Transportation of Business Messages by using Data Encryption System

Thet Htet Aung, Win Mar
Computer University, Maubin
aprilthethtet@gmail.com, winmar@gmail.com

Abstract

In today's business environment, controlling access to data is critical to long-term business survivability. We present the system for encrypting the data types such as text files; word documents and images of different formats. Data in transit, across and between company networks, are usually the focus of extensive security efforts. In this paper, we also describe the design, implementation and testing of a security system that enhances the capability of small business to protect information within the boundary of their networks by using DES algorithm. Within the specified network, transactions are encrypted, decrypted and processed by the Internal Control and Employee Agents. The test results indicate that this additional security layer provides a simple solution to the data sharing and transition within an organization's network. The results of this study will be of significance to owners, managers, and the security personnel responsible for small business network.

Keywords: business information, security system, Internal Control, private keys, organization's network

1. Introduction

Nowadays, communications are moving more and more towards electronic means, such as email, faxes and mobile phones. Every day hundreds or thousands of people interact electronically, where it is through e-mail, e-commerce (business conducted over the Internet), or cellular phones. The need for secure communications is more profound than ever, recognizing that the conduct of much of our business messages and personal matters is being carried out through the medium of computers, which has replaced the traditional medium of papers. The emergence of virtual organizations such e-learning and e-business in general shall rely on a secure way for online transactions. In order for a data to be secured for storage or transmission, it must be transformed in such a manner that it would be difficult for an authorized person to be able to discover its true meaning. Cryptographic techniques can be used to protect the privacy of data. It can provide a "digital signature" to guarantee authenticity. [5]

In this paper, we present the system for encryption of the data types such as text files; word documents and images of different formats. This system converts messages or information being sent into scrambled or unreadable formats employing a dynamic encryption code or key before sending. At the receiver end, the code uses to decode that particular messages supply before the messages could be read. Authorization, Authentication and security process are realized by prompting the receiving user to supply sending users' key to log onto the package. The results obtained in this study are highly useful because the data encryption is dynamic. This means that each encrypted and decrypted message is accompanied by a key (or code) peculiar to that message which determines the complexity of the encryption.

The rest of this paper is organized as follows: Section 2 focuses on the security system components for data encryption system. In section3, we present an execution of data encryption algorithm. Section 4 presents the implementation for transportation of business messages by using data encryption system. We conclude in Section 5.

2. Security System Components for Data Encryption System

Security is fundamentally about protecting assets. Security is a path, not a destination. As we analyze our infrastructure and applications, we identify potential threats and understand that each threat presents a degree of risk. Security is about risk management and implementation effective countermeasures. Security systems pose four main components: security authentication, authorization, access control and encryption. [5]

- Authentication: Usually authentication is realized by a "smart token" which is hardware device in the size of a pocket computer or credit card that creates a password and transfers it to the authentication server that is linked up to the network.
- Authorization: The aim is to supply one secured access point enabling the users to link up to the network once and allow them access to authorized resources. The authorization is examined via software servers enabling the client, acting in the name of the user, to prove his identity

to the authentication server, without sending information over the network that would reveal that the client or the party rendering the service.

- Encryption: Encryption is one of best processes of encoding a message or data through a mathematical key in a manner that hides its substance from anyone who does not process the mathematical key. However, encryption has not always been applicable to network security. Traditionally, encryption data for transmission across a network required that the same encryption key, called a shared secret or a private key be used at both ends of the data exchange. Asymmetric encryption classes usually use two separates keys for encryption and decryption. The device receiving the data uses a private key to decrypt data as it is received. Any remote device wanting to send encrypted data to receiver must use a separate public key to encrypt the data before it is sent. [4]

- Access Control: Access control is implemented via access matrices, access lists, capabilities list. These lists define access authorization to the computer resources for the user.

3. Execution of Data Encryption Algorithm

Data Encryption System (DES) belongs to a category of ciphers called block ciphers. Block ciphers, as opposed to stream ciphers, encrypt messages by separating them into blocks and encrypting each block separately. Stream ciphers, on the other hand, operate on streams of data one bit at a time as continuous stream.

3.1 Plain Text

DES encrypts 64-bit block of plaintext into 64-bit blocks of ciphertext. Plaintext, used in the context of cryptography, is the name commonly given to the body of a message before it is encrypted, i.e., the unaltered text of the message which is to be sent. Likewise, ciphertext is the name commonly given to the encrypted version of the message body which is meant to be indecipherable to any person who does not have the decryption key. [1]

3.2 Cipher Text

In DES algorithm, DES is a Feistel cipher which executes plaintext blocks of n=64 bits, producing 64-bit ciphertext block as shown in Figure 1. The effective size of the secret key K is k=56 bits; more precisely, the input key K is specified as a 64-bit key, 8 bits of which (bits 8, 16,…., 64) may be used as parity bits. The 2^{56} keys implement (at most) 2^{56} of the 2^{64} possible bijections on 64-bit blocks. A widely held belief is that the parity bits were introduced to reduce the effective key size from 64 to 56 bits, to intentionally reduce the cost of exhaustive key search by a factor of 256.

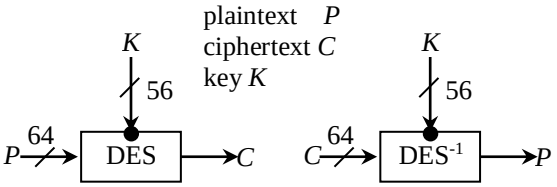

Figure 1: DES Input-Output

3.3 Decipher Text

This DES algorithm is designed to encipher and decipher blocks of data consisting of 64-bits under control of a 64-bit key. Deciphering must be accomplished by using the same key as for ciphering but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to an initial permutation IP, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1}.

3.4 DES Operation

DES encryption operates on a 64-bit block of plaintext. Figure 2 for full details of DES is given in DES algorithm. Both encryption and decryption use the same algorithm expect for processing the key schedule in the reverse order.

After initial permutation, the block is split into two blocks L_i (left) and R_i (right), each 32 bits in length. The permuted plaintext has bit 58 of the input as its first bit, bit 50 as its second bit, and so on down to bit 7 as the last bit. The right half of the data, R_i, is expanded to 48 bits according to the expansion permutation.

The expansion symbol E of $E(R_i)$ denotes a function which takes the 32 bit R_i as input and produces the 48-bit $E(R_i)$ as output. The purpose of operation is twofold-to make the output the same size as the key for the XOR operation, and to provide a longer result that is compressed during the S-box substitution operation.

After the compressed key K_i is XORed with the expanded block $E(R_{i-1})$ such that $T \leftarrow .E(R_{i-1})$ and $T' \leftarrow T \oplus K_i$ for $1 \le i \le 15$, this 48 bits T' is divided into 6-bit blocks. This 48-bit input T' to the S-I boxes are passed through a nonlinear S-box transformation to produce 32-bit output. This 32-bit output T' of the S-box substitution are permuted. This permutation maps each input bit of T' to an output position of T''. The output T'' are obtained from the input T' by taking the 16-bit of T' as the

first bit of T'', the seventh bit as the second bit of T'' and so on until the 25-bit of T' is taken as the 32nd bit of T''. Finally, the permutated result is XORed with left half L_i of the initial permutated 64-bit block. Then the left and right halves are swapped and another round begins. The final permutation is the inverse of the initial permutation and is described as IP^{-1}. The concatenated block $L_{16}||R_{16}$ is used as the input to the final permutation of IP^{-1}.

INPUT: plaintext $m_1 \ldots m_{64}$; 64 bit key $K=k_1 \ldots k_{64}$(includes 8 parity bits).
OUTPUT: 64-bit ciphertext block $C=c_1 \ldots c_{64}$. (For decryption)

1. (key schedule) Compute sixteen 48-bit round keys K_i from K using DES key schedule algorithm.
2. $(L_0,R_0) \leftarrow IP(m_1m_2 \ldots m_{64})$. (Use IP to permute bits; split the result into left and right 32-bit halves $L_0=m_{58}m_{50} \ldots m_8$, $R_0 =m_{57}m_{49} \ldots m_7$)
3. (16 rounds) for I from 1 to 16, compute L_i and R_i using $L_i=R_{i-1}$ and $R_i=L_{i-1} \oplus f(R_{i-1}, K_i)$, computing $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$ as follows:
   (a) Expand $R_{i-1}=r_1r_2 \ldots r_{32}$ from 32 to 48 bits using expansion E and permutation P: $T \leftarrow E(R_{i-1})$. (Thus $T=r_{32}r_1r_2 \ldots r_{32}r_1$.)
   (b) $T' \leftarrow T \oplus K_i$. Represent T' as eight 6-bit character strings: $(B_1, \ldots, B_8)=T'$
   (c) $T'' \leftarrow P(T'')$. (Use expansion E and permutation P to permute the 32 bits of $T''=t_1t_2 \ldots t_{32}$, yielding $t_{16}t_7 \ldots t_{25}$.)
4. $b_1b_2 \ldots b_{64} \leftarrow (R_{16}, L_{16})$. (Exchange final blocks L_{16}, R_{16}.)
5. $C \leftarrow IP^{-1}(b_1b_2 \ldots b_{64})$. (Transpose using IP^{-1}; $C=b_{40}b_8 \ldots b_{25}$.)

Figure 2: Full Details of DES Algorithm

In Figure 3, the key-dependent computation can be simply defined in terms of a function *f*, called the cipher function, and a function *f*, called the DES key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described. Finally, a definition of the cipher function *f* is given in terms of primitive functions which are called the selection function S_i and the permutation function *P*.

The 64-bit input key is initially reduced to a 56-bit key by ignoring every eight bits. These ignored 8 bits, k_8, k_{16}, k_{24}, k_{32}, k_{40}, k_{48}, k_{56}, k_{64} are used as a parity check to ensure that each byte is of old parity and no errors have entered the key.

INPUT: 64-bits key $K=k_1 \ldots k_{64}$(including 8 odd-parity bits)
OUTPUT: sixteen 48-bit keys K_i, $1 \le i \le 16$.

1. Define υ_i, $1 \le i \le 16$ as follows: $\upsilon_i=1$ for $i \in \{1,2,9,16\}$; $\upsilon_i=2$ otherwise. (These are left-shift values for 28-bit circular rotations below.)
2. $T \leftarrow PC1(K)$; represent T as 28-bit halves (C_0, D_0). (Use PC1 to select bits from K: $C_0=k_{57}k_{49} \ldots k_{36}$, $D_0=k_{63}k_{55} \ldots k_4$.)
3. For i from 1 to 16, compute K_i as follows: $C_i \leftarrow (C_{i-1} \leftarrow \upsilon_i)$, $D_i \leftarrow (D_{i-1} \leftarrow \upsilon_i)$, $K_i \leftarrow PC(Ci, D_i)$. (Use PC2 to select 48 bits from the concatenation $b_1b_2 \ldots b_{56}$ of C_i and D_i: $K_i=b_{14}b_{17} \ldots b_{37}$.'$\leftarrow$' denotes left circular shift.

Figure 3: DES Key Schedule

After the 56-bit key was extracted, they are divided into two 28-bit halves and loaded into two working registers. The halves in registers are shifted left either one or two positions, depending on the round. The number of bits shifted is used Permuted Choice 1(PC1). After being shifted, the halves of 56bits (C_i, D_i), $1 \le i \le 16$, are used as the key input to the next iteration. These halves are concatenated in the ordered set and serve as input to the Permuted Choice2 (PC2), which produces a 48-bit key output. Thus, a different 48-bit key is generated for each round of DES. These 48-bit keys, K_1 , K_2 , ...,K_{16} are used for encryption at each round in the order from K_1 through K_{16}.

The DES decryption algorithm is exactly identical to the encryption algorithm except that the round keys are used in the reverse order. Since the encryption keys for each round are K_1 , K_2 , ...,K_{16}, the decryption keys for each round are K_{16}, K_{15}, ... K_1. Therefore, the same algorithm works for both encryption and decryption.

4. Implementation of DES Algorithm

Cryptography is the study of sending messages in disguised form so that only the recipients can remove the disguise and read the messages. In cryptographic terms: clear text is the text which is to be encrypted, and cipher text is the encrypted clear text. Cryptographic system is generically classified along three independent dimensions: (i) the type of operations used for transforming plaintext to cipher text.

This encryption algorithm is based on two general principles: in which each element in the plaintext is mapped into another element and transposition, in which elements in the plaintext is rearranged. The fundamental requirement is that no

information be lost, (ii) If both sender and receiver use the same key: the sender informs this key to the third person, and the third person tells to know the receiver, the system is referred to as symmetric, single-key, and (iii) A block cipher processes the input one block of elements at a time, producing an output for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. [3, 4]

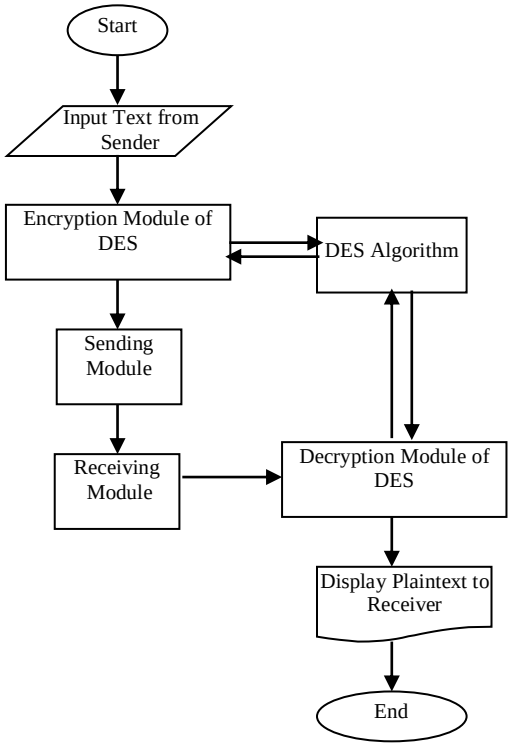

Figure 4: Process Flow for Transportation of Business Messages by using DES Algorithm

In this system, the user enters the plain text. And then, the system takes to encrypt on the plain text using DES algorithm. The plain text is transformed to cipher text. The sending user transmits the cipher text to the receiver site. Receiver site receives this cipher text. The user at the receiver site decrypts the cipher text using the DES algorithm. The plain text is displayed to the user at the receiver site. In Figure 4, we implement the transportation of business messages by using data encryption system.

Before implement this system, User A (sender) and User B (receiver) must install DES.exe file to their personal computer system within the organization. When User A wants to send a business message to the User B, firstly he establishes the connection with User B. In Sender Site, User A enters new or existing file (text file, word document, image file for different formats) to his PC. After that, this file is encrypted by using DES encryption algorithm as shown in Figure 5 and then sent by User B' IP address at the Receiver site in Figure 6. For receiving this file, User B chooses his PC and decrypts this file by using DES decryption algorithm as illustrate as Figure 7.

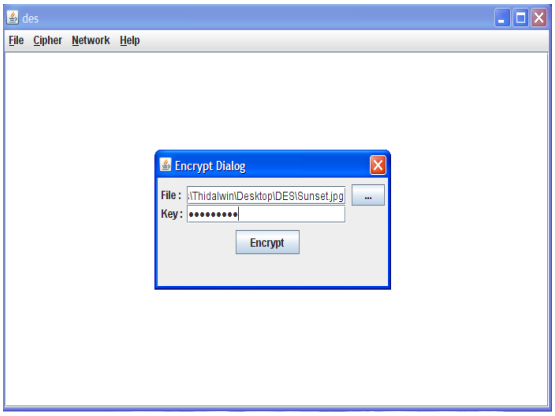

Figure 5: Key Generated for Encryption of Text File

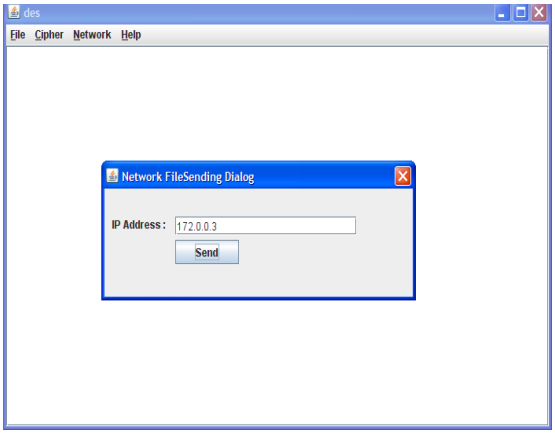

Figure 6: Sending Text File by IP Address

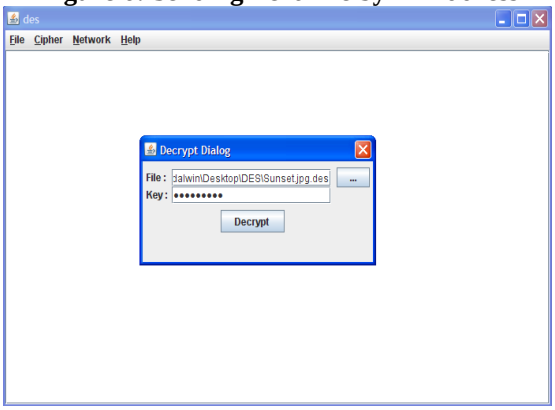

Figure 7: Key Generated for Decryption of Text File

5. Conclusion

Many organizations have for protecting their data and applications from intruders in a large number of user environments can be eliminated or at least attenuated. A new and innovative way to do so is through the implementation of an access security system.

According to the managers and users with many stations execute the large area networks; the DES algorithm will surely reap the communication to transport business messages for various information systems. This system implement working together both the sender and receiver in exchanging data format to improve the system security.

References

[1] W. Diffie, and M. Hellman, "New Directions in Cryptography", IEEE Trans. Inform Theory IT-22, (Nov. 1976), 644-654.

[2] W. Diffie, and M. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard" Computer 10 (June 1977), 74-84.

[3] D. E. Knuth, "The Art of Computer Programming" , Vol 2: Seminumerical Algorithms. Addison-Wesley, Reading, Mass., 1969.

[4] J. Levine, and J.V. Brawley, "Some Cryptographic Applications of Permutation Polynomials", Cryptologia 1 (Jan. 1977), 76-92.

[5] R. Merkle, "Secure Communications over an Insecure Channel", Submitted to Comm., ACM.