Page No.:
Date:

E-mail Security

- Email is perhaps the most widely used application on Internet.

Using Email, an Internet user can send a message to other Internet users. Therefore, Email ~~user~~ security has become an extremely important issue.

- An email message is considered to made up of two portions:- it's contents and headers.

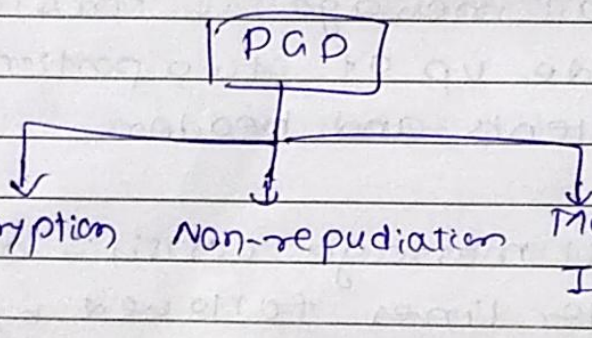
- An email message consists of no. of header lines followed by the actual message content.

- An header line usualy consists of keyword, followed by colon, followed by keywords arguments. Header keywords can be from, To, Subject and Date.

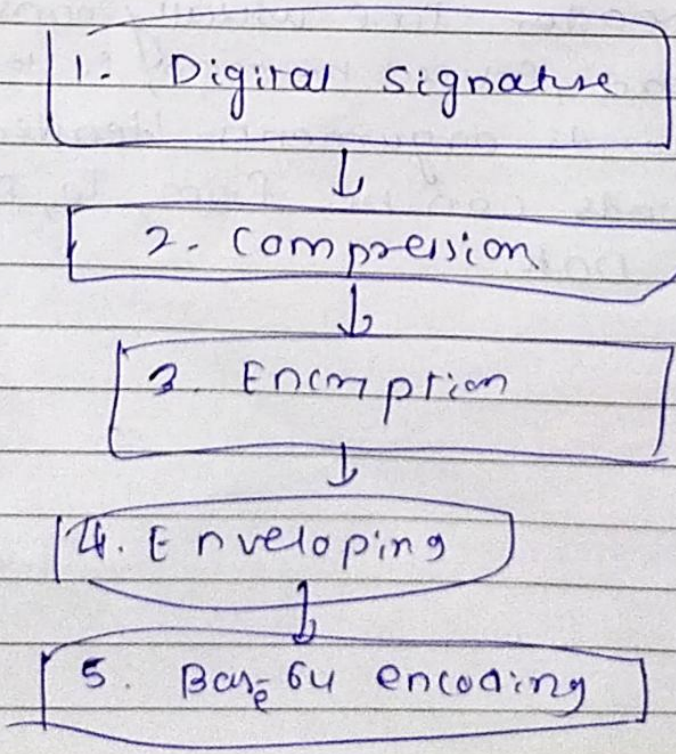
Pretty Good Privacy (PGP) :-

- The aspects of PGP are that it's supports basic requirements of cryptography, is quite simple to use, and is completely free, including it's source code and documentation.

- The email cryptographic offered by PGP :-



- The steps in PGP are :-



- PGP allows ~~for~~ ~~four~~ three following security options:-

1. Signature only.
2. Signature and Base-64 encoding
3. Signature, Encryption, Enveloping and Base-64 encoding.

Step 1:- Digital signature

- In PGP, it consists of creation of message digest of email message using SHA 1 algorithm.
- The resulting message digest is then encrypted with sender's private key. The result is sender's digital signature.

Step 2:- Compression:-

- Additional step in PGP.
- input message and digital signature are compressed together to reduce the size of final message that will be transmitted.
- ZIP program is used.

Step 3:- Encryption

- The compressed output of step-2 are encrypted with symmetric key.
- Generally, IDEA algo. of CFB mode is used.

Step 4:- Digital Enveloping.

- Output of Step 3 is now encrypted with receiver's public key.
- The output of step 3 and step 4 together form digital envelope.

Step 5:- Base-64 encoding,

- The output of Step 4 is now encoded with base-64.

Page No.:
Date:

Secure multipurpose Internet Mail Extensions (S/MIME):-

- The traditional email systems using SMTP protocol are text based, which means we can send only text messages but not multimedia files, etc.

- MIME system extends the basic email system by permitting users to send binary files using basic email system.

- A MIME email message contains a normal Internet text message along with some special headers and formatted sections of text.

- In header, the contenttype MIME header shows that the sender has attached a multimedia file to message.

- Header of MIME contain:-

1. MIME version :- contains version number.

2. Content-Type :- Describes data contained in body of message The content are specified by

Type / subtype

7 ↓ 15 ↓

3. Content - Transfer - Encoding :-

- Specifies the type of Transformation that has been used to represent the body of message.

- Five content - encoding - methods :-
  7 - bit, 8 - bit, Binary, Base-64, Quoted Printable

4. Content ID.

5. Content Description.

- Functionality of S/MIME is quite similar to PGP. It offers functionalities as :-

1. Enveloped data
2. Signed data.
3. clear - signed data
4. Signed and Enveloped data.

- Algorithms used in S/MIME :-

Message Digest	- SHA 1
Digital signature	- DSS, RSA.
Enveloping	- Diffie-Hellman, RSA.
Symmetric key Encryption	- RC4, DES 3.

IP Security :-

- The IP packets contain data in plain text format.

- Anyone watching IP packets can actually change them, read their contents.

- So to secure IP packet we have protocols

Applications of IP sec :-

Secure

1. Remote Internet Access :- Using IPSec, we can connect to organization's network in secure fashion from our home or hotel. we can access corporate network facilities or access remote desktop / servers.

2. Secure Branch Office Connectivity :- Organization can set up IPsec-enabled network to securely connect all its branches over Internet.

3. Setup Communication with other Organizations :- Organization can connect the networks of different org. together in secure fashion

Advantages:

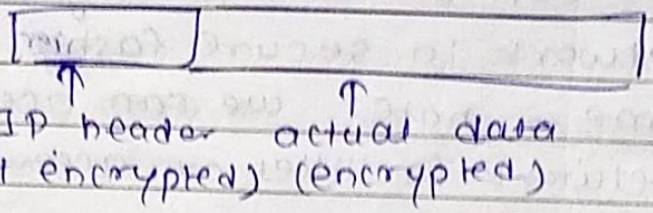
1. IPsec allows interconnectivity between branches/offices in very inexpensive manner.

2. IPsec can allow traveling staff to have secure access to corporate network.

3. IPsec is transparent for end users.

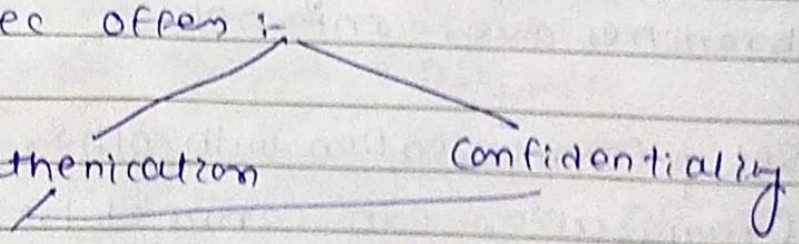
4. IPsec works at network layer. Hence, no changes are needed to upper layers.

- IP packets has: IP header and actual data



- IPsec features are implemented in extension headers which follows standard IP header.

- IPsec offers:-



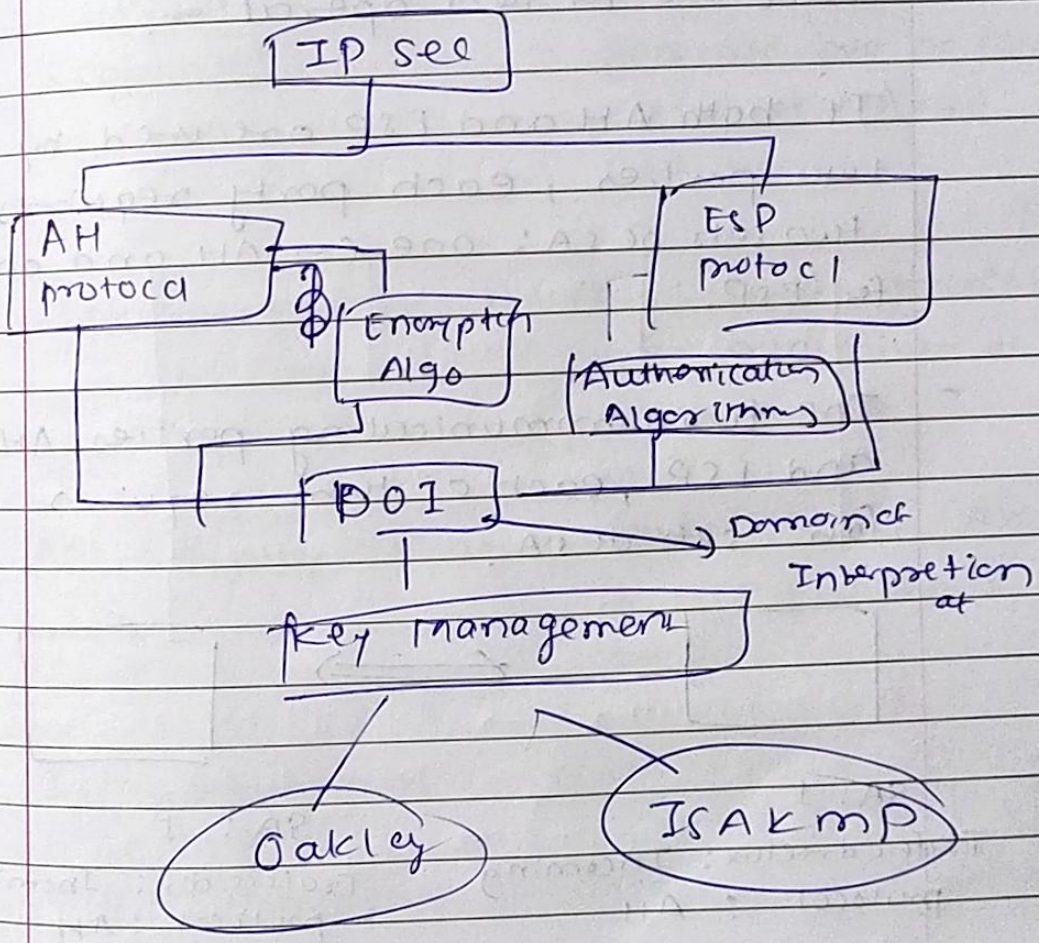
- Each has it's own extension header.

Page No.:
Date:

Protocols

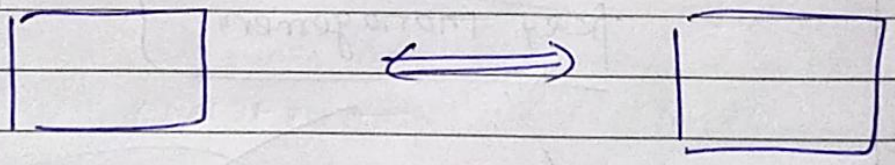
- **Authentication Header**
  - provides authentication and integrity
- **Encapsulating security Payload (ESP)**
  - provides confidentiality

IP Architecture.



Security Association (SA):

- IKE protocol used to establish SA bet^w parties
- Security Association Agreement between communicating parties about factors such as IP sec protocol version in use, mode of operation (transport mode or tunnel mode), cryptographic algorithms, keys, etc.
- Once SA is established, AH and ESP make use for their operation.
- If both AH and ESP are used by two parties, each party requires two sets of SA: one for AH and one for ESP.
- The two communicating parties AH and ESP, each of them requires four sets of SA.



SA: 1
Traffic direction: Incoming
protocol: AH

SA: 1
Traffic dir: Incomin
protocol: AH

SA: 2, Outgoing, AH

SA: 2, Outgoing. AH

SA: 3, Incoming, ESP

SA: 3, Incoming, ESP

SA: 4, Outgoing, ESP

SA: 4, Outgoing, ESP

- For storing information both party need storage. A standard storage area called Security Association Database (SAD).

- Each party maintain it's own SAD, containing SAD entries.

SAD Fields:

1. Sequence number counter — generate seq. no. field, used for AH and ESP header.

2. sequence counter overflow — flag indicates prevent further transmission of packets on SA.

3. Anti-replay window — detect if an AH or ESP packet is replay.

4. AH authentication — contain cryp. algo and key

5. ESP authentication — contain cryp. algo and key

6. IPsec Protocol mode — ~~Indicate which~~ IPsec Protocol mode (Transport or Tunnel)

7. Lifetime — Specifies life of SA. After time, SA must be replaced by new

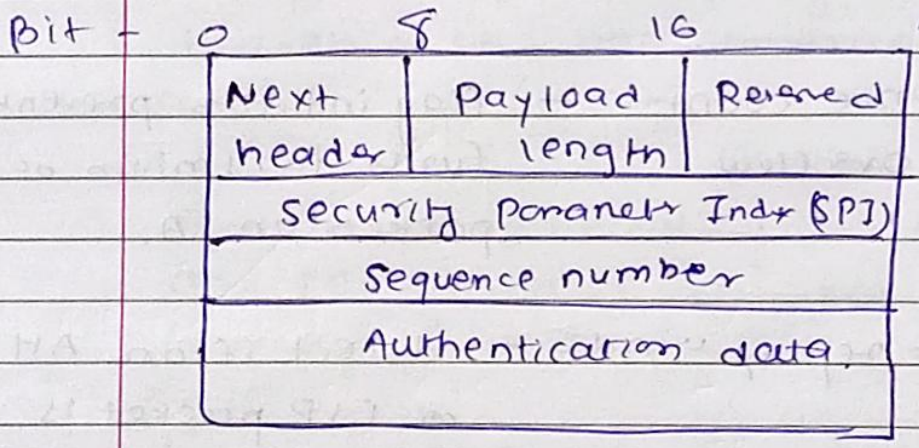
Authenication Header (AH):

- It provides data integrity and authentication of IP packets.

Data integrity service ⇒ entire data is not altered during transmission

Authentication ⇒ authenicate and decide to accept or reject the packet.

- AH Packet format:-



Next header → type of header immediately next to AH.

Payload length → length of AH in 32-bit word minus 2.

Reserved → reserved for future use.

SPI → used in combination of source and destination as well as uniquely identify the SA for traffic.

Page No.:
Date:

sequence no → prevent replay attacks

Authenication data → contain auth. data called Intergrity check value.

* Dealing with Replay Attacks:

- The attacker obtains copy of authenicated data packet and sends it to intended destination. Since the packet is received twice, the destination face some problem. To prevent, AH has seq. number field.

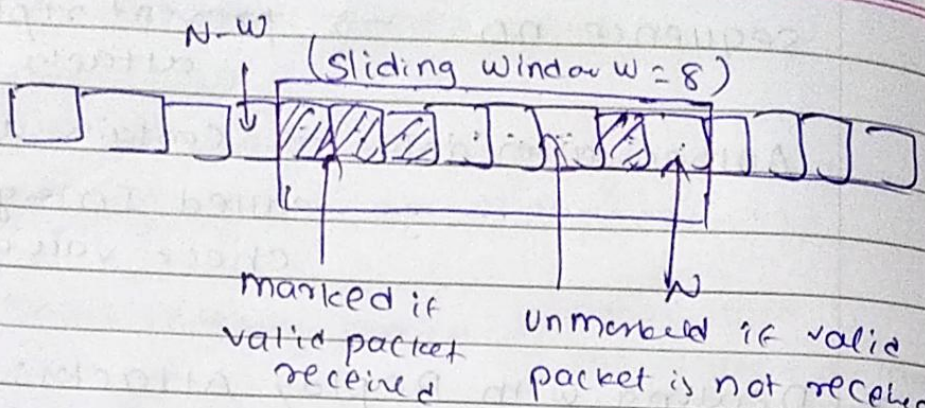
→

- Initially, seq. number is 0

- Every time sender send a packet twice over same SA, it increments value of this field by 1.

- On receiver side, there is some more procesing. The receiver maintains window size W = 64.

- The right edge of window is highest seq. number N received so far, for valid packet.

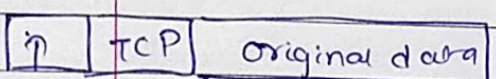


- For any packet with sequence number in range (N-W+1) to N that has been correctly received, the slot is marked in window.
- If valid packet is not received, the slot is unmarked.

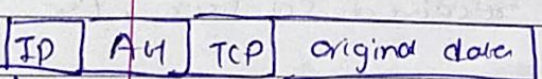
Modes of Operation

AH Transport Mode

- The position of AH is bet^w original IP header and TCP header of IP packet.



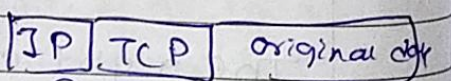
IP header (a) Before



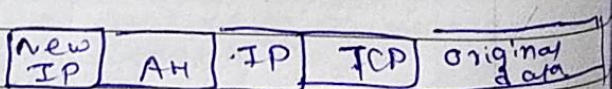
header (a) After

AH Tunnel mode

- the entire original IP is authenticated and AH is inserted bet^w original IP and new IP header.



(a) Before

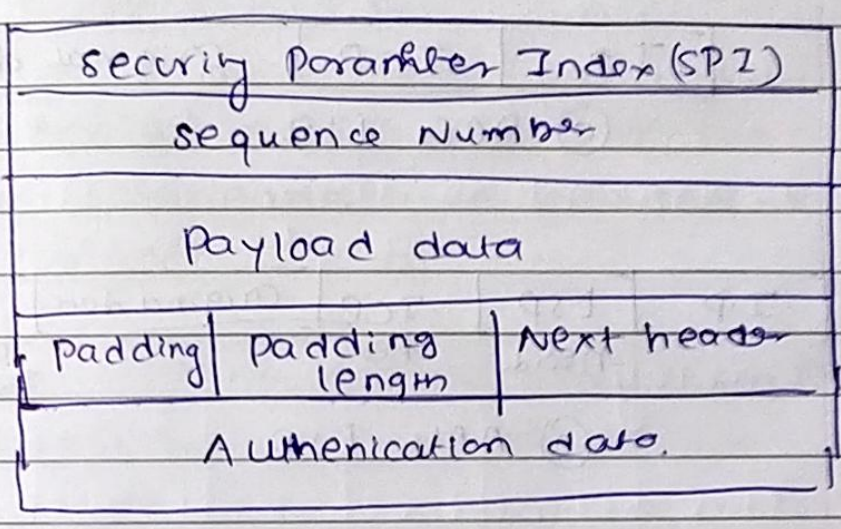


(b) After

* Encapsulating Security Payload (ESP) :-

- provides confidentiality.
- Based on symmetric key cryptography.

Packet Format :-



Payload data → contains transport mode or tunnel mode, encrypted

Padding → contains padding bits if any.

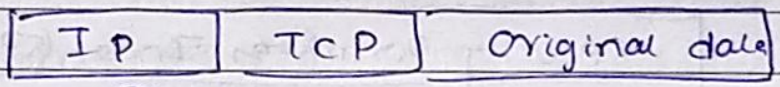
Padding Length → no. of padding bytes

modes of :-

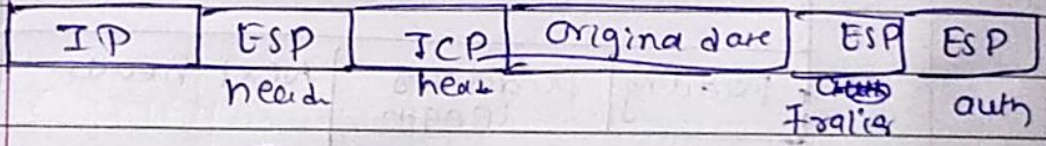
Transpost mode

Tunnel mode

1. ESP Transport mode :-



(a) Befr ESP.



(a) After ESP

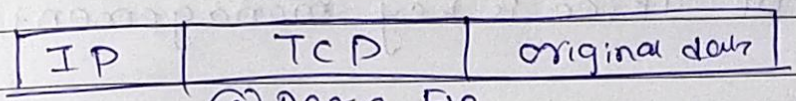
- In transpost mode, the ESP is inserted before TCP and after original IP header

- The ESP trailer is added after IP packet.

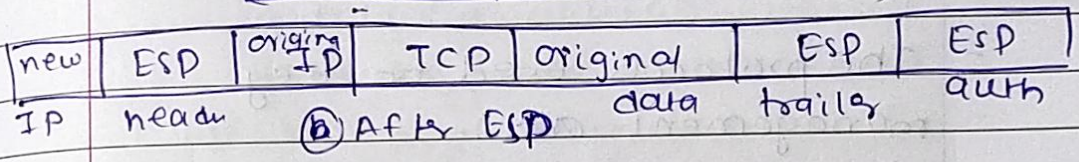
- If authenication is wed, the ESP auth is added after the ESP Trailer.

- The entire transpost layer segment and ESP trailer are encrypted.

2. ESP Tunnel mode:-



(a) Before ESP.



(b) After ESP

- In tunnel mode, the ESP and the new IP header are inserted before the original IP header.
- The ESP trailer and ESP auth are added to end of IP packet.
- The transport layer segment of original IP header, TCP, original data and ESP trailer are encrypted.

* Key management :-

- The third most significant aspect of IPsec is key management.
- Without proper key management, IPsec cannot exist.
- The protocols used for key management are :-
  1. Oakley → based on Diffie-Hellman key Exchange
  2. ISAKMP → Internet Securing Association and key management protocol

1. Oakley :-

- It is refined version of Diffie-Hellman key exchan protocol.
- Oakley protocol retain advantages of Diffie Hellman key exchange and remove its drawbacks.
- The features are as follow :-

1. Feature to defeat replay attacks
   - It implements mechanism called cookies to defeat congestion attacks
   - enable exchange of D-F Hellman public key values
   - ~~It provid~~

- It provides authenication mechanism to man-in-middle attack.

- Oakley support three authenicaes mechanism:-
  1. Digital signature
  2. Public key Encryption.
  3. secret key Encryption

- Oakley protocol support Aggressive key exchange type. It has three message exchange. bet^{w} x and Y.

Message 1 :- X sends cookie and public DF key for this exchange, along with information. X signs this block with it's private key.

Message 2 :- When Y receives message 1,
- verify signature of X using public key of X.
- It prepares acknowledgement msg for X, containing cookie sent by X.
- Y prepares cookie and public DF key and along with information
- It signs whole package with it's private key.

Message 3 :- After receiving msg 2, X verifies it using public key Y.
- X sends message to Y, to inform that has it received Y's public key.

2. ISAkmp :-
- protocol defines establishing, maintaining and deleting SA information.
- ISAkmp msg contain ISAkmp header encapsulated inside transport segment.
- Header Format :-

Initiator cookie				
Responder cookie				
Next payload	major version	minor version	Exchange Type	Flags
message ID				
length				

- Initiator cookie → contain cookie of entity that initiates SA establishment.
- Responder cookie → cookie of responding entity
- Next payload → type of first payload of message
- major version → identify the major ISAkmp protocol.
- minor version → identifies the minor ISAkmp protocol.
- Exchange → type of exchange.

Flags → set of options for ISAKMP exchange.

message ID → unique Id for this msg.

length → total length of message.