Emerging Trends in Network Security using Cryptography

R. Felista Sugirtha Lizy
Assistant Professor
Department of Information Technology
Pope's College, Tamil Nadu, India

Abstract— Network security is one more main concepts to secure the data. It can be implemented by the techniques of cryptographic and wireless security to process the protection mechanism. In this paper we are discussed about cryptography along with its principles. Cryptography and Network security is a subject too broad area to mingle about how to protect the information in digital pattern and to give the guarantee of services. However, the overview of cryptography and network security is maintained and different algorithms are reviewed.

Key words: Attacks, Cryptography, Network Security, Wireless Security

I. INTRODUCTION

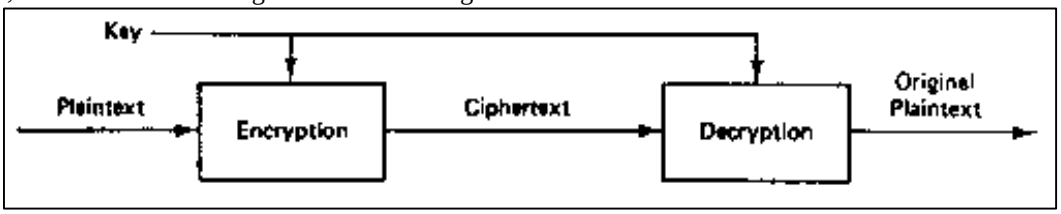
Cryptography provides great significance in the surveillance of data. It makes possible to keep in reserve sensitive data or send the data across the networks so that unlicensed humans cannot swot it. The immense transcend in network technology has ensue from in great prospective for deviating the path we diffuse and do vast employment through the internet. But it is for managing stealthy data, the cost performance and the universal granted by the internet are diminished steadily by the premier drawback of common networks. The demonstratively multiplying development in the stealthy data deal with overcome the internet concocts the security fundamental issue.

II. CRYPTOGRAPHY

Cryptography is a Greek origin word in which "crypto" means hidden and also "graphy" means writing, so cryptography means hidden or secret writing. Cryptography is sometimes also considered as Cipher-system. There are two types of cryptographic techniques, Symmetric Key and Asymmetric Key

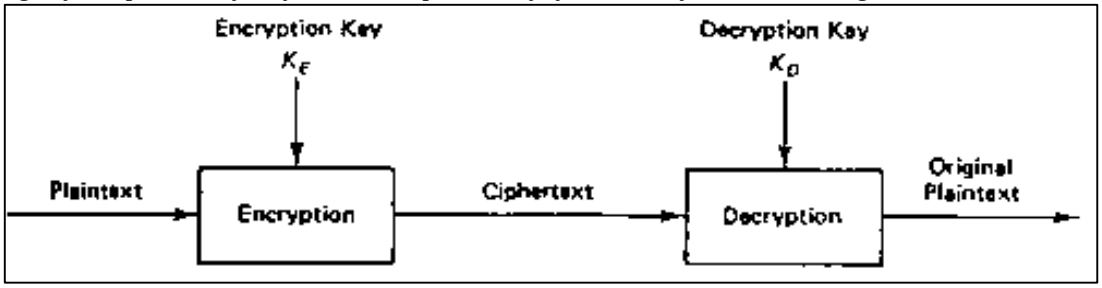
A. Symmetric key Algorithms

This algorithm is sometimes called secret-key cryptography. Symmetric algorithms encrypt and decrypt a message using the same key. If you hold a key, you can exchange messages with anybody else holding the same key. It is a shared secret. But be careful who you give the key to. Once it gets in the illegal hands, there is no getting it back. That person can read all of your past messages, and create new messages that are indistinguishable from valid data.



B. Symmetric key Algorithms

This algorithm use a distinct key to use encrypt than they do to decrypt. The encrypting key is referred to the public key, then the decrypting key is a private key. If you hold the private key, you can only read the message.

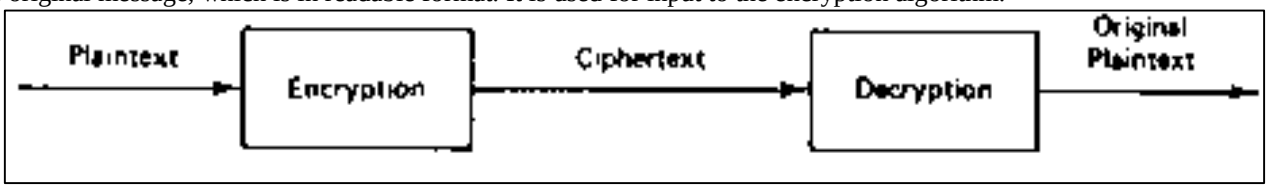


These keys are work in the opposite direction. That is, anything you can encrypt with your private key, and you can decrypt with your public key. You can use to digitally sign a deed. Encrypt it with you private key, and I will able to verify your signature by decrypting with your public key. I have secret that the message came from you, because only someone who holds your private key could have produced a working signature.

The ingredients of traditional encryption algorithms are plaintext, ciphertext, secret key, encryption algorithm and decryption algorithm.

1) Plain Text:

The original message, which is in readable format. It is used for input to the encryption algorithm.



2) Cipher Text:

It is the transformed and changed plain text which is not understandable while merely looking at it. It is obtained after applying encryption algorithm and encryption key over the plain text. It may or may not be safe guarded. If it is not safe guarded then any intruder can access it easily from the public channel using which it is being transmitted. But decoding it without knowing the secret key is the tough task.

3) Encryption Algorithm:

This algorithm perform discrete operations to convert plaintext into ciphertext. This algorithm takes plaintext and secret key as input and produces ciphertext as output [1].

4) Decryption Algorithm:

This algorithm is reverse process of encryption algorithm. This algorithm perform discrete operations to convert ciphertext back into plaintext. This algorithm accept ciphertext and secret key as inputs and generates plaintext as output.

5) Encryption Key:

This key is the value that is, the lead aspect of the cryptographic system which is either known only to sender or to both sender and receiver. Safe guarding of this key is of great importance for making cryptographic system successful. This key is applied within encryption algorithm to generate cipher text out of plain text.

6) Decryption Key:

This key is the value known to receiver and it may or may not be identical to encryption key. It is applied within decryption algorithm to generate the plaintext back from received cipher text. A collection that contains all probable decryption keys is known as Key Space.

7) Secret Key:

This key is also input to the encryption algorithm. The total strength of the procedure depends only on secret key. For same algorithm, same plaintext two different secret key values will produce two different ciphertext.

There are four main goal of cryptography:

1) Data Integrity: The receiver of a message should be able to examine whether the message was altered for the time of transmission, either unintentionally or purposely. Nobody should be able to substitute a false message for the earliest message, or for parts of it.
2) Authentication: The receiver of a message should be able to examine its origin. Nobody should be able to send a message to Bob and pretend to be Alice (data inception authentication). When starting concern, Alice and Bob should be able to recognize each other (entity authentication).
3) Non-repudiation: The sender should not be able to afterwards refuse that she sent a message.

III. SYMMETRIC KEY ENCRYPTION

A. DES (Data Encryption Standard)

DES is a symmetric block cipher developed by IBM. This algorithm uses a 56-bit key to encipher/decipher a 64-bit block, every eighth bit of which is neglected. However, it is customary to set each eighth bit so that each group of 8 bits has an odd number of bits is set to 1.

B. Triple DES (3DES)

3DES is an enhancement of DES; it is 64 bit block-size with 192 bits key size. In this encryption method is alike to the one in the original DES but applied 3 times to rise the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher method.

C. AES

AES is a block cipher. It has the variable key length of 128, 192 or 256 bits [3]; default length is 256 bits. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on discrete platforms specifically in small devices. Also, AES has been carefully tested for many security applications [5].

D. Blowfish

Blowfish algorithm is the important type of the symmetric key encryption that has a 64 bit block size and a variable key length from 32 bits to 448 bits in general [2]. Since the key size is larger it is complex to break the code in the blowfish algorithm. Moreover it is vulnerable to all the attacks except the weak key class attack.

E. RC4

RC4 is accepted as the most commonly avail oneself stream cipher in the world of cryptography. RC4 has a use in both encryption and decryption while the data stream undergoes XOR together with a series of generated keys. It takes in keys of random lengths and this is known as a producer of pseudo arbitrary numbers. The output is then XOR together with the stream of data in order to generate a newly-encrypted data.

IV. ASYMMETRIC KEY ENCRYPTION

A. RSA

Rivest-Shamir-Adleman is the most commonly used public key encryption algorithm. It can be used to send an encrypted message without a separate exchange of secret keys. It can also be used to sign a message. In RSA, this asymmetry key is based on the factoring the product of two large prime numbers. RSA computation occurs with integers modulo n=p*q, for two large secret prime p, q. To encrypt a message m, with a small public exponent e. For decryption, the recipient of the cipher text $c=M^e$ (Mod n) computes the multiplicative reverse d=e-1(mod (p-1)*(q-1)) (we require that e is selected suitably for it to exist) and obtained cd = m e * d = m (mod n). The key size should be greater than 1024 bits for a reasonable level of security.

B. Diffie-Hellman Algorithm

The Diffie-Hellman key exchange method allows two parties that have no previous knowledge of each other to jointly form a served secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The Diffie-Hellman protocol is generally referred to be secure when an appropriate mathematical group is used.

V. TYPES OF ATTACKS

A. Passive Attacks

This type of attacks include observation or monitoring of communication. A passive attack attempts to learn or make use of information from the system but does not affect system resources.
Types of passive attacks:

1) Traffic analysis: The message traffic is sent and receive in an exposed normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
2) Release of message contents: Read contents of message from sender to receiver.

B. Active Attacks

An active attack attempts to alter system resources or affect their operation. It involves some modification of the data stream or the creation of a false stream.
Types of active attacks:

1) Modification of Messages: some portion of an authorized message is altered, or that messages are detained or reordered.
2) Denial of Service: An entity may squash all messages directed to a particular destination.
3) Replay: It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
4) Masquerade: It takes place when one entity pretends to be a different entity.

VI. WIRELESS NETWORK SECURITY

Wireless security is the prevention of illegal access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (*WEP*) and Wi-Fi Protected Access (*WPA*). WEP is a famous weak security standard. The password it uses can frequently be damaged in a few minutes with a basic laptop computer and widely available software tools. WAP security is primarily provided by the Wireless Transport Layer Security (WTLS), which provides security services between the mobile device (client) and the WAP gateway to the Internet. There are lot of approaches to WAP end-to-end security. The WAP architecture is designed to manage with the two limitations of wireless Web access: the limitations of the mobile node (small screen size, limited input capability) and the low data rates of wireless digital networks. Two important WTLS concepts are the secure session and the secure connection, which are defined in the specification as:

1) Secure connection: A connection is a transport (in the OSI layering model definition) that provides a convenient type of service. For Secure Sockets Layer (SSL), such connections are peer-to-peer relationships. The connections are temporary. Every connection is linked with one session. Between any pair of parties (applications such as HTTP on client and server), there may be multiple secure connections.
2) Secure session: An SSL session is a relation between a client and a server. Sessions are created by the Handshake Protocol. Sessions are define a set of cryptographic security parameters, which can be go halves on among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection. There are a number of states associated with each session. Once a session is established, there is a current operating state for both read and write (i.e., receive and send).

A. Electronic Mail Security

Email is susceptible to both passive and active attacks. The protection of email from illegal access and examination is known as electronic privacy. With the explosively growing reliance on e-mail, there grows a demand for authentication and stealthy services. Two schemes stand out as approaches that enjoy widespread use: Pretty Good Privacy (*PGP*) and Secure/Multipurpose Internet Mail Extension *S/MIME*.

PGP provides an *authentication* through the use of digital signature, *confidentiality* through the use of symmetric block encryption, *compression* using the ZIP algorithm, and *e-mail compatibility* using the radix-64 encoding scheme. PGP incorporates tools for developing a public-key trust model and public-key certificate management.

S/MIME is an Internet standard approach to e-mail security that incorporates the same functionality as PGP. It is a security extent to the MIME Internet e-mail format standard based on technology from RSA Data Security.

B. Transport-Level Security

Transport-Level Security (*TLS*) is an IETF standardization initiative whose goal is to produce an Internet standard version of *SSL*. SSL provides security services between TCP and applications that use TCP. The Internet standard version is called Transport Layer Service (TLS). The TLS Record Format is the same as that of the SSL Record Format. SSL/TLS provides stealthy using symmetric encryption and message integrity using a message authentication code. SSL/TLS includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use. HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server. Secure Shell (SSH) provides secure remote logon and other secure client/server facilities. The SSH Connection Protocol runs on top of the SSH Transport Layer Protocol and suppose that a secure authentication connection is in use. All types of communication using SSH, such as a terminal session, are supported using separate channels.

C. Network Security

Network security consists of the provisions and polices assumed by a network administrator to prevent and monitor illegal access, fraud, moderation, or objection of a computer network and network-accessible resources. Network Security helps to understand that no single solution preserve you from a different types of threats [6].

Network security Elements include:

1) Anti-virus and anti-spyware
2) Firewall, to block illegal access to your network
3) Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks.
4) Virtual Private Networks (VPNs), to provide secure remote access.

D. Network Security Model

A message is to be transferred from one party to another across some sort of Internet service. A third party may be liable for circulating the secret information to the sender and receiver while keeping it from any challenger. Security aspects come into apply when it is necessary or desirable to protect the information transmission from any challenger who may present a threat to stealthy, genuineness, and so on. All the techniques for providing security have two components:

A security-related transformation on the information to be sent. Message should be encrypted by key so that it is unreadable by the challenger [4].

An encryption key used in synthesis with the transformation to scramble the message before transmission and unscramble it on reception.

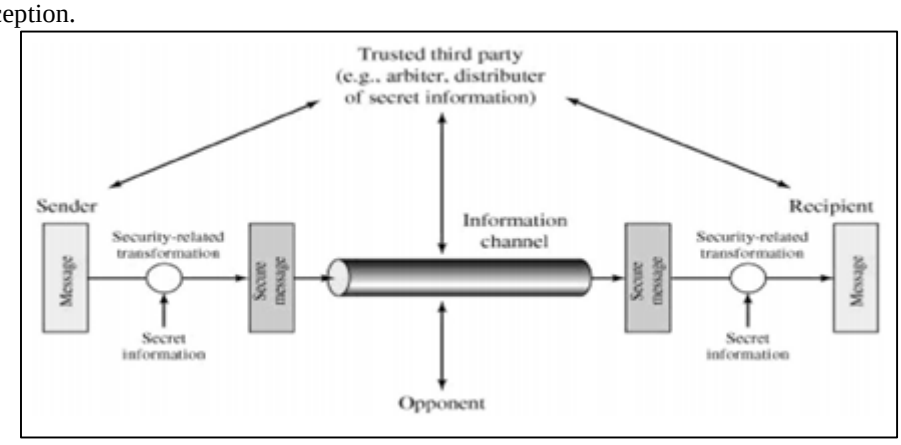


Fig. 1: Model for Network Security

A message is to be transferred from one party to another. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. The general model shows that there are four basic tasks in designing a particular security service:

1) Design an algorithm for performing the security-related transformation. The algorithm should be such that any challenger cannot failure its purpose.

2) Generate the secret information to be used with the algorithm.
3) Develop methods for sharing out and sharing of the secret information.
4) Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

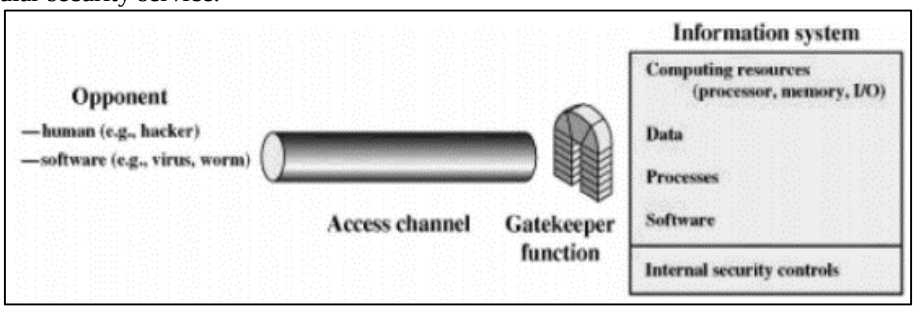


Fig. 1: Network Access Security Model

A general model is illustrated by the above Figure, which reflects a diligence for protecting an information system from illegal access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to lead in systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the interloper can be a disappointed employee who wishes to do damage, or a criminal who seeks to exploit computer assets for financial gain.

VII. CONCLUSION

In the field of computers with the arrival of Internet, the topic secure communication achieved a remarkable emphases. The importance of these topics are both on secure communication that uses encryption and decryption schemes as well as on user authentication for the purpose of non-repudiation. Network security is more important for the personal computer users and organizations, the handling of secret data requires proper security options using cryptography technique.

REFERENCES

[1] William Stallings "Network Security Essentials (Applications and Standards)", Person Education 2004.
[2] Ramesh Yegireddi and R. Kiran Kumar, "A survey on Conventional Encryption Algorithms of Cryptography", 2016, IEEE
[3] Madhuri B. Ghodke, Dr. Suresh N. Mali, "FPGA Based Network Security Using Cryptography", IRJET , Mar-2016, Vol. 03, 469-471
[4] D.Megala and Dr.V.Kathiresan, "Network Security Using Cryptographic Techniques" International Journal of Computerr Application (2250-1797) volume 7 – N0.2, March – April 2017
[5] Daemen,J., and Rijmen,V. "Rijndael: AES-The Advanced Encryption Standard", Springer, Heidelberg, March 2001.
[6] Kamal Shah and TanviKapdi, "Disclosing Malicious Traffic for Network Security", IJAET, Jan 2015, Vol. 7, 1701-1706