ISSN 2319 - 5975

Volume 4, No.5, August - September 2015

International Journal of Networks and Systems

Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns01452015.pdf

A Survey on Existing Network Security Protocols

Harshitha. B[1], Veerabhadra Swamy N.S[2]

[1]*M.S.Ramaiah Institute of Technology, M.S.R.I.T post, Bengaluru-560054., Affiliated to VTU, Belgaum, Karnataka, India, harshi.b112@gmail.com*

[2]*National Institute of Engineering, Mananthavady Road, Mysuru-570008, Affiliated to VTU, Belgaum, Karnataka, India, veeru4u@gmail.com*

ABSTRACT

Network plays a vital role in communication technology. A network is a connection of nodes or entities that provides a communication path. Once the network is established securing network is also a major concern. Many security protocols have been developed and used to protect network from attacks. But yet securing network using protocols and algorithms is not successful. Network security is a challenge in communication technology. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Therefore there is a huge need in securing the network from unauthorized access. This paper lists and provides information on existing security protocols.

Key words: Kerberos, PGP, RADIUS, TLS, VPN

1. INTRODUCTION

Computer and security plays an important role in today's telecommunication network. The rapid growth of internet has created a growing demand for security and privacy in a communication channel. Security is not limited to a particular definition. Security can be defined in many ways as protecting system, keep data confidential, prevent network from hacking, misuse and unauthorized changes to the system. Network security plays a major role in protecting confidential data from attacks and unauthorization. Network security is handled by a network or system administrator who implements security policies, hardware or software needed to protect network and resources in transit. Network security protocols provide rules or procedures that ensure security and integrity of data in a network. Secure communication is necessary because attackers try to eavesdrop on communications, modify messages in transit, and hijack exchanges between systems. Some of the tasks network security protocols are commonly used to protect are file transfers, Web communication, and Virtual Private Networks (VPN). The call for and desire for security and privacy has lead to several security protocols and standards. The primary tool to protect information as it travels across a network is cryptography. Cryptography uses algorithms to encrypt and decrypt data so that it is protected from unauthorized users. Without network security protocols internet functions would not be possible

2. NETWORK SECURITY PROROCOLS

This paper provides information on protocols and standards within the framework of network protocol stack. Network protocol stack is an OSI reference model that defines seven protocol layers that is used in a communication network. Table 1 shows protocol stack along with security protocols.

Table 1: Network Protocol Stack

Application Layer	PGP,SMIME, SET, S-HTTP, HTTPS, Kerberos
Transport Layer	SSL, TLS
Network Layer	IPsec, VPN
DataLink Layer	PPP, RADIUS, TACACS+

2.1 Application Layer Security Protocols

The OSI-ISO model has been divided into upper layers those related with application of data and lower layers those related with transmission of data. Application layer is the top layer of OSI model which acts as the interface between the applications and network. Application layer protocols are as follows:

2.1.1 PGP (Pretty Good Privacy)

PGP is public key cryptosystem that is used to encrypt and decrypt data over the network. PGP is used for signing, encrypting and decrypting e-mails, files, texts etc. PGP consists of pair of users, each user has an encryption key that is known publicly and a private key which is known only to that user. User can encrypt a message sent using a public key and decrypt the message using the private key. PGP uses an encryption algorithm RSA (Rivest-Shamir-Adleman) and Diffie-Hellman algorithm to encrypt the messages. Since PGP can be used to sign messages, it can be used to create digital signatures to authenticate messages. To compute digital signatures, PGP produces a hash code of message, using RSA, MD5 algorithm (message digest). This hash code is then encrypted with the sender’s private key using RSA. When the intended recipient acquires the message, the sender's public key is used to decrypt the signature, and a new signature is also computed for comparison with the sent signature. If the two values match, authentication was successful.

2.1.2 Secure/Multipurpose Internet Mail Extensions (S/MIME)

S/MIME is an e-mail security protocol that was designed to prevent the interception and forgery of email by using encryption and digital signatures. It is a secure method of sending e-mail that uses the RSA encryption system. S/MIME provides a way to send and receive MIME data. MIME is a technical specification of communication protocols that describes the transfer of multimedia data such as pictures, audio and video. S/MIME is an extension of MIME that was developed to add security services that was missing in MIME. S/MIME includes two cryptographic elements digital signatures and message encryption. S/MIME creates digital signature by using a hash code of either 160 bit SHA-1 or MD5 to create message digests. S/MIME supports message encryption that uses three public key algorithms such as Diffie-Hellman, RSA and triple DES.

2.1.3 Secure – HTTP (S-HTTP)

Secure Hypertext Transfer Protocol (S-HTTP) is an application-level protocol that extends the HTTP protocol by adding encryption to Web pages. S-HTTP is designed primarily for commercial transactions between a HTTP client and a server. S-HTTP provides a wide variety of mechanisms to provide for confidentiality, authentication, and integrity. S-HTTP was developed to work in conjunction with HTTP to enable clients and servers to engage in private and secure transactions. It supports a variety of cryptographic algorithms and modes of operation. Messages may be protected by using digital signatures, authentication, and encryption. A number of encryption algorithms and security techniques can be used, including DES and RC2 encryption, or RSA public-key signing. In addition, users can choose to use a particular type of certificate, or no certificate at all. In cases in which public-key certificates are not available, it is possible for a sender and receiver to use a session key that they have exchanged in advance.

2.1.4 Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

HTTPS is a secure communication protocol designed to transfer encrypted information between the computers over the internet. HTTPS is http using a Secure Socket Layer (SSL). SSL is an encryption protocol invoked on web server that uses HTTPS. HTTPS creates a secure channel over insecure network by ensuring protection from attacks such as eavesdroppers and man-in-the-middle attacks. HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.

2.1.5 Secure Electronic Transaction (SET)

SET is communication protocol for securing financial transactions over the internet. SET was developed by VISA and MasterCard in conjunction with IBM, Microsoft, Netscape and others. SET uses cryptographic techniques for providing authentication, message integrity and confidentiality. Authentication is achieved through the use of digital signatures. To ensure integrity hashing algorithm is used to generate message digest (digital signatures). To achieve confidentiality message is encrypted using symmetric key encryption algorithm. With a SET protocol, a transaction has three participants (customer, merchant and bank). All sensitive information sent between three parties must be encrypted. All three parties are required to authenticate themselves with certificates. The merchant never sees the customer's card number in plaintext.

2.1.6 Kerberos

Kerberos is a network authentication protocol that provides authentication for client/server applications by using secret key cryptography. Client/server provides mutual authentication proving to each other their identity across an insecure network communication. Communication between the client and the server can be secure after the client and server have used Kerberos to prove their identity. From this point on, subsequent communication between the two can be encrypted to assure privacy and data integrity. Kerberos client/server authentication requirements are security, reliability, transparency and scalability. To meet these requirements, Kerberos designers proposed a third-party trusted authentication service to arbitrate between the client and server in their mutual authentication. Kerberos uses the concept of ticket as a token that proves the identity of a user. Tickets are digital documents that store session keys. They are used during login sessions and can be used instead of passwords. During authentication client receives two tickets: Ticket granting ticket (TGT) and a service ticket. These tickets include timestamps that indicate an expiration time after which they become invalid. Kerberos is also designed to protect against replay attacks.

2.2 Transport Layer Security Protocols

Transport layer is below application layer and provides end-to-end communication over a network. Secure Socket Layer (SSL) and Transport Layer Security (TLS) are the two transport layer security protocols. These two protocols provide security services over the internet.

2.2.1 Secure Socket Layer (SSL)

SSL is a computer networking security protocol that manages client and server authentication and encrypted communication between clients and servers. It provides an encrypted end-to-end data path between client and a server regardless of platform or operating system. SSL uses a combination of public-key and symmetric-key encryption to secure a connection between two machines, typically a web or mail server and a client machine, communicating over the Internet or an internal network. The SSL protocol includes two protocols: the record protocol and the handshake protocol. Using these protocols clients authenticate server and establish an encrypted SSL connection. After mutual authentication client and server exchange key information using public key cryptography.

2.2.2 Transport Layer Security Protocol (TLS)

TLS resides on the application layer of the OSI model. TLS is the result of the 1996 Internet Engineering Task Force (IETF) attempt at standardization of a secure method to communicate over the Web. The 1999 outcome of that attempt was released as RFC 2246 spelling out a new protocol- the Transport Layer Security or TLS. TLS was charged with providing security and data integrity at the transport layer between two applications. TLS version 1.0 was an evolved SSL 3.0. Frequently, the new standard is referred to as SSL/TLS. The goal of the protocol is to provide security, interoperability, extensibility and data integrity between two applications over a network. Symmetric cryptography is used for data encryption. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol is used for encapsulation of various higher-level protocols. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.

2.3 Network Layer Security Protocols

Network layer is the third layer in the OSI model that provides data routing path for network communication. Network protocols include IPsec (Internet Protocol Security) and VPN (Virtual Private Network). These protocols also address internet communication security.

2.3.1 Internet Protocol Security (IPsec)

IPSec is a suite of authentication and encryption protocols developed by the Internet Engineering Task Force (IETF) and designed to address the inherent lack of security for IP-based networks. The basic idea of IPsec is to provide security functions such as authentication and encryption, at the IP (Internet Protocol) level. IPSec protocols provide data and identity protection for each IP packet by adding their own security protocol header to each packet. IPsec provides two choices of security service: Authentication Header (AH), which essentially allows integrity, authentication of the sender of data, and Encapsulation Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (*payload*) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

2.3.2 Virtual Private Networks (VPN)

A VPN is a private data network that makes use of the public telecommunication infrastructure, such as the Internet, by adding security procedures over the unsecure communication channels. The security procedures that involve encryption are achieved through the use of a tunneling protocol. Tunneling enables the encapsulation of a packet from one type of protocol within the datagram of a different protocol. There are two types of VPNs: remote access which lets single users connect to the protected company network and site-to-site which supports connections between two protected company networks. The two components of a VPN are: Two terminators which are either software or hardware. These perform encryption, decryption and authentication services. They also encapsulate the information. A tunnel – connecting the end-points. The tunnel is a secure communication link between the end-points and networks such as the Internet. The security of VPN technologies falls into three types: trusted VPNs, secure VPNs, and hybrid VPNs.

2.4 Data Link Layer Security Protocols

The data link layer is the second layer in the OSI (open systems interconnection) reference model. The data link layer is responsible for logical link control, media access control, hardware addressing, error detection and handling and defining physical layer standards. It provides reliable data transfer by transmitting packets with the necessary synchronization, error control and flow control. In the Data Link Layer, there are several protocols including: PPP, RADIUS and TACAS+.

2.4.1 Point-to-Point Protocol (PPP)

This is an old protocol because early Internet users used to dial into the Internet using a modem and PPP. It is a protocol limited to a single data link. Each call went directly to the remote access server (RAS) whose job was to authenticate the calls as they came in. A PPP communication begins with a handshake which involves a negotiation between the client and the RAS to settle the transmission and security issues before the transfer of data could begin. This negotiation is done using the Link Control Protocol (LCP). Since PPP does not require authentication, the negotiation may result in an agreement to authenticate or not to authenticate.

2.4.2 Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a widely used protocol in network environments. It is commonly used for embedded network devices such as routers, modem servers, switches, etc. RADIUS is a server for remote user authentication and accounting. It is one of a class of Internet dial-in security protocols that include Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). It is mainly used by Internet Service Providers (ISPs) to provide authentication and accounting for remote users. RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP (Extensible Authentication Protocol). It can be used also in private networks to centralize authentication and accounting services on the network for all dial-in connections for service. It has two main components: authentication and accounting protocols. RADIUS is currently the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems.

2.4.3 Terminal Access Controller Access Control System (TACACS+)

TACACS is commonly referred to as “tac-plus”, is a commonly used method of authentication protocol. It was used for communicating with an authentication server, common in older UNIX networks. It is a strong protocol for dial-up and it offers: Authentication: arbitrary length and content authentication exchange which allows many authentication mechanisms to be used with it. Authorization, Auditing: a recording of what a user has been doing and in TACASCS+, it serves two purposes: To account for services used To audit for security services.

Table 2 gives the list of different security protocols and techniques used in seven layers of network protocol stack.

Table 2: Summary of Security Protocols

OSI Layers	Network Security Protocols	Techniques Used
Application Layer	PGP	RSA, MD5, Diffie-Hellman
	SMIME	MD5, Diffie-Hellman, RSA and triple DES
	SET	Digital signature, symmetric key encryption
	S-HTTP	DES, RC2, RSA
	HTTPS	SSL
	Kerberos	Secret key algorithm, timestamps
Transport Layer	SSL	Public and symmetric key encryption, handshake protocol
	TLS	Symmetric key cryptography, handsake
Network Layer	IPsec	Authentication header, Encapsulation Security Payload, Tunneling
	VPN	Tunneling Protocol
DataLink Layer	PPP	Handshake and Link Control Protocol
	RADIUS	MD5, IPsec tunnels
	TACACS+	AAA architecture, Kerberos

3. CONCLUSION

Network Security is a key in communication world. Security threats are increasing with each new technology and providing security to confidentiality has become a greatest challenge. Even though we have many authentication protocols and mechanisms there is still chance of vulnerability and attacks. The main intention of the paper is to list all network security protocols under one section, so that it gives brief information on what each protocol is about. Cryptographic techniques plays a major role in assuring security.

REFERENCES

[1]. Victor L, Voydock and Stephen T. Kent. Bolt, J. U. ***Security Mechanism in High Level Network Protocols.*** Bolt, Beranel and Newman, Inc, Cambridge, Massachusetts 02238.

[2]. Charles P. Pfleeger, Shari Lawrence Pfleeger ***Security in Computing,*** *5th edition.*H.

[3]. William Stallings and Lawrie brown ***Computer Security : Principles and Practice*** 3rd edition.

[4]. William Stallings ***Cryptography and Network Security:Principles and Practice***, 6th edition