The Safe of the Blade Encryption Sever

Sun Xiuli
School of Control Science and Engineering of University of JINAN , 250022

***Abstract*-The sever is the center of Internet. The user can store and process all information by severs. The safe of sever is main problem. Using encryption technology is the important way. So the safe of information is the main measure. The blade encryption sever can solve the problem of the transmission and storage of information.**

Keywords- Key management, Encryption sever, SSH, SSL

I. THE BASIC PRINCIPLE OF ENCRYPTION SERVER DESIGN

The basic principle of encryption server design: the data information on the public information platform can get clear text only only these authorized users pass the certificate. These not be authorized users, secure channel can only be seen through the clear, Rather than the authorized users no matter by what means are not given any useful information. In order to protect the information transmission and storage of information security, while not changing consumer behavior, does not affect the structure of the database should be transparent to legitimate users. Encryption server schematic shown in Figure 1.

The user terminal connect to server through broadband or PSIN. The encryption server connect to the disk array of network by etheric with the rate of 1000M. The encryption server and disk array constitute the public information platform.

When the users access the public information platform, The first issue is the safe of information transmit from the user terminal to encryption server. Information transmission security is guaranteed by the SSH and SSL. SSH can not only upload and download files but also can manage encryption server (including key generation, replacement keys, restart the machine, install the application software, etc.). SSL is used to ensure the safety of the data transmission network. SSH and SSL client cipher are from the encryption card, Server-side password algorithm is provided by the chips of SSP02-A, SSX04 and WNG-5 on the server chip. Encryption server also can achieve encryption and decryption about data stored on the disk array. The master key is produced by WNG-5 .The WNG-5 is a chip of physical noise sources. And the algorithm is completed by the SSP02-A. Encryption and decryption are operations in the operating system layer. NFS (Network File System) makes all the files on the array to save disk with encrypted text;Use authentication to prevent unauthorized users into the system;Achieve remote management of the encryption server and improve safety of operating systems.

II. KEY MANAGEMENT OF ENCRYPTION SEVER SYSTEM

The certificate used in this system, key: SSH certificate, SSH, SSL certificates, SSL encryption keys, session keys, the main key (file encryption symmetric key). Among them, SSH and SSL certificate, key into the server and client, in the server for server SSH certificate, private key and server SSL certificates, private key at the client as administrators SSH certificate, private key and ordinary users SSL certificate, private key; In SSH session keys are used in communication, SSL encryption keys, the established in each session in conversation, communication generated at the end destroyed; Lord of user data file encryption is used to encrypt the symmetry of keys, the key is stored with cipher-text, namely: on the server with SSH public and SSX04 algorithm chip encrypted save to key storage area. This system is divided into: server management of key techniques in the key of key storage area management; the key to management; user encryption server and client communication process management of session key.

A. Management of key in the server store area

The encryption server use three keys: server key, session key and master key. Session key is one of the temporary keys in the communication process, which is destroyed and not saved in the end of the communication session. Keys stored on the server are the server key and master key; master key is a symmetric algorithm key, which is used for encryption or decryption for user data in the file system; server keys include SSL keys and SSH keys, using them for the messaging security and authentication between the server side and client-side. Server SSH keys, SSL keys and certificates use the key of the private protection module and the SSP02-A algorithm chip for encryption, then will be written into the key areas; master key will be written into key areas after the SSH public chip and the SSX04 algorithm chip being encryption.

Server certificate and the key have been applied by the user from the CA center. CA Center distributes users with a public and private key, which are stored in the user's smart IC card. The smart IC card need to be taken good care by administrator-level users, and the length of the server secret key is1024-bit; master key is produced from the encryption module WNG-4 chip and the key length is 128 bits. The management of above keys includes two aspects: on one hand, it is to prevent illegal measures to add users and change the certificate data in the key areas; on the other hand, to prevent the illegal theft of key data. For these, we take measures to keep the key areas of dense data stored: the server's SSH private key, SSL encrypted private key and certificate use the key of server private key protection module and SSP02-A algorithm chip to be Encrypted and then saved into the encrypted key areas; master key use the chip SSH public key and SSX04 algorithm chip to be encrypted then saved into the key areas; other certificates

Published by Atlantis Press, Paris, France.

are signed by the administrator private key then written into the key areas.

The private key protection module of Encryption module is produced by the W78LE51P MCU. The management key (production generated, each one a key board)is to burn into the microcontroller ROM in the Production processes, and then burn control part of microcontroller blown (MCU and burning software functionality). In this way, procedures and key will be cured into the MCU ROM, and can not be read. In order to ensure the safety of procedures and key, we have also taken methods to keep port (P0 port) of the data from the microcontroller high-voltage fused with the purpose of loss of function. In this state, data in the microcontroller ROM can neither be read out nor be changed. So that, the process and the key curing in the microcontroller can not be read out, so the program and the key are safe.

When cipher-text in Key areas is using, the cipher-text key and data which is encrypted or decrypted will be transported into the encryption module by the application. MPU management of encryption module is responsible for calling the modules or algorithms chip away from the secret key cipher text into plaintext key, and use the clear key for data encryption / de-dense treatment. The secret key out of encryption module is only used in the cryptographic module by the MPU Manager (sent to encryption module chips and used in the algorithm), After MPU manager deal with the key , then clear the corresponding plaintext.

Encryption server reset：After initialization operation, the first work is checking certificate data in the key areas valid or not. If not, the system will waiting for written data of the certificate key to the component, then the system administrator will need to apply for the server certificates. Keys and certificates by administrators written certificate key components and supporting application software then are written into the key port by turns. System management program will be filled to the key areas of space as a certain format. If there is valid certificate data, then close the write ports of the 'written certificate key component', and then check whether there is a valid master key in Key area, if not, management program will generate the master key to send the request to the WNG-4 chip of the encryption module. The WNG-4 chip will generate master key of 128-bit. After being encrypted by SSH public key and SSX04 algorithm, the keys will be stored in the A place.

During encryption server system is working, only the system administrator can manage the server through SSH and any other user can not manage the server. The management features of the system administrator key which is supported by SSH server include:

1)Backup master server encrypted key and replace the server key. Due to the data which is saved into disk array encrypted by the master key cipher-text data, once the master key is destroyed, the cipher-text data will not be restored, the user will get irreparable damage, so it is necessary for the main key to backup. In the first use of encryption server, the system administrator must first backup the master key to the client (the master key after the backup is encrypted cipher-text data), and save the master key into the smart IC card, after saved successfully, the client's master key which has been backup will be deleted, and manage smart IC cards by hand. Server change involves the replacement of SSL keys and SSH keys. If the system administrator replaces the server key, the system administrator need to run SSH client, SSH serves the connections, then establish a secure channel. After the connection is successful, smart IC card which has the server key will be put into the computer, do the command of replacement of the server certificate (including the server's public key and private key). The client first use the administrator private key to sign the server with public key , the server side keep the keys for encryption by the use of encryption module.The 'server private key protection module in the key and SSP02-A chip on the server, SSH private key algorithm, SSL private key encryption) and then save it.

2) Replace the master key. Master key is used to be encrypted or decrypted. In order to improve the security of user data, it should be replaced master key regularly or irregularly. When replacement of the master key is end, the system will use the new, former team for the key again to deal with all user data .In the processing, the user's system will no longer accept any other instructions, when it is a large amount of user data, the process will takes a long time. Therefore, we recommend that the minimum time of master key replacement cycle should be once a day , and arrange it in a less time (such as night).

Master key is produced from the WNG-4 on the motherboard chip which can generate random number. When the user is initialized, the random number generator will generate a master keys, after encrypted by the SSH public key and SSX04 algorithm chip , the master keys are putted into the first location. When the user needs to replace the main key, the new key will be put into the first position and the previous key will be moved into the second position. When the system encrypts files, the system will take away the master key from the secret master key area from the first position and second position respectively. If the key in the second position is available, then the system files deal with the first two master keys when the date be taken away from the secret, then encrypted with the first master key. If not, encrypted or decrypted from the secret master key with the first one, so when the main keys are replaced, SSH client must first backup the new generation of master key and the previous master key. Only after the success of the backup server, the system will notify the newly generated encryption key to load the key in areas, or replacement of key will be failed.

3) Replace administrator certificate. Only system administrators can change administrator certificate. When the administrator certificate needs to be replaced, the system administrator can pass channel through SSH securely. By using the function of 'replacement administrator certificate' which is provided by SSH client software , the user will store keys in smart IC card and administrator encrypted new certificate covering encryption key district administrators on the server certificate. After replacement of an administrator certificate, there will require a new certificate private key to be stored into the key areas and re-signing the certificate. Administrators need to re-start after replacing SSH client, the new certificate to be effective.

4)Add, delete or change the user certificate. System administrators can add user certificate into the key areas by SSH. Only the user's encryption certificate is added to the corresponding space of server key areas, users can access the server via SSL, or users can not access the server. So if you want to cancel the permission of the user access the server, you can delete the user's certificate, if the user changes the certificates, the system administrator is needed to draw to replace the certificate before the new certificate. By default, the user key area of the encryption server can store up to 1016 user certificate, if you need to add more users, you can use the mobile storage area, but the storage area can store up to 3064 user certificate.

*5) Manage and maintain encryption server (reset, restart, etc.).*If it is necessary, System administrator can send the request of reset and restart to encrypted server by SSH in order to make the server restart, but the SSH reset too. After the server restarts, the system administrator needs to reestablish SSH connection.

6)File backup. System administrator can backup the data which is on the disk array into the local hard disk through the SSH channel. Because decrypted data is done automatically by the operating system, so the data from local hard disk is clear-text data.

B. The management of user key

User keys including administrator keys and ordinary users keys. System administrators and ordinary users are required apply for a public key and a private key (the certificate) from CA center and save the into their smart IC card. The length of users key is 1024 bit.

Before using this system, all users (including administrators and ordinary users) should store their certificates in the key center of the server, Administrator certificate is through 'certificate key' to write components, after pass them to server ,the key will be encrypted and write them to the key center .The certificate of ordinary users is signed with their own private key by the administrator, to the server SSH key through a secure channel to zone.

the administrators add, change or delete (destroyed) user certificate through the SSH safe passage.

System administrators can use their own key to manage encrypted server through a SSH secure channel. Ordinary users can only use their private key to access the server through the SSL secure channel, not manage the server. What the server is accessed through the SSL secure channel is limited to WEB application. The user's private key stored in the smart IC card, Users must keep their smart IC safe, in particular, do not let your password out.

C. key management of server and client communication

Encryption server use symmetric algorithm the chip SSP02-A, RSA algorithm coprocessor chip SSX04 and random number generator chip WNG-4. Client use the password secret cards which is recommended by countries. Encryption algorithms card and server's algorithm are in the same chip Key management of SSH communication process

In the process of establishing SSH communication, the public key and private key about administrator, the server and a pair of temporary generated RSA key need to be used. The administrator SSH public key and the server SSH public key and private key are stored on the server in the key areas. Administrator SSH private key is stored in their smart IC card. Therefore, as establishment of SSH communication, the administrator should maintain its own SSH private key first smart IC card into the computer, and then start the SSH client program.

After establishing a SSH secure channel, a symmetric session key will be established In later sessions, they didn’t use public key and private key of the SSH. In this process, the temporary RSA key generatlly are no longer used (to be destroyed out), but symmetric session key is used. In the SSH communications , the algorithm of encryption or de encryption including block ciphers, RSA public key algorithm and the MD5 digest algorithm. The SSL communication process is basically as same as SSH

D. The protection of key data

In physics, the key area (CF card) is encapsulated with a second black resin. The connection lines are not visible from the exterior to ensure that the key store data from being stolen.

We modified the operating system in software. Operating system of ZL-Linux is only open SSH port and SSL port and prepare a special software key areas of operation. And calling the operation is limited to operat system file encryption and decryption modules. In addition to SSH mode, the system does not provide access to key areas of other interfaces through the Ethernet port.

In hardware, there is a watchdog module on the motherboard (made from MCU), The module send the watchdog signal to the server every 30 seconds. When the server board can not detect the signal on time, the keys, certificate and operating system kernel and other data will be destroyed by the relevant tests program on Server board.

In addition, system initialization We designed a specific components to save the server certificate, the administrator certificate. The port is designed to write data only, not be allowed to write .By this way, sensitive data will not be rewritten by the port to steal.

III. SUMMARY

By using cryptography to encrypt the information protection and safety certification, the information can be protected. Server has high security encryption strength and resistance to attack. Based on data information storage and transmission, SJY60 encrypted server are widely used in telecommunications, finance and other vertical industry customers and large enterprise group building. Meanwhile, using organized security public information platform, there will change the traditional ideas gradually. The enterprise will change building network into rent an independent public network .In this way , the enterprises will also the majority of small and medium with minimum capital investment, the fastest speed of network construction, speed up the process of enterprise information.

REFERENCES

[1] LinRu Ma. The design of encrypted server platforms and realization based on Linux.. Chinese national defense science and technology university of people's liberation army, master, , 2002

[2] Wang Gang, network disk array structure and data layout research; Doctor; Nankai university; 2002

[3] William Stallings the translation, password code Stallings principle of learning and network security with practice (second edition), electronic industry press, 2001

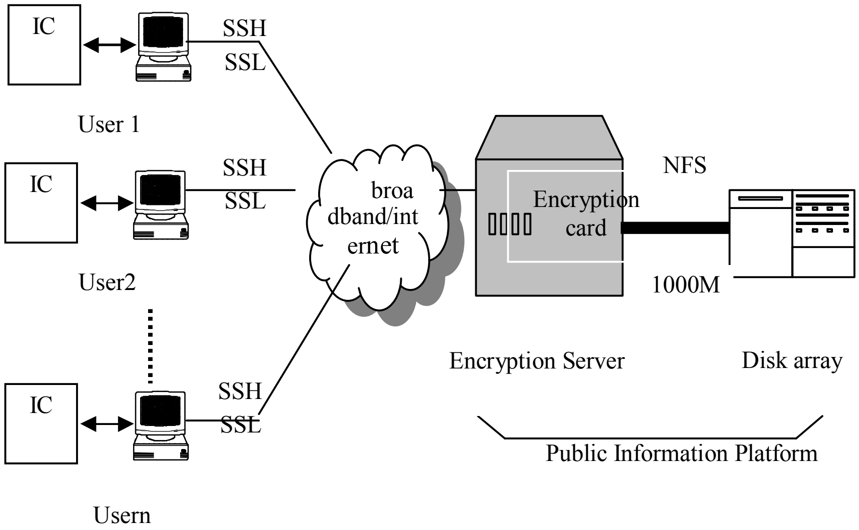

Figure 1. Encrypted Network application server topology