Networks Security Services, Security Mechanisms To Protect Against The Active And Passive Attacks

Prashant P. Pittalia

Associate Professor
Department of Computer Science
Sardar Patel University, Vallbah Vidhyanagar, India

Abstract: In today's global village sharing of information, transferred of the confidential or secret message is become a day to day activity. Network is affected with the online and offline attacks with attackers. The new attacks and countermeasures are taken to prevent the network. This paper discusses about the various active and passive attacks and how it perform the malicious task in the organization like financial, healthcare, government, insurance, transportation. To protect the network against such attacks special services should be implemented in the computer network. This paper explain the various security services like authentication, confidentiality, integrity, authorization and non-repudiation with the security mechanism like encipherment, digital signature, Authentication exchange, traffic padding, routing control and notarization.

Index Terms **– Authentication, Digital Signature, Denial of Service, Traffic Analysis**

1. INTRODUCTION

Computer and network security, the Information technology manager needs to define the requirement for the security activities. Also IT manager has to decide the appropriate approaches to satisfy those requirements. Daily people are moving towards digitization and download the applications to make their tasks smooth. Also at the same time people have accepted that they need the Internet for 24*7. Now smart phones, laptops, tablet, computer and electronic equipment are now connected to each other through the network. As Information Technology becomes ever more important in nearly every aspect of our lives especially with the emergence of ecommerce applications and social media networks, the amount of data stored and generated are rapidly increase which leads to secure the data and ensuring the safe transmission of information across the global network. Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."[3] The sensitive information is easily shared on the network and it can be accessed by the unauthorized user and do the malicious task by getting such credential data. As a result the security services and security mechanism is more important part of the network to help the organizations to make their sensitive data safe and secure from the attacker.

2. TYPES OF SECURITY ATTACKS

Network security attacks are classified in two categories:

2.1 Passive Attacks: In such attacks the intruders aims to observer or monitoring the information passing through communication between the two parties. Such attacks are used to learn or detect the information from the system but it could not harmful for the system. Here the aim of attacker is to just gain an information passing in communication.

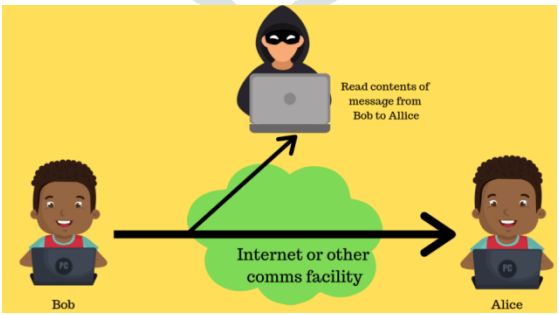

Fig -1: Passive Attack [5]

a) Traffic Analysis: In this attack, Intruder is just read the information passing between sender and receiver and analyzes the data. It may be analyze that which two parties are communicating, what are their IP addresses? which network they are connected?, How frequently they are communicated?, Which type of information are more exchanges?, How much size of the data?, Is the data contain any credential information or not? etc.

b) Release of Message Content: In such passive attacks the intruder aim is to just read what communication is happening between the sender and receiver.

2. 2 Active Attacks: In such attacks the resources are affected as well as the operations performed by the sender or receiver may be changed. It aim is to alteration in the data either it may modify the content, add new content or delete some part of the content. It is strongly harmful for the network.

Fig -2: Active Attack [6]

a) Modification of Message: It means the content of the message is altered by the user or may be delayed the message or discard the message and add new content in a message.

b) Replay Attacks: In replay attack intruder collect the messages transmitted between sender and receiver. After sometime it sends the same message again and again at the receiver side.

c) Masquerade Attack: In masquerade attack intruder will access the resources in unaware of the user when he/she is not communicating with network. In such attacks first the intruder has to identify the credential information about the user on behalf that they want to communicate and also they have to check it out when the legitimate user is not accessing the network.

d) Denial of Service Attack: The aim of DoS (Denial of Service) attack is to slow down or stop the services provided by the server or device to the network users. In such case the intruder will continuously send bulk of packets towards the intended recipient so that recipient is busy to handle bulk of packets at the same time by using its resource and time. Meanwhile the actual users of the system are getting very low response or may be not able to achieve the desired service. [1]

3. Network Security Services

In network when the data is processing or transfer the information it should be protected with the network services to prevent from intruders malicious activities.

Authentication: The legitimate user is allowed to enter into the network system with passing the proper credential information to the server.

Authorization: Users are allowed to access the network resources according to their role. Each user having the predefined role assigned by the server, so he/she could access only content for which they have rights from the server.

Confidentiality: The information cannot be understood by intermediate user except for the actual sender and receiver. The data is converted into encrypted text so only sender and receiver know how to read the messages.

Integrity: The information cannot be altered in storage or transit between sender and intended receiver. If any changes in bit or byte of the message, it alerts the recipient about the alteration and discards the further processing of the packet.

Non-repudiation: When the two parties communicating and transmit the information, after that if any one of them is deny for such transmission than the Non-repudiation service will check the details of the message and identify who is the actual sender and receiver of that message.

4. Security Mechanism

Security mechanism is a process to identify the attacks in the system, protect the system from malicious task and if any problem occurs with the system than recover the data or information into its original form. It is implemented in specific protocol layer to provide some specific services.

4.1 Authentication Exchange: Authentication techniques require that user to prove his/her identity. This can be done by using a password or character sequence known only to you or the program or a physical card that is unique to you or fingerprints, signature, or other item that identifies only you. In Secure Socket Layer (SSL) or Transport Layer Security (TLS) handshake enables the client and server to exchange as well as validating their digital certificates with each other.

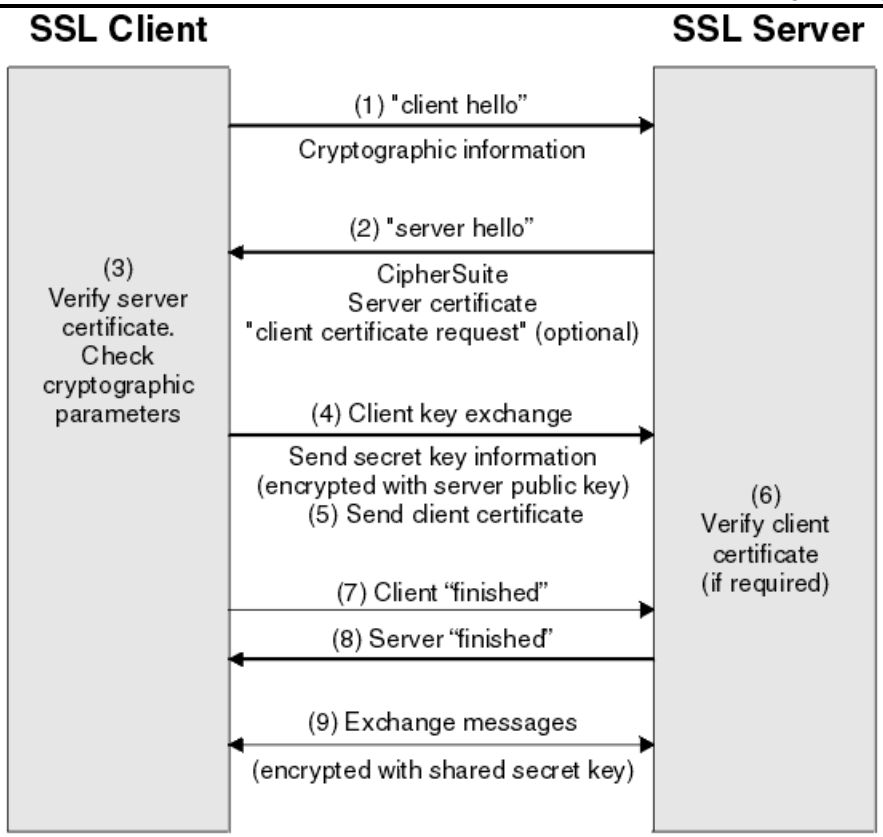

Fig -3: SSL Authentication Exchange [7]

4.2 Digital Signature: A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer [4].

4.3 Encipherment: It is also known as encryption and decryption process. Here the original data or plaintext is converted into cipher text or uninterpreted text with some mathematical function. To recover the original data the knowledge of mathematical algorithm as well as the key used to secret code is required.

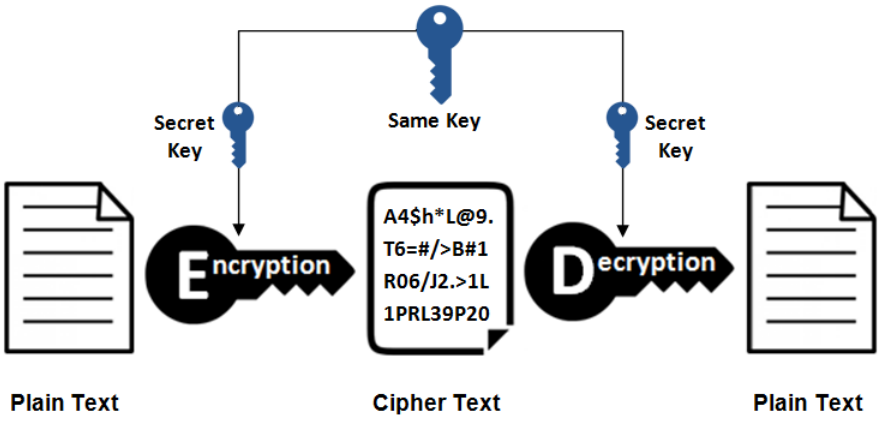

Fig -4: Encryption & Decryption Process [8]

4.4 Traffic Padding: In traffic analysis of passive attacks, intruder may easily analyze the packets. In traffic padding add some extra bits or bytes in the transmitted data and make all the packets of the same size, so it is very difficult for the attacker to analyze the packet.

4.5 Notarization: It means to use the trusted third party during communication to assurance of data exchanges between two parties. Websites that wants to secure the credential information having a digital certificate with them. This digital certificate is issued by the certificate authorities like VeriSign, thawte etc. If any discrepancy occurs between the two parties the third party or certificate authority is responsible to identify the authenticity of the message and its integrity.

4.6 Routing Control: When organization or companies are suffering from some security breaches in the network the companies want to secure communication than they have to decide the new physical path from source to destination and fixed up which trustworthy routers are visited for the communication.

4 CONCLUSION

Network security is an essential part of any organization in today's environment. Most of the companies manage a special budget for the security of the information stored in the server and transfer between devices. Active and passive attacks are used by intruders at the same time the security services and security mechanisms are used to protect the network. Authentication exchange are mostly used by the organizations for secure communication. Most powerful mechanism encipherment is used for authentication using asymmetric key algorithms and confidentiality service is provided by symmetric key algorithms in an organization.

REFERENCES

[1] TCP/IP Illustrated, Volume 1, By Kevin R. Fall, W. Richard Stevens, Second Edition,
[2] Engineering Trustworthy Systems: Get Cyber security Design Right the First Time, O. Sami Saydjari, McGraw Hill Professional, 2018, P-177
[3] https://searchsecurity.techtarget.com/definition/cryptography
[4] https://searchsecurity.techtarget.com/definition/digital-signature
[5] https://www.thecoderzone.com/security-attacks-in-network-security/
[6] https://techdifferences.com/difference-between-active-and-passive-attacks.html
[7] https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm
[8] https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences