The Model Design of the Security of Electronic Records under Digital Office Environment

Gao Wenju
Department of Electronic Engineering
Changchun Institute of Engineering Technology,
Changchun, China
gaowj913@sina.com

Li Qiuyan
Department of Electronic Engineering
Changchun Institute of Engineering Technology,
Changchun, China
liuqiuyan@sina.com

Ren Yueou
Department of Electronic Engineering
Changchun Institute of Engineering Technology,
Changchun, China
renyueou@sina.com

Liu Chao
Department of Electronic Engineering
Changchun Institute of Engineering Technology,
Changchun, China
liuchao@sina.com

Abstract—Digital office environment is the office mode based on WEB or B/S structure. Under the digital office environment, office work digitalizes and documents electronizes. Traditional paper files are easy to mildew, rot and lose, difficult to revise and inquire, and have low efficiency. Electronic records avoid those disadvantages. Under digital office environment, it only takes us a few seconds to access the target record; the problems of files' mildewing, rotting and losing needn't to be worried about; However, while enjoying the convenience of network, digital office system have to confront many threats. In this paper, to meet the security need of electronic records under the digital office environment, technological requirement of the security of electronic records is analyzed, and the security model of electronic records based on IPSec protocol is designed and tested under Windows 2000 Server sytem. As is showed in the test result, this model can secure the electronic records based on digital office environment.

Keywords- Model Design ; Security ;digital office; IPSec protocol; electronic record Environment

I. INTRODUCTION

With the development of computer technology and internet, paperless network office has become a trend. To build the network in office has been the need for the modern enterprise to improve the office efficiency. As the new information carrier, electronic records bear large amount of information which need protecting [1]. If the security of the system was destroyed, sensitive information was exploded or lost, and the network was attacked, very serious consequence would arise.

The explosion of network speed causes more conflicts between the pending data in high-speed network link and the processing capacity of the system. The conflicts are as follow:

1) The limit of PCI-bus speed

The capture and storage of the data packet will be transmitted twice through PCI bus, while the present PCI bus can hardly satisfy the high-speed environment.

2) The limit of capacity of the storage equipment

When capturing the data packet in high-speed link, the daily data size will be counted as TBbytes. So a lot of problems such as the storage, transmission, management and analysis of huge data need solving [2].

3) The conflict of access speed and link speed of ROM and RAM.

The development of high-speed network cause the bottlenecks of network forensics.The data collection and the mass data analysis and storage are both the problems to be solved. While the present research focuses on the collection and storage of distributed data sources, the evidence analysis technique and so on.

This papa presents an economical and extensible network forensics data acquisition model based on network load capacity.

Therefore, to ensure the security of the electronic records under the digital office environment makes an important project for us.

II. THE ANALYSIS OF THE SECURITY OF THE ELECTRONIC RECORDS UNDER THE DIGITAL OFFICE ENVIRONMENT

A. The concept and the characteristic of electronic records

Electronic records are documents which are recorded in code on tape, magnetic disc, or compact disc, accessed in computer system, transmitted on network [3]. It is existed in the form of code, and its content can be expressed by multimedia technology such as picture, sound and animation. Those characteristics make electronic records possess more advantages than traditional paper files, such as taking less space, being transmitted faster, being carried and copied more easily and being used more conveniently.

B. The analysis of the security of the electronic records under the digital office environment

Digital office environment is the office mode based on WEB or B/S structure. B/S structure mode, namely browser/server mode, is a kind of new network structure mode developed from the traditional two layers C/S mode. It is by nature the three layers C/S structure realized on internet. Under the digital office environment, office work digitalizes and documents electronizes. Traditional paper files are easy to mildew, rot and lose, difficult to revise and inquire, and have low efficiency. Electronic records avoid those disadvantages. Under digital office environment, it only takes us a few seconds to access the target record; the problems of files‟ mildewing, rotting and losing needn‟t to be worried about; any records can be revised conveniently; office efficiency can be improved greatly, because computers have mighty power and process data very speedy. However, while enjoying the convenience of network, digital office system have to confront many threats, such as network security, network virus, and hacker‟s intruding, all of which will bring about disastrous results. The security of electronic records becomes our top worry, and how to ensure the validity, integrity, confidentiality and reliability of the electronic recording when transmitted in network has become the prioritized researching project [4].

III. THE MODEL DESIGN OF THE SECURITY OF ELECTRONIC RECORDS UNDER DIGITAL OFFICE ENVIRONMENT

A. The model design of the security of electronic records under digital office environment

At present, the main channels to leak electronic records are as follow: the malicious programs on internet, such as virus, steal the electronic records; electronic records are copied from the office computer with notebook computer, flash-disc, and portable hard disc and so on; electronic records are transmitted to the unauthorized party on internet. On surface, the above leaks are network leak, artificial leak and media leak, however, by nature, they are all information leaks, namely, electronic records existing in plaintext, which decreases the security.

Therefore, the key designing idea of the security model of electronic records under digital office environment is to encrypt electronic records automatically, and store and transmit electronic records in the form of cryptograph, so as to increase the security of electronic records.

B. The security protection mechanism of IPSec

IPSec, namely Internet Protocol Security, is a series of norms to ensure the safety correspondence on internet provided by IETF. It provides the insurance of private data transmitted on public network. IPSec has three functions: certification, secrecy and key management. IPSec is mainly aimed at IP packet protection and is based on end-to-end security model. By using IPSec, safety correspondence with other organization can be achieved, certification and secrecy can be ensured and key exchange mechanism can be provided. It can encrypt and certificate all the network flow in IP layer, so as to protect all the distributed application, including telnet, client/server, email, data transmission and WEB access. The features of IPSec can just meet the needs to secure the electronic records under the digital office environment [5].

C. encryption and decryption

Encryption is to transform the data by cryptarithm, make it unreadable without cipher key. The unreadable data transformed by cryptarithm is called ciphertext [6]. Decryption is the reverse process of encryption. It is to decode the ciphertext by cipher key, and regain the original content. Key certification can protect the two parties of data transmission from being attacked from the third party, but it can hardly guarantee the two parties of data transmission not to forge the key. Digital signature is the best solution to this problem. It can certificate the digital signatures to the two parties‟ keys. The features of the digital signature: it must be able to verify the signer and the signing date and time; it must be able to certificate the content of the date being signed, in cast it is forged and denied; the signature must be arbitrated by the third party, so as to solve dispute [7].

D. IPSec security model

1) IPSec security protocol model

Tunnel mode packages the whole IP message, provide protection to the whole IP package; transmission mode only packages the upper layer information, mainly provides protection to the upper layer protocol, and adds protection to the IP package load meanwhile. As is showed in Fig .1: when a work station and a server share the same protected key, namely in intranet, security certification is confirmed, and transmission mode SA is used; when a server doesn‟t support the certification, and a distant station certificates itself to the firewall to access the intranet, tunnel mode is used. IPSec protocol is packaged in the network equipment, so that the network equipment will encrypt and compress the output data flow, and decrypt and decompress the input data flow. AH supports the data integrity and the certification of IP package, that is to say it can ensure that the content of the datagram should not be changed in transmission, and the terminal system and network equipment should certificate users and application programs, provide flow filtering function; it can also prevent address fraud and replay attack. Therefore, these network equipment actually function as the filter of the network data. For example, in router, the part in IP header doesn‟t change, and the key of IP certification and secrecy lies in security association (SA). An association is the one-way relationship between a transmitter and receiver, and provides security service to both parties.

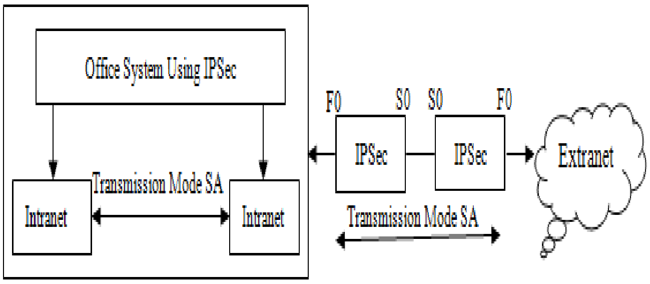

Figure 1. IPSec security protocol model

2) *Key agreement mode*

Key agreement is the crucial part in key management. Key agreement occurs between the two routers which are on IPSec correspondence. As is shown in Fig .2, key agreement is to exchange key safely by IKE protocol on insecure network. It concerns mainly the exchange of IPSec algorithm and the key it uses on insecure network. The key of IPSec equipment is usually informed in an automatic process. In the automatic process, a key management protocol named IKE is used. As a service operation, the key agreement of IKE is in charge of processing users‟ administration and configuration commands, the interaction with the agreement entity, the encrypting certification of IKE load and the interaction of SADB with the same kernel. In addition, IKE never transmits protocol on insecure network. Therefore, by means of IKE, the automatic process can fully considered the complexity of all the key exchanging algorithm used on IPSec and replace the common key management protocol with key management function. After a series of data exchanges, the two parties of correspondence can work out the shared key. Finally, exchanging key safely on insecure network is realized.

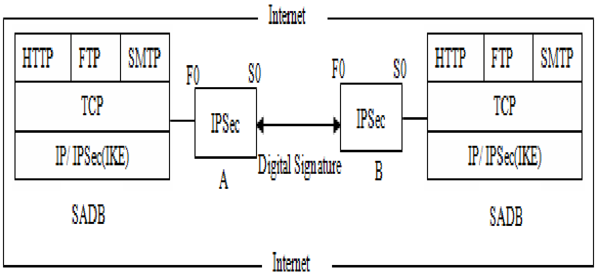

Figure 2. IPSec Key agreement mode

IV. The testing of IPSec security model

IPSec protocol is a protocol suite. It provides transparent security protection to all the upper layer data packaged in IP package and needn‟t revise upper layer protocol. Windows 2000 Servers operation system supports IPSec, with built-in IPSec policies----Clients, server, and Secure server, whose security level is from low to high [8]. IPSec security model designed in this paper is tested in Windows 2000 Server operation system. IPSec mechanism consists of communication protocol, security policy assembly, protocol component of association (SA) and IPSec drivers. The clients operating within domain are managed locally by transmission mode by means of IPSec policy in which domain clients are managed centrally by IP security policy manager. For the remote clients and other relevant domains, IPSec tunnel mode is adopted. IPSec drivers are mainly in charge of monitoring and screening all the datagrams in and out of the system and IP communication, and match each IP datagram with IP filter acting as a part of IP policy [9]. During the testing, this model can realize that IKE be informed immediately to process security negotiation when successfully matched datagram is found. From the above, the conclusion can be reached that IPSec security model in this paper can protect IP datagram and the WEB communication effectively and successfully, prevent the attack from hackers and Trojan program, so as to guarantee the security, integrity and reliability of the transmitted electronic records.

V. Load balancing technology of high-speed network data flow

It is the frame of the parallel acquisition of the high-speed network data, which consist of the load balancer, capturing host and so on. Load balancer acquires the real-time original data flow, then the original data flow is distributed to the evidence collection pool (consisting of capturing hosts).

There are three basic load balancers which are respectively based on TCP connection, application protocol and utility session.

1) *Load balancer based on TCP connection*

Presently, most network flow on the IP network is based on the application of TCP flow (over 90%). The realizing process of the load balancer based on TCP connection is as follow: load balancer records the TCP connection of the network data automatically, and search in hash table according to the connection information---quadruple (sip, dip, sport, dport), if the quadruple has already existed, that means the distribution information had existed, then the distribution is carried on according to the information in the table; otherwise the hash calculation is carried out according to this quadruple, and new connection information is established and distributed through certain load balancing strategy.

Advantages: it guarantees that the data from the same TCP/IP connection is distributed to the same back end processing equipment. It can realize the load balance of network flow compactly.

Disadvantages: distribution equipment has to memorize and maintain large amount of TCP connection identifiers and the inquiry time is much longer. Meanwhile, in some application protocols, a complete session includes more than one TCP connection. For protocol like that, the distribution based on TCP connection will easily make the same application data distributed to the different back end processing equipment, which is difficult to process.

2) *Load balance based on application protocol*

According to the high level protocol bearing in TCP, data will be distributed to the same back end equipment, so that it will guarantee that data of the same application protocol will be distributed to the same back end processing equipment, and all the data from the same TCP/IP network connection will be distributed to the same back end processing equipment.

Advantages: it guarantees that data from the same TCP/IP network connection be distributed to the same back end processing equipment, and the sorting device don‟t have to record and maintain large amount of connection record so as to have shorter inquiry time.

Disadvantages: the same application protocol is distributed to the same back end processing equipment, so that load balance can‟t be truly realized.

3) *Load balance based on utility session.*

It can judge whether a TCP data flow belongs to a application session, and relates to a specific application protocol. Take HTTP protocol as example, when a web page is opened, many data demands will emerge. Among the socket quadruple of TCP connections which belong to the same page request, sip is the client address which sends the page request; dip is the server address which receive a request; sport is generally the temporary port with which the system is equipped; sport is the HTTP port in common use, like 80,8 080. So load balancer can judge whether a data flow belongs to the same utility session through sip, sport in quadruple and the defining time, then distributes the data flow.

Advantages: it guarantees that data from the same TCP/IP be distributed to the same back end processing equipment, and inquiry time is relatively short, so that load balance can be realized well [10].

Disadvantages: distributing equipment have to record and maintain TCP connection identifier record. It is relatively complicated to realize.

In this paper, load balancing algorithm based on utility session is adopted and the thought of distribution based on network load capacity is introduced.

VI. Conclusions

The IPSec protocol security model in this paper is able to provide identity verification, completeness check of connectionless data, confidentiality insurance of content of data, anti-replay protection, and the confidentiality insurance of data flow to electronic records under digital office environment. However, no protection is absolutely safe. Based on the development of network security technology and the need of office work, the protection of electronic records under digital office environment is worth attention and research in the long run.

References

[1] Wu Xiaochun, Wang Xiaoming, Design and Implementation of the Management Information System Based on C/S and B/S [j] E-education research 2013(3):50-52

[2] William Stallings, Cryptography and Network Security-Principles and Practice (Forth Edition) [M] Publishing House of Electronics Industry 2010-11:249-354

[3] Zhu Yanjie, Feng Zhihui, The Principle and Application of IPSec [J] Computer Security: Academic and Technology, 2011-11

[4] Xia Aiyue, The Encryption Method of Network Data and Application Strategy [J] Journal of the Chinese People,s Armed Police Force Academy,2012.(8):93-94.

[5] William Stallings, Cryptography and Network Security-Principles and Practice (Forth Edition) [M] Publishing House of Electronics Industry 2013-11:275-276

[6] Tang Dengping, Make Your System Safer by Using IPSec, [J] Cable TV Technology: Network Management and Maintenance, 2013(4):114

[7] Xiaoming Li "Search Engine," Journal of Changchun University of Technology, vol.428, Oct. 2012, pp. 2127-2130, doi:9.1352/science.1056876.

[8] Hong Tan, Junhong Li, Peng Zhou, etc: LUCENEIN ACTION, Electronics Industry Press, Beijing (2012)

[9] Baowen Xu, Weifeng Zhang: Search Engine and the Technology of Acquiring Information, Tsinghua University Press, Beijing (2013)

[10] Wei Wang, Tieli Zhao, Baixiang Gong, etc: Journal of Changchun University of Technology (Natural Science Edition), 2011.22(02): p. 36-38