Advanced Security Protocol for Network Layer

Shrishti Sao[1], Sunil Kumar Sahu[2]

[1]Mtech Scholar, BCET Durg
Shrishtisao7[at]gmail.com

[2]Assistant Professor, PCEM Bhilai
Sunilsahu.parthivi[at]gmail.com

Abstract— ***Internet has instantly developed into a vast global network that is used by thousands of users and controlled by different administrative entities Network security is mainly concerned with protecting sensitive data from unauthorized users and applications. But in the current scenario securing data is often approached from different viewpoint. With the increasing use of Internet for business applications, there is a great demand for Quality of service. Because of these reasons the need for security in the Internet is stronger than ever.***

Keywords-Protocol,IPSec,Encryption,AH,ESP

1. Introduction

1.1 Network

Network is a set of two or more node or communicating devices connected by communication links that are capable to communicate with each other. A node can be a laptop, computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. Basically a network allows many users to share a frequent pathway for communication. The physical media includes copper wire, coaxial or fibre optics cable, telephone lines etc. The wireless communication includes radio wave, microwave or satellites. Computer networks allow people to:
1. Exchange information (databases, documents, and graphics) via connected workstations.
2. Share resource equipment (computers, printers and scanners).
3. Use shared applications (spreadsheets and word processors).
4. Collaborate and communicate electronically

1.2 Advantages of networking

1. Networking provides the capability of **distributed processing** among the multiple independent computers, in which a task is divided among multiple computers.
2. It provides **fast data transmission** among computers and to make data and programs available to the people.
3. It allows **sharing of resources** of the machines with the aim of making data available to everyone without regard to the location of the resource and user.

1.3 Criteria of network

A network has criteria like reliability, security and performance.

Performance

Performance is mostly measured by throughput and delay. If we try to trnsmit more data to the network, we are increasing the throughput but we increase the delay because of traffic congestion in the network.Performance can be measured in many ways, including transit time and response time. The performance of a network totally depends on the users, the transmission medium and the capabilities of the connected hardware or software.

Reliability

Network reliability is calculated by the occurrence of failure, the time it takes to recover from a failure.

Security

Network security includes defending data from unwanted access, and development, and generating rules and procedures for backup and revival of data failure.

1.4 Categories of networks

Depending upon the geographical area covered by a network, it is classified as:
a. Local Area Network (LAN)
b. Metropolitan Area Network (MAN)
c. Wide Area Network (WAN)

Local Area Network (LAN)

LAN stands for Local Area Network. A LAN is group of computers and networks devices connected together usually within same building, in a single office or campus. A LAN normally covers an area less than 2 miles. It is high speed and inexpensive. LAN uses guided media and are linked together with a certain topology as shown in fig 1.1. These topologies include: bus, ring, and star.

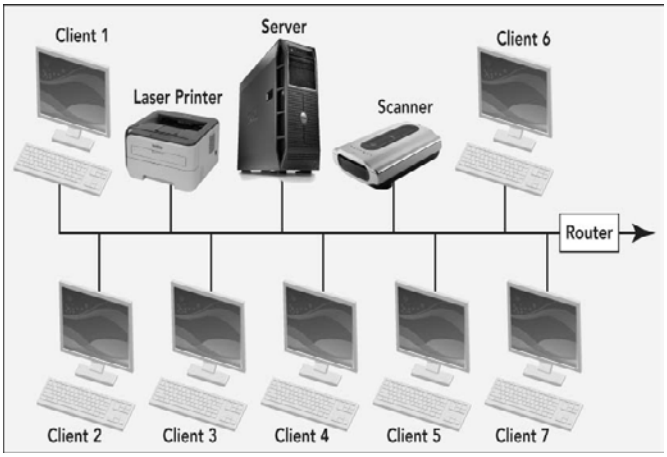

Fig 1.1 LAN

Wide Area Network (WAN)

WAN stands for Wide Area Network which covers a large geographic area such as country, continent or even whole of the world. A WAN is two or more LANs connected together or it can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. Internet is an example of WAN. Another example of WAN is the wireless WAN i.e. Wireless Fidelity (Wi-Fi) that is becoming popular day by day.

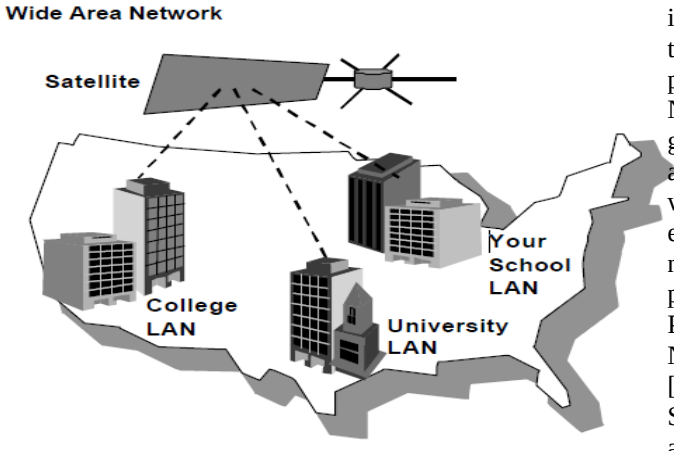

Fig 1.2 WAN

Metropolitan Area Networks (MAN)

MAN stands for Metropolitan Area Network. A MAN is larger network that usually cover several building in the same town. . MAN is a network with a size between a LAN and a WAN. It is slow as compare to LAN and inexpensive and connected with Fiber Optics Cable

2. Literature Review

Paper [1] suggest that the Internet Protocol (IP) is a network-layer protocol that contains addressing information and control information that is used to route the packet through the network. Two versions of IP exists namely IPv4 and IPv6. IPv4 is the current version that is most widely used. It is a connectionless protocol that is mainly concerned with transmitting data from one workstation to another [2]. Each device in the network has an IP address that is used by the IP protocol to ensure that the data packets reach the correct destination. IPv4 uses only 32-bit address, which is a major setback. With the growth of Internet will not only be computers that will need to be addressed but also household appliances such as microwaves, televisions and DVD players may be next. The existing IPv4 protocol would not be suitable for this kind of technology growth and conclude that there is need for security for the existing TCP/IP Model. It also provides new ideas to design efficient security mechanism for the TCP/IP Protocol suite. With minor changes in the existing model, high level of security can be obtained.

A mobile user moves [2] around and switches between wireless cells, subnets and domains, it needs to maintain the session continuity. At the same time security of signaling and transport media should not be compromised. A multi-layer security framework involving user authentication, packet based encryption and access control mechanism can provide the desired level of security [3] to the mobile users. Supporting streaming traffic in a mobile wireless Internet is faced with several challenges due to continuous handoff experienced by a mobile user. This paper describes a simplified version of ML IPsec, an efficient key distribution protocol for initializing secure wireless sessions, and two protocols for managing mobility for these secure sessions. This suite of protocols is called MML-IPsec. MML-IPsec enables performance enhancing algorithm to be introduce into wireless network.

This work [4] focused on describing and exploring the incompatibilities issues between IPSec and IPv4/IPv6 translation gateway and targeted to solve the issues by proposing NAT-PT traversal mechanism called E2E-NATPT. E2E-NATPT is responsible to support and guarantee end toend traversal of IPSec packets between IPv6 and IPv4 nodes. Due to the existence of translation gateway which is transparent to the end nodes, new payloads are exchanged during IKE negotiation to empower the end nodes to support E2E-NATPT capability and to detect the presence of NAT-PT gateway. Moreover, we enhanced the Pluto IKEv1 daemon so that it can be able to react once NAT-PT gateway is detected along the communication path. [5] The proposed E2E-NATPT traversal is integrated into Strong Swan IPSec-based solution and is validated by using a Linux-based testbed

Taking account of defections existed in general methods of implementing IP security (IPsec) in broadband routers, a secure scheme based on fast path and slow path of routers was put forward. The scheme implements IPsec with Encryption chip and IPsec software combined, and adopts Encryption adaptive board to support multi-encryption chips. No requirement for change in original hardware architecture of broadband router makes the scheme universal. Wire-speed data forwarding and encryption are processed in fast path, while local data and protocol data which are non-real time tasks are processed in slow path, in which IPsec security policy (SP) and security association (SA) are also transferred. The scheme was tested in SR1880s, and testing results showed that the proposed scheme can satisfy the security needs of broadband router We present universal security architecture of implementing IPsec with both encryption chip and IPsec software to fully utilize the advantages of fast path and slow path of broadband router. High-speed Encryption chip is utilized to achieve wire-speed encryption and decryption in fast path, while IPsec software is used to process non-real time data passing through slow path.

3.Security Protocol

When two or additional networks are linked, they become an internetwork, joining various government, university and personal computers together and providing an communications for the use of E-mail, bulletin boards, file transfer, hypertext documents, databases, download programs and audio/video conferencing, e-commerce, browsing, explore the web addresses for access through search engine and many more.

A protocol is a set of rules that direct data communications and TCP/IP (Transmission Control Protocol/Internet Protocol) suit used in the Internet. It has 5 layers i.e. Physical layer, Data link layer, Network layer , Transport layer, Application layer.

IP Security (IPSec)

At the network layer TCP/IP supports Internetworking protocol which act as transmission mechanism. It is an unreliable and connectionless protocol that provides best effort delivery service.

IP Security (IPSec) is group of protocols provide security for data packet at the network level as given in fig 3.1. IPSec helps to create authenticated and confidential packets for the IP layer. Both version of IP i.e. IPv4 and IPv6 supported by IPSec and works in two modes-

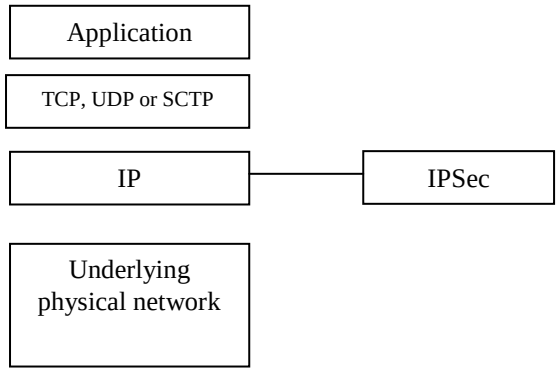

Fig 3.1*TCPIIP protocol suite and IPSec*

Transport Mode

In this mode, IPSec protect the data packets coming from the upper layer to the lower layer. But it only protects the packet from the transport layer (IP layer payload), it does not protect the entire IP packet; this mode is used when we need host-to-host protection of data packets. IPSec helps the receiving host to decrypt and to check the authentication of the IP packet and deliver it to the transport layer.

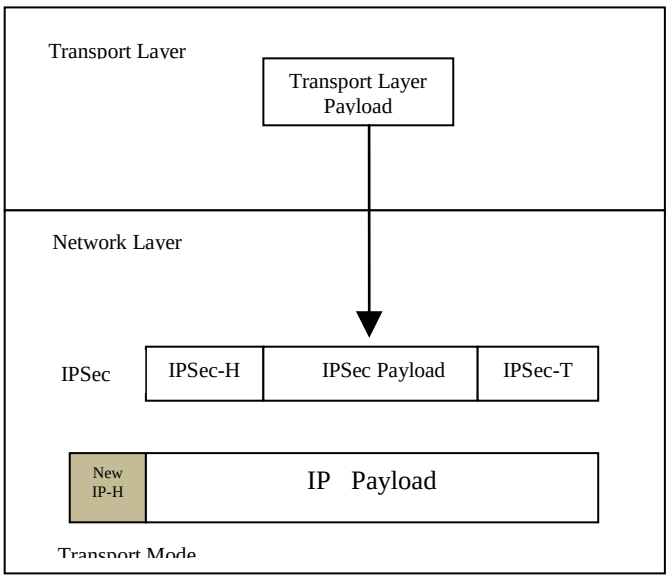

Fig. 3.2Transport Mode

Tunnel Mode

In this mode, IPSec protects the whole IP packet. Tunnel mode uses an IP packet with the IP- header, then applies IPSec security mechanism to the entire packet, and then adds New IP-H (new IP header). This mode is usually used between two routers, between a host and a router, vice versa. The whole packet passed through an imaginary tunnel.

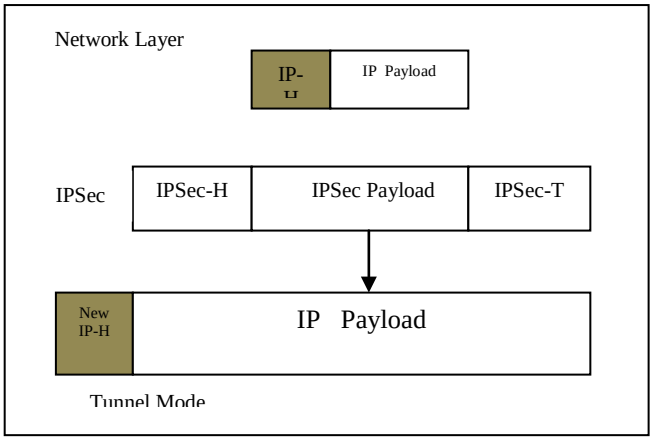

Fig 3.3Tunnel Mode

Security Protocols

Security protocol provides authentication and encryption for data packets at the IP level. IPSec defines two protocols:

(i) AH (Authentication Header) Protocol
(ii) ESP (Encapsulating Security Payload) Protocol

Authentication Header (AH)

The AH Protocol is careful to authenticate the host and make sure the integrity of the payload carried in the IP packet but does not provide confidentiality. It uses a hash function and a symmetric key to create a message digest (MD) which is inserted in the authentication header. The AH is then sited in the suitable location based on the mode (transport or tunnel). The addition of an authentication header follows these steps:

1. An AH is added to the payload with the authentication data field set to zero.
2. Padding may be added to make the total length even for a particular hashing algorithm.
3. Hashing is based on the total packet. However, only those fields of the IP header that do not change during transmission are included in the calculation of the MD.
4. The authentication data are inserted in the authentication header.
5. The IP header is added after the value of the protocol field is changed to 51. AH Protocol includes-

1. Next header- This is 8-bit field defines the type of payload carried by the IP datagram (i.e. TCP, UDP, ICMP, or OSPF).
2. Payload length-This is 8-bit field defines the length of the authentication header.
3. Security parameter index- This is 32-bit field act as VCI (virtual-circuit identifier) and is the same for all packets sent through a connection called as security association

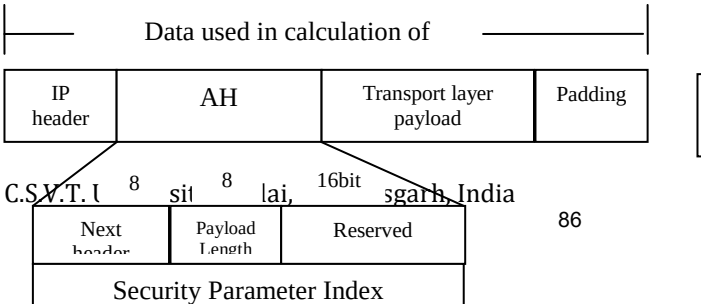

Fig 3.4AH Protocol

4. Sequence number- It is 32-bit field which gives ordering information for a sequence of datagram.
5. Authentication data- This field is the absolute result of applying a hash function to the whole IP datagram except for the fields that are altered during transmission. The part of IP header is included in the calculation of the authentication data.

Encapsulating Security Payload (ESP)

IPSec defined a protocol that gives source authentication, integrity, and confidentiality called as Encapsulating Security Payload (ESP). ESP adds a header and trailer. When an IP datagram carries an ESP-H and ESP-T, the protocol field value is 50. The next-header field inside the ESP trailer holds the original value of the protocol field means the type of payload being carried by the IP datagram, such as TCP or UDP.

The ESP procedure follows these steps:
1. An ESP trailer is added to the payload.
2. The payload and the trailer are encrypted.
3. The ESP header is added.
4. The ESP header, payload, and ESP trailer are used to create the authentication data.
5. The authentication data are added to the end of the ESP trailer.
6. The IP header is added after the protocol value is changed to 50.

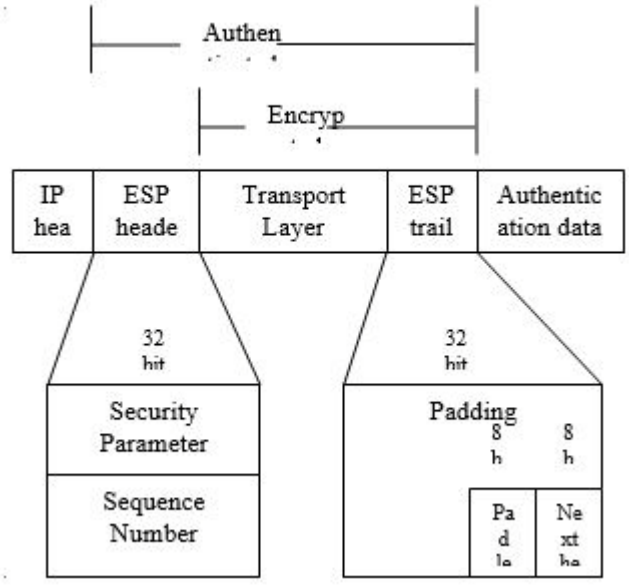

Fig. 3.5ESP Protocol

Here security parameter index and sequence number is 32-bit field is similar to the AH Protocol.
3. Padding- This is variable-length field (0 to 255 bytes) serves as padding.
4. Pad length- It is 8-bit field that defines the number of padding bytes that lies in between 0 to 255.
5. Next header- It is 8-bit field is similar to that defined in the AH Protocol.
6. Authentication data- This field is the result of applying an authentication scheme to parts of the datagram. Here, part of the IP header is not included in the calculation of the authentication data.

References

[1] M.A. Kumar, S. Karhtikeyan "A New Security Architecture for TCP/IP Protocol Suite" International journal of advanced research in Computer Science Vol 1 No.3sep-oct 2010 ISSN No.0976-5697.
[2] T. Gayatri, C. Divya et al "Mobile Multilayer IPsec protocol"International Journal of Engineering and Technology Vol.1(1), 2009, 23-29
[3] Behrouz A. Forouzan, TCP/IP Protocol Suite. New Delhi Tata McGraw Hill Publication, 2003
[4] Bradner, S., "The End-to-End Security," IEEE Security & Privacy, vol.2 no..4, pp, 76-79, 2006.
[5] Caicedo, C.E, Joshi, J.B.D, Tuladhar. S.R," IPv6 Security Challenges", IEEE Journal of Computers, 42(2), 36-42, 2009.
[6] Downnard.I,"Public-key cryptography extensions into Kerberos",IEEE Potentials, 21(5), 30 – 34, 2003.
[7] Dorothy E. R. Denning, Cryptography and Data Security. Massachusetts: Addison-Wesley, 1982.