption. The data encryption system includes four main parts: ciphertext, plaintext, key, and encryption algorithm. The structure of the model composed of these four parts is as follows: There are many technical classification methods in the encryption process, but the traditional classification method is divided into two types of symmetric and asymmetric key decoding technologies according to the characteristics of the key. The ciphers in symmetric key decoding technology can be divided into sequence ciphers and block ciphers. The encryption method can be divided into three types: node encryption, end-to-end encryption and link encryption. The AES algorithm uses multiple sets of key bits: 128-bit, 192-bit, 256-bit, and uses 128 bytes for block encryption and decryption. The traditional key uses the same encryption and decryption data, and the returned data after using the block cipher is the same as the input data. Next, the structure of the loop is used for iterative encryption, and the input data is repeatedly replaced and replaced in the loop. The following figure shows the AES encryption and decryption process. This encryption

  DOI: 10.25236/ictmic.2020.029

algorithm uses a 128-byte square matrix grouping and copies these square matrices to the state array. Each time the encryption step is performed, this state array will change until the last step, the generated state array will be copied. Is the output matrix. In a 128-byte square matrix, the 44 words of the subkey (4 bytes per word) are sorted by column.

The steps of the AES algorithm are mainly divided into four steps: byte replacement, row shift, column mixing, and round key addition. (1) Byte replacement. Use the S-box to replace the above-mentioned packets one by one, in which the 4 high-order bits in the S-box represent row values, and the 4 low-order bits represent column values. The corresponding elements in the table are output values. This step shows the non-linear characteristics of the AES encryption algorithm, which can effectively avoid simple algebraic attacks. (2) Row shift. Using the above grouped list, each row is shifted left by a certain offset. For example, if the first line in the S-box is fixed, the second line can be rotated by a byte offset. Then after all the cyclic shifts are completed, all the columns in the grouping list are combined from the elements in different columns. Each shift is a linear multiple of 4 bytes. (3) Column mixing. After completing the above-mentioned linear transformation of the grouping list, relatively independent operations will be performed for each column. This operation is to use the four elements of a single column as coefficients, merge them into a certain polynomial in a finite field, and use this polynomial and a fixed polynomial to perform a multiplication operation. This process can also be regarded as matrix addition and multiplication operations under the condition of finite fields. After several rounds of row-shifting and column-mixing transformations, all input bits in the grouped list are related to output bits. (4) Round key addition. In the process of row shifting in the second step and column mixing in the third step, each time a key group is generated by the master key, the round key group is the same as the original byte grouping list. The fourth step is to XOR the corresponding elements in the original matrix. Although this cryptographic transformation process is simple, it can affect every element in the grouping list, and the complex extensibility and complexity can effectively improve the security of the algorithm.

3. Factors Affecting Computer Security

According to the current form, most computers are mainly based on Microsoft's Windows system, so the unity of the system naturally becomes the main target of hacking. With the continuous improvement of people's requirements for computer network technology, the vulnerabilities in Windows systems have gradually been exposed, which has caused serious threats to the security of computers and has become the biggest hidden danger. If a hacker implants a virus through a vulnerability in the Windows system, it can control the computer of a financial enterprise in an all-round way, and the data in the computer can be stolen and modified, which seriously affects the security of the computer during use. The Windows system is a very large system. Even with a high level of technology, there will still be certain security issues during the system design process. This is why Windows systems often have some patches to comprehensively address these vulnerabilities The nature of the repair is mainly to improve the security of the computer and the confidentiality of the data, so according to the current system situation, it is not absolutely safe in the Windows system.

With the continuous development and progress of the social economy, computers have continued to be popularized in various fields. According to the current situation in China, most families and units in China already have computers. In people's lives and work, computers have been Plays a crucial role and impact. However, while the Internet brings convenience to people, it also brings certain security risks to people. No matter what kind of loopholes appear in the Internet protocol, it will lead to the implantation of Trojan horse viruses in the system. These viruses will follow the data. The file transfer and the direct implantation into the calculation, once the user triggers the virus during the use process, the computer will be infected by the virus, which poses a serious threat to the security of data information in the computer. At present, in many of my units and enterprises, data warehouse systems are used when storing related information, and the data warehouse system itself has many security risks. If there are certain loopholes in the structured language, hackers will

use the loopholes as a starting point to directly find the location of the data warehouse, and will copy the information used in it, which will cause serious economic losses to the enterprise to a large extent. Especially for some Internet companies in China, if the account information of the data warehouse management system is not encrypted, the data in the data warehouse management system is very easy to be stolen, and its consequences are unthinkable.

4. Application of Data Encryption Technology in Computer Security

At present, the more commonly used data encryption tools in the market include disc encryption, hardware encryption, and compression package decompression. Let's start with disc encryption tools. The CD encryption tool is relatively safe and easy to operate. The main principle of the tool is to make reasonable modifications to the image file and use the medium image file on the CD to hide it well. In the process, change the ordinary file directory to the file directory. Can effectively prevent the theft of user information; followed by hardware encryption tools. The hardware encryption tool is simply to encrypt the user's information. It is mainly to use an effective encryption tool on the parallel port of the computer or the USB interface of the computer to encrypt the computer software and computer data, which can effectively protect the intellectual property rights of computer network users; Finally, when using a compressed package to decompress, if you want to obtain the data information contained in it, you must obtain the corresponding password. Therefore, in the actual application process of decompressing the compressed package, while ensuring the confidentiality of data transmission by computer network users, it can effectively prevent third parties from stealing computer network user information and ensure the security of the information.

With the development of information technology networks and the continuous improvement of people's lifestyles, e-commerce has gradually entered people's lives, and people's consumption patterns have also changed. The emergence of e-commerce has not only promoted the development of society, but also Promote Chinese enterprises to go international. At the same time as the development of e-commerce, its network security issues have gradually emerged. If the internal information is lost, the impact will be overwhelming, which will not only seriously damage the company's economic benefits, but also directly affect the user's property. Information security, so it is very important to apply data encryption technology reasonably and effectively in the field of e-commerce. According to the current situation, e-commerce mainly uses the SSL and SET security protocols to comprehensively protect the security of computer systems, and uses digital visas and digital signatures to encrypt computers to ultimately improve e-commerce security. aims.

At this stage, among all data encryption technologies, the key technology is widely used in various fields because of its unique technology. The main working principle of key technology includes two parts. The first part is the encryption of computer network data; the second part is the decryption of computer network data. In general, key technology is mainly used in online shopping for effective applications, mainly because there are two types of keys, the first is a public key and the second is a private key. When shopping online, sellers generally use public keys for encryption. For private keys, the same key is used for data encryption and data decryption during use, so its security is compared. high. Although the security of the private key is relatively high, there will still be many problems in the actual application process. For example, the actual keys used by computer network users are different, and the keys used are also different. In this process, Will seriously affect the computer network system, causing the system to appear some uncertain errors. So in this process, the user can use public keys to solve this problem. In the actual operation process, the user transmitting the data information can use the public key method to encrypt the transmitted data, thereby ensuring the security and confidentiality of the data. By using this method, not only the data transmission process can be simplified, and the types of private keys can be effectively reduced during the data transmission process. In addition, the situation of private key leakage can be effectively avoided.

5. Conclusion

The development prospect of data encryption technology will be very broad, and it will be widely used in all sectors of society. With the continuous development of computer science and the progress of the network, the application of data encryption technology in computer network security has become an inevitable trend of social development. It can not only promote the development of computer network technology, but also ensure the security of data information in computer networks. . However, once the application of data encryption technology has serious security loopholes in the system, data encryption technology cannot guarantee the security of the data. It can only delay the time when data information is stolen, so we must fundamentally improve the computer. The security of data information requires regular updates to the system, timely loopholes, and timely killing of computer viruses. Only in this way can the security and confidentiality of computer data be effectively and comprehensively protection of.

References

[1] Qin Jingwei. Research on Application Value of Data Encryption Technology in Computer Network Security [J]. Science Technology and Life, 2012, 000 (016): 97-97,101.

[2] Zhang Feng. Research on Application of Data Encryption Technology in Computer Network Security [J]. Computer and Telecommunications, 2014 (5): 56-57.

[3] Wu Sujuan. Application Research of Data Encryption Technology in Computer Network Security [J]. Computer Knowledge and Technology: Academic Exchange, 2014 (12X): 8633-8634.

[4] Gao Hui. Research on Application of Data Encryption Technology in Computer Network Security [J]. Science and Technology Innovation, 2018 (13): 62-63.

[5] Li Li. Research on the Application of Data Encryption Technology in Computer Network Security [J]. Youth and Youth, 2017 (3): 539-539.

[6] Zhu Qiang. Application of Data Encryption Technology in Computer Network Communication Security [J]. Electronic Production, 2018, 000 (016): 61-62.

[7] Xu Xueyu, Li Wei. Research on the Application of Data Encryption Technology in Computer Network Security [J]. Electronic World, 2017 (11).