Collect and Broadcast News in Security

Heng-Sheng Chen, Tsang-Yean Lee, Huey-Ming Lee
Department of Information Management
Chinese Culture University
55, Hwa-Kung Road, Yang-Ming-San, Taipei (11114), TAIWAN
{chenhs, tylee, hmlee}@faculty.pccu.edu.tw

ABSTRACT

The data must keep security in the computer system. We collect all data (news) and broadcast them to all users. We avoid the data to be modified by attacker and broadcast the wrong message. We propose the method to collect the news and store them in computer system in security. We encrypt the news and store the encrypted news in the encrypted news database. We set encryption data table and use it to encrypt the news file to encrypted news data. The news has different location code in the news information database. We use location code to insert encryption data table to encrypted news and store the encrypted news to encrypted news database. We create the broadcast list table to broad the order of news. When we want to broadcast, we decrypt the encrypted news first and then show out. We use this location code of news in the news information database to get encryption data table in the encrypted news. We use encryption data table to do decryption. When we install these algorithms in the computer system to process, it is securer.

Keywords

Algorithm, Cipher text, Decryption, Encryption, Plaintext

1. INTRODUCTION

The functions of security system are security, authenticity, integrity, non-repudiation, data confidentiality and accessed control [2,15,16]. Rivest et al. [14] proposed public cryptosystem. In 1974, IBM proposed an algorithm to review. In 1977, NBS (National Bureau of Standards, U.S.A) [9,10] suggested this proposed algorithm as data encryption standard (DES). McEliece [7] used algebraic coding theory to propose public key. Diffie and Hellman [3] proposed the concept of pubic key. 1988, Miyaguchi [8] developed fast data enciphered algorithm (FEAL-8). NIST (National Institute of Standards and Technology) [11,12] proposed secure hash standard (SHS). Biham and Shamir [1] proposed differential attack. When new encryption is proposed, cryptanalysis starts to develop to attack.

Lee and Lee [6] used the basic computer operations of insertion, rotation, transposition, shift and pack to design encryption and decryption algorithms. The encryption data table is stored in the computer system and is fixed. Lee and Lee [4] extend to store the encryption data table in the cipher text and it is different each time. It is more difficult to do cryptanalysis.

The encryption programs and files may be stolen. The thieves use volume of data (same or different) to test and get many cipher text. They analysis the cipher text and do cryptanalysis. Lee and Lee [5] proposed the following items must be solved in the encryption algorithm:

1. Brute-force by volume of data to test;
2. Data uncertainty;
3. Change contents of plaintext;
4. Position exchange;
5. Simple computation;
6. Encryption data is variable.

We explain how to solve above items as following:

1. Brute-force by volume of data to test:
   Volume of same data are received, we need length and content of the cipher text to be different each time. We divide the data to blocks and rotate each block and set different length and content of encryption data table to solve.
2. Data uncertainty:
   We insert dummy data to the trail of news.
3. Change contents of data:
   We set left shift table each time. Following this table, we left shift each byte of data. The contents of data will be changed.
4. Position exchange of news data:
   We use displace offset to change the order of news data.
5. Simple computation:
   We use shift, insert, transpose and rotate of computer basic operations to encrypt the news data.
6. Encryption data table is variable:
   The length and value of the encryption data table are different each time. We store it to the cipher text (encrypted news data). We use it to do decryption.

In this study, we collect news data from local and remote sites. We set location code and encryption data table each time. We use encryption data table to encrypt news data to produce encrypted news data. We use the location code to insert the encryption data table to produce new encrypted news data. When we want to broadcast, we use location code to get encryption dada table and use it to decrypt remaining encrypted news data to produce the original news data. If

ICIS 2009, November 24-26, 2009 Seoul, Korea
Copyright © 2009 ACM 978-1-60558-710-3/09/11... $10.00"

these methods are installed to computer system, the news data processed and stored is more secure.

2. THE PROPOSED METHOD DESCRIPTION

The proposed method is to collect and broadcast the news in security. We receive the news and create news information database. It contains date, category, serial number, location code, length of encryption data table and length of news. We set different encryption data table. We use this encryption data table to encrypt this news to produce encrypted news data. We get location code from news information database. We insert encryption data table to the point of location code of encrypted news data. We store his encrypted news to encrypted news database (ENDB) in computer system. When we want to broadcast the news, we get encrypted news from ENDB and location code in NIDB. From the location code, we get the encryption data table from the encrypted news. We use encryption data table to decrypt remaining encrypted news to get the news and broadcast. When these methods are installed in the computer system, we will collect and broadcast news more secure.

We explain table, file, database and processes as follows:

2.1 Table, File and Database

The tables, files and database are as following.

2.1.1. News File

Receive the news file as Table 1.

Table 1. News file

News

2.1.2 News Information Data Base (NIDB)

The NIDB contains date, category (CG), serial number (SN), location code (LC), length of encryption data table (LEDT) and length of news (LN) as Table 2.

Table 2. News Information Data Base (NIDB)

Date	CG	SN	LC	LEDT	LN

2.13 Encryption Data Table (EDT)

EDT contains format code (FC), direction flag (DF), number of block (NB), number of rotated byte (RB), left shift table (LST) and displace offset (DO) as Table 3.

Table 3. Encryption Data Table (EDT)

FC	DF	NB	RB	LST	DO

Where FC:	Format Code;
DF:	Direction Flag
NB:	Number of Blocks;
RB:	Number of Rotated Byte;
LST:	Left Shift Table;
DO:	Displace Offset.

2.1.4 Encrypted news Data Base (ENDB)

The encrypted news data is stored in encrypted news data base (ENDB). It contains category (CG), serial number (SN) and encrypted news data (END). It uses CG and SN as key to create ENDB as Table 4.

Table 4. Encrypted News Data Base (ENDB)

CG	SN	END

2.1.5 Broadcast List Table (BLT)

BLT contains category (CG) and serial number (SN), as Table 5. We use BLT to broadcast the news in order.

Table 5. Broadcast List Table (BLT)

CG	SN

2.2 Processes

To process news data, we have the following operations.

2.2.1 Create news information database (CNIDB)

Set date, category and serial number, location code, length of encryption data table and length of news. Write it to NIDB (News Information Data Base)..

2.2.2 Create encryption data table(CEDT)

Set different encryption data table as following:
Set format code (FC), direction flag (DF), number of block (NB).
Number of rotated byte (RB), left shift table (LST) and displace offset (DO).
Compute the length of encryption data table (LEDT).
Store LEDT to news information database (NIDB).

2.2.3 Encrypt news data file

Follow encryption algorithm to encrypt the news data to produce encrypted news data.

2.2.4 Store encrypted news data

Use category (CG) and Serial number (SN) as key to store encrypted news data to encrypted news database (ENDB).

2.2.5 Create broadcast list

It creates the order of broadcast list. It will insert or delete the entry and produces new broadcast list.

2.2.6 Decrypt encrypted news data.

The processes are as following:
Get category and serial number to find location code (LC) and length of encryption data table (LEDT) in NIDB.
From category (CG) and serious number (SN) find the encrypted news data in ENDB.
From LC and LEDT, get encryption data table in the encrypted news data.
Use this encryption data table to decrypt the remaining encrypted news data.
Get the news data.

2.2.7 Broadcast news

It broadcasts the news to the request.

3. THE PROPOSED MODEL

We present the news process module (NPM) on the computer system. It contains collect news process module (CNPM) and broadcast news process module (BNPM). NPM module is shown in Figure. 1.

CNPM processes to collect news data and produce encrypted news data. It stores it to computer system.

BNPM processes to follow the broadcast list to decrypt the encrypted news data and broadcast them to request.

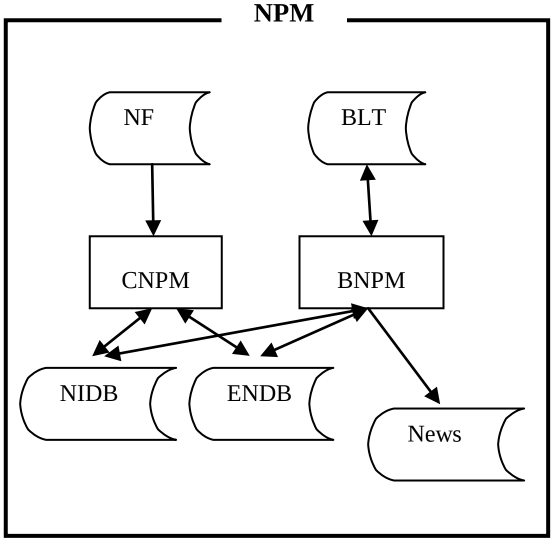

Figure. 1 Framework of the proposed NPM

3.1 Collect news process module (CNPM)

CNPM has create news information component (CNIC), create encryption data table component (CEDTC), encrypt news data component (ENDC) and store encrypted news component (SENC). CNPM is shown in Figure. 2.

The functions of these components are as the follows:

3.1.1 Create news information component (CNIC):

CNIC receives news data from local or remote sites. It sets date, category (CG), serial number (SN), location code (LC), length of encryption data table LEDT) and length of news (LN). It creates news information data base (NIDB).

3.1.2 Create encryption data table component (CEDTC)

CEDTC creates the encryption data table (EDT) to encrypt news data. The content of EDT is as Table 3.

3.1.3 Encrypt news data component (ENDC)

ENDC uses EDT to encrypt new data to produce encrypted news data.

3.1.4 Store encrypted news data component (SENDC)

SENDC uses CG and SN in NIDB as key to store encrypted news data to encrypted news data base (ENDB).

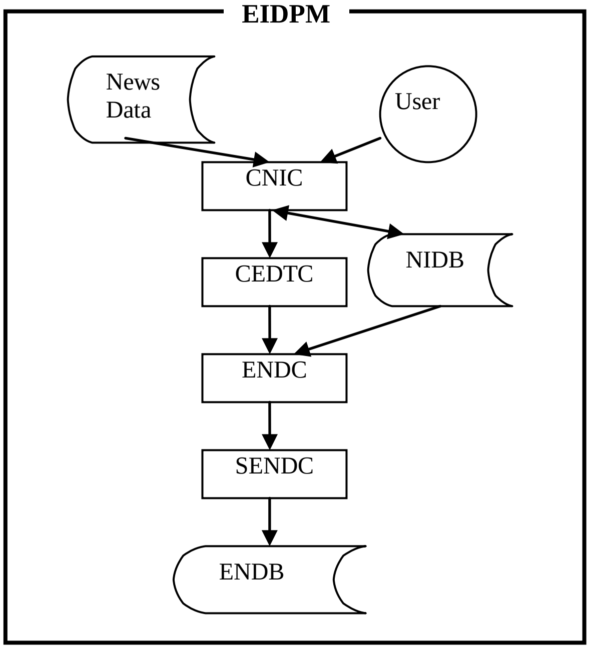

Figure 2. Architecture of the CNPM

3.2 Broadcast news process module (BNPM)

BNPM has create broadcast list component (CBLC), decrypt encrypted news component (DENC) and broadcast news component (BNC). BNPM is shown in Figure 3.

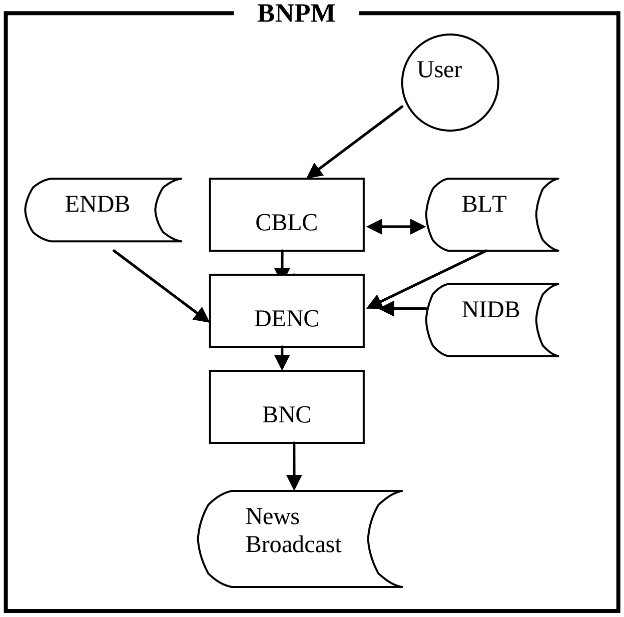

Figure 3. Architecture of the BNPM

The functions of these components are as the follows:

3.2.1Create broadcast list component (CBLC)

CBLC creates the order of broadcast list. It will insert or delete the entry and produces new broadcast list.

3.2.2 Decrypt encrypted news component (DENC)

DENC decrypts the encrypted news data to get the original news data.

3.2.3 Broadcast news component (BNC)

BNC broadcasts the news to the request.

4. ENCRYPTION AND DECRYPTION ALGORITHMS

4.1 Encryption algorithm (NDEC news data encryption component)

Based on Lee and Lee [6], we propose the encryption algorithm in the following steps.

4.1.1 Get News.

Get news data file and its length LN. Store news data to symbol table (ST). Set category (CG) and serial number (SN).

4.1.2 Set news information data base (NIDB).

Set location code (LC) of this news and length of news (LN). Store CG, SN, LC and LN to NIDB;

4.1.3 Set encryption data table (EDT).

Set fields of EDT. It contains format code (FC), direction flag (DF), number of blocks (NB), number of rotated byte (RB), left shift table (LST) and displace offset (DO). Compute the length of EDT as LEST. Store LEDT to NIDB.

4.1.4 Direction change

Get DF from EDT. If DF is set, we reverse the ST to get symbol table after direction (STAD).
Get NB from EDT. We insert dummy symbol to STAD and let STAD is multiplier of NB.

4.1.5 Rotate the symbol table

Divide STAD into NB blocks. Get RB from EDT. From the beginning block, we repeat rotate each block left RB bytes and right RB bytes. We get the symbol table after rotation (STAR).

4.1.6 Left shift each byte

Get left shift table (LST) from EDT. Following each half byte of LST, left shift each byte of STAR. Wwe get symbol table after shift (STAS).

4.1.7 Position exchange:

Get displace offset (DO) of EDT. Extract each byte of STAS offset DO bytes and store it to symbol table after extract (STAE) to end of data. Decrease DO by 1, repeat above process. Process above until DO equals to 0 and get symbol table after extract (STAE).

4.1.8 Create encrypted news data file

From location code, we compute location point (LP).
Insert EDT to the LP of STAE.
Get the encrypted news data file.

4.2 Decryption Algorithm (NDDC news data decryption component)

Decryption algorithm is the reverse of encryption. The steps of decryption are as follows:

4.2.1 Get encryption data table (EDT)

Get the encrypted news data file.
From CG and SN, get LC and LEDT from NIDB.
From LC, compute location point (LP).
Extract EDT from LP of encrypted news data and the remaining data to symbol table after extraction (STAE).

4.2.2 Change the order

Get displace offset (DO) of EDT.
Set symbol table after append (STAA) and the length is as STAE..
Extract each byte of STAE and place offset DO bytes to STAA to end of STAA.
Decrease DO by 1, repeat above process.
Processes above until DO equals to 0 and get new STAA.

4.2.3 Left shift each byte

Get left shift table (LST) from EDT.
Set each half byte of new LST as 6+ half byte.
Following each half byte of LST, left shift each byte of STAA.
Get symbol table after shift (STAS).

4.2.4 Rotate the symbol table

Get NB (number of block) from EDT.
Divide STAS into NB blocks.
Get RB (rotated byte) from EDT;
From the beginning block, we repeat to rotate each block right RB bytes and left RB bytes.
We combine to get the symbol table after rotation (STAR);
Get LN in NIDB. We get first LN bytes of STAR to STAR.

4.2.5 Reverse the content

Get direction flag (DF) of EDT;
If DF is set, we reverse STAR to get symbol table after direction (STAD). STAD is our original news data.

4.3 Location code (LC) and location point (LP)

Get the location code (LC) and the length of news data (LN) in NIDB. We set the value LP as following rules:
1. If LN > LC then LP=LC;.
2. If LN < LC then LP=mod(LC/LN).
The LP is the location to insert EDT to encrypted news data.

4.4 Format code

The fields in EDT have format code (FC), direction flag (DF), number of blocks (NB), rotated byte (RB), left shift table (LST), and displace offset (DO).

The FC is in the first place. The different format of EDT is depending on format code as Table 6.

The length of FC, DF, NB, RB, DO are fixed. The length of LST may be variable. We compute LEST and store it to NIDB.
These formats are stored in the computer system and used to encrypt and decrypt.

Table 6. Encryption data table format (EDTF)

FC	DF, NB, RB, LST, DO
1	DF, NB, RB, LST, DO
2	DF, NB, RB, DO, LST
3	DF, NB ,LST, RB, DO
4	DF, NB, LST, DO, RB
5	…

5. COMPARISON

The difference between the proposed algorithms with others method is as following:

There is no mathematical formula. We use basic computer operations like shift, rotate and move. The same plaintext has different cipher text. Because (1) The length and content of the encryption data table (EDT) and LST are different. (2) The fields in EDT are different order. Encryption data table is stored in the cipher text and is used to do encryption and decryption. We use location code to store encryption data table to cipher text.

6. IMPLEMENTATION

In this section, we implement the proposed algorithms. The computing environment is shown in Section 6.1. The processing time of encryption and decryption are shown in Section 6.2.

6.1 Computing Environment

Computer type:	INTEL, Pentium D830;
Memory size:	DDR 512 MB * 2;
Computer Language:	C Language.

6.2 Executing Results

Table 7. Encryption processing time

Encryption	Symbol table size (Bytes)			
Times [1]	128	512	1024	4096
1M	41	144	280	1036
4M	165	563	1158	4155
8M	325	1125	2300	8386

[1] M=1000000 processing times.

[2] processing time in second

Table 8. Decryption processing time

Decryption	Symbol table size (Bytes)			
Times [1]	128	512	1024	4096
1M	53	199	388	1484
4M	213	784	1572	6053
8M	424	1570	3154	12000

[1] M=1000000 processing times.

[2] processing time in second

The processing time of the different combinations of symbol size and executing times are as shown in Table 7 and Table 8. Table 7 is the encryption processing time. We also get the decryption processing time in Table 8.

7. CONCLUSION

In this study, we use the basic computing operations to design encryption and decryption algorithms. It doesn’t need any special hardware. Finally, we make some comments about this study.

The news data may be any combination of letters, graphic and any other figures. It is safer, because we must know the following to do the decryption. (1) the encryption data table in cipher text. (2) the different format of encryption data table. (3) the value of each field in encryption data table.

When encryption program is stolen, the thief uses the same data to get encrypted news data file. Each cipher text may have different length and content

By these encryption and decryption algorithms, we can process news data more safe.

8. REFERENCE

[1] Biham E. and Shamir A.1991. Differential Cryptanalysis of DES-like Cryptosystem. Advances in Cryptology-CRYPTO ’90 Proceedings, Springer-Verlag Berlin, 2-21.

[2] Denning, D. 1982. Cryptography and Data Security, Addison-Wesley.

[3] Diffie W., and Hellman M. E. 1976. New directions in cryptography. IEEE Trans. on Inform Theory, 644-654.

[4] Lee, H.-M., Lee, T.-Y., Lin, L., Su, J.-S. 2007. Cipher text containing data and key to be transmitted in network security. In Proceedings of the 11Th WSEAS International Conference on System (CSCC’07) (Agios Nikolaos, Crete Island, Greece July 23-28, 2007), 275-279.

[5] Lee, H.-M., Lee, T.-Y. 2007. Analysis of algorithm of cipher text containing data and key in network security, In Proceedings of the Second International Conference on Innovative Computing, Information and Control. (September 5-7, 2007, Kumamoto City International Center, Kumamoto, Japan.)

[6] Lee, T.-Y., Lee, H.-M. 2006. Encryption and decryption algorithm of data transmission in network security. WSEAS Transactions on Information Science and Applications, Issue 12, Volume 3, 2557-2562.

[7] McEliece, R.J. 1978. A Public-Key System Based on Algebraic Coding Theory, 114-116. Deep Sace Network Progress Report, 44, Jet Propulsion Laboratory, California Institute of Technology.

[8] Miyaguchi, S. 1990. The FEAL-8 cryptosystem and call for attack. Advances in Cryptology-CRYPTO’89 proceedings, Springer Verlag Berlin, 624-627.

[9] National Bureau of Standards 1977. NBS FIPS PUB 46: Data Encryption Standard, National Bureau of Standards, U. S. A. Department of Commerce, (Jan. 1977).

[10] National Bureau of Standards, 1980. NBS FIPS PUB 81: Data Modes of Operation, National Bureau of Standards, U. S. Department of Commerce, (Jan. 1980).

[11] National Institute of Standards and Technology (NIST) 1993. FIPS PUB 180: Secure Hash Standard (SHS), (May 11, 1993).

[12] National Institute of Standards and Technology (NIST) 1994. NIST FIPS PUB 185, Escrowed Encryption Standard, (February 1994).

[13] Pieprzyk, J., Hardjono, T., Seberry, J. 2003. Fundamentals of Computer Security, Springer-Verlag Berlin Heidelberg.

[14] Rivest, R.L., Shamir, A., and Adleman, L .1978. A method for obtaining digital signatures and public –key cryptosystems. Communications of the ACM, Vol. 21, No. 2, 120-126.

[15] Stallings, W. 2003, Cryptography and Network Security: Principles and Practices, International Edition, Third Edition by Pearson Education, Inc. Upper Saddle River, NJ 07458.

[16] Stallings, W. 2003. Network Security Essentials Application and Standards, Second Edition by Pearson Education, Inc. Upper Saddle River, NJ 0745.