Secure Web Development with Triple DES Algorithm

Aye Aye Mon ,Khin Thet Mar
University of Computer Studies, Pathein
Htut 50 @gmail.com,moenaychikhin@gmail.com

ABSTRACT

Today's connected society requires secure information system to preserve data privacy and authentication in critical applications. This paper intends to implement secure web development system for critical applications. The Triple Data Encryption Standard (Triple-DES) algorithm has emerged to be the most commonly used in varying application because it is still reasonably secure. Key Distribution Center (KDC) is used for secret key sharing between sender and receiver. This can then be used to encrypt subsequent communications using a symmetric key cipher. The main objective of this paper is to provide a secure web development system by taking the advantages of Triple-DES cryptographic algorithm and Key Distribution Center (KDC).

Key Words: *Triple-DES, KDC*

1. INTRODUCTION

Beyond any doubt, the need for secure storage or transfer of information is an inextricable part of human history. This need was initially created by the difference in social, political, military or even religious persuasions among people. Nowadays, the rapid evolution of communication systems offers, to a very large percentage of population, access to a huge amount of information and a variety of means to use in order to exchange personal data. Therefore, every single transmitted bit of information needs to be processed into an unrecognizable form in order to be secured. This decipherment of the data is necessary to take place in real time and for this procedure a variety of encryption algorithms have been developed.

Nowadays, there are a lot of encryption algorithms and key establishment protocols that is used for encryption algorithms. Triple-DES, AES, and RC4 encryption algorithms are widely used in many critical applications. And, Diffie-Hellman (D-H) key exchange, Key Distribution Center (KDC) and RSA algorithm are used for key establishment.

Due to recent advances in computer technology, some experts no longer consider DES secure against all attacks; since then Triple-DES has emerged as a stronger method. Using standard DES encryption, Triple-DES encrypts data three times and uses a different key for at least one of the three passes giving it a cumulative key size of 112-168 bits. If we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows: encrypt with K1, decrypt with K2, encrypt with K3. Decryption is the reverse process: decrypt with K3, encrypt with K2 and decrypt with K1.

Information security means protecting information and information system from unauthorized access, use, disclosure, disruption, modification, or destruction. So information security plays an important role in various communication channels. Therefore many cryptography techniques have been developed to protect data in communication channel.

Generally, there are two types of cryptographic algorithm; symmetric algorithm or secret key and asymmetric key or public key algorithm. As using only a secret key to encrypt data, the symmetric algorithm is faster than asymmetric algorithm. So it is widely used to encrypt bulk of data. In the fact, secret key sharing is essential to be safe. For key establishing, it is used centralized and decentralized key distribution.

Centralized key distribution need a Key Distribution Center(KDC) and decentralize key distribution used key exchange protocol such as , Diffie-Hellman (D-H) key exchange and elliptic curve cryptography (ECC) based on public key system. This paper tries to present a secure information system that combines Key Distribution Center (KDC) with Triple-DES encryption algorithm.

For symmetric encryption to work, the two parties to an exchange must share the same key, and that must be protected from access by others. Furthermore, frequent key changes are usually desirable to limit life time of key compromised if an attacker learns the key. Therefore, the strength of any cryptographic system rests with the key distribution technique, a term that refers to the means of delivering a key to two parties. And so KDC makes distribution a key between sender and receiver to provide both authentication and confidentiality.

This paper is organized as follows: Section 2 shows the related works of this paper. Section 3 describes the background theory. Section 4 describes the system implementation. And finally section 5 concludes this paper by summaries the key points and other related considerations.

2. RELATED WORK

A set of related papers to ours are [1],[2],[3],[4]and[5].

A. N. Oo [1] gave the combination of RSA asymmetric encryption algorithm and DES symmetric encryption algorithm as a distributed hybrid system. In this hybrid system, RSA is used for key generation and DES is used for message encryption.

B. Schneier [2] presented applying cryptography, second edition: protocols, algorithm and source code in C.

David Hook [3] showed the beginning cryptography with java.

K. P. P. Than [4] presented a secure banking system for banking transactions: deposit, withdrawal and transfer, based on Key Distribution Center (KDC), Data Encryption Standard (DES) algorithm and Message Digest Function (MD5).

N. N. Lin [5] showed the e-mail security system using Triple-DES algorithm and took the advantages of Triple-DES algorithm.

In this paper, we employed the advantages of Key Distribution Center (KDC) and Triple-DES algorithm to construct the secure web development system.

3. BACKGROUND THEORY

Cryptography is usually referred to as 'the study of secret", while nowadays is most attached to the definition of encryption. Encryption is the process of converting plain text "unhidden" to a cryptic text "hidden" to secure it against data thieves. Figure 1 shows the simple flow of commonly used encryption algorithms.

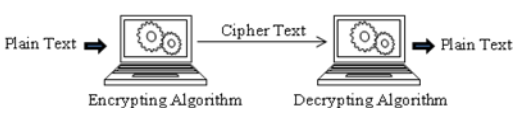

Figure 1: Process of Encryption-Decryption

The original message is called the plaintext, and the disguised message is called the cipher text. The final message, encapsulated and sent, is called a cryptogram. There are two general types of key-based algorithms: symmetric and public-key. **Symmetric algorithms**, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms. Encryption and decryption with a symmetric algorithm are denoted by:

$$E_K(M) = C \quad [1]$$

$$D_K(C) = M \quad [2]$$

Public-key algorithms (also called asymmetric algorithms) are designed so that the key used for encryption is different from the key used for decryption. Furthermore, the decryption key cannot (at least in any reasonable amount of time) be calculated from the encryption key. The algorithms are called "public-key" because the encryption key can be made public. Encryption using public key K is denoted by:

$$E_{K(pub)}(M) = C \quad [3]$$

Even though the public key and private key are different, decryption with the corresponding private key is denoted by:

$$D_{K(pri)}(C) = M \qquad [4]$$

3.1 Key Distribution

Some cryptosystem, two entities can be used to establish a shared secret key. The establishment of secret key is a major problem and that there are basically two approaches to address the key establishment problem:

(i) The used of Key Distribution Center (KDC).
(ii) The use of key establishment protocols.

In the description of this system, we will apply the Key Distribution Center (KDC).

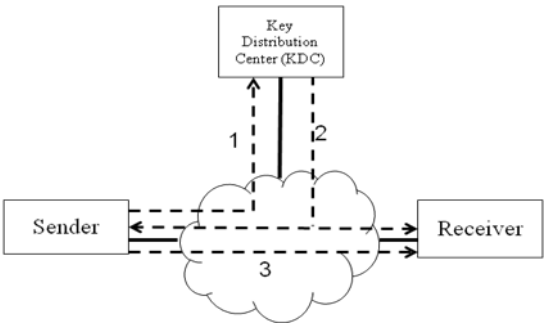

Figure 2: Overview of Key Distribution Center

KDC works as follows:

1. Request connection and ask KDC for session key.
2. KDC distributes session key to both units.
3. Transmit encrypted data.

3.2 Key Distribution Scenario

Sender (A) issues a request to KDC for a session key to protect a logical connection to Receiver (B). The message includes the identity of A and B, and a unique identifier **nonce**. The nonce may be a timestamp or a random number.

The KDC responds to A with a message encrypted using K_A. Thus, A is the only one who can successfully read the message, and the message includes two items intended for A:

- The one-time session key, K_s, to be used for the session.
- The original request message, including the nonce, to enable A to match this response with the appropriate request.

The KDC also sends to B the message encrypted using K_B. It includes two items intended for B:

- The one-time session key, K_s to be used for the session.
- An identifier of A (e.g., its network address), ID_A .

Using the newly minted session key for encryption, A sends N_2 (nonce) to B.

Also using K_s, A responds with f (N_2), where f is a function that performs some transformation on N_2 (e.g., adding one).

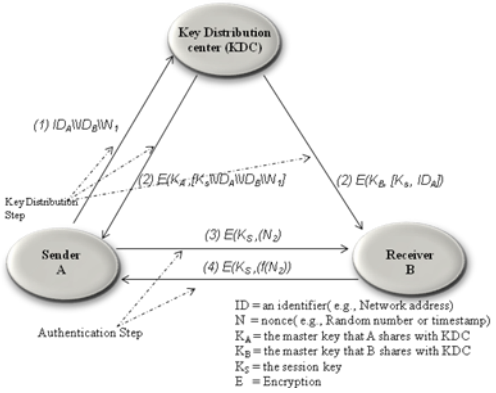

Figure 3: Key Distribution Scenario

3.3 Data Encryption Standard (DES)

DES is a symmetric block cipher operating on 64-bit blocks using 56-bit key. DES encrypts data in the blocks of 64 bits. The input of the algorithm is 64- bit block of plaintext and the output from the algorithm is 64- bit block of cipher text after the 16 rounds of identical operation. The key length is 56 bits by stripping off the 8 parity bits ignoring every 8^{th} bit from the given 64-bit key. The basic building block of DES is a combination of permutation and substitution on the

plaintext. Both encryption and decryption use the same algorithm except for the key schedule in the reverse order. Figure 4 shows the DES computation path.

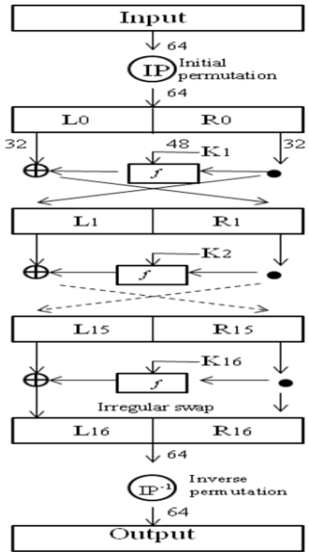

Figure 4: DES Computation Path

3.4 Triple Data Encryption Standard (Triple-DES)

Triple-DES is the application of DES cipher three times over a single message by using three different keys. The process is a 168-bit key block cipher, and run like DES except 48 rounds (3*16 rounds). Therefore, Triple-DES is more secure three times than DES. The general operation flow of Triple-DES is that:

Encryption operation: the transformation of a 64-bit block ***I*** into a 64-bit block ***O*** that is defined as follows:

$$O = EK_3\,(DK_2\,(EK_1\,(I))) \quad [5]$$

Decryption operation: the transformation of a 64-bit block ***I*** into a 64-bit block ***O*** that is defined as follows:

$$O = DK_1\,(EK_2\,(DK_3\,(I))) \quad [6]$$

Triple-DES has three key options:

Option 1: $K_1 = K_2 = K_3$

Figure 5 shows the key option 1 operation.

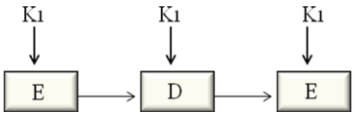

Figure 5: Key Option 1

Option 2: $K_1 = K_3$ and K_2 is independent

Figure 6 shows the key option 2 operation.

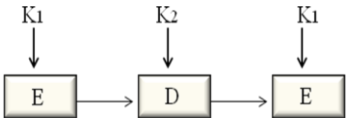

Figure6: Key Option 2

Option 3: K_1, K_2 and K_3 are independent

Figure 7 shows the key option 3 operation.

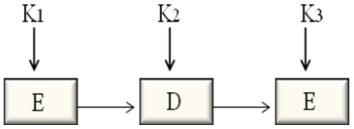

Figure7: Key Option 3

Triple-DES with two keys (***K1=K3, K2***) is a relatively popular alternative to DES. Figure 7 shows the flow Triple-DES algorithm.

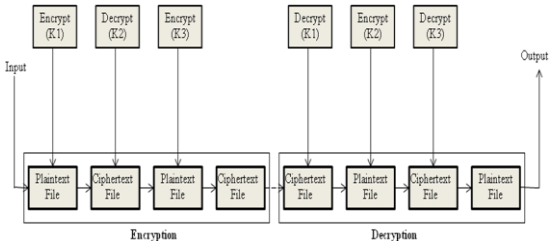

Figure7. Flow of Triple-DES Algorithm

4. SYSTEM IMPLEMENTATION

There are three main parts in this system; key distribution (KDC), data encryption and decryption. KDC is part of a cryptosystem intended to reduce the risk inherent in exchanging keys.

KDC distributes a symmetric secret key with every user in the network. KDC operates as network services that supplies tickets and temporary session keys. JDC often operates in systems within which some users may have permission to use certain services at sometimes and not at others. KDC generate session key and distribute it to each entity. Data encryption and decryption use Triple-DES algorithm. Firstly, KDC stores the master keys of sender and receiver. Figure 8 shows the overview of the system.

The sender requests the session key to the KDC. Then, KDC generate the session key (Triple-DES key) and encrypt the session key by using master keys of sender and receiver. After that the KDC sends this session key to the sender and receiver. Sender and receiver decrypt the encrypted session key by using their master keys. And then, sender encrypts the plain text data by using Triple-DES algorithm and sends to the receiver. The receiver decrypts the encrypted data with Triple-DES algorithm. And finally display the original plain text data.

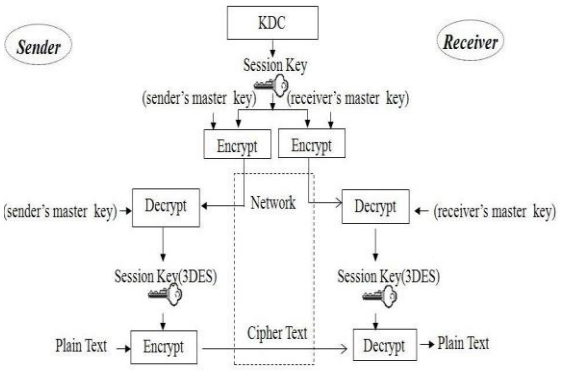

Figure 8: Overview of the System

The process of key distribution is as follows:

(1) The sender requests the key to receiver by using sender's ID and receiver's ID.
(2) Then, KDC generates the session key (K_S).
(3) After that, KDC encrypts session key by using sender's and receiver's master keys that is used as Triple DES key.
(4) Finally, the KDC send encrypted session key to sender and receiver.

The process of key distribution is shown in Figure 9.

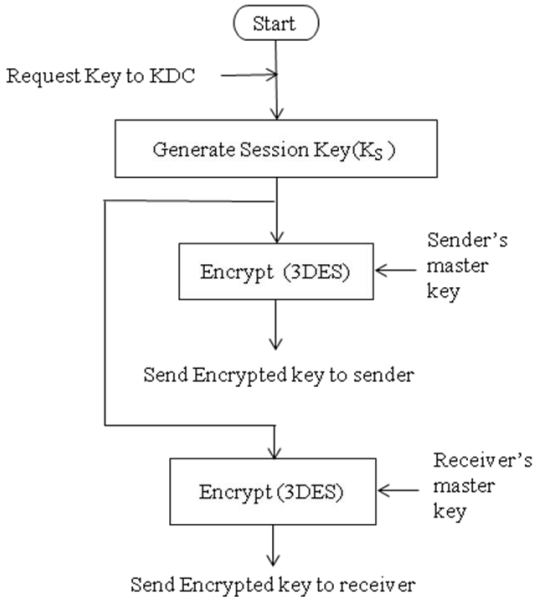

Figure 9: Process flow of KDC

Sender issues a request to KDC for a session key to protect a logical connection to receiver. Then sender will do the following steps. It is shown in Figure 10.

(1) Firstly, the sender take the session key (Triple-DES key) from KDC.
(2) Then encrypt the plaintext data with Triple-DES algorithm and then get the
(3) cipher text data.
(4) After that, the sender sends the ciphered data to the receiver across insecure channel.

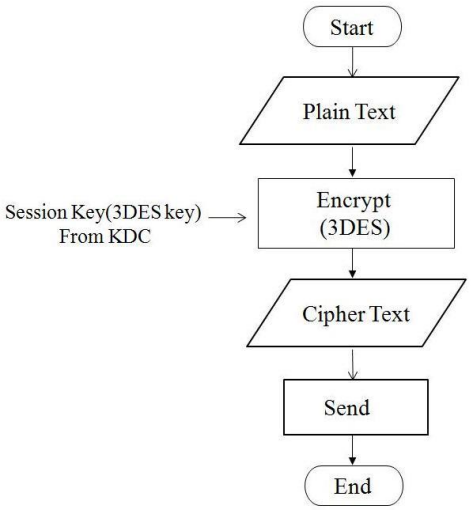

Figure 10: Process flow of sender's side

The receiver also does the following steps:

(1) Firstly, the receiver take the session key (Triple-DES key) from KDC.
(2) Then receives the ciphered text data from the sender.
(3) Finally, the receiver decrypts this ciphered text data with Triple-DES algorithm and display the original plain text data.

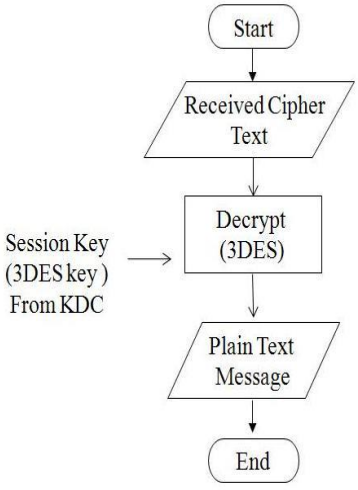

Figure 11: Process flow of receiver's side

5. CONCLUSION

Symmetric cryptography is used for data encryption , decryption and the session keys are generated by the KDC in response to requests from clients and are securely distributed to the appropriate principals. Any file types can be encrypted and decrypted. This system will be applied to ensure reliable, trustworthy transmission of information data. This system can provide the security of data and transferring message across insecure channel for all applications.

REFERENCES

[1] A. N. Oo, "Distributed Hybrid Cryptosystem using the Combination of RSA and DES", M.C.Sc (thesis), University of Computer Studies, Yangon, January 2006

[2] B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C", John Willy& Sons, Ltd., ISBN: 0471128457, January 1996.

[3] David Hook, " Beginning Cryptography with Java", Wiley Publishing,Inc., 2005 http:// www.wiley.com

[4] K. P. P. Than, "Implementation of Secure Banking System Using Key Distribution Center", M.C.Sc (thesis), University of Computer Studies, Yangon, June 2008.

[5] N. N. Lin, "E-mail Security using Triple-DES", M.C.Sc (thesis), University of Computer Studies, Yangon, November 2006.

[6] R. Wobas; Translated by Angelika Shafir, "Cryptology Unlocked", John Wiley& Sons,Ltd., England, August 2007.