Survey on Network Security with Cryptography

NEETHU. C

cneethu313@gmail.com

MSc. Computer Science, Final Year

Cherpulassery College of Science and Technology for Women (Affiliated to University of Calicut)
Karalmanna, Cherpulassery, Palakkad Dist

ABSTRACT: Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main form of secure data transmission over unreliable network. It comprises authorization to access of information in a network, controlled by the network administrator. The task of network security is not only requires ensuring the security of end systems but of the entire network. Network security covers variety of computer networks, both public and private. That are used in everyday jobs conducting transactions and communications among commercial enterprise, government agencies and individuals. Networks can be private or public access. Network security is involved in organizations, and other types of institutions. In this paper we also studied purpose of cryptography, some network security problems,cryptography mechanisms and symmetric and asymmetric encryptions are outlined .

Keywords: Network Security, Cryptography, Decryption, Encryption, malicious, intruder.

I. INTRODUCTION

Network Security is the most significant component in information security because it is responsible for securing all information passed through networked computers.

Network security problems can be divided into four closely intertwined areas: secrecy, authentication, no repudiation, and integrity control. Secrecy, also called confidentiality, has to do with control information out of the hands of unauthorized users. This is what generally comes to mind when people think about network security. Authentication deals with determining whom you are talking to before expose sensitive information or entering into a business deal. No repudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to assure that the content of their communication is not altered, either maliciously or by accident, in transmission.

Cryptography is an emanate technology, which is important for network security. The widespread use of computerized data storage, processing and transmission makes sensitive, relevant and personal information vulnerable to unauthorized access while in storage or transmission. Cryptography is a important 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 deflect 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].

II. PURPOSE OF CRYPTOGRAPY

Cryptography is the science of writing in secret code and is an antique art. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic dispatch to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the diffuse development of computer communications. In data and telecommunications, cryptography is mandatory when communicating over any entrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or modification, but can also be used for user authentication.

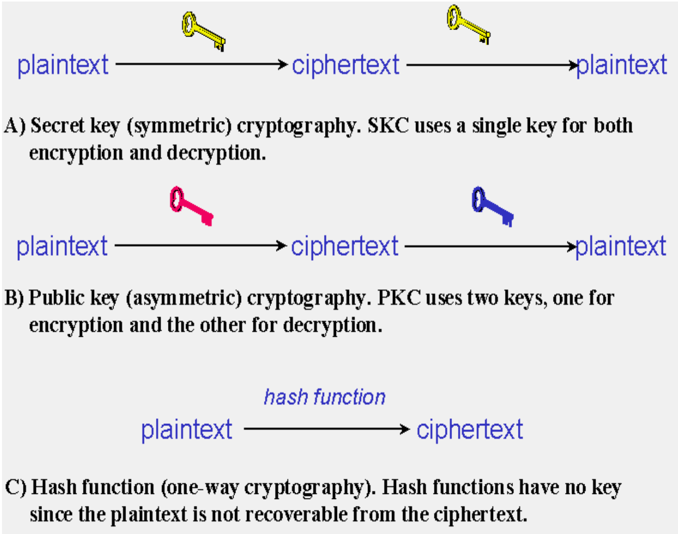
There are, in general, three types of cryptographic schemes typically used to accomplish these goals:

a) Secret key (or symmetric) cryptography

b) public-key (or asymmetric) cryptography

c) Hash functions

In all cases, the basic unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in usually be decrypted into usable plaintext. In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common taxonomy in the crypto field and literature to make it easier to identify the communicating parties.



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Fig1

III. NETWORK SECURITY

Security is a broad topic and covers a majority of sins. In its simplest form, it is concerned with making sure that intrusive people cannot read, or worse yet, secretly modify messages intended for other recipients. It is perturbed(concerned) with people trying to access remote services that they are not authorized to use[2]. Most security problems are intentionally caused by malicious people trying to rise some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwind areas:

a) Secrecy

b) Authentication

c) Non repudiation

d) Integrity control

A. Secrecy

Secrecy, also called confidentiality, has to do with storing information out of the hands of unauthorized users. This is what normally comes to mind when people think about network security. Authentication deals with determining whom you are talking to before exposing sensitive information or entering into a business deal. No repudiation deals with signatures within the context of any application-to-application communication, there are some specific security requirements including: authentication.

- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Message Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *on-repudiation:* A mechanism to prove that the sender really sent this message.

B. Authentication

The primary forms of host-to-host authentication on the Internet today are name based or address-based, both of which are especially weak. Both the sender and receiver need to confirm the identity of other party involved in the communication - to confirm that the other party is indeed who or what they claim to be. Face -to-face human communication solves this problem quickly by visual recognition. When communicating entities exchange messages over a medium where they cannot "see" the other party, authentication is not so simple. Why, for instance, should you believe that a received email containing a text string saying that the email came from a friend of yours absolutely came from that friend? If someone calls on the phone claiming to be your bank and asking for your account number, secret PIN, and account balances for verification prospect, would you give that information out over the phone? Hopefully not.

C. *Non repudiation*

Non-repudiation is a mechanism to prove that the sender actually sent this message. It deals with signatures having established what we mean by secure communication; let us next consider exactly what is meant by an "insecure channel."

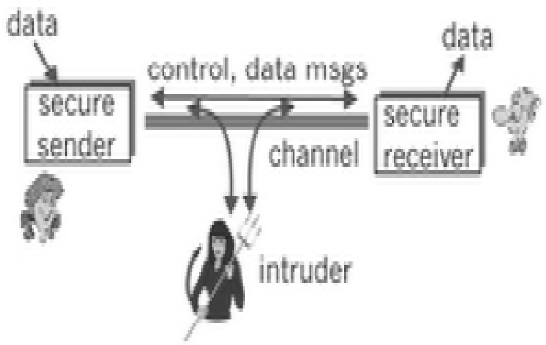


Fig 2

Alice, the sender, needs to send data to Bob, the receiver. In order to securely exchange data, while meeting the requirements of secrecy, authentication, and message integrity, Alice and Bob will exchange both restrict message and data messages . Some of these messages will typically be encrypted[3]. A passive intruder can listen to and record the control and data messages on the channel; an active intruder can remove messages from the channel and/or itself add more messages into the channel.

D. *Integrity Control*

Assuring the receiver that the p received message has not been altered in any way from the original. Even if the sender and receiver are able to authenticate each other, they also want to assure 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[4].

IV. CRYTOGRAPHIC PRINCIPLES

A. *Redundancy*

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

B. *Freshness*

Cryptographic principle 2: Some method is needed to foil replay attacks. One such measure is including in whole 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, as any replays sent more than 10 seconds later will be rejected as too old[4].

V. CRYPTOGRAPHY MECHANISM

Cryptography is a strategy for putting away and transmitting information in a special frame so that those for whom it is expected can read and process it. The term is regularly connected with scrambling plaintext message (customary content, in some cases alluded to as cleartext) into ciphertext (a procedure called encryption), then back once more (known as decoding). There are, as a rule, three sorts of cryptographic plans commonly accomplish to achieve these objectives: symmetric key (or mystery) cryptography, open key (or hilter kilter) cryptography, and hash works, each of which is portrayed underneath[5].

Key : A key is a numeric or alpha numeric manuscript or may be a unique figure.

Plain Text : The first message that the particular wishes to speak with the other is characterized as Plain Text. For instance, a man named Alice wishes to send "Hi Friend how are you" message to the distinct Bob. Here "Hi Friend how are you" is a plain current message.

Cipher Text : The message that can't be comprehended by any one or an aimless message is the thing that we call as Cipher content. Ciphertext is not to be misled for code content in light of the fact that the last is an aftereffect of a code, not a figure.

Encryption : A procedure of changing over plain content into figure content is called as Encryption. This procedure requires two things-an encryption calculation and a key[7]. Calculation implies the system that has been handled as a part of encryption. Encryption of information happens at the sender side.

Decryption : A quirk around procedure of encryption is called as Decryption. In this procedure Cipher content is changed over into Plain content. Decoding process requires two things-an unscrambling calculation and a key. Calculation implies the method that has been utilized as a part of Decryption[6].

VI. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

There are commonly two types of techniques that are used for encrypt/decrypt the protected data related Asymmetric and Symmetric encryption technique.

Symmetric Encryption

If there should be an occurrence of Symmetric Encryption, like cryptography keys are utilized for encryption of plaintext and unscrambling of figure content. Symmetric key encryption is speedier and fewer difficult yet their principle downside is that both the clients need to move their keys security. There is only one key used both for encryption and decryption of data[8].

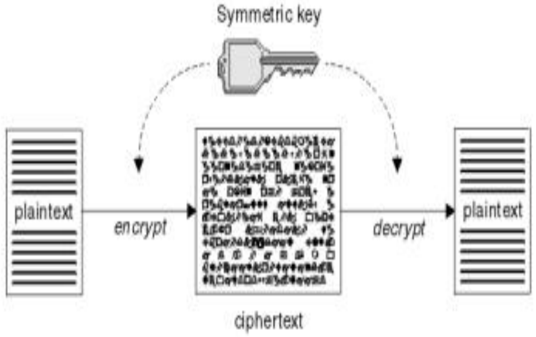


Fig3

Asymmetric Encryption

Asymmetric encryption cause two keys and also known as Public Key Cryptography, because user uses two keys: public key, which is known to public and a private key which is only known to user. Asymmetric key Encryption, the diverse keys that are used for encryption and decryption of facts that is Public key and Private key.

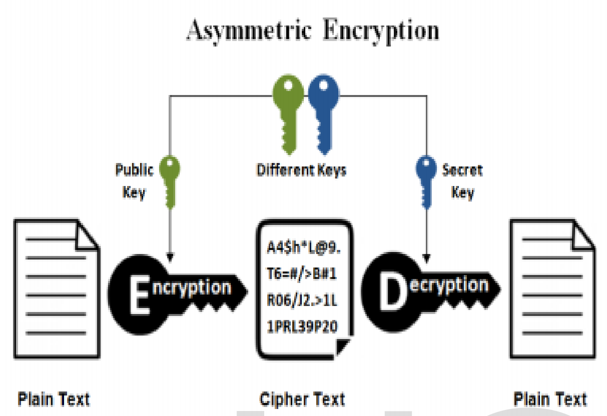


Fig4

VII. CONCLUSION

This paper has described briefly about cryptography mechanisms ,encryption techniques, some network security problems. Network Security is the most important component in information security because it is responsible for securing all information passed through networked computers. Cryptography is a particularly interesting field being of the amount of work that is, by necessity, done in secret. 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

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

[2] Trappe, W., & Washington, L.C. (2006). *Introduction to Cryptography with Codin Theory*, 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall.

[3] Denning, D.E. (1982). *Cryptography and Data Security*. Reading, MA: Addison-Wesley.

[4] Network Security Essential, William Staling, Pearson Publications Ltd.

[5] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001.

[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] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. 3Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. "A. Handbook of Applied Cryptography". ISBN 0-8493-8523-7.