Proficiency Based Scrutinizing Diverse attacks and Protocol assets to mould Information Security

S. GOBINATH[1] C. SUBASHINI [2] K. ARTHI[3]

[1,2,3]*Final year M.Tech, (CSE), Christ college of Engineering and Technology, Pondicherry University, Pondicherry, India.*

Abstract

Network security is a wider term used to represent security measures applied to the network, which acts as a broadcasting Environment. Computer network is the collection of computers which includes protocol and hardware to connect them in order to share information and data's across wireless or wired technology. Cryptography, Authentication and access control Mechanisms play a vital role in secure communication over the network. In order to transfer data in a safety manner there are several security measures available. Network security can also be referred to as network safety. Network security is used to prevent the attacks by using protocols during the communication of data. This paper describes the several types of attacks, threats and protocols which attempts the secure communication between client and server.

1. Introduction

Network security provides the security by access control to allow only the authorized users. Network security is mainly used to prevent the attack over the network. Network security is involved in the everyday jobs conducting transactions, private sectors, government agencies and individuals. Network administrator is used to prevent and monitoring the unauthorized access, misuse and modification. Network security included many cryptographic techniques which are helps to prevent the attack for improving the enhancement of the Network Security. This paper is divided into six sections. Section 2 reviews the general information about the attacks. Section 3 describes different types of attacks. Section 4 presents how to maintain Information Security. Section 5 outlines various protocols to provide security to the network. The paper concludes in Section 6.

2. What is Attack?

An attack is a technique used to exploit vulnerability. There are two categories of attacks namely Passive and active attack. Passive attacks are very difficult to detect the original message but there is no possibility to modify. Example: Passive attacks are packet sniffing or traffic analysis. Active attacks are easier to detect the original message and also possibility to modify the message. Example: Active attack is denial of service [3].

2.1 Plaintext and Cipher Text Attacks

There are six related attacks over the network, including three plaintext-based methods and three cipher text-based methods:

- **A known plaintext attack:** It is an attack where a cryptanalyst has access to a plaintext and the corresponding cipher text and find the correlation between these texts.
- **Cipher text-only attack:** It is an attack where a cryptanalyst has access to a cipher text. It does not have access to corresponding plaintext. With simple ciphers, such as the Caesar Cipher, this can be used to break the cipher by frequency analysis.
- **Chosen plaintext attack:** It is an attack where a cryptanalyst can encrypt a plaintext of his choosing and examine the resulting cipher text. Cryptanalyst has access to a public key.
- **Chosen cipher text attack:** It is an attack where a cryptanalyst chooses a cipher text. It deals to find a matching plaintext. This is also often performed on attacks against public key encryption. It initiates with a cipher text and find for matching plaintext data.
- **Adaptive Chosen Plaintext and Adaptive Chosen Cipher text Attacks:** Both adaptive attacks are cryptanalyst chooses further plaintexts or cipher texts based on the results.

3. Types of Attacks in Network

3.1 Denial of service

Denial of Service (DOS) attack is a type of attack over the network to disturbing the authorized use of networks, systems or applications by sending the messages which exhaust service provider's resources such as network bandwidth, system resources, and application resources.

3.2 Spoofing (Identity Spoofing or IP Address Spoofing)

Usually computers connected to internet by sending IP Datagram s into the network. These data packets that are passed through internet carry the senders IP Address with application layer data. An attacker can gain control by using the software that runs on network device, they can easily change device protocols to replace with an arbitrary IP Address into the source address field of the data packet and this is called as IP Spoofing.

The problem of spoofing can effectively handled by a process called Ingress Filtering and this is done by routers. In ingress filtering process, the routers checks the IP address of incoming data grams and ensure that the source address that are reachable through that inter face. If it's not in the legal range, then such packets will be deleted.

3.3 Sniffing

The interception of data packets travelling over a network is called as packet sniffing. A sniffer program combines with network interface cards in order to confine all traffic that is travelling to and from internet host site. Through this mechanism, a sniffer that is installed in any of backbone device will now able to monitor the whole network. There are numerous sniffer programs are available on the internet at free of cost in order to make active intrusion in the network.

Sniffing can be identified by two ways they are:

Host based: This runs on individual host computers to check if the NIC is running in active mode.

Network-based: It checks for currently running process and log files.

3.4 Mapping (Eavesdropping)

Mapping is the process of gathering information such as IP address of computer, the operating system its running, and what are all the services available. By collecting this vital information an attacker can easily attack in focused manner.

If an attacker eavesdropping (i.e. mapping the information) the network communications, then it s referred as sniffing or snooping. The process of mapping a network is a security problem which seriously considered by an enterprise.

The only solution to handle mapping is to providing strong encryption methods based on cryptography which avoid the valuable user data that are read by others when it flows through the network.

3.5 Hijacking (Man-in-the-middle attack)

Hijacking is a process in which an attacker between the user and the person with whom the user are communicating can be monitored, captured and controlled transparently. For example, an attacker may redirect the data exchange. This is usually happens when computers that are communicating at network layer, is unable to decide with whom they are exchanging data.

Man-in-middle attack works by recognizing the identity of the user in order to read the user message. In this manner, the person in the opposite end may believe it is user, because the attacker might be actively replying as the user, and maintain the exchange continues in order to gain more information.

3.6 Trojans

Trojans appears to be normal software with the collection of programs, but they perform accidental or malicious actions when they are posted on the network. Spyware programs that are activated through remote control belong to this type. The Trojan file which consists of Trojan techniques appears to be a standard file and standard size as a compromised system file. This type of attacks can be faced with the help of cryptographic checksum or binary digital signature procedure.

3.7 Social Engineering

Social engineering attack is usually carried by telephone or e-mail message. Social engineering performs cheating to gain access to information systems. The main purpose of social engineering is to make human element to involve in the network. Examples of social engineering include faked email, helpful help desk and fictitious competition.

4. Maintaining the Information Security

To enhance the Information security, we should maintain the authentication, integrity, availability and confidentiality.

Information security = Confidentiality + Integrity+ Authentication + Availability.

The Primary Key to securing the information over the network is cryptography. Cryptographic terms are mentioned below:

Confidentiality: The ability to encode or encrypt a message or data to be transmitted over the network.

Authentication: The ability to verify the identity of entity or individuals on the network.
Access control: The ability to be in charge that is control of the level of access either authorized or unauthorized user.
Integrity: The ability to ensure that a message has not been modified .It should maintain the originality of the messages.
There are two types of encryption techniques are available to maintain security such as,
1) Symmetric key Encryption: In the Symmetric key Encryption, encrypting the original message by using the secret or private key. Symmetric key Encryption includes DES, SKIPJACK, RC4 and IDEA.
2) Asymmetric Key Encryption: In the Symmetric key Encryption, encrypting the original message by using the public key. Asymmetric key cryptosystem consist of three public key algorithms such as Diffie-Hellman, Digital Signature Algorithm (DSA) and RSA. These three Algorithms are providing enhance the security by using exchanging the key, digital certificates and integer factorization respectively.

4.1 E-mail Security

E-mail is always vulnerable to disclosure in one or another way. Because E-mail server that are traversed many networks to reach its corresponding destination. During transmission, e-mail messages may pass through many mail servers over the network. It is vulnerable to, replication, interception, disclosure or modification anywhere along its prescribed path. The fundamental requirements of secure e-mail are described as follows:
1) Message integrity: Secure e-mail ensures that the message has not been altered during transmission and provides a method to verify the message's integrity by using message digest or hashing algorithm.
2) Verification of sender: Secure e-mail provides the cryptographic technique to ensure the identity of the sender with a high degree of confidence. This method or technique is achieved by digital signature technology.
3) Verification of recipient: The verification can be achieved by employing the public key encryption techniques.

The computing standards and products for secure e-mail transmission are Secure Multipurpose Internet Mail Extension(S/MIME), Pretty Good Privacy (PGP), Privacy Enhanced Mail (PEM), Message Security Protocol (MSP) and MIME Object Security Services(MOSS).

4.2 Operating System Security

Operating Systems provide the fundamental mechanisms for securing computer processing. It is ensuring the security that has become an issue for all operating system. If a system design does not target for achieving the secure operating system requirements then its security features are fails to protect the system. Therefore system design helps to protect the operating system.

5. Protocols for Network Security

5.1 Kerberos key exchange

Kerberos key exchange is a network authentication protocol. It was developed at MIT. This protocol is designed to provide the strong authentication for client/server applications by using a combination of both secret key and public key cryptography [1]. If the Single central server utilizes the Kerberos protocol then it is referred to as a trusted server and to act as a trusted third party to authenticate users and control access to resources on the network.
Limitations of Kerberos can be given below,

If the Kerberos server is down, one cannot access network resources, since access to all network resources must be authorized through the Kerberos server. Kerberos design is particularly vulnerable to denial of service attacks.

5.2 Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, in general a personal computer connected by phone line to a server. It is a full-duplex protocol which can be used on different physical media, including twisted pair or fibre optic lines or satellite transmission. It uses a variant of High Speed Data Link Control (HDLC) for packet encapsulation [2].
PPP can be fragmented into three parts:
1. Encapsulation
2. Link Control Protocol (LCP)
3. Network Control Protocol (NCP)

Functions of point-to-point protocol as follows,
PPP (Point-to-Point Protocol) is broadly used in the analogue modem access to the Internet Service Provider (ISP), where one end is PC and the other end is the ISP router. The functions performed are:

It has designed to transport multi-protocol packets between two peers connected by simple links. These links provide full-duplex concurrent bi-directional process.
Components of PPP:
PPP supports either asynchronous link with 8 bit of data, or with bit-oriented synchronous link. It is a

method for encapsulating multi-protocol datagram's. Link Control Protocol (LCP) is for establishing, organizing, and testing the data link connection. This allows the two ends to agree different link layer options.

The Network Control Protocols (NCP) for establishing and configuring different network-layer protocols. This permits the two ends to negotiate various network layer options.

Operation of PPP:

To start communications over a point-to-point link and to configure and test the data link the PPP first sends LCP frames. Then the link has been recognized and facilities have been conferred as desired by the LCP. To choose and configure one or more network layer protocols the PPP sends NCP frames. From each network layer protocol packet can sent to the link. The link will remain organized for communication until LCP or NCP frames close the link [7].

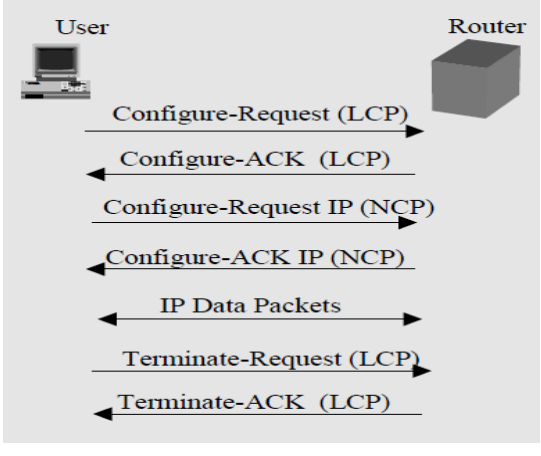

Fig.1: Sequence of the PPP operation (Ref: [7])

5.3 Remote authentication dial-in user service (RADIUS)

RADIUS stands for Remote Authentication Dial in User Service, is a protocol, which is used for remote user authentication and accounting. It is one of the categories for Internet dial-in security protocols that include Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP).

To provide authentication and accounting for remote users it uses Internet Service Providers (ISPs). It also used in private networks to centralize authentication and accounting services on the network.

RADIUS has designed to authenticate and log dial-up remote users to a network.

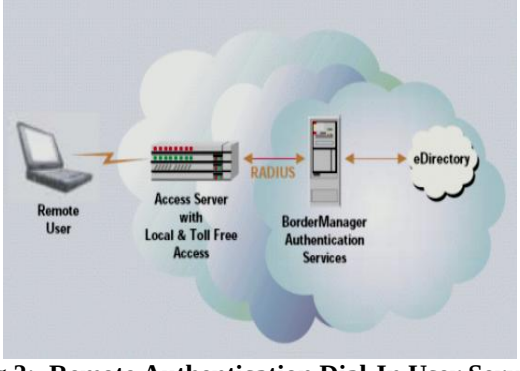

Fig.2: Remote Authentication Dial-In User Service (RADIUS) (Ref: [6])

5.4 Terminal access controller access control system (TACACS+)

TACACS+ stands for terminal access Controller Access-Control System Plus, is an authentication protocol that can be used to validate users who are trying to gain access to information servers, networks, and remote access servers.

There are three versions of the protocol: the original TACACS as just stated, XTACACS (Extended TACACS), and TACACS+.

It runs as an individual third-party authentication server that gives verification services. To gain access to secure system first it prompts the user for a name and password. Then the system passes the information to the TACACS server and requests authentication services.

The main protocols typically used to give Authentication, Authorization, and Accounting (AAA) services on network devices.

Table 1: Difference between RADIUS and TACACS+ (Ref:[9])

RADIUS	TACACS+
It combines authentication and authorization.	Separate the 3 elements of AAA, and it more flexible
Encrypts only the password.	It Encrypts both username and password.
Requires each network	Central management for

device to contain authorization configuration.	authorization configuration.
No command logging.	Complete command logging.
Minimal vendor support for authorization	Supported by most main vendors.
Designed for subscriber AAA	Designed for administrator AAA

5.5 Internet Protocol Security (IPSEC)

The IPSec is an encryption protocols and it is developed by the Internet Engineering Task Force (IETF) and designed to address of security for Internet Protocol based networks. The latest version is IP Version 6(IPv6).This protocol perform the several services at the network layer.

IPSec provides the following services at the network layer:

Access Control: It allows authorized user to access in order to prevent an unauthorized access to the resource.

Connectionless Integrity: It is used to maintain the originality of the messages as well as to give an assurance that the traffic received has not been modified.

Confidentiality: It ensures that the Internet traffic is examined by the authorized parties. In Datagram data field segment that is TCP, UDP, ICMP or any other datagram data field segment are encrypted.

IPSec protocol consists of two protocols.

1. Authentication Header (AH) protocol: This protocol provides the data integrity and authentication of IP Packets.

2. Encapsulation Security Payload (ESP) protocol: This protocol provides data integrity, authentication and message content confidentiality.

5.6 Virtual Private Networks

VPN stands for "Virtual Private Networking "or "Virtual Private Network". A VPN is a private network that it carries the information and also proving protection by using various security mechanisms between known authorized users [8]. In VPNs, various networking technologies are applied for providing private communications within the public telecommunication infrastructure such as the Internet.

Virtual Private Network is broadly classified into four categories such as trusted VPN, Secure VPN, Hybrid VPN, Provider-provisioned VPN and two types such as,

Site to site VPNs: It supports connections between two protected company networks by using ISDN, Frame Relay or ATM.

Remote Access VPNs: It provides the remote access which lets single users connect to the protected company network. It provides remote access to mobile or any other resources by using internet.

5.7 Pretty Good Privacy

PGP stands for Pretty Good Privacy. PGP deals with encryption and decryption, it also provides an authentication for data transmission over the network. PGP is a public key cryptosystem. Secure e-mail communication is achieved by combining cryptographic algorithms. It generates the public /private pairs for secured communication [8].

Pretty Good Privacy includes several services such as authentication, compression, confidentiality, and segmentation and E-mail compatibility.

5.8 S/MIME

S/ MIME stands for Secure/ Multipurpose Internet Mail Extension. This protocol is combines together the encryption and digital signature techniques. MIME deals with transfer of multimedia data (video, audio, pictures). By using Diffie-Hallman, RSA and Triple DES public key algorithms and session keys for transmission along with the message has been encrypted.

Some of the basic services provided by S/MIME includes Privacy, data security, Authentication and Message Integrity.

5.9 S-HTTP

S-HTTP stands for Secure-Hyper Text Transfer Protocol. S-HTTP is a secure message – oriented communications protocol [8]. It supports certain mechanisms to provide an authentication, confidentiality, and message integrity. It provides the secure communication between the client and the server in order to enable secure commercial transactions for a wide range of applications.

S-HTTP messages consist of two parts. They are headers and body. S-HTTP uses headers for authentication, message encryption and digital certificates in the form of HTTP format. It contains instructions on how to decrypt the message body.

5.10 HTTPS

HTTPS stands for Hyper Text Transfer Protocol over Secure socket layer. It is a Web protocol. HTTPS encrypt and decrypt the user's pages in order to prevent unauthorized access. It ensures privacy and providing secure processing for several users. It provides security in online credit card processing and banking websites.

6. Conclusion

This paper describes the information about different attacks and protocols to prevent the attacks. Security is maintained by the different cryptographic techniques applied over the data that pass through the network. Network Security plays a vital role in the field of information systems. It protects the system connected to network by externally and internally. Furthermore, it provides effective standards and security protocols for analysis, monitoring and testing.

References

[1] B. C. Neuman and T. Tso, "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications*, Vol. 32, No. 9, pp. 33 – 38, Sept. 1994.
[2] S. Garfinkel, PGP: Pretty Good Privacy, *O'Reilly*, Dec. 1994, ISBN: 1565920988.
[3] D. E. Comer, *Computer Networks and Internets*, 5th Edition, Prentice Hall, Apr. 2008, ISBN: 0136061273.
[4] B. Ramsdell, *S/MIME Version 3 Message Specification*, IETF RFC 2633, Jun. 1999.
[5] Gray,T.,et al(Mar.2002).Network Security credo.[Electronic version].Retrieved Nov.25,2005,from http://staff.washington.edu/gray/papers/credo.html.
[6]http://support.novell.com/techcenter/articles/nc2001_12d.html
[7]http://www-ee.uta.edu/online/wang/ppp.pdf
[8]www.utc.edu/~jkizza/Books/Springer3/Notes3/Chapter16.ppt
[9]http://www.tacas.net