IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-2, Issue-8 E-ISSN: 2347-2693

Mechanisms for Secure Data Transmission: A Survey

B. Jyoshna

Department of CSE, Nishitha College of Engineering & Technology
jyoshnabejjam@gmail.com

www.ijcaonline.org

Received: 11 July 2014 Revised: 22 July 2014 Accepted: 19 August 2014 Published: 31 August 2014

***Abstract*—** In today's communications, data transmission play a vital role, but sending data in secure is crucial and important and it should free from unauthorized access. There are various possible techniques like Cryptography, Steganography, and Quantum Cryptography are available for secure transmission of data .This paper discusses some of the mechanisms for secure data transmission securely.

Keywords— Cryptograph; Steganography; Quantum cryptography

I- INTRODUCTION

Data transmission in a network suffers from several problems. Hence, the requirement is a secure mechanism for transmission of data securely. The main objective is to keep the data secure from unauthorized access.

A) Basic terminology

Plaintext: it is the actual message, composed of English words, which is in readable form.

Cipher text: the plain text is changed into other form (unreadable form), which cannot be read directly.

Encryption: it is a mechanism used to change plain text to cipher text. It is done at sender side.

Decryption: It is the reverse operation of encryption, which changes cipher text to plain text. It is performed at receiver side.

Key: it is the necessary element for performing encryption and decryption.

B) Security Services

Confidentiality: when sender transmits data to receiver, it should read by the receiver only, unauthorized party should not read it ie secrecy of the message.

Authentication: this service proves that data was sent by authorized sender only. That is proving the identity.
Integrity: the transmitted data should not be changed or modified by an unauthorized party.

Non repudiation: The sender and receiver should accept the message being transmitted.

jyoshnabejjam@gmail.com

II-Cryptography

Cryptography is an art of secret writing. The basic service provided by cryptography is the ability to send information between two parties in a way that prevents others from reading [1].

A) Symmetric cryptography

In this technique same key is used for encryption and decryption. It is called also called as classical cryptography. The algorithm used in these is called symmetric algorithms. These algorithms can be of two type's stream cipher and block cipher.

Stream cipher: the information is divided into bits and encrypted one bit at a time.

Block cipher: the information is divided into blocks depending upon the size of the block.

Some Symmetric Cryptographic Algorithms
DES, AES, Triple DES, RC2, RC5, IDEA, CAST, Blowfish

Advantages [4]
1Simple
2. Encrypt and decrypt your own files
3. Fast

Disadvantages [4]
1. Need for secure channel for secret key exchange
2. Origin and authenticity of message cannot be guaranteed

B. Asymmetric Cryptography

In this technique to different keys are used public and private. It's a pair of keys one key is used for encryption and the other is for decryption. Private Key is kept secret and public key is publicly known. To achieve confidentiality, the

sender has to get the public key of the receiver to encrypt the data.

Advantages [4]

1. Convenient
2. Provides message authentication
3. Provides non-repudiation

Disadvantages [4]

1. Public keys should/must be authenticated
2. Slow
3. Widespread security compromise is possible
4. Loss of private key may be irreparable

Diffie-Hellman key agreement: Diffie-Hellman key agreement algorithm was developed by Dr. Whitfield Diffie and Dr. Martin Hellman in 1976. Diffie-Hellman algorithm is not for encryption or decryption but it enable two parties who are involved in communication to generate a shared secret key for exchanging information confidentially[5].

Rivest Shamir Adelman (RSA): Ron Rivest, Adi Shamir, and Len Adleman released the Rivest-Shamir-Adleman (RSA) public key algorithm in 1978. This algorithm can be used for encrypting and signing data. The encryption and signing processes are performed through a series of modular multiplications [5].

Elliptic Curve Cryptography (ECC): Elliptic Curve Cryptography (ECC) provides similar functionality to RSA. Elliptic Curve Cryptography (ECC) is being implemented in smaller devices like cell phones. It requires less computing power compared with RSA. ECC encryption systems are based on the idea of using points on a curve to define the public/private key pair[5].

ElGamal: El Gamal is an algorithm used for transmitting digital signatures and key exchanges. The method is based on calculating logarithms. El Gamal algorithm is based on the characteristics of logarithmic numbers and calculations [5].

III- Steganography

Steganography means covered writing. Its goal is to the hide the fact that communication is taking place is mainly applied to media such as images, video clips music and sounds. Image steganography is generally more preferred media because of its harmless and attraction [2].

IV- Quantum Cryptography

The tracks of Wieners idea, Benet and Brassard proposed in 1984 a protocol to distribute secret keys using the principles of quantum mechanics called Quantum Cryptography. Or more precisely quantum key distribution. Properties of quantum mechanism developed a way to exchange a secret key whose secrecy is guaranteed by the laws of physics following the uncertainty principle, an eavesdropper can know anything about a photon that carries a key bit and will destroy a part of the information. Hence, eavesdropping causes errors on the transmission line which can be destroyed by the communicating parties [3].

V- Proposed work

There are many symmetric algorithms good for encryption but weak at key exchange. When cryptographic techniques are used for encryption the existence of data is known but in unreadable form. Steganography technique uses some media like an image to hide the existence of data. In this mechanism encrypted data is embedded in an image. Finally my proposed method for secure data transmission is apply any cryptographic algorithm for encryption and key can be transferred by quantum key distribution and stego image is used to cover the encrypted data. This method provides efficient security.

VI. CONCLUSION

There are many techniques and many algorithms are available for encryption. The selection of an algorithm depends on the criteria like requirement, application, to what extent security is required. combination of one or more methods provides better security.

VIII. REFERENCES

[1]. Prof. Pooja Shah , Dr. (Prof.) Subhash Desai, Prof. Amita Shah EEE: Efficiency Evaluation of Encryption Algorithms in Data Security.

[2]. MohitKumar, Abhishek Gupta, Kinjal Shah, Atul Saurabh, Pravesh Saxena, Vikas Kumar Tiwari Jaypee" Data Security Using Stegnography and Quantum Cryptography".Network and Complex Systems, ISSN 2224-610X (Paper) ISSN 2225-0603 (Online) Vol 2, No.2, 2012

[3].GillesVanAssche quantum cryptography and secure key distillation , Cambridge university press.

[4].http://voices.yahoo.com/comparing-symmetricasymmetric-key-encryption-6329400.html

[5].http://www.omnisecu.com/security/public-key-infrastructure/asymmetric-encryption-algorithms.php

[6].Network Security and cryptography Principles and practices by William Stallings 2nd Edition.

Authors Profile

B.Jyoshna persuing Ph.D at KLU Vijayawada . Currently working as a Assoc.professor in CSE Department at Nishitha College of Engg.&Tech.