Study of File Encryption and Decryption System using Security Key

Gang Hu
School of Computer Science and Technology
Sichuan Police College Luzhou, China
lzjx_hu@sina.com

Abstract*-The paper tries to have made a study of the security keys of USB, which can achieve these functions such as data encryption, digital signature, and identity authentication. Based on the analysis of the security key system, the paper also introduces its formation ,functions and cryptosystem while putting forward a file encryption project on the basis of the USB security key. The project adopts the combination of soft hardware, the software conducting the process of file encryption and hardware taking charge of the management of secret key and the encryption of session key. The project makes a full use of the respective advantages upon the Symmetetric-key cryptosystems and the Publed-key cryptosystem ,which means to encrypt the electronic documents by using the algorithms of the Symmetetric-key cryptosystems and transmit its secret key by employing the ones of the Public-key cryptosystem . Simultaneously, the validation of the informative integrity and authenticity have been realized by the use of information abstract algorithms. With high secrity , high efficiency and user-friendliness, the project achieves the file encryption with the strong extendibility of the system on the basis of the characteristics of USB security key.

Keywords-Cryptology; File Encryption/Decryption; USB Security Key

Development of information technology bring us the convenience and efficiency together with new challenges on information security. Only by ensuring the security of information transmission, can people make better use of information services[1,2].

Through the above analysis of the current using situation and its existed problems of electronic documents, we understand the importance of information protection problem in the electronic document.File encryption, as a basic means of protection, is force on the outside the system memory to the computer data, especially on the theft of data and destructive activities[3-5].When file encrypted, even if the key documents leaked or lost ,they can hardly be deciphered, thus greatly increased the security of key documents.On the other hand, file encryption can be set to each user (or user group) by the user's own key encryption, even when sharing the computer, other people can not decrypt properly and get the access to plaintext because they do not know the key, thus ensured the security of personal documents. In addition, through encryption, backup file has become a ciphertext so that it can reduce losses caused by heft or loss of backup media. There are many secure file system has been achieved both at home and abroad [6-8], but generally lack of security key management functions, or exist security vulnerability of the key management. In the way, it reduces the system security.

I. PROGRAMME DESIGN

The encryption saves usually has three ways to realize [9-12]: Direct encryption document, encryption document through storage medium and encryption document through filing system. The direct encryption document uses the various kind of password technology to carry on the encryption after the document text and deposits it on the hard disk. When use this document, one must use the corresponding decipher algorithm first. It will not leak any information when illegally duplicated. Even if the illegal user log in the computer, it will not cause the information divulging. It is realized by the intensified encryption software Thus it is impossible fro the illegal users to decipher non-authorized document information. The storage medium encryption is usually realized in the device driver level. The encryption operation is carried on by the driver procedure. They usually created a vessel document and realizes the virtual disk encryption through some kind of mechanism. For example, in Linux, there is a kind of loop equipment (retrace equipment) the technology. It can reflect consecutive documents to a virtual disk, then it may be used as a original physical disk to create the filing system and deposit data. The entire vessel document is encrypted and uses as a virtual partition to load and use. Cryptographic system which uses this method includes PGPDisk, BestCrypt, TrueCrypt. The encryption filing system is realized the encryption function by the filing system. It uses the same way as Storage Medium Encryption. It can provide the users with transparent document encryption function. Compared with Storage Medium Encryption, its main character is the realization of Supporting documentation granularity encryption. That is to say the users can choose which documents to encrypt. Because it opens files directly on the physical system not in the vessel documents, what’s more, it does not use the entire memory volume encryption, the Storage Medium Encryption will provide a better service. The space of encryption processing compared to the handling ability of CPU can not be ignored. However, a minority of documents need to be encrypted in a filing system. As a result, encryption filing system will have a big advantage compared to storage medium encryption. Encryption filing system, at the same time, supports the granularity encryption of users, i.e. different users will have their own passports to encrypt their files, but the Storage Medium Encryption only has one system encryption key, therefore all users are the transparent visitors and are unable

978-1-4244-6349-7/10/$26.00 ©2010 IEEE

to provide the corresponding protection among others. For the Encryption Filing System, the big file processing is not a question, because it is only necessary to tackle parts of the document which has been visited, rather than encrypting the whole document. The aim of the design is to realize the safe storage of electronic documents. The following factors are considered on its safety characters: the key of produced dialogues are random, Encryption algorithm's working strength is quite high and hard to decode, the encryption document is easy to backup, the keys are easy to carry, keep and use. The simplicity of operating is required in specific functions and the details in terms of the first floor of shields to the users need to be achieved. Considering the above factors, we need to adopt the method by which the software and hardware are combined , make the main engine carry on the encryption to the document and let the hardware (USB security key)take charge of the management of the secret key. System logic structure drawing shown in Figure 1.

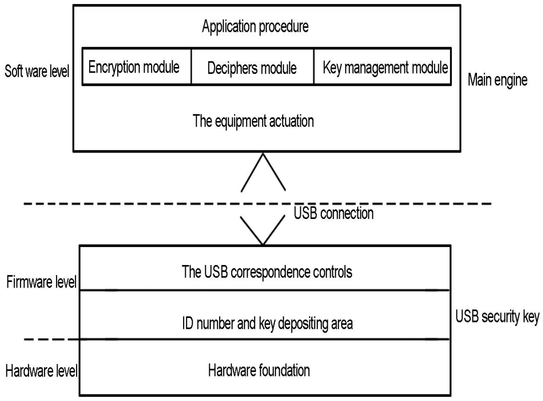

Figure1. Logic System Structure

II. ENCRYPTION ALGORITHM

According to the design goals and functional requirements, you must use the existing mature symmetric key encryption algorithm, because their encryption and decryption is faster than public key encryption algorithm [13]. Theoretically, in order to provide maximum security ,symmetric key encryption algorithm should be used in a sequence,and each byte encrypted before it depends on the number of bytes. However,the fact that the sequence of encryption algorithm is used to encrypt the entire file directly means that for every sub decrypt file a byte is necessary to decrypt all the bytes in front of it, which is intolerable in performance. [14]The biggest negative factor file encryption causes is that the efficiency of the computer system will be reduced, because frequent file encryption operation will result in frequent needs to decrypt the data in the hard disk,and made the system speed affected badly. Handling improperly will make the computer's response time become intolerable, and file encryption will lose its meaning. On the other hand, the ciphertext may cause the expansion of space after file encryption. At the same time, the key storage needs to take up some storage space,and all of this will add space occupancy to the system. In fact, the efficiency, especially the time costing,is an important factor to affact file encryption. Therefore, speed and strength should be taken into account comprehensively. RSA is a public key algorithm, while traditional encryption refers to symmetric algorithms. The symmetric algorithm is often used to encrypt the information before the publish of the key algorithm. However, because symmetric key encryption algorithm and decryption key are the same,a cipher key can only be used once for the consideration of security. The most typical example is the one-time secret code books, with which the key management become very difficult. However, the public key algorithm won't replace the the symmetric algorithms since public key algorithm is used to encryption keys rather than encrypt the message. There are two reasons for this: public-key algorithm is slower than the symmetric algorithm, and symmetric algorithm is generally faster than public key algorithm by one thousand times; public-key algorithm is fragile to the attack of choosing regulations.

III. DESIGN OF SECURITY KEY SYSTEM

A complete USB security key system consists of three parts [15]: Security Key clients: generally single-chip computer with a USB interface; PC side: made up by any one PC which can access the network, and install the PC side with the user authentication software ; Server-side: Any installation of a network server for the authentication of the Server-side software. But in the USB security key system, PC is only the intermedium, but in this program , the PC side also have the function of file encryption and decryption. The system's software architecture shown in Figure 2. It is divided into hardware COS, the core driver, device interface, password service components and application layer several parts. Hardware COS (Chip Operating System), which mainly control the information exchange betweem the security key and the outside world that we called it the inside operating system of the security key. Cryptographic Services PKI system component is the application layer when a request for cryptographic services used some of the standard interface function, which shielded the differentiation of client encryption product, well realized the upper application's different interoperability of encryption products.

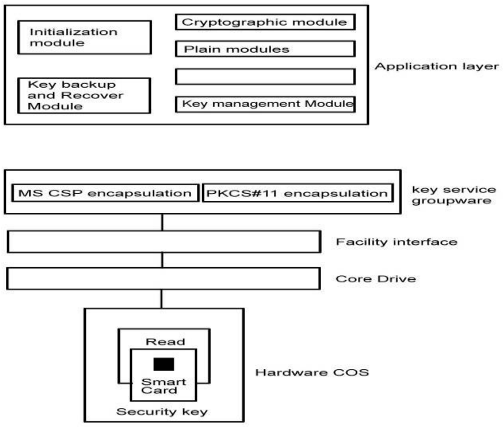

Figure2. Software framework structure

A. USB Security Key Initialization Module

It needs to be initialized Before using the USB security key , only when the USB security key been initializatized , the subsequent operation of the application generated the datas,such as the RSA key pair, the process keys, digital certificates and cryptographic operations in the plaintext or ciphertext will have the appropriate place to store. Of course, the application calls the relevant function, CSP must be able to find a USB security key in the appropriate file at the same time have the ability to read and write the files. Because PIN control the smart card operation and the access authority to other documents of the USB security key, so the USB security key access password PIN is necessary. The general function of this module the role of each of the security key once.During the Initialization,we should follow the following steps: establish the appropriate file system; to set access password PIN (Personal Identification Code); create and initialize the specified which used to store public and private key file; create and initialize the specified use to store passwords in plaintext or ciphertext operations documents; insert the CSP's information into the specified file.

B. Encryption Module

Encryption function is part of the core of the system, before encryption the first thing is detecting the USB interface, we should stop the operation if there is no USB security key. Then, the PIN requires authentication security key code, the wrong type will result in the suspension. Encryption, the system can be divided into two parts operations, as part of the security key to complete, including the security of key internal random number generator to generate the session key, then key in the RSA algorithm for encryption processing engine session key: Ek (K1) = Mk, and then send K1, Mk to the computer; the second part compeleted by the computer, symmetric algorithm is achieved by the code, choose 128-bit AES, encryption keys are generated by the security key K1, EK1 (T) = MT, the final tesk is link the MT that is the encrypted files and the encrypted key Mk to create a new file a ciphertext M.

C. Decryption Module

Decryption function is part of the core of the system,before the decryption,we should also check the security keys and the authentication PIN code, otherwise, the operation ended. In the decryption, the key decryption of the key shoud be finished inside the security key , aim to guarantee the private key never leave the security keys in order to prevent malicious programs to steal.While the file is encrypted on your computer to complete, so improving the efficiency of declassified documents. Decryption process is as follows: First, read MK from the ciphertext M, MK is sent to the security key, by the RSA algorithm processing engine which in the USB security key to decrypt the session key K1, DK (MK) = K1, obtained K1 will be sent to the computer, the computer will decrypt Mp, DK1 (MT) = T, P to plaintext, and need to restore the file type of the plaintext.

D. Key Backup and Recovery

To prepare for an encrypted USB security key is lost and the adverse consequences the key backup module provides a backup feature. Backup, USB security key to first verify that the administrator PIN code, and then enter the password used to protect the key pair, and store the document as a file. The key recovery module provides a key recovery. Recovery, we must first verify that password of the backup file in the security key, then enter the new administrator PIN code of the USB security key .Restored, the new USB security key can be used to decrypt the file.

IV. Conclusion

In this paper, in-depth study of the theory of cryptography based on the analysis of electronic documents stored in many factors of insecurity, proposed a new key-based security technology solutions for file encryption system, using the security key on the key implementation of effective management to ensure that only authorized users can decrypt the file and make the appropriate operation, and use the hash algorithm for file integrity verification, and thus effectively improve the security of electronic documents, ensuring its integrity.

Reference

[1] T.Chiang and Y.-Q. Zhang, “A new rate control scheme using quadratic rate distortion model,” IEEE Trans. Circuits Syst. Video Technol., vol. 7, no. 1, pp. 246–250, Feb. 1997.

[2] D. Kwon et al. “Rate Control for H.264 Video with Enhanced Rate and Distortion Models,” IEEE Trans Circuits and Syst. Video Technol., Vol. 17, pp. 517 - 529, May 2007.

[3] Z. G. Li, F. Pan, K. P. Lim, and S. Rahardja, “Adaptive rate control for H.264,” in Proc. IEEE Int. Conf. Image Process., Oct. 2004, pp. 745–748.

[4] Z. He, et al, “Optimum bit allocation and accurate rate control for video coding viaρ-domain source modeling,” IEEE Trans. Circuits Syst. Video Technol., vol. 12, no. 10, pp. 840–849, Oct. 2002.

[5] Ozcelebi and De Vito, “An Analysis of Constant Bitrate and Constant PSNR Video Encoding for Wireless Networks,” Commun. ICC06, vol. 12, no. 10, pp. 840–849

[6] ISO/IEC 14496-10 AVC, Advanced video coding for generic audiovisual services, ITU-T, May 2003.

[7] Timebleby, H. W., Cairns, P. A., and Jones, M, “Usability analysis with Markov models”, ACM Transactions on Computer-Human Interaction, 2001, vol.8(2), pp. 99-132.

[8] Timebleby, H. W. “User interface design with matrix algebra”, ACM Transactions on Computer-Human Interaction, 2004, vol.11(2), pp. 181-236.

[9] Sucrow, B. E. “Describing a continuous collaborative specification process of human-computer interaction by graph rewriting”, Journal of Integrated Design & Process Science, 5(1), 2000, pp. 87-114.

[10] JIANG Le-tian, XU Guo-zhi, YING Ren-dong, ZHANG Hao, “Application of Stochastic Petri Net to System Availability Analysis”, Journal of System Simulation (in Chinese), vol.14(6), 2002, pp. 796-799.

[11] Timebleby, H. W. and Gow J, “Computer algebra in interface design research”, Proceedings of the 9th International Conference on Intelligent User Interface, Island of Madeira, 2004, pp. 366-367.

[12] Nancy Thorley Hill, Susan E. Perry, Steven Andes. Evaluating Firms in Financial Distress: An Event History Analysis [J]. Journal of Applied Research 1995 12(3).

[13] Stephen A. Ross. Corporate Finance, 5th [M]. The McGraw-Hill Companies, Inc, 1999.

[14] Tirapat Sunti, Nittayagasetwat, Aekkachai. An Investigation of Thai Listed Firms' Financial Distress Using Macro and Micro Variables [J].Multinatioal Finance Journal, 1999, 3(2)