Encryption Technology in Information System Security

Siliang Suo[1, a], Wei Xi[1, b], Tiantian Cai[1, c], Ganyang Jian[1, d], Hao Yao[1, e] and Jin Li[2, f]

[1]Electric Power Research Institute, CSG. Guangzhou,China

[2]Beijing Smart-Chip Microelectronics Technology Co., Ltd. Guangzhou, China

[a]suosl@csg.cn, [b]xiwei@csg.cn, [c]caitt@csg.cn, [d]jiangy@csg.cn, [e]yaohao@csg.cn, [f]lijin3@sgitg.sgcc.com.cn

Abstract. With the rapid development of network, all kinds of information systems bring convenience to enterprises at the same time, it also brings more and more hidden dangers to information security. Encryption technology is the core technology of network security technology, which plays an increasingly important role in protecting network information security. This paper analyses the current information encryption technology, expounds the advantages and disadvantages of encryption algorithm, and expounds the application scenario and development trend of encryption technology.

Keywords: information security, network security, encryption technology.

1. Necessity of Information Security Construction(Introduction)

With the popularization of computer networks and the continuous development of information technology, information systems generated by the combination of information and network are more and more widely used in enterprises. The use of information system brings great convenience to people's life and work. At the same time, information security problems are gradually exposed. Information security is the guarantee of an enterprise, an important part of the operation of an enterprise information system, and the flow process of information flow and capital flow. Its advantages are embodied in the full sharing of information resources and the high efficiency of the mode of operation. The importance of its security is self-evident, once there is a security problem, it may bring irreparable losses to enterprises. Therefore, the security protection of information system is becoming more and more important.

2. Information Encryption Technology

Among the various technologies involved in the field of information security, encryption technology is the core and key technology of information security. Encrypting data information through encryption algorithm can improve the security of data transmission to a certain extent and ensure the integrity of data transmission.

2.1 Data Encryption Technology

Data encryption technology is mainly divided into data transmission encryption and data storage encryption. Data transmission encryption technology mainly encrypts the data stream in transmission. There are three commonly used ways: link encryption, node encryption and end-to-end encryption.

The node encryption method similar to link encryption is to use a cryptographic device connected with the node machine at the node. The ciphertext is decrypted and re-encrypted in the device. The plaintext does not pass through the node machine, thus avoiding the vulnerability of the link encryption node.

End-to-end encryption is a way of encrypting data from one end to the other. Data is encrypted at the sender and decrypted at the receiver. The intermediate node does not appear in plaintext. End-to-end encryption is done at the application level. In end-to-end encryption, messages except headers run through the whole transmission process in the form of ciphertext. Only at the sending end and receiving end can the encryption and decryption devices be installed, but at any intermediate node,

Copyright © 2019, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

the messages are not decrypted. Therefore, no cryptographic devices are needed. Compared with link encryption, the number of cryptographic devices can be reduced. On the other hand, information is composed of header and message. Message is the information to be transmitted and header is the information to be routed. Because routing is involved in network transmission, both of them must be encrypted in link encryption. In end-to-end encryption, because each intermediate node on the channel does not decrypt the message, but in order to transmit the message to the destination, it must check the routing information, so it can only encrypt the message, but not the header. In this way, it is easy to be detected by some communication analysis and get some sensitive information from it.

Link encryption is relatively easy for users, using fewer keys, while end-to-end encryption is more flexible and visible to users. End-to-end encryption can also be used when the security of each node in link encryption is not assured.

2.2 Data Encryption Algorithms

There are many kinds of data encryption algorithms. The standardization of cryptographic algorithms is the inevitable trend of social development and the premise of ensuring the transmission of information security on the Internet. Common encryption algorithms can be divided into three categories: symmetric encryption algorithm, asymmetric encryption algorithm and Hash algorithm. Symmetric cryptography is mainly divided into two categories: block cipher and stream cipher. Block cipher encrypts plaintext messages in blocks and outputs ciphertext blocks, while stream cipher encrypts plaintext messages using key stream generated by key stream. Symmetric encryption algorithms include SM1, SM4, SM7, DES and AES; asymmetric encryption algorithms include RSA, ECC, SM2, SM9, knapsack password, Rabin, elliptic curve and so on.

At present, SM1, SM2 and SM3 are the most common algorithms used in data communication of enterprises and institutions in China.

3. Development of Encryption Technology

In order to ensure the security of commercial passwords, the State Office of Commercial Password Management has formulated a series of cryptographic standards, including SSF33, SM1, SM2, SM3, SM4, SM7, SM9, Zuchongzhi's cryptographic algorithm and so on. Among them, SSF33, SM1, SM4, SM7, Zuchong's cipher is symmetric algorithm; SM2, SM9 are asymmetric algorithm; SM3 is hash algorithm. At present, the published algorithm texts include Zu Chongzhi's sequence cipher algorithm, SM2 elliptic curve public key cipher algorithm, SM3 cipher hash algorithm, SM4 block cipher algorithm and so on.

Cryptographic machine is the most commonly used cryptographic device in the process of data encryption and decryption. In order to enhance the stability and reliability of cryptography, modular design mode is usually adopted in cryptography software. The system is mainly divided into three layers: system layer, function layer and system layer. At each level, each module is divided into different modules. Each module is responsible for a relatively independent function. The modules are independent of each other. It can avoid the interference and interaction between different modules, thus improving the stability and reliability of the system.

The cipher machine adopts SM1, SM2, SM3, SM4, SM7 and other algorithms authorized by the State Cryptographic Administration, as well as high-speed hardware data cipher card or chip implementation through security authentication, which ensures the security and accuracy of the algorithm implementation. The cryptographic operation functions such as data encryption, decryption, digital signature and signature verification of cryptographic machine are implemented by hardware data cryptographic card. The security of cryptographic algorithm and key generation is entirely guaranteed by hardware data cryptographic card.

All kinds of keys are generated by hardware physical noise sources. Under no circumstances, keys do not appear outside the cryptographic machine in plaintext. At the same time, the process of key generation has nothing to do with designers, operators and users. The password machine adopts

identity recognition technology to effectively prevent illegal users from operating the password machine or illegal users from using the security services provided by the password machine.

The cipher machine has the function of self-checking. The self-checking module starts to work when it starts, and initializes and self-checks the cipher machine. Self-checking includes self-checking of hardware cipher module, self-checking of key, self-checking of network interface card and so on. The cryptographic machine adopts the anti-demolition and anti-prying structure design, and adopts the technology of fully sealed case and physical lock control open panel to provide strong protection for the security of the cryptographic machine.

3.1 SM1 Symmetric Password

At present, cryptography technology has penetrated into most security products and is developing towards chipping. In the field of chip design and manufacturing, although the research in the field of cryptographic chip started relatively late in China, in recent years, the innovation and self-development ability of integrated circuit technology in China has been improved, and the microelectronics industry has been developed, thus promoting the development of cryptographic chip. Speeding up the development of cryptographic chip will promote the perfection of information security system in China.

SM1 is a block cipher algorithm. The length of the block is 128 bits and the length of the key is 128 bits. The security and confidentiality of the algorithm and the performance of the related hardware and software are comparable to those of AES. The algorithm is not public and only exists in the chip as an IP core. Using this algorithm, we have developed a series of chips, smart IC cards, smart password keys, encryption cards, encryption machines and other security products, which are widely used in various fields of e-government, e-commerce and national economy (including national government affairs, police affairs, etc.).

3.2 SM2 Elliptic Curve Public Key Cryptography

SM2 algorithm is ECC elliptic curve cryptography mechanism, but in signature and key exchange, it is different from ECDSA, ECDH and other international standards, but adopts a more secure mechanism. In addition, SM2 recommended a 256-bit curve as the standard curve.

SM2 standard includes four parts: general principles, digital signature algorithm, key exchange protocol and public key encryption algorithm. The details and examples of implementation are described in detail in the appendix of each part.

On the basis of the general principles, digital signature algorithm (including digital signature generation algorithm and verification algorithm), key exchange protocol and public key encryption algorithm (including encryption algorithm and decryption algorithm) are given. In each part, the algorithm description, algorithm flow and related examples are given.

Digital signature algorithm is suitable for digital signature and verification in commercial applications. It can meet the security requirements of identity authentication and data integrity and authenticity in various cryptographic applications. The key exchange protocol is suitable for key exchange in commercial cryptographic applications. It can satisfy two or three optional information transfer processes for both parties to calculate and obtain a shared secret key (session key) determined jointly by both parties. Public-key encryption algorithm is suitable for message encryption and decryption in national commercial cryptographic applications. Message senders can encrypt messages by using the public key of the recipient, and the recipients can obtain messages by using the corresponding private key.

Digital signature algorithm, key exchange protocol and public key encryption algorithm all use SM3 cryptographic hash algorithm and random number generator approved by the State Secret Administration. Digital signature algorithm, key exchange protocol and public key encryption algorithm select finite field and elliptic curve according to the general rule, and generate key pairs.

In the process of data interaction based on authentication, in order to prevent all kinds of counterfeit attacks, it is necessary to authenticate two-way authentication between clients and database servers before performing real data access operations, such as data transmission between

database system servers and servers. Authentication is done through digital certificates. The signer encrypts a signature with a secret key (including name, document number, short message, etc.). The receiver can decrypt it with a public key of his own. If successful, it can ensure that the information comes from the owner of the public key.

In the process of authentication, the most important is key generation technology and authentication algorithm. In computer networks, the conventional way to authenticate the entities of both sides of communication is to use encryption authentication protocol. The famous Kerberos protocol is an authentication protocol based on the layer code system. Kerberos is a two-way authentication protocol based on the symmetric cryptosystem. Each station obtains the secret key for communicating with the target site from the key management center. In this protocol, each site obtains the key used to communicate with the target site from a key management center site, so as to communicate securely. Because the key management center is responsible for managing and distributing a large number of keys safely, it is easy to cause system performance bottleneck, and there must be a key management center trusted by all sites in the system, so there are some limitations in the application of this protocol.

In order to simplify the distribution of communication keys between sites, two-way authentication technology based on public key cryptosystem is generally used in open network applications. In this technology, each site generates a public key pair of asymmetric cryptographic algorithms (such as RSA), in which the private key is saved by the site itself and distributed to other sites in the system through trusted channels. In this way, any two sites can use the obtained public key information to verify each other's identity.

3.3 SM3 Hash Algorithm

SM3 cryptographic hash algorithm gives the calculation method and steps of hash function algorithm, and gives an example. This algorithm is suitable for digital signature and verification in commercial cryptographic applications, generation and verification of message authentication codes and generation of random numbers, and can meet the security requirements of various cryptographic applications. It is used in SM2, SM9 standard. This algorithm generates a hash value of 256 bits for 64-bit messages whose input length is less than 2 by filling and iterative compression. It uses XOR, module, modular addition, shift, and, or, non-operation, which consists of filling, iteration, message expansion and compression functions.

The security of hash algorithm is related to hash length. According to the principle of "birthday attack", for a hash algorithm whose hash length is m, given M, finding another message X and satisfying H(M) = H(x) requires about 2m/2 computational complexity. The output hash value of SM3 algorithm is 256 bits. To find a collision that meets the requirements, the complexity is about 2128, which cannot be completed in the feasible time. Therefore, SM3 algorithm has high security.

4. Concluding Remarks

Information security concerns not only personal privacy, but also social stability and national security.

As the main body of information carrying and transmitting, information system needs to achieve higher security in design, use, operation and maintenance and daily office work.

In the process of system design, we need to adopt integrity and correctness checking protection to ensure that key leakage or change can be avoided in all links; file access has security mechanisms such as security status, file access rights, encryption and verification control, especially for some files that are not open to all users, access rights can also be set as unreadable or writable, strict. It controls access to files and ensures the security of reading and writing the contents of files. In the process of using, it is necessary to record and audit the whole process of user behavior, ensure the traceability of all operations, and provide the basic ability of random auditing in the whole process. In the process of login, the number of password errors is limited, the user will lock the account if the error password exceeds the limit, no longer respond to any operation, and prevent the attack from proceeding. This

can prevent illegal users from using exhaustive or guessing methods to steal passwords. In the process management, the security standards are implemented from the physical environment, personnel selection, network settings and other aspects. When transmitting data in the network, files must be encrypted to ensure data security in the computer network; at the same time, workspace should be divided into several security levels and physical access control measures of different strict degrees should be implemented; after using, documents should not be discarded at will, and centralized management or destruction must be carried out to ensure the security of environment and personnel factors in the daily office process.

At present, all countries in the world have fully realized that information security involves major national interests, is the commanding point of the Internet economy, and is also the key to promote the development of the Internet, e-government and e-commerce. The development and use of information security technology is an urgent requirement, and encryption technology will play an increasingly important role in the field of information security.

References

[1]. Zhou Jijun, Cai Yi. Basis of Network and Information Security [M]. Beijing: Tsinghua University Press, 2008.

[2]. Pan Minghui. Principle and Application of Network Information Security Engineering [M]. Beijing: Tsinghua University Press, 2011.

[3]. Zhang Xiaoqiang, Wang Feng, Gao Kaiming. Research and Design of Data Security Transmission Based on Encryption Algorithms [J]. Computer and Digital Engineering, 2008 (5).

[4]. Li Yumin. A secure data transmission process based on encryption algorithm in e-commerce environment [J]. Market Modernization, 2009 (5).