The Design of Smart Fingerprint Portable Storage Device with Encryption Function

LIU Zhaoqing  HAO Kecheng  ZHANG Yigang  NIU Xiamu
Information Countermeasure Technique Institute
Harbin Institute of Technology
Phone (451) 8641-3532   Fax (0451) 8640-2953   E-Mail:liuzq@hit.edu.cn

Abstract: Portable storage devices have small size, large capacity, portability and some other good features, so it has been widely used. However, security problems limit their usage in some occasions with high security demand. In this paper, A novel design scheme of portable storage devices providing biometric recognition and asymmetric cryptographic mechanism is proposed. Identity authentication is realized by the fingerprint recognition module effectively. As the device is compatible with PKCS and CryptoAPI standard, it can utilize an existing PKI system to carry out the secure key management. After the decryption, the plaintext is stored in a temporary plaintext storage area and can be deleted immediately after the transfer to further ensure the security.

I. Introduction

With the rapid development of information technology, computers have become an indispensable part of our daily lives. Hard disk has also turned into the main media for storing information instead of the traditional paper. Meanwhile, as information stored on the hard disk could be easily accessed, the problem of information security stands out. For instance, information on the hard disk may be maliciously stolen through the network if “back doors” were installed by the computer hardware or software manufacturers, which will cause great loss on individuals or even on the country.

Portable storage devices have small size, large capacity, portability and some other good features, so it has been widely used. Yet most portable storage devices currently in use store files with the plaintext format, even the so-called secure portable storage devices only adopt simple password-based access control and symmetric encryption algorithm. They cannot meet the high requirement for security. Furthermore, even if encryption mechanism is provided, protection of the plaintext is often ignored after the decryption processing. All these security loopholes could be taken advantage of by an attacker to steal the stored data illegally. In this paper, a novel design scheme of portable storage device providing biometric recognition and asymmetric cryptographic mechanism is proposed. Sensitive files stored are independent of computers and the operating systems, and are en/decrypted in the device completely by hardware. Fingerprint recognition modules are also included in our scheme, which further upgrade its security level. Our proposed smart portable device is suitable for organizations with high security requirement. And its potential market is prominent.

The rest of this paper is organized as follows: section II presents the encryption scheme and key management. Section III gives the overall design of the device. Section IV shows the design of fingerprint recognition module and en/decryption module. And we conclude with a summary in section V.

II. Encryption scheme and key management

In the present system of encryption, the technology of encryption can be divided into symmetric encryption algorithm and asymmetric encryption algorithm. The mostly used symmetric encryption algorithms are DES, IDEA and so on. Symmetric encryption algorithm has quick encryption speed, high degree of secrecy and other good advantage, but the distribution of the key is a very difficult problem. Asymmetric encryption algorithm mainly is RSA algorithm, which is the most successful asymmetric encryption algorithm at present. The
The advantage of asymmetric encryption algorithm is that it is easy to distribute the key and doesn’t need cryptic channel and complicated protocol to transfer the key. But the en/decryption speed is very low.

The encrypted data stored in the portable storage device need be transferred to the others through the Internet, so the encryption scheme and key management is very crucial. In order to make it convenient for key distribution and management, the smart fingerprint portable storage device adopt a kind of encryption method combining symmetric encryption algorithm and asymmetric encryption algorithm, namely the device combine and use DES and RSA encryption algorithm. The process of encrypting the data stored in the portable storage device is described as follows: firstly it creates a 128 bits of symmetric key of DES algorithm and encrypts the plaintext with the key. Then, he symmetric key is encrypted the public key of RSA algorithm. At last, the data stored in the storage device include: the ciphertext encrypted by DES algorithm and the symmetric key encrypted by RSA algorithm, the private key the process of decryption could be described as follows: the user decrypts the symmetric key with the private key at first, then decrypts the ciphertext with symmetric key and DES decryption algorithm.

The exiting PKI system is utilized to distribute and manage the key. The pair of the asymmetric key is created by hardware inside the portable storage device. The private key is stored in the security area of the portable storage device and nobody has the right to get it. The public key is sent to Certificate Authority (CA) of the PKI system through the Internet, and CA takes responsibility for distributing the key. The data stored in the portable storage device can be transferred safely through the network.

III. Overall design of system

Design the whole structure of the smart fingerprint portable storage device, the structure figure as follow:

The core processor of the system is DSP, which manages the whole operation of the portable storage device, such as reading and storing the file data, en/decrypting data, communicating with user’s computer and so on.

The fingerprint recognition technique is adopted as visiting control of the device. Fingerprint recognition has stability, uniqueness, simple sampling, few store data and other features. At present, fingerprint recognition has already become a kind of ripe biometric recognition technique. The problem of the identification can be solved very well by fingerprint recognition. And the device of fingerprint recognition has the characteristics of small, so it is especially fitted for being applied to portable storage device. Before using the potable storage device, the user’s fingerprint should be compared. The fingerprint sampled at locale should be compared with fingerprint data stored in the potable storage device. Only the result is right, the user has right to operate data stored in the device. The fingerprint recognition technique adopted as visiting control avoids the defects in the traditional method based on password. The problem of the identification is solved very well.

The en/decryption module support DES and other symmetric encryption algorithms and RSA asymmetric encryption algorithm. En/decrypting data is entirely realized by hardware and has high quality of anti-interference. The module could realize secure key management and support data secure exchange and identification combining existing PKI system. ABesides, it is compatible with PKCS and CryptoAPI standard and offers the applied interface, so the device can be applied in all kinds of convenient accord with these two criterions.

USB2.0 communication protocol is adopted for data transfer. The transfer rate of 480Mb/s has fully guaranteed the high speed of data transmission.

The storage area of the device is divided into two
parts: secure storage area and temporary plaintext area. The user’s private key, the encrypted symmetric key, user’s encrypted fingerprint data and encrypted file data. The plaintext is stored in the temporary plaintext area in the decryption proceed. When user wants to read the data in the potable storage device, the cipher is transferred to the en/decryption module to be decrypted by the operation system on chip. Plaintext is stored in the temporary area then is transferred to the user’s computer. After that the plaintext should be deleted quickly, Figure2 shows the working flow. The plaintext only resides in user’s computer, so this could effectually guarantee the security of the plaintext.

IV. module design

A. Fingerprint recognition module

The identification function is realized by the Fingerprint recognition module, which includes fingerprint sample sensor, DSP and storage device. The module samples fingerprint data by high-performance silicon chips and deals with fingerprint data by DSP. It can complete the preprocessing of fingerprint image, extraction of feature point, classification and match of fingerprint, encryption of fingerprint data inside the module.

B. En/decryption module

The en/decryption module supports symmetric encryption algorithm such as DES, IDEA and RSA asymmetric encryption algorithm. DES and IDEA algorithm is realized by FPGA chip, RSA algorithm is realized by big number modular exponentiation multiplier. Figure 3 shows the work flow. The module is compatible with PKCS and CryptoAPI standard. A PKI system can be used to carry out the secure key management, secure data exchange and authentication.

V. Conclusion

Our proposed smart portable device guarantees the security of data storage by adopting symmetric and asymmetric hybrid encryption algorithm along with fingerprint recognition scheme. As the device is compatible with PKCS and CryptoAPI standard, it can utilize a existing PKI system to carry out the secure key management. The smart device is suitable for organizations with high security requirement. The potential market is prominent.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Project Number:
60372052), the Foundation for the Author of National Excellent Doctoral Dissertation of China (Project Number: FANEDD-200238), the Multidiscipline Scientific Research Foundation of Harbin Institute of Technology (Project Number: HIT.MD-2002.11).

The Foundation for the Excellent Youth of Heilongjiang Province, and the Program for New Century Excellent Talents in University.

REFERENCES