International Conference on Innovative Research in Engineering, Management and Sciences
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 9 | ISSN : 2456-3307

Information Security with Cryptography

E. Jansirani[1] , N. Kowsalya[2]
1Lowry Memorial College, Bangalore
2Sri Vijay Vidyalaya College of Arts & Science, Nallmpalli, Dharmapuri

ABSTRACT

Cryptography and Information Security help to protect data and network. Information security is the concept of transferring information over the wireless network in secure way. Nowadays transferring information from one place to another place can be easier but providing security for our information is quite difficult. Information security helps to protect our information form unauthorized users and attackers. Cryptography is a tool which satisfies information security over the computer network. Cryptography achieves information security by using encryption and decryption methods. Encryption is a process of converting original data into unreadable format and decryption is a process of converting unreadable format into readable format. In this paper we discuss about how cryptography provides secure data transmission over the Internet.

Keywords : Cryptography, Attackers, Encryption, Decryption

I. INTRODUCTION

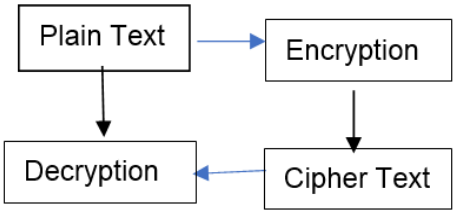
In 1994, the Internet Architecture Board (IAB) issued a report entitled "Security in the Internet Architecture" (RFC 1636). The report stated that the Internet needs more and better security, and it identified key areas for security mechanisms. Among these were the need to secure the network infrastructure from unauthorized monitoring and control of network traffic and the need to secure end- user-to-end-user traffic using authentication and encryption mechanisms. Cryptography is the concept of sending secret messages between users. Cryptography focuses on the following things which helps to provide secure transmission.

Security Attack: The action that affects security of an information

Security Mechanism: The process which helps to secure our information from unauthorized access over the Internet

Security Service: Service which helps to transfer information between sender and receiver

Cryptography focusing on the above thing in wireless network to achieve information security. Cryptography works as follows:



The above diagram illustrates about how cryptograph transfers information in secure way over the wireless network.

• The original information called plaintext that goes to the method called encryption

• Encryption is the process of converting original information into unreadable format. This is done by encryption algorithm there are many algorithms used for this conversion we can choose any of the algorithm to convert original data into unreadable data. Eg: AES, DES, RSA

• The information which is in unreadable form known as cipher text

• Decryption is the process of converting unreadable format to readable format. The algorithm which has been chosen for encryption the same algorithm reverse logic will be used to get original data

The above four necessary steps are called cryptosystem. Cryptosystem needs plain text which has to be transferred to receiver, encryption algorithm which helps to convert original data into unreadable format, cipher text which does not read by others and decryption algorithm which helps to get back original data this will happen on receiver's system.

II. Security Attack

The action which has been taken against our information over the wireless network known as attack, the person who is doing this activity in computer network known as attacker or intruder. There are two types of security attacks

• Passive Attack

• Active Attack

A. Passive Attack

Passive attack technique attacks only on information. The message which is transferred between sender and receiver that gets affected by this technique. Passive attack can be done by two ways.

• Release of message contents: In this type of attack, the attacker will be focusing on sensitive information transferred from sender to receiver. The attacker will take over the message and the receiver will receive only empty messages from sender

• Traffic analysis: In this type of attack, the attacker keeps on focusing the route between sender and receiver and the attacker redirects the original route. So, the information will get delayed. Receiver may not get original information on time, receiver may lose important information.

B. Active Attack

Active attack technique attacks and modifies original data. The message between sender and receiver will be stolen and that get modified by the attacker that modified data will be transmitted to receiver. So, the receiver receives modified data and he will do work on wrong information

• Masquerading: In this technique one person pretends to be a different person. Here attack sends information to the receiver as sent by the sender

• Replay: In this technique attack captures message form sender to receiver, later the attack replays the message to the receiver

• Modification of messages: In this technique the message which is transferred by the sender will be captured immediately by the attacker and the attacker will do some modification on the message, that modified message will transfer to the receiver

• Denial of Service: In this technique attacker will be attacking the server system, whenever sender tries to transmit information to the receiver, he will get network error or server error. So, he will not be able to transmit information to the receiver

III. Security Services

Security services helps to transmit information form one place to another place in secure way. Security services will be done by the security system in cryptography and this system prevents modification on original information. The following are security services:

• Confidentiality: This service helps to protect our information from passive attack. Always it ensures the message is sent to valid receiver. Here only the valid receiver will open the message others cannot open it

• Authentication: This service transmits information between authenticated users which means before

sending and receiving information both the users, identity will be verified. If both are valid transmission will be taken

place or else communication line will get closed

• Integrity: This service does not allow other to do modification on original content. Only authorized persons can do changes in original content

• Non-repudiation: This service helps to prove that the message is really sent by the original sender, either sender or receiver can deny the message no one else

• Access Control: This service helps to gives access permission to the users with the help of this access permission users can send and receive messages over the network. This service prevents the attacker take over the control of computer network

IV. Security Mechanism

Security mechanism implements security for the information. This security mechanism can be implemented in several ways. Users can choose any one of the following security mechanisms to transfer information from one place to another place

• Encipherment: This security mechanism follows the mathematical functions to convert original data

• Digital Signature: Here signed document will be transmitted between sender and receiver

• Access control: only authorized accesses can be performed by the users. For example, if user A allows only to send data over the network, he can only transmit information to all his recipients

• Data Integrity: This mechanism assures the quality of original data. This mechanism does not allow others to do modification

• Authentication Exchange: This mechanism verifies and proves both the sender and receiver before data transmission. It allows communication only between proven sender and receiver

• Traffic padding: This is the special mechanism that fills gaps with extra bits on original information, receiving end all those extra bits will be removed. If anyone tries to misuse the data, they will get wrong information

• Routing Control: This mechanism helps to monitor the route or path between sender and receiver. Due to network traffic this mechanism helps to control the route from sender to receiver

• Notarization: This mechanism helps to send acknowledge for each message transmitted between sender and receiver

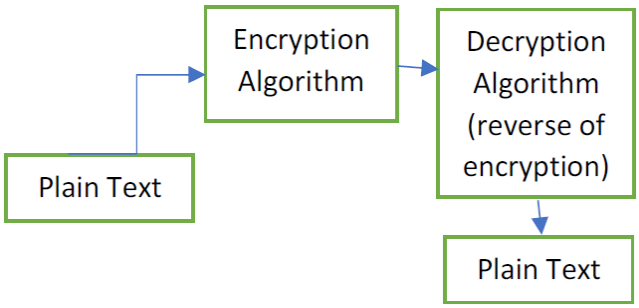
V. Cryptosystem

As we discussed earlier about cryptosystem, it is a system that helps to transmit information from one place to another place in secure way. Cryptosystem follows encryption and decryption methods to achieve security in network. Cryptosystem uses keys to convert original data into unreadable format. There are two keys used in crypto system one is public key and another one is private key. These keys will be used by the sender and receiver to convert and get back the information. This cryptosystem can be used by two ways

• Symmetric Cryptosystem

• Asymmetric Cryptosystem

Symmetric Cryptosystem



The above diagram describes the process of symmetric cryptosystem. This algorithm uses single key to convert information. Initially key will be shared among users.

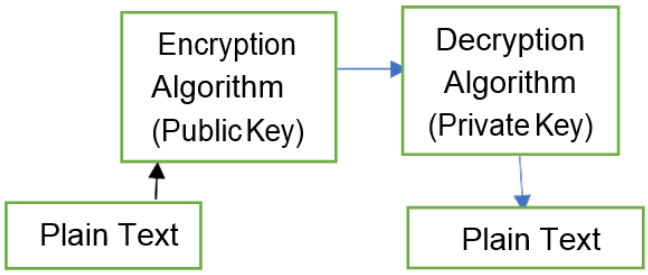
• Plain text is also known as original data which is generated by the sender

• Encryption algorithm helps to convert original data into unreadable format with the help of key value

• Cipher text is known as unreadable data

• Decryption algorithm helps to get back original data by using reverse process of encryption with the help of key

Symmetric cryptosystem is also known as single key cryptosystem. This single key is known as public key. Before data transmission public key will be shared among sender and receiver. Sender uses encryption algorithm along with public key to produce cipher text. Receiver uses decryption algorithm along with public key to get original data



Asymmetric Cryptosystem

Asymmetric cryptosystem is also known as public key cryptosystem it uses two keys. They are public and private keys. Public key used for encryption algorithm and private key used for decryption algorithm. Data encrypted by one public key and the data decrypted only by its corresponding private key. Symmetric cryptosystem uses the same key for both encryption and decryption but here it uses two different keys for encryption and decryption. So, asymmetric cryptosystems provide more security than the symmetric cryptosystem

Cryptography Algorithms

The following are cryptographic algorithms help to provide information security over the network

- ✓ Data Encryption Standard (DES): Developed by IBM for the US government, it supports 64-bits and 128-bits keys for data encryption and decryption
- ✓ Advanced Encryption Standard (AES): Designed by Rijmen-Deamen, it supports 128-bits,192-bits and 256- bits keys for data transmission
- ✓ Secure Hash Function (SHA): This algorithm helps to compress long messages into short form to save space over the network
- ✓ Rivest, Shamir and Adelman (RSA): This is asymmetric key cryptographic algorithm, it uses public and private keys for data encryption and decryption

Conclusion

Information security is the most important aspect in computer network during data transmission. In this paper we discussed about how information security is achieved using cryptography. Cryptography is a powerful technique over the Internet for secure data transmission. Here we discussed security attacks, services and mechanisms on computer network and how cryptosystem works. Nowadays we all need security for transferring sensitive information. This cryptography helps to transmit information from one place to another place by using various algorithms. We can also choose any one of the algorithms for information security

II. REFERENCES

[1]. Behrouz A. Forouzan, Debdeep Mukhopadhyay: Cryptography and Network Security, 2nd Edition, Special Indian Edition, Tata McGraw-Hill, 2011.

[2]. Michael E. Whitman and Herbert J. Mattord: Principles of Information Security, 2nd Edition, Thomson, Cengage Delmar Learning India Pvt., 2012.

[3]. William Stallings: Network Security Essentials: Applications and Standards, 4th Edition, Pearson Education, 2012.