SDMS-based Disk Encryption Method

Dokjun An, Myongchol Ri, Changil Choe, Sunam Han, and Yongmin Kim

Faculty of Mathematics, Kim Il Sung University, D.P.R.K
mathcci@yahoo.com

Abstract. We propose a disk encryption method, called secure disk mixed system (SDMS) in this paper, for data protection of disk storages such as USB flash memory, USB hard disk and CD/DVD. It is aimed to solve temporal and spatial limitation problems of existing disk encryption methods and to control security performance flexibly according to the security requirement of system. SDMS stores data by encrypting with different encryption key per sector and updates sector encryption keys each time data is written. Security performance of SDMS is analyzed at the end of the paper.

1 Introduction

Massive use of mobile storage media raises data security problem seriously. Data security of mobile storage media can be realized in different ways, e.g., file unit encryption, file system level encryption, and full disk encryption [1, 3, 4, 5, 6]. Reliability of security system should not be based on system mechanism or complexity of system analysis, and it should guarantee safety even if system mechanism or encryption algorithm is opened to third party. We analyze security problems of existing disk encryption methods in the next section and describe our disk encryption method based on SDMS in the following section. In the last section, we analyze security performance of our system.

2 Previous Works

Several different methods for disk encryption, such as LoopAES, EFS, TrueCrypt, NCryptfs, were suggested [4, 5, 9, 10, 11]. In these methods, encryption of disk block is expressed as follows.

$$C = OP(BE(OP(P, DEK, i), DEK), DEK, i)$$

Here, BE is block encryption function (AES, 3DES, etc), OP is operation function (CBC, LRW, XTS, etc), DEK is disk encryption key, C is ciphertext, P is plaintext and i is block index. As above expression shows, these disk encryption systems encrypt plaintext using symmetric-key algorithm through certain operation and apply this operation again to encrypted result. [7] and [8] explain BitLocker disk encryption method and its security strength, which is offered in Windows Vista. Here, plaintext is XORed with sector key, passed two diffusers

in succession, and finally encrypted using AES of CBC mode. These disk encryption methods have some weakness in terms of time passage and space expansion. We call it temporal limitation and spatial limitation, respectively, in this paper.

- *Temporal limitation*
  If third party succeed to detect encryption key of a certain sector, data which is stored later in this sector can be decoded.
- *Spatial limitation*
  If third party succeed to detect encryption key of a certain block, whole data of disk is in danger of being decoded.

GBDE based encryption method which was implemented in FreeBSD overcame these temporal and spatial limitations to a certain extent [6]. In this method, data is stored in sector by being encrypted with different key each time data is writen, because it generates random data newly and encrypt plaintext using it. Therefore, it is impossible to decrypt data stored newly even though third party succeeds to detect key by attacking a sector. And each key encrypting plaintext sectors are different each other when it writes data on disk, because GBDE encrypts plaintext using randomly generated key. Thus, it is impossible to decrypt data of other block even if third party detects encryption key by attacking a data sector. Although GBDE based disk encryption method overcomes temporal and spatial limitations of previous disk encryption methods considerably, it still has some security problems to be solved.

At first, key-key for a given sector is fixed because it is decided depending on the sector address. That is, when it was writen new data on sector, sector key is encrypted by same key-key. Then, if attacker detect 128bit sector key by attacking AES/CBC/128 encrypted plaintext data and detect key-key subsequently by attacking AES/CBC/256 encrypted sector key, it is possible to decrypt newly stored data on this sector. We think this is temporal limitation of GBDE based disk encryption.

Next, it is easy to get keychain used to encrypt plaintext data, if the correlation between random data generated consecutively by PRNG is revealed, because it directly uses random data generated by PRNG as key for plaintext. However, strictly speaking, PRNG generates data deterministically based on the initial value. If attacker succeeds to get sector key by attacking key sector and subsequently succeeds to know inner state of PRNG, he can detect following sector keys easily. This allows possibility of decrypting consecutive ciphers by attacking one sector. Of course, it is possible to make difficult to predict future data from past data using cryptographically secure PRNG, but it causes another security problem that safety of system depends on the safety of PRNG too much. We think this is spatial limitation of GBDE based disk encryption. In the next section, we present a new disk encryption method based on the SDMS.

3 SDMS-Based Disk Encryption

In section 2, we discussed temporal and spatial limitations of previous works for disk encryption and concluded that GBDE still has security problem to be

solved, while it is a good disk encryption method. In this section, we propose SDMS (secure disk mixed system) aimed to solve temporal and spatial limitation of existing disk encryption methods and to control security performance flexibly according to the security requirement of system.

3.1 SDMS

SDMS is a method to encrypt each sector by generating sector key using randomly generated SEED and disk encryption key DEK. In our method, encryption key of each sector is different each other and it is changed whenever encryption is done.

Data Structure SDMS manages data area of media by dividing into SDMS blocks. Each block consists of SDMS_BLOCK_DA area storing encrypted data and SDMS_BLOCK_SA area storing random numbers which are used to generate encryptioin key for the encryption of SDMS_BLOCK_DA area.

SDMS_BLOCK_SA area consists of SDMS_UNIT_SEEDs which are SEED data for each sector. Fig. 1 shows data structure of SDMS. Size of each area is determined depeding on the size of random data SDMS_UNIT_SEED needed to generate sector key.

$$SIZE(SDMS\_BLOCK\_DA) = \\ SIZE(SDMS\_BLOCK\_SA)/SIZE(SDMS\_UNIT\_SEED) \times 512$$

If we store SDMS_BLOCK_SA in one sector, the number of sector of SDMS_BLOCK_DA is equal to 512 / SIZE(SDMS_UNIT_SEED). For example, if we set SIZE(SDMS_UNIT_SEED) = 8 byte (128 bit), then the number of sectors of SDMS_BLOCK_DA is equal to $512 \times 8/128 = 64$. That is, 64 plaintext sectors constitute a SDMS block (SDMS_BLOCK) and one SEED sector (SDMS_BLOCK_SA) is in this block.

There is no constraint that SDMS_BLOCK_SA must be one sector in SDMS block. System designer can adjust this setting freely according to the security requirement and this setting will change processing of blocks of SDMS.

Data Encryption Encryption mode of SDMS is expressed as follows.

$$C = EA(P, RTEK)$$

Here, EA is encryption function, RTEK is encryption key, C is cipher, and P is plaintext. RTEK is determined on the fly in time of real-time encryption (or decryption) as follows.

$$RTEK = DK\_Func(DEK, SEED, i)$$

Here, DEK is disk encryption key, SEED is random data in SDMS_UNIT_SEED area, i is sector index and DK_Func is key derivation function. DK_Func is a

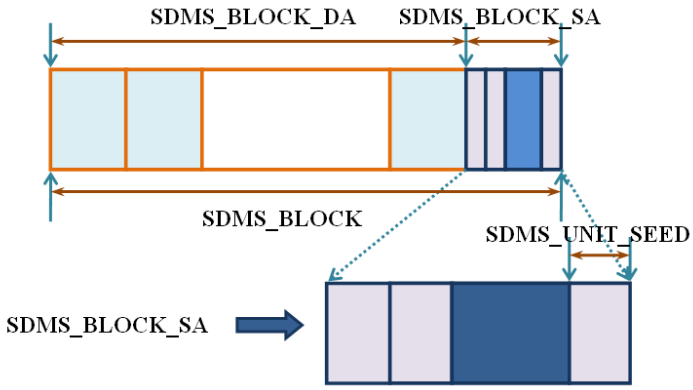

Fig. 1. Data structure of SDMS

function to derive real-time encryption key from disk encryption key, SEED and sector index. It is a one-way function where the length of output is constantly the same as the length of RTEK. Encryption and decryption algorithms of SDMS are as follows.

- *Encryption*
  - Writing request for i-th sector
  - Random generation of SEED
  - Calculation of RTEK
  - Encryption of plaintext with RTEK
  - Writing cipher on SDMS_BLOCK_DA
  - Writing SEED on SDMS_BLOCK_SA
- *Decryption*
  - Reading request for i-th sector
  - Getting SEED from SDMS_BLOCK_SA
  - Reading cipher from SDMS_BLOCK_SA
  - Calculation of RTEK
  - Decryption of cipher with RTEK

3.2 DEK Management

DEK is generated when disk is initialized and is used to encrypt whole data of disk. If DEK is revealed, attacker can decrypt whole data of disk. DEK can be stored in the same disk with plaintext or in physically separated memory device such as USB memory or file server of high security level. No matter it is stored in data disk or physically isolated memory device, DEK must be encrypted based on the user authentication information. User can be authenticated through PKCS#5 based password authentication or PKCS#11 based smart card

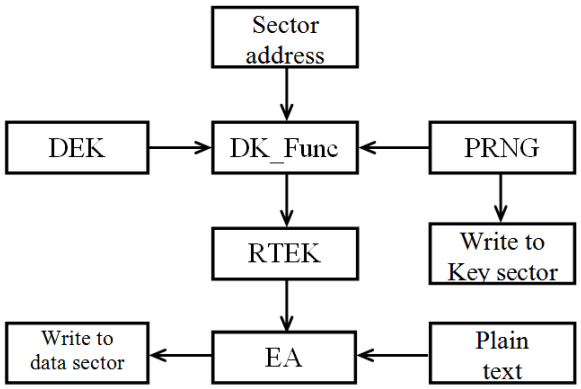

Fig. 2. Data encryption in SDMS

authentication or SSL based network authentication, but what is important is to receive key safely for the decryption of DEK [12, 13]. In this paper, we only consider disk data encryption which uses DEK, on the premise that DEK is managed safely, though DEK is very important for the reliabile management of data.

3.3 Sector Key Derivation Function DK_Func

DK_Func is a function to get sector encryption key RTEK in real time for the encryption of sector.

$$RTEK = DK\_Func(DEK, SEED, i)$$

As we can see here, it outputs sector key for sector encryption from DEK, SEED corresponding to the sector, and the sector index. Input data space must be larger enough than output data space in the design of DK_Func. For instance, if DEK is 2048 bit, sector index is 32bit and SEED size is 128bit, then input data space is $2^{2048+32+128}$. Therefore, in case of using AES/XTS for sector encryption, 512 bit key is needed, and hence output space is 2^{512} which is smaller enough than input space. DK_Func must be implemented so as to satisfy one-wayness and collision resistance as possible. So it is desirable to construct DK_Func using cryptographically safe hash function or hash chain.

3.4 Security Feature of SDMS

Firstly, SDMS solved temporal limitation problem of data encryption. SDMS generates encryption key by generating random SEED newly each time when writing request occurs. This makes it impossible to decrypt sector data written later, although attacker succeeds to break RTEK of the sector.

Secondly, SDMS solved spatial limitation problem of data encryption to a certain extent. In SDMS, even though attacker succeeds to attack EA encrypted certain sector, the only thing he knows is RTEK of that sector. He cant read the contents of other sectors unless he knows DEK through the attack on EA or DK_Func. In this way, SDMS overcomes remarkably security weakness that whole data of disk can be revealed by succeeding to attack a particular sector.

Thirdly, SDMS can control security performance flexibly according to the sequrity requirements. SDMS generates encryption key using disk encryption key DEK and random SEED. DEK can be set big enough according to the security requirement. For instance, if we set DEK as bigger than 1024 bit, then search space will be increased more than 2^{1024} when attacker attacks DKFunc to know DEK. The size of SEED (SIZE(SDMS_UNIT_SEED)) which is used to generate sector key for sector encryption can also be set big enough according to the security requirement of system and there is no restriction that SDMS_UNIT_SEED must be arranged to each sector. Configuring system to generate sector key by arranging one SDMS_UNIT_SEED to several sectors, we can coordinate balance between security performance and operation cost reasonably.

4 Analysis Result

4.1 Cost of Brute Force Search

Attacker must attack encrypted sector data unless he knows user authentication information or decrypted DEK by evil code. If sector keys that encrypted sector data have no statistical characteristics and there is no information or algorithm helpful to estimate sector key, brute force search will be appropriate method. In case using AES/XTS/256 for sector encryption, the amount of computation will be equal to $W_{AES/XTS/256} \times 2^{512}$. Here, AES/XTS encryption is expressed as follows [16].

$$C_i = E_{k1}(P_i \ XOR \ (E_{k2}(n) \times a^i)) \ XOR \ (E_{k2}(n) \times a^i)$$

Here, $\times$ is multiplication operator in modulo $GF(2) = x^{128} + x^7 + x^2 + 1$, K1 is key of symmetric key encryption algorithm (E), K2 is secondary key, i is block index in encryption unit (sector), n is address of encryption unit (sector) and is base of GF (Galois Field).

Attacker also can decrypt whole data of disk if he knows DEK. Therefore, attacker may try to attack DEK and then to decrypt sector data using it. To attack DEK, he must attack DK_Func which derives sector key. He can find necessary items in $2^{SIZE(DEK)}$ space because he knows SEED and sector index which are the inputs of DK_Func. For instance, if SIZE(DEK)=2048, attacker must search 2^{2048} space. In case AES/XTS/256 is selected as EA, 256bit key for XTS operation and 256bit key for final AES block encryption are needed, and thus totally needed key is 512bit. Therefore, attacker can find candidates outputting same RTEK if he calculate DK_Func for about 2^{512} DEK candidates

with computation $W_{DK\_Func} \times 2^{512}$. There exists about $2^{2048-512}$ candidates in this case.

Now consider the case decoding an other sector using this candidate. Assuming sector index is 32bit, the possibility of successful decryption of next sector is very small.

$$1/2^{2048-512+32+SIZE(SDMS\_UNIT\_SEED)} = 2^{-(2048-512+32+SIZE(SDMS\_UNIT\_SEED))}$$

That is because we use sector index and SEED when we calculate RTEK for other sector. To get correct DEK from $2^{2048-512}$ DEK candidates in 2^{2048} space is very difficult, though it would be possible to get sector key by attacking particular sector.

4.2 PRNG and Security Performance

Security problem in case using the result of PRNG as key directly for sector encryption was considered in section 2. SDMS uses the output of PRNG as input of DK_Func for getting sector key and stores output of PRNG on disk without changing. To attack disk data encrypted using SDMS needs not attack PRNG. Random data generated by PRNG

- solves temporal limitation of disk encryption by changing sector key each time it writes data,
- solves spatial limitation of disk encryption by setting sector key of each sector differently,
- makes it more difficult to attack DK_Func.

That is, performance and quality of PRNG in SDMS have no big relevance with security performance of system.

References

1. Myongchol Ri: A method for upgrading copy speed in mobile storage device of disk encryption Mode. Journal of Kim Il Sung University, Vol 57, No 4, 2011.
2. W. Stallings: Cryptography and Network Security. Principles and Practices. Fourth Edition, Prentice Hall, 592 pages, 2006.
3. Rick Lehtinen: Computer Security Basics. 2nd Edition, O'Reilly, 310 pages, 2006.
4. Tom Olzak: Evaluation of TrueCrypt as a Mobile Data Encryption Solution. 2008.
5. Clemens Fruhwirth: Hard disk encryption with DM-Crypt, LUKS, and cryptsetup. ISSUE 61, 2005.
6. P.H.Kamp: GBDE-GEOM Based Disk Encryption. BSD Con'03, 57-68, 2003.
7. Niels Ferguson: Microsoft AES-CBC + Elephant diffuser A Disk Encryption Algorithm for Windows Vista, 2006.
8. Microsoft Corporation: Bitlocker drive encryption technical overview. Technical report, Microsoft Corporation, 2008.
9. Jari Ruusu: LoopAES, 2005, http://loop-aes.sourceforge.net/.

10. Microsoft Corporation: Encrypting File System for Windows 2000. Technical report, 1999.
11. S. Shepler: NFS Version 4 Protocol. Tech. Report RFC 3010, Network Working Group, 2000.
12. RSA Laboratories: Password-Based Cryptography Standard. Technical Report PKCS #5, RSA Data Security, 1999.
13. PKCS#11 v2.10: Cryptographic Token Interface Standard. RSA Laboratories, 1999.
14. A. Srinivasan, M. Mascagni, and D. Ceperley, Testing parallel randomnumber generators, Parallel Comput., vol. 29, No.1, pp. 6994, 2003.
15. Laszlo Hars and Gyogy Petruska, "Pseudorandom Recursions: Small and Fast pceudorandom Number Generators for Embedded Applications"EURASIP Journal on Embedded Systems, No1, 2007.
16. R. K. Watkins, J. C. Isaacs, and S. Y. Foo: Evolvable random number generators: A schemata-based approach. In 2001 Genetic and Evolutionary Computation Conference Late Breaking Papers, pages 469473, 2001.