Symmetric Encryption

Session 2

LEARNING OBJECTIVES

On completion of this session you should:

- Appreciate the role of cryptography in achieving security
- Understand symmetric (private key) encryption and message confidentiality
- Be familiar with different symmetric encryption algorithms
- Understand cipher block modes of operation
- Understand "Key" distribution issues

Contents

2.0 Introduction
2.1 Symmetric Encryption
2.2 Symmetric Encryption Algorithms
2.3 Cipher Block Operations
2.4 Key Management
2.5 Conclusion
2.6 References

Reading

Prescribed readings

Reading 1: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 42 to 48.

Reading 2: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 48 to 55.

Reading 3: Read http://www.cescomm.co.nz/about/aes.html

Read http://csrc.nist.gov/encryption/aes

Reading 4: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 46 to 51.

2.0 Introduction

Cryptography is the basis for secure communication. It refers to the study of mathematical techniques to achieve various aspects of information security, e.g., authentication, data integrity and confidentiality. We need to understand three main cryptographic techniques: symmetric encryption, asymmetric encryption and hash function. Cryptography is the major technology behind network security, and cryptographic algorithms and protocols are the necessary building blocks. Cryptography and hash function techniques are combined to generate digital signature.

The basic idea of cryptography is to protect data in transit. It can also be used to protect data in a file by encrypting the data before storing in the file, or encrypting the whole file. A cryptographic system does not differentiate between legitimate and illegal users if both have the keys to decrypt the information. A cryptographic "key" is a digital object that is used to encrypt, decrypt, and sign information [2, p. 5]. Some keys are

private and others are shared, and must be distributed in a secure manner. Creating and distributing the keys securely is the most important key management issue. So, there must be control over the encryption keys and the system.

There are two primary types of encryption techniques: symmetric and asymmetric encryptions. Symmetric encryption will be presented first in this study guide, and asymmetric encryption will be presented in the next study guide.

2.1 Symmetric Encryption

In symmetric encryption, a secret key is established and shared between the communicating parties. The same key is used to encrypt and decrypt the message at both sides. Since sender and receiver use the same key, it is referred to as symmetric cryptography, also as private (secret) key cryptography. A symmetric encryption scheme has the following five components [1, p. 28]

- Plaintext: is the original message fed into the algorithm as input.
- Encryption algorithm: performs various substitution and transformation on the plaintext.
- Secret key: this key is also used as an input to the algorithm. The exact substitution and transformation performed by the algorithm depend on this key.
- Ciphertext: is the scrambled message produced as output by the algorithm. For a given message, two different keys will produce completely different ciphertexts.
- Decryption algorithms: is basically the encryption algorithm run in reverse. It takes the ciphertext and the same secret key to produce the original plaintext.

To communicate securely between two parties **A** and **B**, the following steps take place.

- **A** shares a secret key K with **B**. The key may be distributed by a key distribution center or by other secure means.
- **A** encrypts a plaintext message P by applying an encryption function **E** and the key K to create a ciphertext $C=E_K(P)$

- **A** sends the ciphertext ***C*** to **B** over a communication channel. Even if anyone other than **B** gets hold of a copy of ***C***, he cannot decrypt the message unless he has the key ***K***. If the key distribution is perfect or **B** does not accidentally or intentionally disclose it, then nobody other than **B** is supposed to have the key ***K***.

- On receiving ***C***, **B** apply decryption function ***D*** and key ***K*** on ***C*** to recover the plaintext message ***P***. $D_K(C)=D_K(E_K(P))=P$.

A simple symmetric encryption algorithm is the Caesar Cipher. It replaces each letter in the original message with the letter of the alphabet *n* places down the alphabet. The algorithm shifts the letter to the right while encrypting and shifts it to the left while decrypting. Two basic types of symmetric encryptions are block cipher and stream cipher. Block cipher processes on a block of data while stream cipher processes one bit or byte of data at a time.

An attacker may try different types of attacks on the encrypted message to discover the plaintext or secret key. The process to discover the plaintext or key is called cryptanalysis. Table 2.1 of the textbook gives a list of the types of attacks known to cryptanalyst. A brute-force attack tries every possible key until an intelligible translation of the ciphertext is obtained. On average, a successful break would require half of the all possible keys. With parallel processing in many machines simultaneously, it is possible to try 1 million keys per microsecond. This will require only ten hours to break a 56-bit symmetric encryption. Therefore, an encryption of this key length is no longer be guaranteed to be secure. Nevertheless, the higher length key does not necessarily make an encryption more secure. It also depends on the algorithm used to encrypt/decrypt the plaintext. An algorithm that is more complex and takes more time to decrypt will take more time to decode an encrypted message by the attackers.

Reading 1:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 42 to 48.

2.2 Symmetric Encryption Algorithms

The followings briefly describe a number of symmetric algorithms [1].

- Data Encryption Standard (DES) : DES was developed by IBM in 1970s and has been widely used for almost a quarter of a century. DES operates on 64-bit blocks of data and 56 bits key. The 56-bit key is divided into 16 subkeys, each subkey is used in each round of processing, in a total of 16 rounds. DES's 56-bit key length was sufficiently secure during the first two decades of operation. DES was proved insecure in July 1998 by Electronic Frontier Foundation (EFF) by demonstrating that DES encryption can be broken in less than three days. Today's cheaper and more powerful hardware makes DES totally vulnerable.

- Triple DES: The strength of DES can be improved by applying the algorithm multiple times. Research indicated that applying the algorithm twice does not bring any improvement because of the existence of a specific cryptanalysis attack. Triple DES uses three keys and three executions of the algorithm. The functions follow an encrypt-decrypt-encrypt sequence. However, the use of Triple DES is not very efficient (three times slower than DES) and many real-time applications require faster encryption [3].

- International Data Encryption Algorithm (IDEA): IDEA was developed by Xuejia lai and James Massey in 1991 to replace DES. It uses a 64-bit block cipher but 128-bit key. IDEA differs markedly from DES in both the round function and subkey generation. IDEA is used in PGP (Pretty Good Privacy) as an alternative and also in a number of commercial products.

- Blowfish: It was developed by Bruce Schneier in 1993. It is a DES-like algorithm that uses a 64-bit block cipher, 16 rounds and variable key lengths up to 448 bit; 128 bit key is commonly used in practice.

- RC2, RC4, RC5 and RC6: These are the encryption algorithms developed by Ron Rivest for RSA Security Inc. and are used in a number of products of the same company. RC5 is a block cipher that is configurable with regard to word length and number of rounds. The key length is also variable. RC6 is an improvement over RC5.

- Advanced Encryption Standard (AES): In 1997, the US National Institute of Standards and Technology (NIST) officially endorsed AES to replace DES. The algorithm was developed by Joan Daemen and Vincent Rijmen from Belgium and known as Rijndael algorithm. The algorithm uses 128-bit block cipher, three different key lengths: 128, 192 and 256 bits, and 10 to 16 rounds. AES offers

lots of flexibility and can be implemented efficiently in both hardware and software. Its very low memory requirement makes it very well suited for mobile and wireless environment [2, p. 11].

Reading 2:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 48 to 55.

Reading 3:
Read http://www.cescomm.co.nz/about/aes.html
Read http://csrc.nist.gov/encryption/aes

2.3 Cipher Block Operations

Four common modes exists in which plaintext, secret key and the ciphertext are combined to generate the stream of ciphertext. These are as follows [1].

- Electronic Code Book (ECB): each block of plaintext (64 bit) is processed at a time, but uses the same key. So, the same plaintext value will always result in the same ciphertext value; it does not hide data patterns. If the message has repetitive elements, then these elements can be identified. The advantage is that error propagation is limited to a single block. To overcome the above limitation, we need a mechanism that transforms repetitive blocks into different ciphertexts.

- Cipher Block Chaining Mode (CBC): each plaintext block is XORed with the previous ciphertext block and then encrypted. An initialization vector is used as a "seed" for the process. The same key is used for each block. The repeating patterns are not exposed because of the XOR operation with the preceding block. Different initialization vectors are used for different messages with the same key and are preferably randomly chosen.

- Cipher Feedback Mode (CFB): any previous ciphertext block is encrypted and the output produced is combined with the plaintext block using XOR to produce the current ciphertext block. The XOR operation conceals plaintext patterns. It is possible to define CFB

mode so it uses feedback that is less than one full data block. An initialization vector is used as a "seed" for the process.

- Output Feedback Mode (OFB): This mode is similar to CFB mode except that the quantity XORed with each plaintext block is generated independently of both the plaintext and ciphertext. One advantage of OFB mode over CFB mode in that any bit error that might occur during transmission is not propagated to affect the subsequent blocks.

Reading 4:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 64 to 69.

2.4 Key Management

For symmetric encryption to work, both parties must exchange the secret key in a secure manner. In fact, the strength of the cryptographic system depends on the establishment of a secure key distribution technique. Key distribution can be achieved in a number of ways [1].

- Key can be generated by **A** and physically delivered to **B**.
- Third party can select a key and physically deliver it to **A** and **B**. Both these methods involve manual delivery of key.
- If **A** and **B** have recently used a key, one party can transmit a new key to the other encrypted by the old key.
- If **A** and **B** each have an encrypted connection to a third party **C**, **C** could deliver a key on the encrypted links to **A** and **B**.

For communicating between small number of parties, manual distribution of keys may be feasible. However, for communication between large number of parties, the concept of Key Distribution Center (KDC) is more practical. Again, two kinds of keys can be generated: Session key and Permanent key. Session key is a key valid only for a particular communication session. Permanent key is used between the parties for distributing session keys.

2.5 Conclusion

In this study guide, we briefly discuss the importance of computer cryptography in achieving security. There are two types of encryption techniques: symmetric and asymmetric encryptions. The basic operation of symmetric encryption, different encryption algorithms and their features are presented. Four modes of cipher block operations, and their advantages and disadvantages are discussed. Key management issues are critical for successful implementation of symmetric encryption and key distribution center plays an important role in exchanging secret keys between the communicating parties.

2.6 References

[1] W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010.

[2] M. Kaeo, Designing Network Security : A Practical Guide to Creating a Secure Network Infrastructure, Cisco Press, 2004.

[3] R. Oppliger, Security Technologies for the World Wide Web, Artech House, 2003.