Survey on Network Security and Cryptography

Ms. T. Lakshmi
Assistant Professor
Department of Computer Technology (IT&CT)
Vellalar College for Women, Erode, India

Abstract— Network Security & Cryptography is an idea to protect network and data transmission over remote network. Data Security is the principle part of secure data transmission over untrustworthy network. Network security includes the authorization of access to data in a network, which is controlled by the network administrator. Clients pick or are assigned an ID and password or other authenticating information that permits them access to information and programs inside their authority. Network security covers a diversity of computer networks, both public and private, that are utilized in regular employments directing exchanges and interchanges among organizations, government offices and people. In this paper likewise portrayed cryptography alongside its principles. One fundamental viewpoint for secure communications is that of Cryptography. The idea of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with making one of the most punctual cryptographic systems to send military messages to his generals. Cryptography is developing innovation, which is critical for network security. Research on cryptography is still in its creating stages and a significant research exertion is as yet required for secured communication. The cryptographic models and algorithms are sketched out.

Key words: Network Security, Accountability, Access control, Management policy, Cryptography, Cryptosystem, Encryption, and Decryption

I. Introduction

A. Network Security

Network Security is the most crucial segment in information security because it is in charge for securing all information went through networked computers. Network security comprises of the strategies and practices received to prevent and monitor unauthorized access, mistreat, alteration, or denial of a computer network and network-accessible resources. Network Security alludes to all equipment and programming capacities, qualities, highlights, operational strategies, responsibility, measures, access control, and administrative and management policy required to give an acceptable level of protection for Hardware and Software , and information in a network[1].

Network security problems can be partitioned generally into four intently interwoven territories:

1) Secrecy

Secrecy, also called confidentiality, needs to do with keeping information out of the hands of unauthorized clients.

2) Authentication

Authentication deals with deciding whom you are conversing with before uncovering sensitive information or going into a business deal.

3) Non repudiation

Non repudiation deals with signatures.

4) Integrity control

Message Integrity: Even if the sender and recipient can verify one another, they likewise need to safeguard that the substance of their correspondence isn't changed, either maliciously or coincidentally in transmission. Extensions to the check summing practices that encountered in solid transport and data link protocols.

B. Cryptography

Cryptography is a developing innovation, which is critical for network security. Cryptography is a helpful and generally utilized tool in security designing today. It included the utilization of codes and ciphers to change information into jumbled data. Cryptography or cryptology (from Greek word kryptós, "hidden, secret"; and graphein, "writing", or logia, "study", respectively) is the training and investigation of methods for secure communication within the sight of outsiders called adversaries. Modern cryptography is deeply founded on scientific hypothesis and computer science practice; cryptographic calculations are planned around computational hardness suspicions, making such algorithms difficult to break in practice by any adversary.

The far reaching utilization of computerized data storage, processing and transmission makes perceptive, important and individual information powerless against unauthorized access while in storage or transmission. Because of proceeding advancements in communications and eavesdropping technologies, business organizations and private individuals are starting to ensure their information in computer systems and networks utilizing cryptographic techniques, which, until very recently, were entirely used by the military and diplomatic communities. Cryptography is an imperative of the present computer and communications networks, protecting everything from business e-mail to bank exchanges and web shopping. While traditional and current cryptography utilize different numerical methods to keep away from learning the substance of encrypted messages. Computer systems and networks which are storing, processing and communicating delicate or profitable information require protection against such unauthorized access.

The main general way to deal with sending and storing data over media which are lacking confidence is to utilize some type of encryption. An essential concern is that numerous attacks entail secret manner access to information resources, and organizations are regularly unconscious of unauthorized access to their information systems. For that reason the quantum cryptography used. According to [7], the Julius Caesar utilized simple cryptography to secrete the meaning of his messages. As per [7], The Caesar cipher is a monoalphabetic cryptosystem, since it replaces each given plain text letter, wherever in the first message it occurs, by the similar letter of the cipher text alphabet. Anyway the ideas of source and recipient, and channel codes are present day thoughts that have their foundations in the data theory. Claude Shannon exhibited an idea of security in communications in 1949, it suggests that an encryption scheme is perfectly secure if, for any two messages M1 and M2, any cipher-text C has the similar likelihood of being the encryption of M1 as being the encryption of M2 [6]. Shannon was developed two significant cryptographic concepts: confusion and diffusion. According to Salomon [8], the term confusion means to any strategy that makes the factual connection between the cipher-text and the key as tricky as possible, and diffusion is a general term for any encryption technique that expands the measurable properties of the plaintext over a range of bits of the cipher-text.

II. Types Of Security Attacks

Networks are subject to assaults from malevolent sources. With the advent and increasing utilization of internet attach is most commonly growing on increasing. The principle classifications of Attacks can be from two classes: "Passive" when a network intruder intercepts data going through the network, and "Active" in which an intruder starts commands to disrupt the network's normal task. There are some more kinds of attack that are additionally fundamental to be considered [3]:

A. *Passive Attack*

A passive attack controls unencrypted traffic and searches for clear-text passwords and sensitive data that can be utilized in different kinds of attacks. The monitoring and listening of the communication channel by unapproved attackers are known as passive attack. It incorporates traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication data such as passwords.

B. *Active Attack*

In an active attack, the attacker endeavours to bypass or break into secured frameworks in the going on communication. This should be possible through stealth, viruses, worms, or Trojan horses. Active attacks incorporate attempts to circumvent or break protection features, to present malicious code, and to steal or modify data. The unauthorized attackers monitors, listens to and alters the data stream in the communication channel are known as active attack.

C. *Distributed Attack*

A distributed attack necessitates that the adversary establish code, such as a Trojan horse or back-door program, to a trusted component or software that will later be disseminated numerous different organizations and clients. Distribution attacks centre on the malicious modification of hardware or software at the factory or through distribution.

D. *Insider Attack*

As per a Cyber Security Watch review insiders were observed to be the reason in 21 percent of security breaks, and a further 21 percent may have been because of the activities of insiders. BYOD programs and file sharing and collaboration services like Dropbox imply that it will be harder than at any other time to hold corporate information under corporate control even with these benevolent yet untrustworthy representatives.

E. *Close-in Attack*

A close-in attack includes somebody attempting to get physically close to network components, information, and systems in order to take in more about a network. Close-in attacks comprise of ordinary individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, assembling, or denying access to data. One prominent type of close in attack is social engineering.

F. *Spyware attack*

A genuine computer security threat, spyware is any program that monitors your online exercises or introduces programs without your assent for benefit or to capture individual data.

G. *Phishing Attack*

In phishing attack the hacker makes a fake web site that looks precisely like a famous site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message endeavouring to trap the client into clicking a connection that prompts the fake site.

H. *Hijack attack*

In a hijack attack, a hacker assumes control over a session among you and another individual and disconnects the other individual from the communication.

I. *Spoof attack*

In the spoof attack, the hacker adjusts the source address of the packets he or she is sending with the goal that they give off an impression of being originating from another person.

J. *Password attack*

An attacker attempts to split the passwords stored in a network account database or a password- secured document. There are three major kinds of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack.

K. *Buffer overflow*

A buffer overflow attack is the point at which the attacker sends a greater number of information to an application than is normal. A buffer overflow attack usually results in the attacker increasing regulatory access to the framework in a command prompt or shell.

L. *Exploit attack*

In this type of attack, the attacker is aware of a security crisis inside an operating system or a part of software and leverages that knowledge by exploiting the vulnerability

III. Cryptographic principles

A. *Redundancy*

Cryptographic principle 1: The main rule is that all encrypted messages must contain some redundancy, that is, information not expected to comprehend the message. Messages must contain some redundancy [9].

B. Freshness

Cryptographic principle 2: Some technique is expected to foil replay attacks. One such measure is incorporating in every message a timestamp legitimate just for, say, 10 seconds. The receiver can then immediately keep messages around for 10 seconds, to contrast recently arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds after the fact will be dismissed as excessively old.

IV. Cryptosystem Types

Cryptography is the act of encoding information with the goal that it must be decoded by particular people. A system for encrypting and decrypting information is a cryptosystem. These typically include an algorithm for combining the original data ("plaintext") with at least one “keys” - numbers or strings of characters known only to the sender and/or recipient. The resulting output is known as “ciphertext”. A strong cryptosystem will deliver ciphertext which appears random to all standard statistical tests and can oppose every single known methods for breaking codes. One or more cryptographic primitives are regularly used to build up a more complex algorithm, called a cryptographic system, or cryptosystem. Cryptosystems (e.g., El-Gamal encryption) are intended to give specific usefulness (e.g., public key encryption) while ensuring certain security properties (e.g., chosen-plaintext attack (CPA) security in the random oracle model). Cryptosystems utilize the properties of the hidden cryptographic natives to help the system's security properties.

Cryptosystem is the foundation or condition to actualize the cryptographic procedures. It provides vital information security services. It is additionally called as Cipher System. Cryptosystem assumes sole liability to convey the message to the authorized receiver only. It protects information from any spillage by securing with encrypted codes. In general cryptosystems are taxonomies into two classes, symmetric or asymmetric, depending just on whether the keys at the transmitter and receiver are easily computed from each other. In asymmetric cryptography algorithm a dissimilar key is used for encryption and decryption. In the symmetric encryption, Alice and Bob can have the same key (K), which is obscure to the attacker, and utilizations it to encrypt and decrypt their communications channel. Cryptographic systems are utilized to give privacy and authentication in computer and communication systems. As shown in Fig. 1, encryption algorithms encipher the plaintext, or clear messages, into ambiguous ciphertext or cryptograms using a key. A deciphering algorithm is used for decryption or decipherment with the end goal to reestablish the original information. Ciphers are cryptographic algorithms; cryptography refers the knowledge of secret communications; cryptanalysis is the art of breaking ciphers; and cryptology is the skill of cryptography and cryptanalysis.

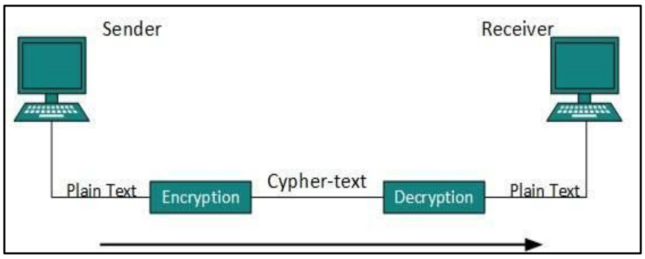

Fig. 1: General secrecy system

There are two basic types of cryptosystems: Symmetric Key and Asymmetric Key.

A. Asymmetric Cryptosystems

Asymmetric cryptosystems also called as Public key cryptosystem in which both sender and receiver use the different key for the encryption and decryption of the information. Public key cryptosystem encryptions (Scrambling) and decryptions (Unscrambling) are performed by adapting two distinct keys are alluded to as the Public key and Private keys. Key is an important constraint utilized in the encoding and decoding methodology.

There are useful issues related with the generation, distribution and protection of a large number of keys. A solution to this key-distribution problem was recommended by Diffie and Hellman in 1976 [10]. A type of cipher was proposed which utilizes two different keys: one key utilized for enciphering can be made open, while the other, utilized for deciphering, is kept secret. The two keys are produced with the end goal that it is computationally infeasible to locate the secret key from the public key. If client X needs to communicate with client Y, X can utilize Y's public key (from a public directory) to encipher the data. Only Y can decipher the ciphertext ever since he alone possesses the secret deciphering key. The system explained is called a public-key cryptosystem or an asymmetric cryptosystem [11]. If asymmetric algorithms gratify definite restrictions, they can also be utilized for creating so-called digital signatures [12].

B. Symmetric cryptosystems

Symmetric key algorithms are the fast and frequently utilized type of encryption. It is refers to encryption methods in which both the sender and receiver share the same key for both encryption and decryption. Symmetric key ciphers are executed as block ciphers or stream ciphers.

In symmetric cryptosystems (also referred to as conventional, secret-key or one-key cryptosystems), the encryption and decryption keys are either identical or simply related. Two keys should be reserved secret, and if either is compromised additional secure communication is unfeasible.

V. Cryptographic Model and Algorithm

A. Encryption model

Encryption is the way toward encoding messages or data so that just approved gatherings can get to it. In an encryption scheme, the expected data or message, alluded to as plaintext, is encrypted utilizing an encryption algorithm, creating ciphertext that must be perused whenever decoded. For specialized reasons, an encryption scheme usually uses a pseudo-random encryption key created by an algorithm[4]. There are two encryption models in particular they are as per the following: Symmetric encryption and Asymmetric encryption.

B. Decryption model

Decryption is the procedure of changing over ciphertext information into plaintext information. This term could be utilized to portray a technique for un-encrypting the data physically or with un-encrypting the data using the correct codes or keys.

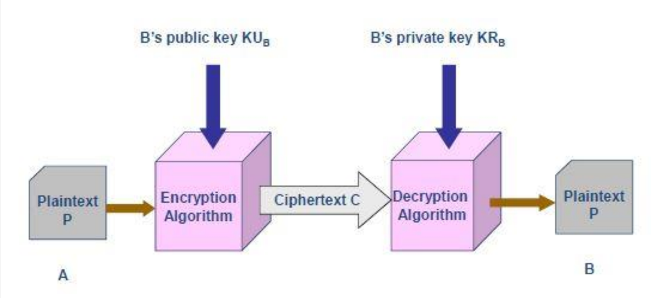

Fig. 2: Encryption and Decryption process

C. Algorithm

An algorithm stands a definite requirement of how to solve a class of issues. Algorithms can perform data processing, calculation and automated reasoning tasks. There are of course a wide range of cryptographic algorithms in use [2]:

1) DES: The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit.
2) Triple DES: Triple DES is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is expanded in Triple DES to guarantee extra security through encryption abilities. Each block contains 64 bits of information. Three keys are alluded to as package keys with 56 bits every key.
3) RSA: RSA is a public-key system designed by Rivest, Shamir, and Adleman. RSA is asymmetric cryptosystem and is generally utilized for secure information transmission. In this method[5], the asymmetric key is open and it is not the indistinguishable as the symmetric key and kept secret(private).
4) HASH: A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is for a moment refers to as a 'message digest' or a 'fingerprint'.
5) MD5: MD5 is a 128 bit message digest function. It was developed by Ron Rivest.
6) AES: This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST. The more famous and generally adopted symmetric encryption algorithm prone to be experienced nowadays is the Advanced Encryption Standard (AES). The selection process for this new symmetric key algorithm was fully open to public scrutiny and comment [5].
7) SHA-1: SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits (20 bytes).Because of the large digest size, it is less likely that two various messages will have the equivalent SHA-1 message digest. Hence SHA-1 is prescribed in inclination to MD5.
8) HMAC: HMAC is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

VI. CONCLUSION

Network Security is the fundamental part in data security since it is accountable for securing all data went through networked computers. Here studied various cryptographic techniques to increase the security of network. Cryptography, together with appropriate communication protocols, can give a high level of protection in digital communications against intruder attacks the extent that the communication between two dissimilar computers is concerned.

REFERENCES

[1] Prof. Mukund R. Joshi, Renuka Avinash Karkade, “Network Security with Cryptography”, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue. 1, pg.201 – 204, January 2015.
[2] Sumedha Kaushik and Ankur Singhal, “Network Security Using Cryptographic Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012.
[3] Kartikey Agarwal, Dr. Sanjay Kumar Dubey, “Network Security : Attacks and Defence”, International Journal of Advance Foundation and Research in Science & Engineering, Volume 1, Issue 3, August 2014.
[4] Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir and Mustafa Mat Deris, “A Survey on the Cryptographic Encryption Algorithms”, International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017.
[5] Gurpreet Singh and Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications (0975 – 8887), Volume 67, No.19, April 2013.
[6] J. S. Coron, Luxembourg Univ, Luxembourg, “What is cryptography?”, IEEE Security & Privacy Journal, Volume: 4, Issue 1, Jan. Feb, 2006.
[7] Charles. P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, “Security in Computing”, Prentice Hall, 2015.
[8] Salomon. D, “Coding for Data and Computer Communications”, New York, NY: Spring Science and Business Media, 2005.
[9] William Stallings, “Cryptography and Network Security: Principles and Practice”, 6th Edition.
[10] Diffie. W, and Hellman. M, “New directions in cryptography”, IEEE Transactions on Information Theory, Volume 22, Issue 6, Nov 1976.

[11] Gustavus J Simmons, “Symmetric and Asymmetric Encryption”, ACM Computing Surveys (CSUR), Volume 11, Issue4, Pages 305-330, Dec. 1979.

[12] Rivest. R. L, Shamir. A, and Adleman. L, “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, Volume 21, Issue 2, Pages 120-126, Feb. 1978.