UDC 681.327.638

Secure PC Card

●Naoya Torii ●Takayuki Hasebe ●Seigou Kotani

(Manuscript received February 17,1998)

The mobile terminal is expected to become an indispensable tool for business, and the security of data held on these devices will become an important problem. This paper introduces the Secure PC card, which is a user-friendly, high-speed file encryption tool for mobile security that can be automatically combined with application software and provides user authentication for control of access to encrypted files.

1. Introduction

The mobile terminal is expected to become an indispensable tool for business. Mobile terminals are light-weight and small for easy handling. However, these features also make it easy for mobile terminals to be lost or stolen and a consequent loss or leak of confidential information to occur. Therefore, the security of confidential information stored in a mobile terminal is an important issue.

This paper introduces the Secure PC Card for Windows 95, which is an encryption tool for files held in mobile terminals.

2. Development aim of the Secure PC card

The aim of developing the Secure PC card was to provide a user-friendly tool for file encryption.

2.1 Automatic combination with application software

By using a special file driver, the file encryption/decryption function is enhanced without the need to make any changes to the application software. Files are encrypted or decrypted automatically by reading or writing from a conventional word processor or spread sheet application.

2.2 High-level security and wide usage

User authentication for encrypted files is provided. Key management is done using a hierarchical key structure, which provides a simple but high-level security suitable for business use. Key management includes a recovery operation in case the hardware fails or is lost and supports a variety of applications.

2.3 High-speed encryption

Because of the high-performance configuration and high-speed PC interface of the Secure PC card, it can encrypt data on a standard PC without causing processing delays.

3. Features of the Secure PC card

Figure 1 shows a picture of the Secure PC card, and **Table 1** shows its main specifications.

3.1 Automatic combination with application software

The original configuration of encryption files is used to enable random access to file data and to minimize the overhead. Also, a security driver is used to encrypt or decrypt files automatically.

3.1.1 Encryption file configuration

The Secure PC card encrypts files into a

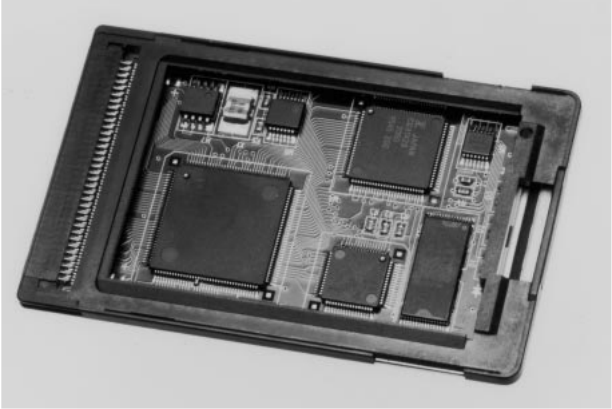


Figure 1.
Secure PC card.

Table 1. Main specifications of the Secure PC card.

Interface	PCMCIA Type II
Encryption algorithm	DES
Mode of operation	CBC (8-bit OFB[note1)])
Thoughput	1 M bytes /s
Power consumption	0.6 W
Weight	28 g

note1) Applied to data blocks less than 8 bytes long.

unique configuration. The encryption algorithm is the Data Encryption Standard (DES) of the United States.[1)]

Files are encrypted in CBC mode operation[2)] to achieve high security. Files are configured for random access, and the plaintext and ciphertext are the same size.

The plaintext file is divided into 512-byte blocks, and each block is encrypted in CBC mode. In general, changing intermediate data in the encrypted file in CBC mode affects all of the subsequent data. Even if just a single byte in the first part of a CBC-encrypted file is changed, encryption operations will have to be performed right up to the end of the file. In the Secure PC card, on the other hand, a change made to an encrypted file affects up to only 512 bytes (file sector size) of data, depending on the file configuration. This enables fast and easy access to an encryption file even if an application makes random accesses to it.

When a file is encrypted, its size remains the same. A file is encrypted in units of eight bytes in DES CBC mode for fast processing. If the last data block of the file contains less than eight bytes, the Secure PC card encrypts it in OFB mode[2)] .

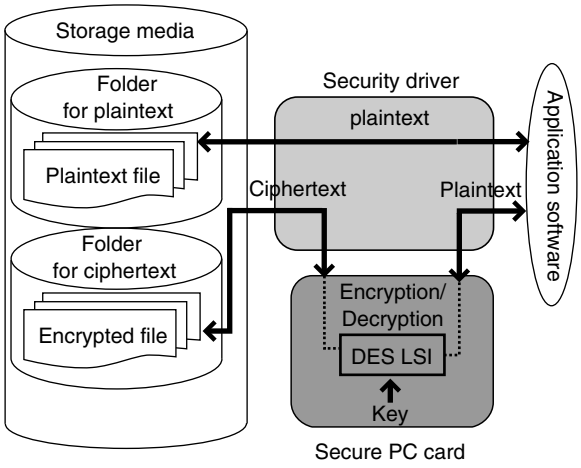


Figure 2.
Secure PC card.

3.1.2 Security driver

Once the Secure PC card is installed on a PC, a special file driver called the security driver is installed. Using this driver, a folder on the storage device, (e.g., hard disk or MO) is assigned to the encrypted file. This folder is called the encrypted folder and is created when the security driver is activated the first time after installation. (**Figure 5(a)** shows the dialog box for creating an encrypted folder.)

Figure 2 shows the role of the security driver. The security driver monitors accesses to the encrypted folder by the application software. When an access is detected, the security driver hooks the access and the file access is processed via the Secure PC card, which encrypts and decrypts the file. When the security driver accesses another folder, it bypasses the access. The security driver works only when the password authentication to the Secure PC card has been validated.

The security driver performs a file read operation as follows.

First the security driver hooks the read request from the application software and obtains the read function parameters such as the read

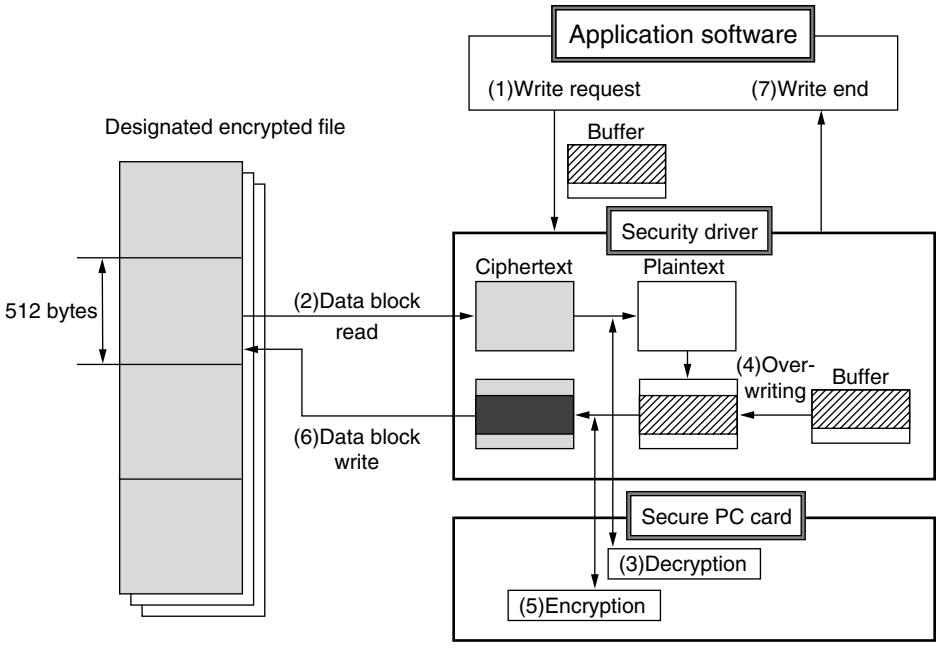


Figure 3.
File write operation.

point, read size, and return address for the file system. Then, it searches for the required encrypted block and reads it. The security driver transfers the block data to the Secure PC card for decryption and then receives the decrypted block. The security driver retrieves the requested data, writes it to a buffer, and informs the application that the read operation has been completed. If the requested data covers two blocks, they are read, decrypted, and retrieved successively.

The file write operation performed by the security driver is shown in **Figure 3**. The application software writes data to the buffer and requests the file system to save it in a folder. The security driver hooks the request and obtains the write function parameters such as the write point, write size, and return address for the file system. Then, it searches for the appropriate encrypted block and reads it. Then, the security driver decrypts the block using the Secure PC card, overwrites the decrypted (plaintext) block with the buffer data, encrypts the block using the Secure PC card, and writes it to the file. Finally, the security driver informs the application that the write operation has been completed.

From these operations, it is clear that the security driver does not generate a temporary file for decryption. Decrypted data exists only in the memory of the PC. This method of reading/writing prevents the leakage of information which can occur when a conventional PC system hangs up.

3.2 Security

The user authentication performed to validate accesses to an encrypted file and the key management of the Secure PC card is described below.

3.2.1 User authentication

To access an encrypted file in the encrypted folder, a user must pass a user password authentication test. The user's identification number (ID) and password are registered in advance with the Secure PC card. The ID and password are linked to the user key for file encryption.

Figure 5(b) shows the dialog box for user authentication.

Because an encrypted file cannot be decrypted without the associated key, the user can prevent access simply by removing the Secure PC card.

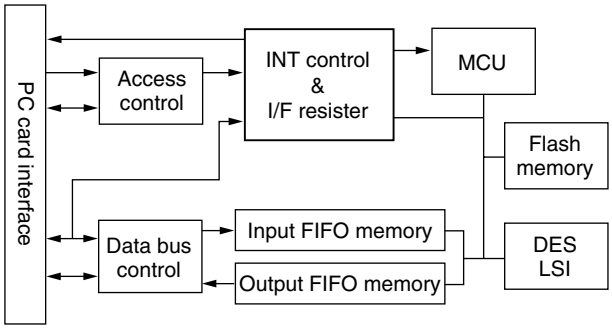
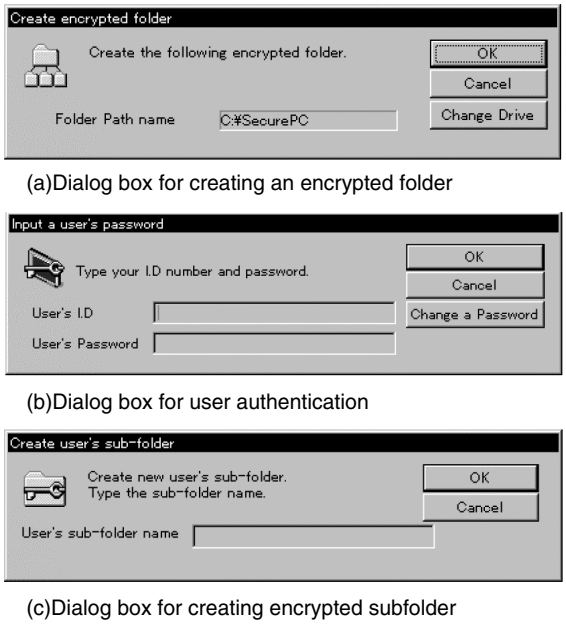


Figure 4.
Hardware block diagram.



(a)Dialog box for creating an encrypted folder

(b)Dialog box for user authentication

(c)Dialog box for creating encrypted subfolder

Figure 5.
Dialog box for user interface.

3.2.2 Key management

There are two types of keys in the Secure PC card: user keys and card keys. The user keys are used for file encryption and decryption, and the card keys enable the key encryption key to load the user keys. Card keys and user keys are managed in three layers: the top layer, middle layer, and bottom layer. Each card can generate card keys and user keys for any layer beneath it.

Each card has a unique card ID (Identification), card key, user IDs, and user keys. Keys are generated by ID (Identification)-based generation.

The key manager for the top layer can decrypt all encrypted files in all three layers.

3.2.3 Countermeasures for hardware problems

A method for file decryption is needed in the event that a Secure PC card becomes broken or lost. It is clear from the previous section that the card for the top layer can regenerate a card key and user key for the middle layer and bottom layer. Encrypted files in the bottom and middle layers can be decrypted after the top layer key manager regenerates their card keys and user keys.

If a PC containing files encrypted by a Secure PC card is stolen, the encrypted files cannot be decrypted without the Secure PC card.

3.2.4 Firmware exchange

The firmware for the MCU(Micro Controller Unit), which controls the Secure PC card, is stored in a 4 M-bit flash memory. Once the firmware is written in the flash memory, it cannot be changed by the firmware structure or hardware. To load the firmware into a card, the card must be a virgin card, which means that all information in the flash memory and hardware is initialized.

The firmware for the Secure PC card can be created and modified using the unique or special development tool. The Secure PC card can support a variety of functions which require a DES engine.

3.3 High-speed encryption

This section describes the hardware configuration which enables high-speed encryption and describes the hardware's performance.

3.3.1 Hardware configuration

Figure 4 shows the hardware configuration of the Secure PC card.

The card is controlled by a Fujitsu 8-bit MCU. The DES LSI, which was specially developed by Fujitsu, is the encryption engine containing the DES algorithm. The card supports CBC/OFB mode operation. To achieve a high-speed data interface, two FIFO (First In First Out memories) are provided. The 16-bit input data from the PC

card interface is routed to the input FIFO memory via the data bus control. Then, the data is input to the DES chip in 64-bit blocks, where it is encrypted or decrypted. The output of the DES chip goes to the output FIFO memory and then to the PC card interface via the data bus control.

This configuration enables pipelining of input processing, output processing, and encryption processing, and thereby enables high-performance data encryption.

Commands to the card arrive at the MCU via the I/F register. To give a command, the command data is input to the FIFO memory, then a flag in the I/F register is set to indicate that the FIFO memory has received a command. Next the MCU reads the command data from the input FIFO memory and processes it. The hardware specifications are shown in Table 1.

3.3.2 Performance

The hardware configuration shown in Subsection 3.3.1 enables high-performance operation. The hardware can encrypt a file at the rate of 1 Mbytes/s. The throughput shown in the table was obtained on an FMV 5120, which has a 120 MHz Pentium processor and 32 Mbytes of memory. The DES chip can encrypt a file at 16 Mbytes/s. The throughput is determined mainly by the PC card interface.

4. Applications for the Secure PC card

The Secure PC card can support 16 user keys, so the encryption folder can have up to 16 sub-folders. This enables the encryption folder to be used in a variety of ways; for example, a single user can use all 16 sub-folders or a Secure PC card can be shared by up to 16 users, with each user having access to one sub-folder in the encryption folder. A sub-folder is created when a new ID is input at user authentication. **Figure 5(c)** shows the diaglog box for creating an encrypted sub-folder.

Layered key management is suitable for company organization because companies commonly give higher-level personnel wider access to confidential files.

A card for an upper layer can decrypt a file in a lower layer, but a card for a lower layer cannot decrypt a file in an upper layer. However, a special function is provided which decrypts an encrypted file using a top layer user key and encrypts it using a lower layer user key in the Secure PC card. This function can be used only by the upper layer key manager.

5. Conclusion

This paper introduced the Secure PC card, which is a compact DES hardware engine that provides high-security functions. This is the first file security system which does not require changes to applications and does not generate a temporary plaintext file. We will continue with our work to create a card for the finance/business world which operates on various OS platforms, for example, Windows NT/98.

Trademarks

References

1) FIPS PUB 46 : Data Encryption Standard. Federal Information Processing Standards Publication 46, U. S. Department of Commerce/National Bureau of Standards/National Technical Information Service, Springfield, Virginia, 1977.

2) ISO8372 : Information processing - Modes of operation for a 64-bit block cipher algorithm. International Organization for Standardization, Geneva, Switzerland, 1987.

Naoya Torii received the B.E. and M.E. degrees in Communication Engineering from Osaka University, Suita, Japan in 1981 and 1983, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1983, and has been engaged in research and development of voice scramblers, high-speed encryption engines, and information security systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan and the IEEE.

Takayuki Hasebe received the B.E. and M.E. degrees in Electronics Engineering from Tokyo Institute of Technology, Tokyo, Japan in 1983 and 1985, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1985, and has been engaged in research and development of package exchange networks, voice scramblers, and information security systems.
He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Seigo Kotani received the B.S. degree in Physics from Tohoku University, Sendai, Japan, the M.S. degree in Material Engineering from Tsukuba University, Ibaragi, Japan, and the Ph.D degree in Electronic Engineering from Nagoya University, Nagoya, Japan in 1980, 1982, and 1991, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1982, and has been engaged in research and development of Josephson logic circuits, information security, and file systems.