Sultana *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429(Print)
ISSN: 2616-6003(Online)

LGU International Journal for
Electronic Crime Investigation

Research Article Vol. 2 issue 1 January-March 2018

Information Security with Cryptography

Tayyaba Sultana[1] , Zaka Ullah[2] , Muhammad Zulkifl Hasan[3], Taimoor Hassan[4]
Department of Computer Science
Lahore Garrison University, Lahore, Pakistan
tayyabaanwar66@gmail.com,zakaullah@lgu.edu.pk,
Zulkifl.hasan@lgu.edu.pk,taimoorhassan@lgu.edu.pk

Abstract:

The purpose of Information Security and Cryptography is to secure the data transmission and network over wireless network. The main feature of data Security is to protect transmission of data over unsecure network. The authorization of access over the data within the network is included in Information Security and which is managed by the administration of network. The users are authorized and have their own ID and password or may be some other validating information which permits them to access the programs and information under their limited authority. Diversity of computer networks is covered by information Security, private and public both, which are used in daily routine jobs directing communications and transactions among individuals, businesses and government agencies. Network might be open for the public to access or they can be private like within a company. Businesses, organizations and other kind of institutions are covered by Information Security. We will study about the cryptography and its principles in this paper. Cryptographic systems with ciphers are presented. The cryptographic algorithms and models are outlined.

Keywords: ID, Diffie Hellman, eavesdrop, Ciphers, Cryptography, IS.

1 Introduction

The most important factor of information security is cryptography because its responsibility is to secure all the information delivered by the networked computers. Information Security denotes to all software and hardware programs, features, characteristics, accountability, operational procedures, access control, measures, management, administrative policy needed to give an adequate level of security for Software, Hardware, and network information. The problems of Information Security can be categorized into four closely knotted areas: nonrepudiation, authentication, integrity control, and secrecy. Secrecy in other words, confidentiality has to do with securing information from unauthenticated users. This is the major thing which is considered when people think about Information Security.

Authentication or verification deals with finding whom you are talking before telling any critical information or making a business deal. Signatures are referred by nonrepudiation. Message reliability: However, the receiver and sender can verify each other, they also wish to make sure that the material of their conversation is not changed either by accident or meanly, in the transmission. Extensions to verify summing techniques that we faced in a secure transport and data link protocols. Cryptography is very essential for Information Security which is an evolving technology. The transmission and processing produces delicate, the extensive use of computerized data storage, in storage and transmission the personal and worthy information is susceptible to the unauthenticated access. Because of ongoing progressions in spying and communication technologies, private individuals and business organizations are starting to secure their information.

In networks and computer systems using different techniques of cryptographic, which until very freshly, were solely utilized by the diplomatic and military communities. Cryptography is dynamic of communication and computer networks of today, securing everything from email of business to transactions of bank and online shopping while modern and classical cryptography employ different techniques of Math to evade listeners from learning the data of messages which are encrypted. Computer networks and systems are required security against such unauthenticated access while processing, storing, and communicating critical and worthy information [1]. Some form of encryption is the only common method for storing and sending data over the media, which are unreliable. The major concern is that most of the attacks contain secret methods of access to information sources, and organizations and corporates are not aware of unauthenticated access to their information systems. The quantum cryptography is used for that purpose. The quantum cryptography security preserves in its capability to interchange the key of encryption with absolute security. Cryptography has its foundation in the antique world. According to [7], a very simple cryptography was used by the Julius Caesar to hide the meaning of messages. According to [7], the Caesar cipher is an analphabetic cryptosystem, hence it replicated each provided plain letter of text, wherever in the real message it happens, by the same cipher text letter alphabet. Though the ideas of receiver and source, and channel codes are advance concepts that have their origins in the information theory. In 1948, Claude Shannon proposed a theory of information based on secrecy, which states that the value of ambiguity that can be presented into a message in encoded form cannot be larger than that of the key of cryptography used for its encoding

[9]. In 1949, Claude Shannon proposed this idea of communication security. It indicates that a scheme of encryption is strongly protect if, for any two messages M1 and M2, any cipher-text C has the same possibility of being the encryption of M1 as being the encryption of M2 [6]. Two major and essential cryptographic ideas was developed by Shannon: diffusion and confusion. According to Salomon[8], any approach that created the numerical relationship between the cipher-text and the key as difficult as possible can be defined as confusion, and diffusion can be stated as a common term for any technique of encryption that extends the numerical characteristics of the plain text over a variety of bits of the cipher-text.

2 Cryptographic Principles

Redundancy Cryptographic principle 1: all messages which are encrypted must consist of some redundancy which is first principle, that is, information not required to understand the message. Message should have some redundancy.

Freshness Cryptographic principle 2: there is a need of some approach to stop the repetitive attacks. One that extent is comprising in every message timestamp effective only for, say, 10 seconds. The receiver can keep messages let's say for almost 10 seconds, to relate new messages with old messages to validate duplicates. The messages can be thrown out which are older than 10 seconds, however any replays delivered more than 10 seconds will be prohibited as too old.

3 Cryptosystem Types

Commonly cryptosystems are classified into two categories, symmetric and asymmetric, which depends only on whether the key at the receiver and at the transmitter are comfortably computer from each other. A different key is used for the purpose of encryption and decryption in asymmetric cryptography algorithm, Bob and Alice can share the same key (K) in the symmetric which is not known to the attackers, and uses it to decrypt and encrypt their channel of communications.

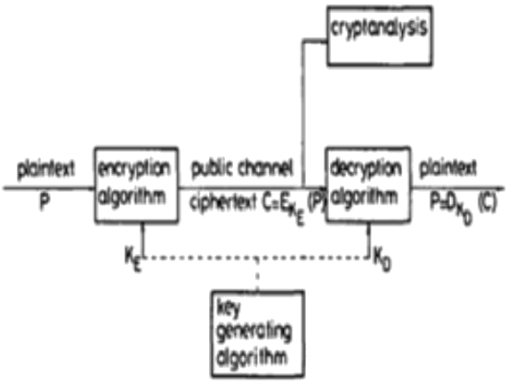

Fig. 1 General secrecy system

Cryptographic systems are used to give authentication and security in communication and computer systems.

As shown in Fig. 1, encryption algorithms encipher the plaintext, or clear messages, into inarticulate cipher text or cryptograms using a key. In order to restore the original information, a deciphering algorithm is used for decipherment or decryption. Ciphers are cryptographic algorithms; cryptography is the science of secure communications; cryptanalysis is the science of breaking ciphers; and cryptology is the science of cryptanalysis and cryptography. Cryptosystems are either symmetric, in which both the cases deciphering and enciphering keys should be kept secure, or asymmetric, in which case one of the keys may be made open public without conceding the other.

Asymmetric cryptosystems there are everyday problems related with the security, distribution and generation of a great amount of keys. Hellman and Diffie provided the solution to this problem of key distribution in 1976 [10]. A kind of cipher which uses two different key was presented: one key of enciphering made open public and the other one of deciphering is kept secret and secure.

The two keys are produced like that it is very hard computationally to reach the secret key from the open public key. if first user wishes to connect with the second user to encipher the data, first user can use public key of second user (from a public directory). Since second user owns the secret key of deciphering, only second user can decipher the cipher text. Above mention scheme is known as asymmetric cryptosystem or public-key cryptosystem [11]. After satisfaction of confirm restrictions by asymmetric algorithms, they can also be utilized for producing supposed digital signatures [12].

Symmetric cryptosystems the deciphering or enciphering keys are either same or simple connected in symmetric cryptosystems (also named as one-key cryptosystems or conventional secret-key) i.e. 684 *IEE PROCEEDINGS, Vol. 131, Pt. F, No. 7, DECEMBER 1984* one of them can be comfortably derived from the other. It is necessary to keep the both keys secret, further protected communication is not possible if either is conceded. Keys must be interchanged between users, regularly over a poor protected channel, the numbers of keys and a private courier can be very huge, if all users pair needs a separate key, even for a restrained number of users, i-e n(n-1)/2 for n users. This will produce a problem of key distribution which is partly resolved in the asymmetric systems. The DES (data encryption standard) [4] and rotor ciphers are the examples of symmetric systems.

4 Cryptographic Model and Algorithm

Encryption model following are the two models of encryption: one is symmetric encryption and other is Asymmetric encryption. Encryption key is equals to Decryption key in Symmetric encryption. While for Asymmetric encryption, Encryption key Decryption key.

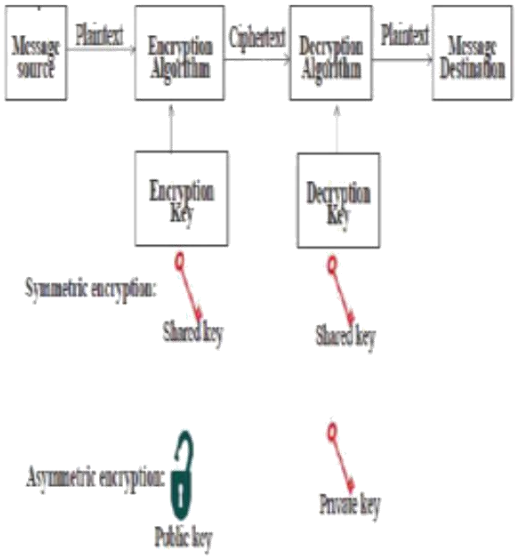

Fig 2: Cryptography

Algorithm there are a huge variety of useful cryptographic algorithms. The most well-known are as follows:

1) **DES*:*** this stands for 'Data Encryption Standard'. This uses a 56-bit key and operates on 64-bits block of data, and it is actually a cipher. It is a system of 'private key'. Furthermore about the DES algorithm.

2) **RSA:** Adleman, Rivest, and Shamir design this public key system known as RSA. Furthermore about the RSA algorithm

3) **HASH*:*** the purpose of using a 'hash algorithm' is to computer a reduced demonstration of a message of fixed length. This is occasionally called as a 'fingerprint' or a 'message digest'.

4) **MD5*:*** it is a message digest function of 128-bit. Ron Rivest developed MD5. Furthermore about the MD5 algorithm.

5) **AES:** This is the modern Encryption Standard (using the Rijndael block cipher) permitted by NIST.

6) **SHA-*1:*** SHA-1 produces a digest of 160 bits and it is also an algorithm of hashing alike in structure to MD5. It is less possible that two various messages will keep the same SHA-1 message digest because of large size of digest. Because of this reason, SHA-1 is preferred to MD5.

7) **HMAC*:*** it is also a hashing approach that utilizes a key in aggregation with an algorithm such as SHA-1 or MD5. Thus one can denote to HMAC-SHA1 and HMAC-MD5.

5 Conclusion

Information Security is the very important factor in information security the reason is it is accountable for protecting all the information over the networked computers. Information Security contains the comestibles created in a fundamental computer network organization, plans assumed by the administration of network to secure the network first and then the resourced which are accessible by network from unauthenticated access, and frequent monitoring and measurement and reliable of its efficiency or lack pooled together. There are a lot of different cryptographic techniques to increase the protection of a network. Cryptography, jointly with the relevant communication protocols, can give a high range of security in digital communication against stalker attacks as far as the communication between two separate computers is concerned.

6 References

[1] DENNING, D., and DENNING, P.J.: 'Data security', ACM Comput. Surveys, 1979, 11, pp. 227-250

[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

[3] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[4] 'Data encyption standard', FIPS PUB 46, National Bureau of Standards, Washington, DC Jan. 1977

[5] Murat Fiskiran, Ruby B. Lee, ―Workload Characterization of Elliptic Curve Cryptography and other Information Security Algorithms for Constrained Environments‖, IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.

[6] Coron, J. S. , “What is cryptography?”, IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.

[7] Pfleeger, C. P., & Pfleeger, S. L.,” Security in Computing”, Upper Saddle River, NJ: Prentice Hall.2003.

[8] Salomon, D., “Coding for Data and Computer Communications”, New York, NY: Spring Science and Business Media. 2005.

[9] Shannon, E. C.," Communication theory of secrecy system", Bell System Technical Journal, Vol.28, No.4, 1949, pp.656- 715.

[10] DIFFIE, W., and HELLMAN, M.: 'New directions in cryptography', IEEE Trans., 1976, IT-22, pp. 644-654

[11] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', ACM Comput. Surveys, 1979, 11, pp. 305-330

[12] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 1978, 21, pp. 120-126

[13] Algorithms: http://www. cryptographyworld. com/algo.htm