Network Security with Cryptography

OPEN ACCESS

Volume : 6

Special Issue : 1

Month : November

Year: 2018

ISSN: 2321-788X

Impact Factor: 3.025

Citation:
Pasupathy, V. "Network Security with Cryptography." *Shanlax International Journal of Arts, Science and Humanities,* vol. 6, no. 1, 2018, pp. 41–45.

DOI:
https://doi.org/10.5281/zenodo.1614380

V.Pasupathy
Assistant Professor, Department of Computer Applications
Sri Kaliswari College, Sivakasi

Abstract

Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. In this paper, we also studied cryptography along with its principles. Cryptographic systems with ciphers are described. The cryptographic models and algorithms are outlined.

Keywords: Cryptographic systems, Data Security, privacy, security, Network Security

Introduction

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software, and information in a network.

Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the ha nds of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. Extensions to the checksumming techniques that we encountered in reliable

transport and data link protocols. Cryptography is an emerging technology, which is important for network security. The widespread use of computerised data storage, processing and transmission make sensitive, valuable and personal information vulnerable to unauthorized access while in storage or transmission. Due to continuing advancements in communications and eavesdropping technologies, business organisations and private individuals are beginning to protect their information in computer systems and networks using cryptographic techniques, which, until very recently, were exclusively used by the military and diplomatic communities. Cryptography is vital of today's computer and communications networks, protecting everything from business e-mail to bank transactions and internet shopping While classical and modern cryptography employ various mathematical techniques to avoid eavesdroppers from learning the contents of encrypted messages. Computer systems and networks which are storing, processing and communicating sensitive or valuable information require protection against such unauthorized access[1].

The only general approach to sending and storing data over media which are insecure is to use some form of encryption. A primary concern is that many attacks involve secret manner access to information resources, and organizations are often unaware of unauthorized access to their information systems. For that reason the quantum cryptography used. The security of quantum cryptography maintains in its ability to exchange the encryption key with absolute security. Cryptography has its origin in the ancient world. According to [7], the Julius Caesar used simple cryptography to hide the meaning of his messages. According to [7], The Caesar cipher is a monoalphabetic cryptosystem, since it replaces each given plain text letter, wherever in the original message it occurs, by the same letter of the cipher text alphabet. However, the concepts of source an d receiver, and channel codes are modern notions that have their roots in the information theory. Claude Shannon, in 1948 provided the information theory basis for secrecy, which defines that the amount of uncertainty that can be introduced into an n encoded message can't be greater than that of the cryptographic key used to encode it [9]. Claude Shannon presented this concept of security in communications in 1949; it implies that an encryption scheme is perfectly secure if, for any two messa ges M 1 and M 2, any cipher-text C has the same probability of being the encryption of M 1 as being the encryption of M 2 [6]. Shannon was developed two important cryptographic concepts: confusion and diffusion. According to Salomon [8], the term confusion means to any method that makes the statistical relationship between the cipher-text and the key as difficult as possible, and diffusion is a general term for any encryption technique that expands the statistical properties of the plainte xt over a range of bits of the cipher-text.

Cryptographic Principles

Redundancy

Cryptographic principle 1: The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message. Messages must contain some redundancy.

Freshness

Cryptographic principle 2: Some method is needed to foil replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly 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 later will be rejected as too old.

Cryptosystem Types

In general, cryptosystems are taxonomies into two classes, symmetric or asymmetric, depending only on whether the keys at the transmitter and receiver are easily computed from each other. In asymmetric cryptography algorithm, a different ke y is used for encryption and decryption. In the symmetric encryption, Alice and Bob can share the same key (K), which is unknown to the attacker and uses it to encrypt and decrypt their communications channel.

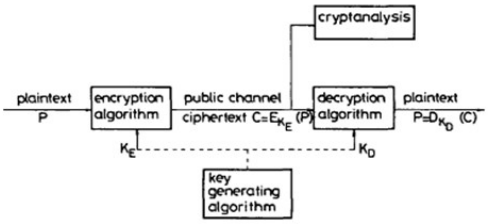

Fig. 1 General secrecy system

Cryptographic systems are used to provide privacy and authentication in computer and communication systems. As shown in Fig. 1, encryption algorithms encipher the plaintext, or clear messages, into unintelligible ciphertext or cryptograms using a key. A deciphering algorithm is used for decryption or decipherment in order to restore the original information. Ciphers are cryptographic algorithms; cryptography is the science of secret communications; cryptanalysis is the science of breaking ciphers; and cryptology is the science of cryptography and cryptanalysis. Cryptosystems are either symmetric, in which case both the enciphering and deciphering keys must be kept secret, or asymmetric, in which case one of the keys can be made public without compromising the other.

Asymmetric cryptosystems

There are practical problems associated with the generation, distribution and protection of a large number of keys. A solution to this key-distribution problem was suggested by Diffie and Hellman in 1976 [10]. A type of cipher was proposed which uses two different keys: one key used for enciphering can be made public, while the other, used for deciphering, is kep t secret. The two keys are generated such that it is computationally infeasible to find the secret key from the public key. If user A wants to communicate with user B, A can use B's public key (from a public directory) to encipher the data. Only B can deciphe r the ciphertext since he alone possesses the secret deciphering key. The scheme described above is called a public-key cryptosystem or an asymmetric cryptosystem[11]. If asymmetric algorithms satisfy certain restrictions, they can also be used for generating so-called digital signatures[12].

Symmetric cryptosystems

In symmetric cryptosystems (also called conventional, secret-key or one-key cryptosystems), the enciphering and deciphering keys are either identical or simply related, i.e., 684 IEE PROCEEDINGS, Vol. 131, Pt. F, No. 7, DECEMBER 1984 one of them can be easily derived from the other. Both keys must be kept secret, and if either is compromised further secure communication is impossible. Keys need to be exchanged between users, often over a slow secure channel, for example, a private courier, and the number of keys can be very large, if every pair of users requires a different key, even for a moderate number of users, i.e., n(n — l)/2 for n users. This creates a key-distribution problem which is partially solved in the asymmetric systems. Examples of symmetric systems are the data encryption standard (DES) [4] and rotor ciphers.

Cryptographic Model and Algorithm

Encryption model

Encryption key = Decryption key. In Asymmetric encryption, Encryption key ¹ Decryption key

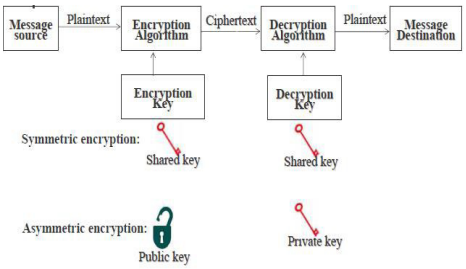

Fig 2: Cryptography

Algorithm

1) DES: This is the 'Data Encryption Standard.' This is a cipher that operates on 64-bit blocks of data, using 56-bit key. It is a 'private key' system. Further Details on the DES Algorithm.
2) RSA: RSA is a public-key system designed by Rivest, Shamir, and Adleman. Further Details on the RSA Algorithm.
3) HASH: A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest,' or a 'fingerprint.'
4) MD5: MD5 is a 128-bit message digest function. It was developed by Ron Rivest. Further Details on the MD5 Algorithm.
5) AES: This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST.
6) 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 different messages will have the same SHA-1 message digest. For this reason, SHA-1 is recommended in preference to MD5.
7) 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.

Conclusion

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combinedr. We have studied various cryptographic techniques to increase the security of network. Cryptography, together with suitable communication protocols, can provide a high degree of protection in digital communications against intruder attacks as far as the communication between two different computers is concerned.

References

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

Algorithms: http://www.cryptographyworld.com/algo.htm

Coron. J. S. (2006) "What is cryptography?", *IEEE Security & Privacy Journal,* 12(8), p. 70-73.

'Data encryption standard,' FIPS PUB 46, National Bureau of Standards, Washington, DC Jan. 1977.

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

Denning. D. & Denning. P. J. (1979) 'Data security,' ACM *Comput. Surveys,* vol. 11, pp. 227-250

Diffie. W. & Hellman. M. (1976) 'New directions in cryptography,' *IEEE Trans.,* IT-22, pp. 644-654.

Murat Fiskiran, Ruby B. Lee, (2002) Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments, IEEE International Workshop on Workload Characterization, 2002. WWC-5.

Pfleeger. C. P. & Pfleeger. S. L. (2003) *"Security in Computing,"* Upper Saddle River, NJ: Prentice Hall.

Rivest. R. L., Shamir. A. & Adleman. L (1978) 'A method for obtaining digital signatures and public-key cryptosystems,' *CACM,* 21, pp. 120-126

Salomon. D. (2005) *"Coding for Data and Computer Communications,"* New York, NY: Spring Science and Business Media.

Shannon. E. C. (1949) "Communication theory of secrecy system," *Bell System Technical Journal,* vol.28, no.4, pp.656- 715.

Simmons. G.J. (1979) 'Symmetric and asymmetric encryption,' *ACM Comput. Surveys,* 11, pp. 305-330.

Web Sources

https://ijcsmc.com/docs/papers/January2015/V4I1201544.pdf

https://www.ijeecse.com/N1031.pdf