The application of data encryption technology in computer security

Na Wu[1, a], Guorong Chen[2, b]
[1]Nanchang institute of science & technology，China
[2]Software College of Jiangxi Ahead University，China
[a]email: 35482278@qq.com, [b]email:46996285@qq.com

Keywords: data encryption technology, computer, security

Abstract: At present, the rapid development of information technology brings great convenience for people's life, at the same time, also brings all kinds of security problems. The application of data encryption technology in the process of information transmission, provides a favorable safeguard for information security, is the main effective way to guarantee the computer security currently. The author introduced several data encryption technology, analyzed its application in computer security.

1. The hidden troubles that computer security faced currently

1.1 Computer network

The function of the computer network is mainly used in communications, the information is easy to be stolen, monitored, etc in the process of communication. With the increase in the number of people into network, network crime is increasing, network security is more difficult to guarantee. The instability of network environment leads to any intentional or unintentional attacks are likely to cause a large area of network or computer paralysis, thus causes more serious damage. And if there is no data encryption in the process of communication, criminals are easy to use a loophole in the various protocols, disguise as a destination IP, intercept, modify, or even reverse attack on data.

1.2 Computer operating systems

The vast majority of users are using Windows system in global, but there are many loopholes in Windows system, whether it is Windows system or Unix or class Unix system, there are the Root users (administrator users), if the Root password leaked, the whole system will be controlled by others. At the same time, no matter what kind of operating system, its programs all can be dynamically linked and created a process, and the intruders can also use this way to create their own process, to steal and modify user's data, and even spread the virus.

1.3 Database management

In order to facilitate the storage of information and data, most companies or government agencies are used to classify, store and manage data through a database. With the increase in business dealings, more data is stored in the database, as a result, the security of database is more important. For example, some time ago, the accounts of a large number of users were stolen on domestic electric business platform, the social accounts of some famous people were leaked in foreign countries, which mainly caused by the vulnerabilities of database management. Once the whole database was attacked, modified, or intercepted, the resulting losses are incalculable.

2. Summary of data encryption technology

2.1 Information security technology

The confidentiality of information is an important research in data encryption, data encryption is one way to enhance the confidentiality of information, generally speaking, that is to reorganize and rearrange the text through mathematical means, only the legal talents can deciphering. From the application requirements of password to analyze, there are mainly two types of encryption technologies: block cipher and public key cryptography. The existed time of block cipher (DES) is very long, is the most widely used, but due to the length of the password is too short, so it is very vulnerable to be attacked by searching. Public key encryption technology makes it possible to establish a secure and confidential information channel without changing the key for both parties. In

some computers or communications channels that are not safe, data exchange can also be assured. At present, there are two main kinds of public key encryption technologies, which are recognized by the users, one is public key encryption technology (RAS public key cryptography system) based on the large integer factorization problem, another is the public key encryption technology (elliptic curve public key cryptography system) based on the discrete logarithm problem. With the development of the computer, the ability of computers to decompose large integers is enhanced, the security of RAS password is threatened, so the elliptic curve public key cryptography system is paid more and more attention.

2.2 Information authentication technology

The authentication of information is an important aspect to guarantee the information security, is mainly to ensure that the senders of information are legal and the contents of the information are complete. In the aspect of authentication technology, generally can be divided into three types: digital signature, identity recognition and hash technology. Digital signature technology is a kind of technology to use the public key encryption , applies the principle of one-way function. Two algorithms are often used, one is for signature, another is for validation. The signer encrypts the information with the private key, then publishes the public key, uses the public key to deciphering and compare the encrypted information. Identity recognition is mainly used to identify the legitimacy of identity of communication users or terminals. In data encryption, there are mainly two ways that is to use password and use the holder. The authentication process of password simply to say is that the user 1 transmits one-way function values to the computer, the computer to complete the calculation of this value and the value that machine stored, and to compare these values. Because there is no one-way function value stored in the computer, so, even if the computer has been invaded, it also unable to get a one-way function value. Using the holder is the holding of legal person, similar to the function of key. This item need to meet at least two conditions, one is the identifier 1 can prove the identifier 1 is correct to the verifier 2, at the same time, after the validation, verifier 2 can’t get any validation information, and verifier 2 can’t imitate identifier 1 to identify the verifier 2 is identifier 1 to other identifiers. Hash technology is a kind of many to one function, to output the string with fixed length, through calculating the string with arbitrary length which input by the users. Among this conversion process, requires a hash value, and the requirements of the hash value is the calculation process to transmit the input string into a fixed string is very easy, but the inverse is very difficult. According to the level of computer currently, the length of the output string at least above of 128bit, can guarantee to resist the birthday attack. At present, the hash algorithm is applied to a variety of purposes, due to these hash functions all belong to pseudo-random functions, therefore, any hash values are possible. The output result can’t be identified by the input contents, so, even if there is only one bit difference between the input strings, it is possible to make more than half of the bit in the output string is different.

2.3 key management technology

The security of password does not depend on the strength of the hardware or the security of the system, but mainly depends on the protection of the key. So, even if the equipment was replaced or lost, as long as key is not lost, then can guarantee the security of information. Key distribution protocol need to meet two conditions: first, the transmission and storage capacity is not big. Second, each pair of users of U, V can separately calculate a secret key K. At present, a lot of key distribution protocols can meet these two conditions, such as Diffie-Hellman key pre-distribution agreement. Secret sharing technology: because all the key need to be stored in the system, the security depends on the master key. However, there are two very obvious flaws, namely the master key was exposed or missed, the system will be vulnerable be attacked or information can't be used. Therefore, we need to use a solution, namely, threshold method. Key escrow technology: because encryption technology can bring more security for people's life, but also cover up the crime fact for criminals, we need to consider using a kind of means to obtain and recovery the encryption technology specially.

3. The application of data encryption technology in the computer security

3.1 The application of data encryption technology in database encryption

Database is different from general file, is only one type, can undertake the whole encryption, database is a collection of a large number of data types, all kinds of data storage management ways are different. With the difference from traditional data encryption technology, the database encryption has its own requirements, first in terms of hardware, database built directly on the hard drive, secondly in terms of software, operating system is universal. The main purpose of database encryption is to prevent the illegal users to maliciously steal, modify and delete sensitive data, ensure the normal legal of the data, at the same time, safeguard the access of legitimate users can be normally proceeded. Therefore, the first condition of data encryption technology is to guarantee the security of the data. Fast storage: if the legitimate user in the process of using the database, every operation has the process of file encryption or decryption, all of them, will make execution efficiency become low, so, the data encryption of the database needs to adopt a rapid random access method. Storage capacity: if the database due to the large storage to cause the storage time is too long, it is easier to be cracked by illegal users. So, the database storage encryption needs to use the high efficiency algorithm to guarantee the key regular replacement. Different unit different key: in the process of database encryption, must ensure that the structure of data in database, and if the keys of the entire database are the same, it is easier to make illegal users get decryption method by means of statistical rule, therefore, need to match the different encryption units with different keys, to ensure that even if the same data in the database, but the corresponding key is different.

3.2 The application of data encryption technology in the software encryption

The research and development of computer software requires developers to invest a lot of energy, many developers have joined the encryption in the development of software, encryption mode is mainly divided into two categories, that is the hardware encryption and software encryption. Hardware encryption is to give users a object similar to the key, also can be some parameters information can't be changed of the equipment, such as MAC address of network card, CD or some tokens. But at the same time, the production of hardware can’t be more favorable to control or extract information from software developers, and can't quickly update software via the Internet. The main way of software encryption is to activate the software in the form of serial number or code. Software through access to information of computer host ID and so on, transfer to software service providers through the Internet, software providers through data encryption technology to create the serial number or registration code with the corresponding host ID, and send to the legitimate users via the Internet, the user as long as input the corresponding serial number in the software activation screen.

3.3 The application of data encryption technology in e-commerce

In the course of electronic commerce, must ensure the complete security of the data information and the legitimacy of the transaction object. This need to determine whether the other party is legal through the encrypted data, this is the first guarantee of electronic commerce. As long as the user's private key is not leaked, it can ensure that the source of the data is safe. Information needs to use the sender's public key to deciphering in the process of decryption, as long as decryption success can confirm the identity of the sender is legal. In the process of data communication, the the completeness and consistency of information is very important, here you can use the digital signature technology, the sender sends the digital signature and information content, the receiver uses the public key provided by senders to deciphering the digital signature, then can get text. Because the algorithm used is same and information content got is consistent between the two sides, others want to camouflage to send encrypted information is hard. In the transactions of e-commerce, inevitably exists some denial behaviors, you can submit the digital signature and information to the authoritative legal certification bodies similar to a managed approach, due to the digital signature of both parties is encrypted with sender's private key, others do not have access to the private key, can’t be faked, and the sender's public key is public, so the certification institution can use this public key to deciphering the digital signature and information from the receiver, to determine whether there is a denial behavior.

4. Conclusion

With the development of computer technology, the decryption ability of the computer has been further promoted, brings more security hidden danger to computer, therefore, to enhance the level of information encryption technology is very important. The application of data encryption technology is becoming more and more widely, and gradually to the direction of education, medicine, finance and electricity, not only brings convenient security for enterprises and government agencies, but also provides security for people's life.

References

[1]Junmei Zhao. Research on the application of data encryption technology in the security of computer [J] The innovation and application of science and technology, 2014 (19) : 66.

[2]Xiangjun Kong. The application of data encryption technology in the security of computer [J]. Journal of network security technology and its application, 2014 (6) : 97.

[3]Wei Lu. Research on the application of data encryption technology in the security of computer [J]. Journal of silicon valley, 2014 (14) : 102.