Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 339-342
doi:10.4028/www.scientific.net/AEF.6-7.339

Application Model and Implementation about Team Secrecy Encryption

Zhenliu Zhou

Shenyang Key Laboratory of Information Security for Power System, Institute of Engineering, Shenyang , China

zhouzl@sie.edu.cn

Keywords: Team Secrecy; Encryption System;Key Management; Encryption Model

Abstract. Personal and network encryption application models nowadays are analyzed in this paper, then a team secrecy encryption application model is proposed based on practical applications. In this model, members of one team have same access authority for electronic documents, and team is the smallest unit of key distribution. Procedures of distribution, transmission and updating key are offline. This model is suitable for co-confidential application among many departments which are loose coupling. An encryption system is implemented based on this model aimed at protecting Microsoft office document.

Introduction

There are diverse electronic document encryption products on the market. Result of investigation on these products shows that these products can be categorized into two types. One is encrypting file system provided by operating system such as transparent encrypting file system in secure linux[1,2,3] or in windows 2000 ,windows xp ,or windows 7. The other is encryption tools developed by the software or hardware manufacturers other than operating system manufacturers, including transparent file encryption based on filter driver[4] and file encryption based on virtual disk[5].

There are four kinds of encryption application model nowadays. The first is personal encryption application model on single computer such as encryption file system[1,2] and professional encryption tools[4,5,6]. The second is personal encryption application model of network storage[6]. Characteristics of these two model include: key management is simple, no key exchange among users. The third is Intranet interactive encryption application model and the fourth is Internet interactive encryption application model. These two models are all based on complicated key exchange and management mechanism, and there are more security risks about these models [7].

To solve some practical team secrecy problems, this paper proposes a team secrecy encryption application model.

Team Secrecy Encryption Application Model

In practical, among some branches or departments, there is a kind of demand for electronic document secrecy: authorize access authority to electronic documents by unit of team, only members of that team can access those electronic documents. One member of a team can authorize access authority of a electronic document to another team. A team may consist of one or many members. In this team secrecy application model, team is the smallest unit of authorization, distinguishing from above-mentioned any model which the smallest authorization unit is individual.

Specially, there are loose coupling relationships among these teams. Teams may connect with network, or there is no sharing network connection at all, and usb-disk or optical-disk are used to exchange data. So it may be impossible to rely on network to transfer those authorization information among teams.

So team secrecy encryption application model can be described as following: (1) Team secrecy (or secrecy data) can be exchanged through peer-to-peer network, network servers, or portable storage device. (2) Asymmetric key is distributed to team, that is, each member of a team has same public key

and private key. (3) Symmetric key that is generated randomly is used to encrypt secrecy data, public key of team is used to sign and protect symmetric key, private key of team is used to unsign digital signature. (4) All keys, including symmetric key, public key and private key, are stored in hardware smart usb-key for distribution and using. (5) Each smart usb-key has a unique hardware serial number to identify one team member with another. (6) Smart usb-key must be updated while keys is needed to be updated periodically.

Offline Key Management

Every smart usb-key has a unique hardware serial number to identify one team member with another. There is a list of team public key stored in every smart usb-key. Each record of this list includes two items: identity of team and public key of team, illustrating as table 1.

Table.1 STRUCTURE OF List of team public key

Identity of team	Public key of team

Security administrator initializes each smart usb-key on offline secret computer. Procedure of initializing smart usb-key is: (1) Generate public and private key pair <PKu ,SKu > for a team randomly. (2) Create list of team public key in each usb-key. After initializing, security administrator writes a record of these usb-keys and distributes these usb-keys to members of each team. Security administrator is also responsible for others management of key such as withdrawing, updating, and etc. After getting usb-key device, members of a team must set Personal Identification Number of his/her smart usb-key. In application, members of team use his/her own smart usb-key device to encrypt or decrypt authorized electronic file.

Principle of Office Plug-in Transparent Encryption

There are so many Plug-in products for Microsoft corporation's office software because of its wide usage. Principle of transparent encryption using plug-in to encrypt/decrypt office document is illustrated as figure 1.

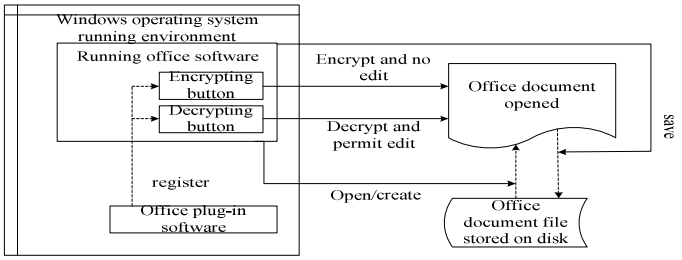

Fig.1 Principle of office plug-in transparent encryption

First, run regsvr32 command to register office encryption plug-in, then when office software is running, two button will be added to its tool bar, one is encrypting button, the other is decrypting button. Once the encrypting button is clicked, data in edit area will be changed from plaintext into ciphertext, and cannot be edited again. Then if the decrypting button is clicked, data in edit area will be changed from ciphertext into plaintext again, and be allowed to edit again. So users can see the result immediately when they do encrypt or decrypt operation. If users save the document with saving operation, the content saved in the file will be as same as the displayed in edit area, that is, plaintext displayed, plaintext saved, ciphertext displayed, ciphertext saved, which is so called 'what you see is what you get'.The encrypted file is saved as normal office document file format.

Procedure of Authorization and Encryption for Team Secrecy

Define following symbols:

K_O :symmetric key, used for encrypting data of office document.

SK_A : private key of member A of team A, stored in smart usb-key of member A.

SID_A : serial number of smart usb-key of member A of team A.

PK_B : public key of member B of team B, stored in list of team public key in smart usb-key of member A.

Sig_o: digital signature.

Figure 2 illustrates the member A how to use office encrypting plug-in and initialized smart usb-key to encrypt data of office document file which is opening and editing.

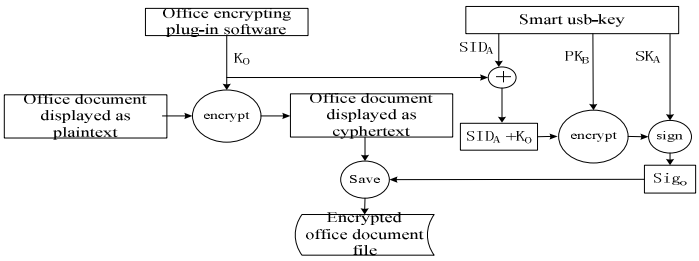

Fig.2 Procedure of authorization and encryption

(1)Symmetric key K_O is generated randomly by office encrypting plug-in.

(2)Office encrypting plug-in encrypts data of office document, then transfers the key K_O to smart usb-key.

(3)Smart usb-key concatenates its own SID_A with the key K_O, assuming result is R1, and encrypts result R1 using public key PK_B of member B, assuming result is R2, then makes a signature operation to the result R2 using the private key SK_A, the signature operation result is Sig_o.

(4)Smart usb-key transfers Sig_o to office encrypting plug-in.

(5)Office encrypting plug-in saves the encrypted office document file with the digital signature Sig_o together.

The digital signature Sig_o of concatenation result of SID_A and K_O encrypted with the public key PK_B can only be decrypted using private key SK_B by members of team B, that is, only members of team B can decrypt the file, Members of others team except team B can not decrypt the encrypted file. Because signed with the private key SK_A, people can know which team has authorized and encrypted this file, and because the signature Sig_o including the serial number of smart usb-key SID_A, people can know which member of team A has authorized and encrypted this file.Every office document file is encrypted with different symmetric key, that is, the symmetric key is generated randomly, this method reduces the risk of batch crack over encrypted office documents.

Procedure of Authentication and Decryption for Team Secrecy

Define following symbols:

PK_A : public key of member A of team A, stored in list of team public key in smart usb-key of member B of team B.

SK_B : private key of member B of team B, stored in smart usb-key of member B.

After getting the encrypted office document file, the member B uses his/her own smart usb-key to authenticate and decrypt the file as following:

(1)Office encrypting plug-in gets the digital signature Sig_o from the encrypted office document file, transfers the digital signature Sig_o to the smart usb-key.

(2) The smart usb-key receives the digital signature Sig_o , unsigns it with the public key PK_A stored in list of team public key, then decrypts the result using the private key SK_B of team B, The operation result will get $SID_A'$and K_O'. If unsign or decrypt operation fails, then stop to decrypt the office document file.

(3)The smart usb-key sends success message and the symmetric key $K_O'$to the office encrypting plug-in. The office encrypting plug-in then decrypts the office document file using this symmetric key.

System Analysis

The security characteristics of team secrecy encryption application model and the example system implemented in this paper include:

(1)Key management is offline, simple and effective. This can avoid the security vulnerabilities and complexity of management arosed by using of PKI[7].

(2)It can trace who has authorized a file afterwards.

(3)Symmetric key used to encrypt file data is generated randomly, this can reduce the risk of batch crack over encrypted file.

(4)It can be applied securely among different sections or departments whether a share network exists or not.

(5)Keys are stored securely in hardware device smart usb-key.

Conclusion

A kind of team secrecy encryption application model is proposed and implemented in this paper. According to practical application case, offline key management is adapted in this model, and smart usb-key is used as key carrier. An encryption system is implemented based on this model to protect Microsoft office document. It proves that this model is simple and effective for co-confidential application among many sections or departments which are loose coupling.

Acknowledgments

This work was supported by a grant from the natural science foundation of Liaoning Province (No.20102158). We thank for their support.

References

[1] M. Blaze. A cryptographic file system for Unix. In Proceedings of the First ACM Conference on Computer and Communication Security, pages 9–15, Nov. 1993.

[2] Wei pei-hui, Qing si-han, Liu hai-feng.Design and Implementation of a Transparent Cryptographic File System Based on Secure Operating System. Computer science, 2003, 30(7): 132-135.

[3] D. Mazi`eres, M. Kaminsky, M. F. Kaashoek, and E. Witchel. Separating key management from file system security. In Proceedings of the 17th ACM Symposium on Operating Systems Principles (SOSP ’99), pages 124–139, Dec. 1999.

[4] Zhao ming-wei, Mao rui, Jiang rong-an. Transparent Encryption File System Model Based on Filter Driver. Computer Engineering, 2009, 35(1): 150-152.

[5] Li qing-jun, Gan Meng. File Encryption Approach Based on Virtual Disk. Computer Engineering and Design, 2006, 27(15): 2835-2838.

[6] E. L. Miller, D. D. E. Long, W. E. Freeman, and B. C. Reed. Strong security for network-attached storage. In Proceedings of the FAST 2002 Conference on File and Storage Technologies, Monterey, CA, Jan. 2002.

[7] Lopez J,Oppliger R,Pernul G. Why public key infrastructures have failed so far-[J] .Internet Research,Emerald, 2005, 15 (5) :544-556 .