Journal of Advances and Scholarly Researches in Allied Education
Vol. 13, Issue No. 1, April-2017, ISSN 2230-7540

Framework of Network Security and Cryptography: An Impact Analysis

Shikha Kuchhal*

Assistant Professor, Department of Electronics & Communication, SPTM

Abstract – Computer networks that are involved in regular transactions and communication within the society, government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. Cryptography historically dealt with the construction and analysis of protocols that would prevent any third parties from reading a private communication between two parties. In the digital age, cryptography has evolved to address the encryption and decryption of private communications through the internet and computer systems, a branch of cyber and network security, in a manner far more complex than anything the world of cryptography had seen before the arrival of computers. Secure Communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security. Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography. In this paper cryptography along with its principles and cryptographic systems with ciphers are studied.

Key Words: Network Security, Cryptography, Security Challenges, Threats, Encryption, Decryption

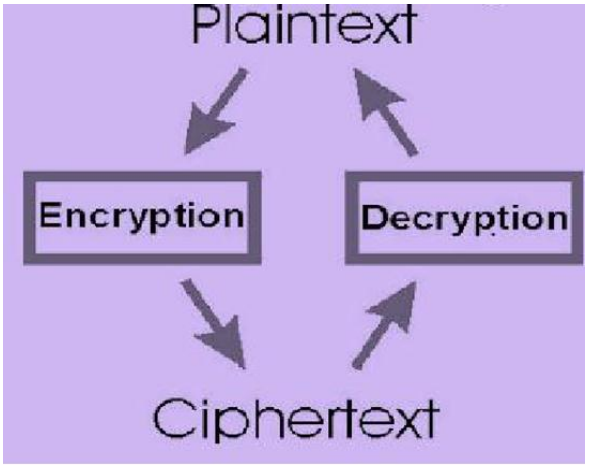
----------X----------

1. INTRODUCTION

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats. Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

The fast development of the modern Internet technology and information technology cause the individual, enterprise, school and government department joining the Internet, Which cause more illegal users to attack and destroy the network by using the fake websites, fake mail, Trojan horse and backdoor virus at the same time. Target of the attacks and intrusion on the network are computers, so once the intruders succeed, it will cause thousands of network computers in a paralyzed state In addition, some invaders with ulterior motives look upon the military and government department as the target which cause enormous threats for the social and national security.

Cryptography means "Hidden Secrets" is concerned with encryption. It is helpful for examining those conventions, that are identified with different viewpoints in data security, for example, verification, classification of information, non-denial and information uprightness.



Cryptography is the science of writing in secret code. More generally, it is about constructing and analyzing protocols that block adversaries; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.

The aim of cyber security is to attempt to create encryption systems that perform perfectly on all four of the above-mentioned parameters. This can

be almost impossible to fully accomplish, since the strength of the encryption depends not only on computer programs but also on human behavior. The best security systems in the world can still be defeated by an easily-guessed password, or the user not logging out after a session or discussing security information with outsiders.

Today, cryptography uses some of the finest computer and mathematical minds on the planet. Every industry on the planet, from war to healthcare makes use of encryption to protect sensitive information that is being transmitted across the internet.

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.

We are living in the information age where information needs to be kept about every aspect of our lives. This information can be thought of as an asset, and like every other asset, this information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entry when it is needed (availability). Thus, confidentiality, integrity and availability can be termed as the three most important security goals.

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 hands of unauthorized users. This is what usually comes to mind when people think about network security. No repudiation 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 check summing 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 makes sensitive, valuable and personal information vulnerable to unauthorised 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 a 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.

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. However the concepts of source and receiver, and channel codes are modern notions that have their roots in the information theory. Claude Shannon, in the 1948 provided the information theory basis for secrecy, which defines that the amount of uncertainty that can be introduced into an encoded message can't be greater than that of the cryptographic key used to encode it . Claude Shannon presented this concept of security in communications in 1949, it implies that an encryption scheme is perfectly secure if, for any two messages 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 . 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 plaintext over a range of bits of the cipher-text.

2. LITERATURE SURVEY

- Shouhuai Xu et. al. proposed new complex systems that can be developed by exploiting trust based social networks (such as Facebook) to store protected data in a distributed manner, using threshold cryptography, to develop certain functional qualities.

- Lo-Yao Yeh et. al. discuss peer to peer online social networks that are currently vulnerable without a solid batch authentication method. Three new protocols are proposed, including one way hash function, proxy encryption, and certificates as underlying cryptosystems. These have lower computational cost than the standard methods.

- Ralf Kusters et. al. discuss the problem of establishing a standard framework of cryptographic verification of Java and Java like programs which are still open. The noninterference properties of Java like programs can be used to provide cryptographic guarantees; in particular, computational in distinguishability, using simulation based security. This is achieved using a new extended language called Jinja+ , which extends from Jinja. Jinja provides major Java functionality. It is used to provide the framework for cryptographic verification required.

- Salah k et. al. proposes and analyzes a general cloud-based security overlay network that can be used as a transparent overlay network to provide services such as intrusion detection systems, antivirus and antispam software, and distributed denial-of-service prevention. The paper analyzes each of these in-cloud security services in terms of resiliency, effectiveness, performance, flexibility, control, and cost.

- Yu Zhang et. al. discuss bout the authenticity of nodes in an ad hoc network which cannot be guaranteed. Hackers misuse this fact and simulate an active node in the network to carry out malicious activities. An audit based technique is proposed. Nodes which continuously or selectively drop packets are termed misbehaving and this mechanism enables to detect and isolate these misbehaving nodes in a wireless ad hoc network.

- Udi Ben-Porat et. al. discusses Distributed Denial of Service attacks that degrade server performance of not only the host but of every client by repeatedly transmitting trivial packets across the network. The study on one of the most common data structures in Network Systems (Hash Tables), attempts to establish effective protection mechanisms against DDoS attacks. This study also contrasts Open vs Closed hashing from a security perspective.

- Ahmed et. al. discusses the Digital TV band insecurity against Primary User Emulation Attacks. An AES encryption standard can be implemented to further secure it. By allowing a shared secret between the sender and receiver, the sync bits of DTV data frames can be used to regenerate the sender signal to identify authorized users, thus stopping PUE attacks. It can also detect a malicious presence whether the primary user is present or not.

3. CRYPTOGRAPHIC PRINCIPLES

A. 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.

B. Freshness

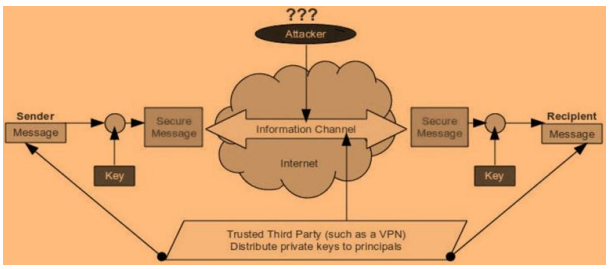
Cryptographic principle 2: Some method is needed to foil replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

3.1 Network Security Model

Figure demonstrates the model of system security. A message is to be exchanged starting with one gathering then onto the next over some kind of Internet administration. An outsider might be in charge of appropriating the mystery data to the sender and beneficiary while keeping it from any rival. While building up a safe system, the accompanying should be considered.

1. **Confidentiality**: It means that the non-authenticated party does not examine the data.

2. **Integrity**: It is a certification that the information which is gotten by the collector has not been change or Modified after the send by the sender.



All the techniques for providing security have two components

- A security-related change on the data to be sent. Message ought to be scrambled by key with the goal that it is confused by the adversary.

- An encryption enter utilized as a part of conjunction with the change to scramble

the message before transmission and unscramble it on gathering

Security perspectives become an integral factor when it is fundamental or alluring to shield the data transmission from a rival who may display a danger to classification, realness, etc.

3.2 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 key 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.

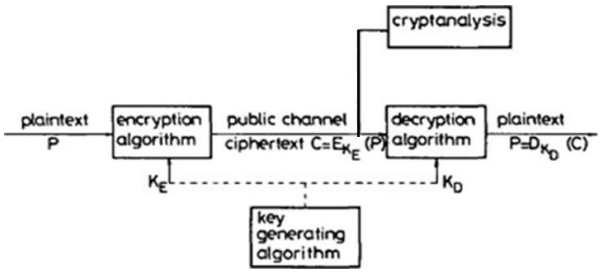


Fig. 1 General secrecy system

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.

A. 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. 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 kept 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 decipher the cipher text since he alone possesses the secret deciphering key. The scheme described above is called a public-key cryptosystem or an asymmetric cryptosystem. If asymmetric algorithms satisfy certain restrictions, they can also be used for generating so-called digital signatures.

B. 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) and rotor ciphers.

3.3 Cryptographic Model and Algorithm

A. Encryption model

There are two encryption models namely they are as follows: Symmetric encryption and Asymmetric encryption. In Symmetric encryption,

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

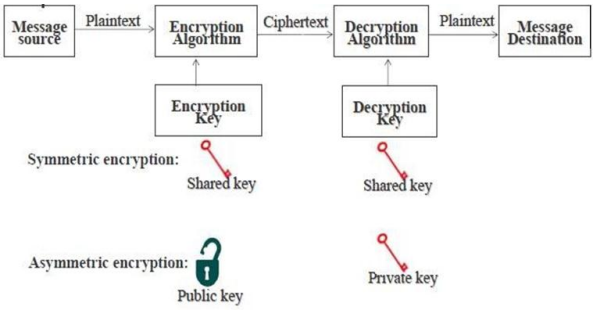


Fig 2: Cryptography

B. Algorithm

There are of course a wide range of cryptographic algorithms in use. The following are amongst the most well-known:

1) DES: This is the 'Data Encryption Standard'. This is a cipher that operates on 64-bit blocks of data, using a 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.

3.4 Comparison of Various Encryption Algorithm

In the following Table, Comparative study of various encryption algorithms on the basis of their ability to secure and protect data against attacks and speed of encryption and decryption.

SYMMETRIC ENCRYPTION:	KEY SIZES	In Steps Of
DES	40 – 56 bits	8 bits
Triple-DES (two key)	64 – 112 bits	8 bits
Triple-DES (three key)	120 – 168 bits	8 bits
PUBLIC KEY ENCRYPTION:		
Diffie-Hellman	512 – 2048 bits	64 bits
RSA *	512 – 2048 bits	64 bits
DIGITAL SIGNATURES:		
DSA	512 – 2048 bits	64 bits
RSA *	512 – 2048 bits	64 bits

4. CONCLUSION

As the relevance and importance of privacy of data is continuously increasing, the importance of network security and cryptography is increasing parallely. Providing Network Security is never an absolute process, but rather an iterative one. Hence, Network Security and Cryptography are on the cutting edge of research today. 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) combined together. 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.

5. REFERENCES

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

2. Yossi Gilad, Amir Herzberg, Haya Shulman (2013). “Off path hacking: The Illusion of Challenge-Response Authentication”, IEEE Security & Privacy, Issue 99, pp. 1, Oct 2013, DOI: 10.1109/MSP.2013.130.

3. Stainslaw Jarecki, Jihye Kim, Gene Tsudik (2011). “Flexible Robust Group Key Agreement”, IEEE Transactions on Parallel & Distributed Systems, Volume 22, Issue 5, pp. 879 - 886, DOI: 10.1109/TPDS.2010.128.

4. Andrew Chi-Chih Yao, Yunlei Zhao (2014). “Privacy-Preserving Authenticated Key-Exchange over Internet”, IEEE Transactions on Information Forensics and Security, Volume 9, Issue 1, pp. 125 - 140, DOI: 10.1109/TIFS. 2013.2293457.

5. Ning Cai, Raymond W. Yeung (2011). “Secure Network Coding on a Wiretap Network”, IEEE Transactions on Information Theory, Volume 57, No. 1, pp. 424 - 435, DOI: 10.1109 /TIT.2010. 2090197.

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

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

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

9. 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.

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

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

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

13. Shannon, E. C. (1949). “Communication theory of secrecy system”, Bell System Technical Journal, Vol.28, No.4, pp. 656-715.

14. DIFFIE, W. and HELLMAN, M. (1976). “New directions in cryptography', IEEE Trans., IT-22, pp. 644-654

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

16. RIVEST, R.L., SHAMIR, A., and ADLEMAN, L. (1978). 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 21, pp. 120-126.

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

Corresponding Author

Shikha Kuchhal*

Assistant Professor, Department of Electronics & Communication, SPTM