Research on Module Function for Key Management System

Chunqiang Li

School of Information Management, Beijing Information Science and Technology University, Beijing, 100101, China

642510571@qq.com

Keywords: key management; system function; management principles; system composition

Abstract. Abstract. The password technology is one of the core technology of information security problem. The purpose of the key management is the key of the production, storage, distribution, update, control and destroyed in the process of the whole life cycle to ensure the safety of the key. Key management system is an effective means of management, to a key study in this paper, the system function. Based on the principle of key management, based on key management system composition, key management system's module structure was designed, and the key generation, key distribution, key services, key recovery, the key audit, equipment monitoring subsystem functions such as illustrated. The research content of this article has paved the way for the key management system development, to strengthen the key process management, guarantee the network security is of great significance.

Introduction

Key generally refers to the production, the life are applied to all kinds of encryption technology, to personal information to provide effective supervision, business secrets, key management is refers to the behavior of the key management, such as encryption, decryption, crack, etc. With the rapid development of network technology and computer technology, information network has penetrated into all walks of life and the life of the people, the network is gradually changing people's production and life style, to promote the social progress and the continuous reform of mechanism, system. However, with the informatization construction boom of computer and Internet crime also appear constantly, information security problem is increasingly apparent, such as the rapid spread of viruses, the invasion of computer "hackers", important information leaks, etc. [1, 2]. Information network security once destroyed, impact or loss will be huge. Information security has become a relationship to the country's economic, political, military and so on various important issues. Electronic certification is an important infrastructure of network security, can effectively solve the network of fake information, information interception, tampering and denied. In advancing the process of informatization, especially in the United States and other developed countries in all countries of the world to build the electronic certification system based on PKI, strive to resolve the network identity authentication, information confidentiality, information integrity and non-repudiation, network security issues.

As common in e-government and e-commerce and the increasing demand for electronic certification, at the same time scale information network system and digital certificate number of users has been expanded, and the core content of the electronic certification service is a key management. According to the commercial passwords related regulations of the state, key management system must be authorized by the national cipher management department, and undertake all types of users of key generation, storage, transfer, to protect the safety of the whole life cycle management's responsibility and moral duty. While many enterprises and government departments have been completed or are planning to construction to certification center to strengthen the electronic commerce and electronic government affairs information security, but at present, lack of independent key management system. Key management as an important link of data encryption technology, provides for the life cycle encryption certificate key to the whole process of management, the purpose is to ensure the security of key, and be able to serve different to provide key. Intuitive and simple operation page users don't need to be concerned about the complex

© 2016. The authors - Published by Atlantis Press

algorithm and the underlying implementation. Therefore, the key management system has very broad market prospect.

Principles on Key Management

Key password for the transformation parameters, have the effect of "keys", by encryption transformation operations, can be clear transformation for the cipher text, or by decrypting transformation operations, will be resumed ciphertext is clear; In an encryption scheme need not worry about the security of the algorithm, which can be thought of as algorithm is an open, just protect the key, obviously, protect key is better than protection algorithm is much easier; Can use different keys to protect the secret, which means that when someone breached a key threatened is the breach of information protection by key, the secret of the other is still safe, thus it can be seen The key in the cipher algorithm is at the centre of the very important position. Key management needs to follow the following principles [3-5]:

(1) To distinguish the key management strategy and mechanism. Strategy is the key management system of advanced guidance. Strategy focuses on the principle of guidance, rather than focus on the specific implementation. Key management mechanism is the implementation and execution strategy of technology institutions and methods.

(2) The entire security principle. Must be in the key generation, storage, backup, distribution, organization, use, update, termination and destroyed in the process of the keys to take proper safety management.

(3) The principle of minimum power. Should only distributed to the users to meet the need of a particular transaction minimum set of keys.

(4) The separation of duties principle. A key a function should be professional, don't let a key of several kinds of functions.

(5) Key classification principle. Can reduce the number of key protected, and can simplify the key management. General keys can be divided into three: master key, and secondary keys, primary keys.

(6) Key update principle. Keys must be updated in time. Otherwise, even if is to use strong password algorithm, the longer you use, the opponent to intercept the cipher, the more the greater the possibility of breaking ciphers.

(7) The key should be of sufficient length. Password safe is a necessary condition for the length of the key have enough. The longer the key, the greater the key space, against the more difficult, and therefore the more security.

(8) Different password system, the key management is not the same as traditional cryptography and public key cryptosystem is different two password, so they are quite different in the key management.

Consisting on key management system

Key management center is in the information security protection system based support system of the core part of the password, is to realize the core application security, data security and network security technology management system [6]. Key management system is developed specifically for key management center system, should include the following functions: implementation of key generation and distribution, update, storage, destruction and use of the full life cycle of management; Use level 3 symmetric key system, including the master key, transmission and working keys; Realize the centralized management of the key and safe storage, support the SM1, SM2, published by the state password administration SM3 and SM4 algorithm; According to the needs of the development of the business system, by adding the safety equipment to improve dynamic key management performance of the system. Key management system is shown in Fig. 1.

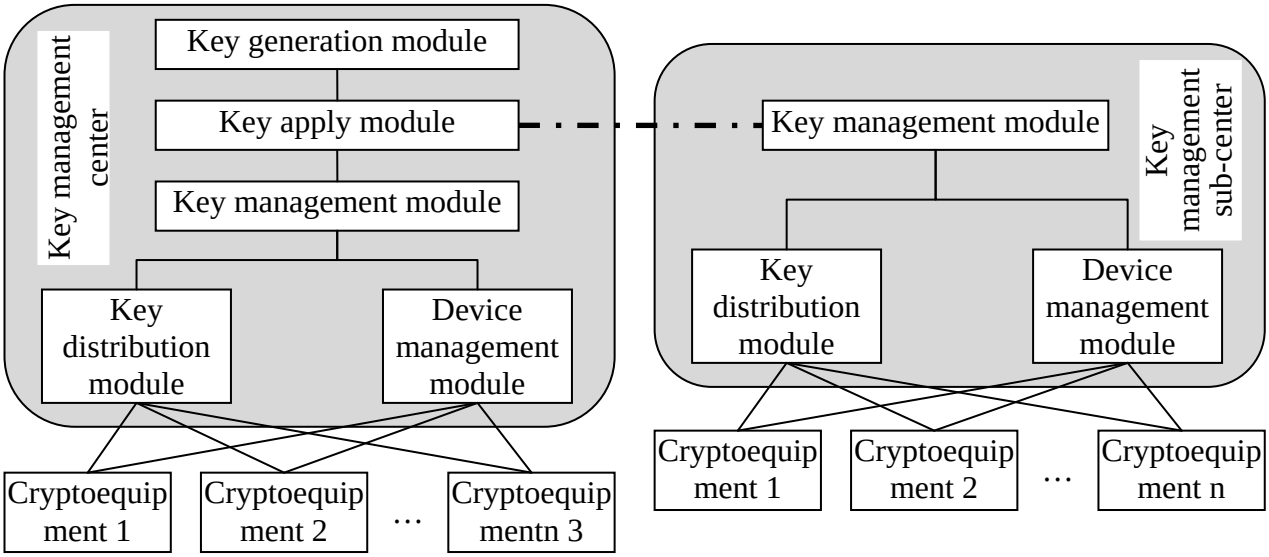

Fig. 1. Consisting on key management system

Function on Key Management System

Function design of the software design is the most important content. Functional design is based on software, form with the results of the model of the software functions, and quantitative or qualitative description of the functions of the software is put forward. Functional design usually adopts the modular system structure. Modules can be combined, decomposition and replacement of the unit. Modularity is a complex system is decomposed to be better approaches to management module, by setting up different functions in different components, dividing a problem into many small independent and interact with each other component, to deal with complex, large software. Key management system function design of module structure is shown in Fig. 2.

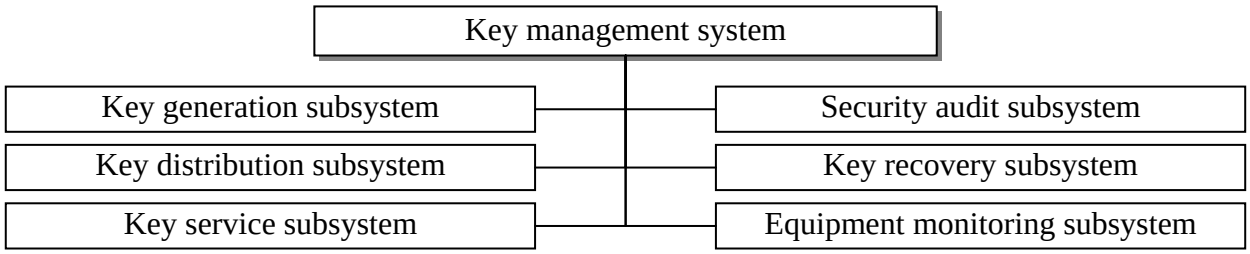

Fig. 2. Function on key management system

(1) Key generation subsystem

Generally need to consider when key generation randomness, key strength and key space. A suitable key is not only beneficial to information confidential, and makes it hard for an attacker to crack. The current generation of key generation technology to achieve the automation, not only reduce the workload of artificial key, and eliminates the human error caused by leakage [7].

Asymmetric keys algorithm, you need to use by a private key and the corresponding public key of asymmetric key pair. Used for each operation key depends on the encryption process is executing. Each public keys or private key for only associated with an entity, the entity is known as the key to the owner. Public key can be anyone to know, and the owner of the private key can only be the key to know and use. Key pair by owner, or in a safe way to provide owners with the key of the trusted party. The trusted party all parties trust must be using the public key.

Symmetric key for information encryption, decryption, or verify the protection. Symmetric key algorithm using keys, usually known as the secret key, can only be used by authorized entities, decrypt or verify protection know. Normally key generated by a single entity, and use. Key should pass to the Shared secret to generate one or more entities, or in a safe way to forecast sharing entities to provide key generated by the trusted party. Trusted party must be on all entities will be

Shared key is credible, and not to the other party without authorization public key or key abuse in other ways.

(2) Key distribution system

Key distribution is the core of the key management issues. Key distribution is a common encryption communication both sides to establish material process, requirements to ensure the integrity of the material source, authenticity and confidentiality. Key distribution protocol or the purpose of the key agreement protocol, is to make the communication after the implementation of this agreement, both sides can establish a common communication keys, and key value will not be stolen by any third party[8].

Key preassigned hair, before is communication, by the credible institutions through the establishment of communication security for both parties involved in the communication channel key. Each pair of communication partners U and V, authorities need to select a random key of U and V as a user communication, and through a safe channel pass key to users U and V.

Key online distribution, it is before the start of the secure communications through the communication channel distribution session key. Using online key distribution, each network user does not need to store keys, communicate with other users of communication for each user and network authority share a secret key, just keep this key, the session key to each pair of users by authorities. The keys that are widely used in the distributed online there are generally two kinds of circumstances, based on the symmetric key system of key distribution center mode, based on the certificate of key center mode.

(3) Key service subsystem

The password service is responsible for provide password support for key management system in all kinds of business. Password service module configuration is approved by the competent department of the state password asymmetric encryption algorithms, symmetric encryption algorithm and data based algorithm, etc. Key services business administrators and key management services business operators, by running parameter configuration functions needed to complete the key generation operation parameter configuration. Operation parameters configuration should include: encryption machine configuration, key automatically archive policy configuration, interface service certificate configuration, interface service port configuration. Among them, the machine configuration includes encryption machine IP, port and other information; Key automatic archiving strategy should include the key of the filing period and archive storage path; Interface service certificate configuration including root certificate, signature and encryption certificate; Interface service port configuration includes configuring security channel service port, secure channel service operation. CA institutions to secure channel launch key service request, provided by the key service function based on CA mechanism request information, provide the key application or resume or keys to cancel the service response.

(4) Key recovery subsystem

Key recovery is the key lost, forgotten, or damaged, etc., need to take a mechanism to recover the key to decrypt the information, allow the authorized entity under specific conditions, access to key, decrypt the information. Key recovery implementation is based on the user to encrypt information at the same time, in the form of encryption key generated information, to form the back door of the recovery key in the future [9].

According to the key hold or get way, key recovery can be divided into two types, key escrow and key encapsulation. Key escrow, use by the government or a number of trusted third party entities to serve as escrow agent to hold the user really key or the corresponding key component; Key encapsulation, using a number of trusted third party entities to get the key in encrypted form enclosed, this kind of mechanism to ensure that only the specific trusted third party called a recovery agent entities that can perform unlock operation to restore the hidden in one of the key information.

Key recovery implementation logically includes three stages: the first stage, the registration key recovery, need key recovery service of one party and hosting or recovery agent between some initialization; The second stage, key recovery starts, to participate in the secure communications of

the parties to perform some operation makes key recovery be implemented; The third stage, the key recovery request, restore data encryption keys authorized party, by request, in recovery server and a number of escrow agency or restore help restore key used to encrypt data.

(5) Security audit subsystem

Security audit subsystem includes the following functions: operation parameters configuration, safety auditors by running parameter configuration functions needed to complete the security audit function of a operation parameter configuration. Operation parameters configuration should include: encryption machine configuration, automatic log archive policy configuration. Among them, the machine configuration includes encryption machine IP and port information, journal automatic archiving strategy should include the filing period and archive storage path; Event audit function, key generation, key recovery, key management service, will happen at the safety certification through the function of event log is sent to the audit service; Audit results query, safety auditors ask business functions, events, belong to submit the event occurs, conditions, such as by the security audit function complete event query and return the query results; Audit results, safety auditors submit event related statistical conditions, by the security audit function complete event statistics and returns the result; Audit data archiving, safety auditors to submit after filing time and file storage path information, by the system the data file to the specified path to the file; Audit data recovery, safety auditors will be archived data submitted to the system, by the system to complete the audit data recovery and return to restore the results; Archived data management, safety auditors submit data after the download, delete, and so on, by the system to complete the corresponding operations [10].

(6) Equipment monitoring subsystem

Password the supervisory control subsystem of equipment includes the following four functions: one is that password detection device status information acquisition function. Password line equipment monitoring protocols used in the equipment used by password key type, version, such as query, query and acquisition in the status of all kinds of cryptographic device, running state and other state information; The second is, the password device status information records and audit analysis function. Record the password device status information, comprehensive audit analysis of cryptographic device status information, timely report; Three is that password device status information query and exception alarm function. Provide a password classification of equipment state information query function, abnormal state of password equipment alarm and event; Four is that state information database backup function. State of database data backup, if necessary, can restore, prevent monitoring effectiveness due to equipment failure, loss of data.

Conclusion

Password technology is the core of information security technology, one of the key management technology is the foundation of the password techniques, the key generation, storage, distribution, update, revoked, control and destroyed in the process of the whole life cycle of key to ensure the safety of the key to ensure the effect of the symmetric key and asymmetric keys and security management, and provide the efficient and economic key service is key. Along with our country social rapid application and development of information and network, network security problem in information systems in various industries is more and more prominent, using the symmetric and asymmetric keys of data encryption technology is important to communicate data encryption and authentication mechanisms. The research content of this article has paved the way for the key management system development, is of great significance to guarantee the network security.

Acknowledgement

This work is supported by Major special project of nuclear high-base (2012ZX01039-004-48); School fund of Beijing information science and technology university (0925020).

References

[1] Babak Daghighi, Miss Laiha Mat Kiah, Shahaboddin Shamshirband, et al, "Key management paradigm for mobile secure group communications: Issues, solutions, and challenges," Computer Communications, vol. 72, no. 12, pp. 1-16, 2015.

[2] Jun Zhou, Zhenfu Cao, Xiaolei Dong, et al, "A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," Information Sciences, vol. 314, no. 9, pp. 255-276, 2015.

[3] Road passenger Baba online document sharing platform, "Key management technology," http://www.doc88.com/p-9189414521488.html, 2016-1-5.

[4] Tenfyguo technology column, "Several design principles of key management," http://blog.csdn.net/tenfyguo/article/details/15813521, 2016-1-2.

[5] Kyungroul Lee, Hyeungjun Yeuk, Jaein Kim, et al, "An efficient key management solution for privacy masking, restoring and user authentication for video surveillance servers," Computer Standards & Interfaces, vol. 42, no. 2, pp. 137-143, 2016.

[6] Y. D. Chen, T. Zhang, R. Zeng, et al, "Research and Implementation of Key Management System," Computer Technology and Development, vol. 22, no. 2, pp. 156-159, 2014.

[7] C. L. Shu, W. J. Liu, B. Wang, "Design and implementation of key management system," Journal of Liaoning Technical University, vol. 21, no. 5, pp. 619-622, 2002.

[8] Doc in Douding, "Key distribution and key exchange in secure communication," http://www.docin.com/p-206813899.html, 2016-1-3.

[9] X. Y. Lu, C. Zhong, "Analysis of key recovery technology," Journal of Guangxi University, vol. 26, no. 1, pp. 36-39, 2001.

[10] Z. J. Gao, "Design and implementation of key management system," Master's degree of Beijing University of Posts and Telecommunications, 2012.