"श्री"

Lecture:

Security Protocols:

★ Application Layer — PGP, S/MIME

↓

Transport Layer — SSL/TLS

↓

Network Layer — IPSec

PGP: Pretty Good Privacy } For EMail Security

SSL: Secured Socket Layer
TLS: Transport Layer Security } For Transport Layer Security

IPSec: IP Security Protocol } For N/W Layer Security

★ Why do we need Security at Network Layer?

→ Not all client/server programs are protected at the application Layer. For example, PGP, S/MIME protect only email.

→ Not all client-server Programs at the application layer use the services of TCP to be protected by SSL/TLS; some programs use service of UDP.

→ Routing Protocols directly use service of IP

☆ IP Security = Collection of Protocols designed
(IPSec) by IETF to provide security for a packet at the network level

IPSec helps create authenticated and Confidential packets for the IP layer

☆ IPSec is useful in several areas

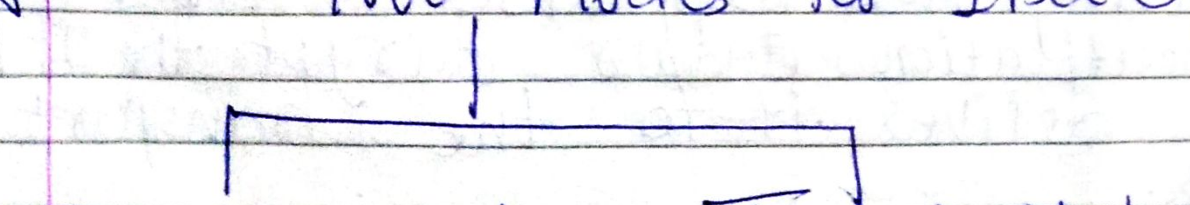
① It enhances the security of those client/server programs, such as e-mail, that uses its own set of protocols.

② It can enhance the security of client/Server programs, such as HTTP, that use the security services provided at the Transport Layer.

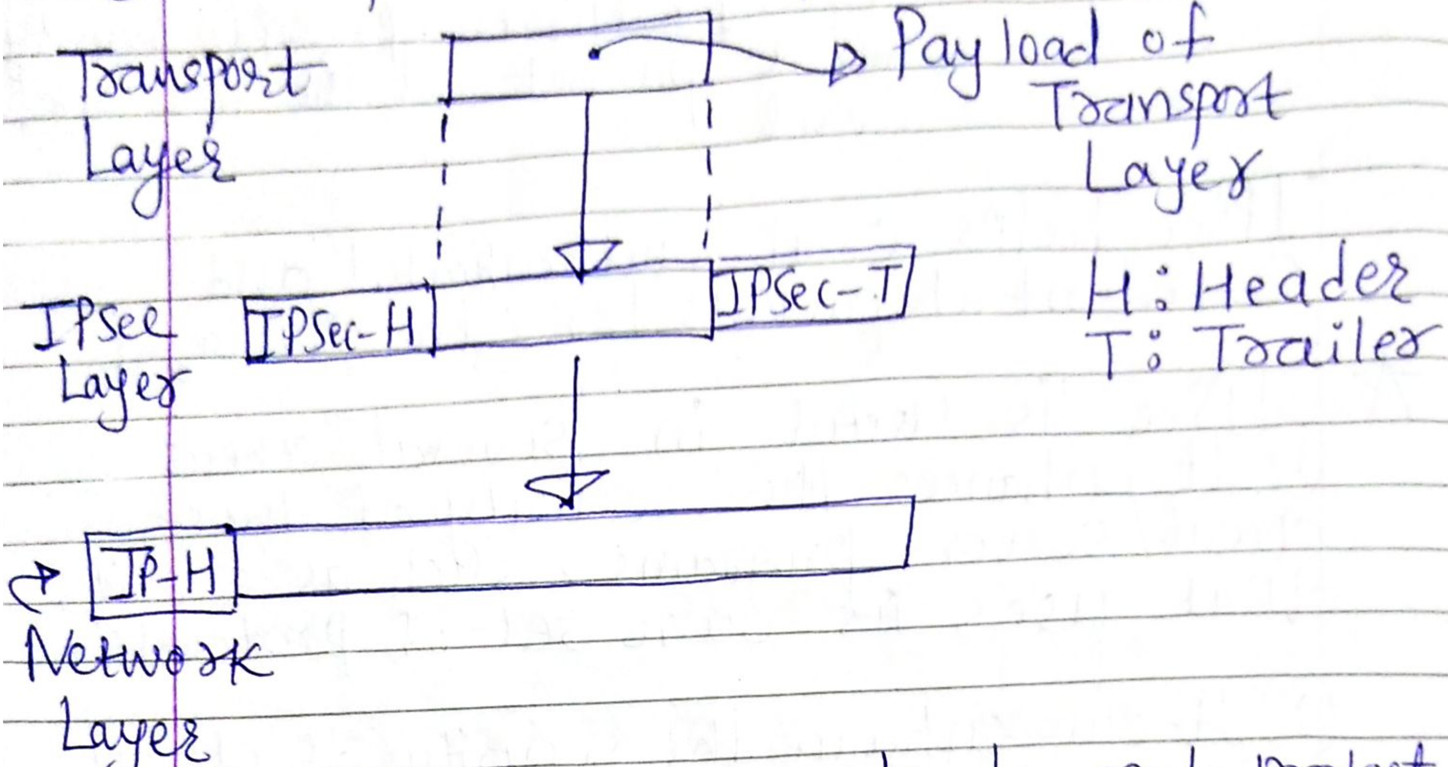
③ It can provide security for those client/server programs that do not use the Security Services provided at the Transport layer.

④ It can provide security for node-to-node Communication programs such as routing protocols.

☆ Two Modes for IPSec Operations



① Transport Mode operation.



→ IPSee in transport mode does not protect the IP header; it only protects the information coming from the transport layer.

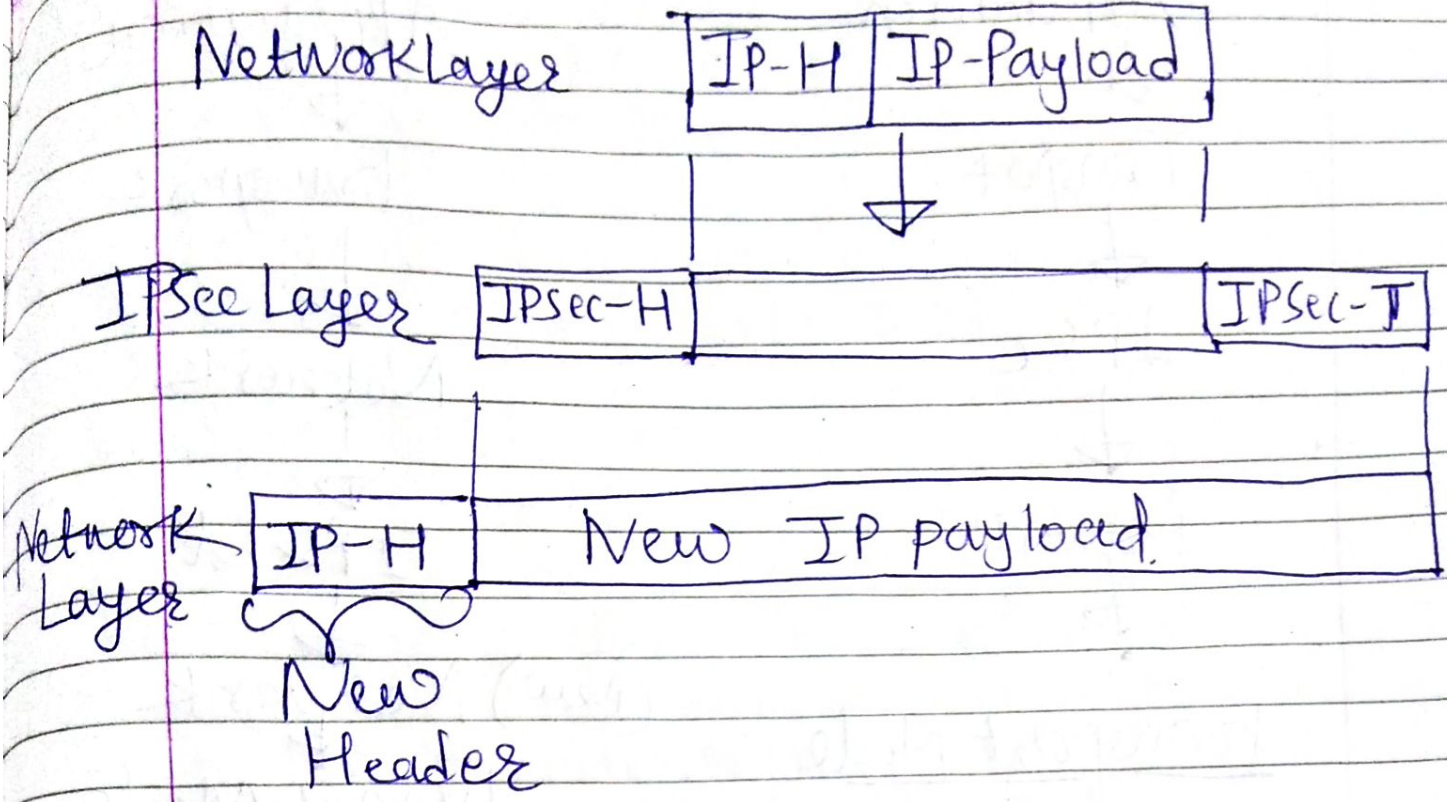
→ Transport Mode is normally used when we need host-to-host (end-to-end) protection of data.

→ Sending host uses IPSec to authenticate and/or encrypt the payload delivered from the Transport Layer.

→ Receiving host uses IPSec to check the authentication and/or decrypt the IP Packet and deliver it to the Transport Layer.

Date
Page

② Tunnel Mode Operation



→ New IP-Header, has different information than the Original IP header.

→ Tunnel Mode is normally used between two routers, between a host and a router, or between router and host.

→ Entire packet is protected from Intrusion between the sender and the receiver, as if the whole packet goes through an imaginary tunnel.

Note: IPSec in Tunnel Mode Protects the Original IP header.

☆ Comparison

Application
↓
Transport
↓
IPSec
↓
Network
↓
.

Transport Mode

Application
↓
Transport
↓
Network
↓
IPSeet
↓
(New) Network
↓
.

Tunnel Mode

☆ Two Security Protocols: → For Encryption, authentication for packets

AH (Authentication Header)

ESP (Encapsulating Security Payload)

☆ AH: Authentication Header:

→ It is designed to authenticate the source host and to ensure the Integrity of the payload carried in the IP packet.

→ Steps:

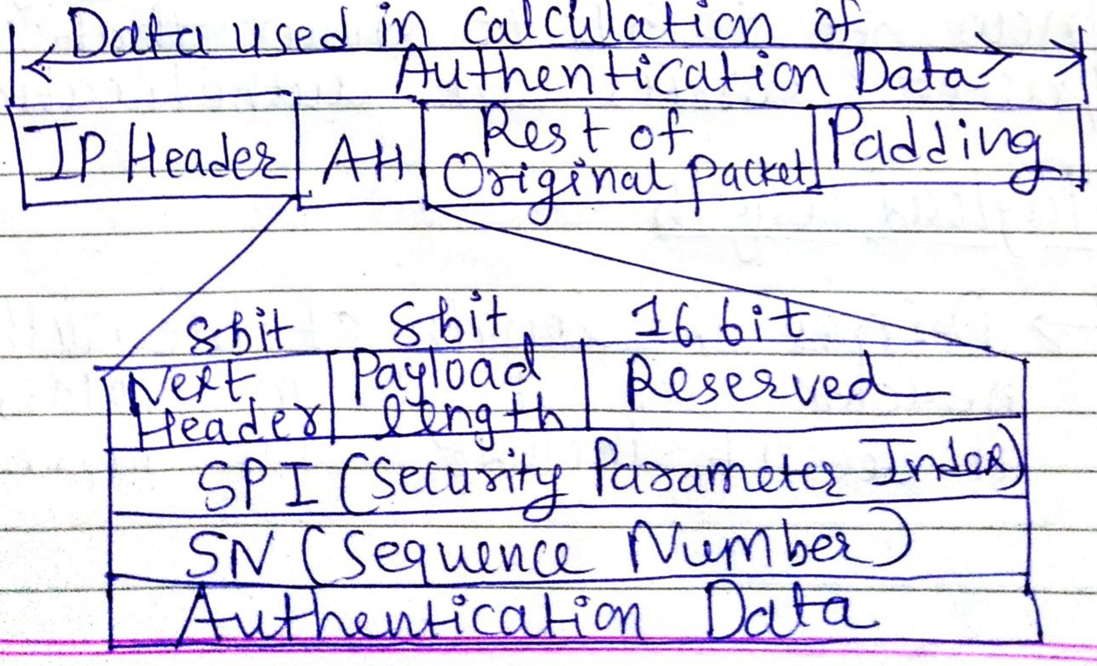
① AH is added to the payload with the authentication data field set to 0.

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 donot change during transmission are included in the calculation of the message digest.

④ Authentication data are inserted in the authentication header.

⑤ The IP-Header is added after changing the value of the protocol field to 51.



8bit	8bit	16 bit
Next Header	Payload length	Reserved
SPI (Security Parameter Index)		
SN (Sequence Number)		
Authentication Data		

Note: When an IP Datagram carries an authentication header, the original value in the protocol field of the IP header is replaced by the value 51.

→ A field inside the authentication header (the next header field) holds the original value of the protocol field.

Fields

① Next Header: The 8 bit next header field defines the type of payload carried by the IP Datagram (such as TCP, UDP, ICMP, OSPF).

→ In other words, the process copies the value of the protocol field in the IP Datagram to this field

→ The value in the new IP Datagram is now set to 51 to show that the packet carries an authetication header.

② Payload Length

↳ Defines the length of the authentication header in 4-byte multiples, but it doesn't include the first 8 bytes.

③ **Security Parameter Index:**

32 bit field plays the role of a Virtual Circuit Identifier and is the same for all packets sent during a connection called a Security Association.

④ **Sequence Number:** 32 bit field provides Ordering information for a sequence of datagrams.

→ It prevents a playback

→ Sequence Number is not repeated even if a packet is retransmitted.

→ A sequence Number doesn't wrap around after it reaches 2^{32}; a new connection must be established.

⑤ **Authentication Data:** It is the result of applying a hash function to the entire IP-Datagram except for the fields that are changed during transit (e.g. Time to Live)

Note: AH provides Source Authentication and data Integrity, but not privacy.