Cryptography and network Security

Module 5

① Explain the overview of an IP security.

→ IPsec provides the capability to secure communications across a LAN, across private and public WANs and across the internet.

1) Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks saving costs and network management overhead.

2) Secure remote access over the internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider and gain secure access to a company network.

3) Establishing extranet and intranet connectivity with partners: IPsec can be used to secure communication with other organization, ensuring authentication and confidentiality and providing a key exchange mechanism.

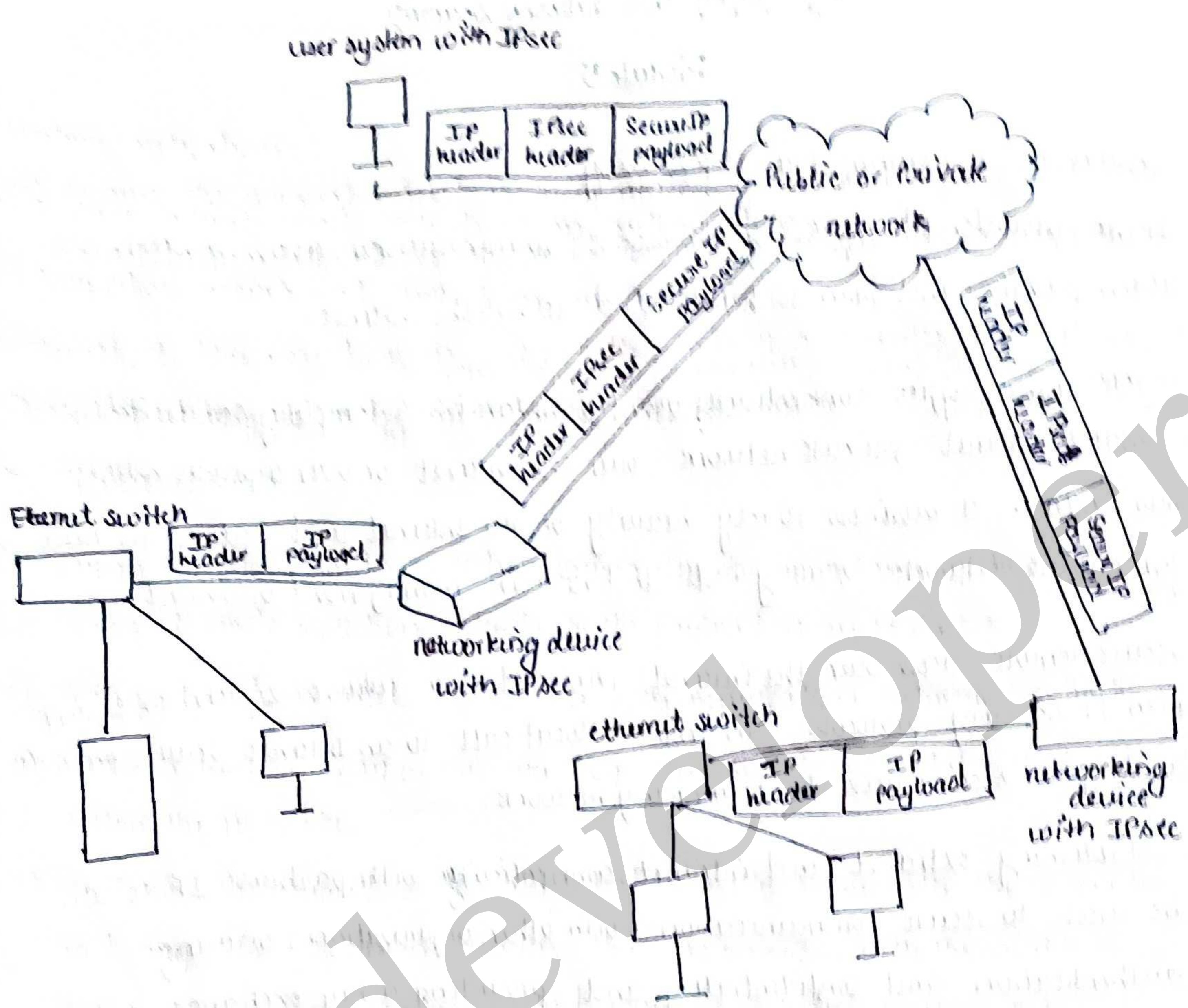
4) Enhancing electronic commerce security: Even though some web and electronic commerce application have built in security protocols, the use of IPsec ~~each~~ enhances that security.

The below diagram shows typical scenario of IPsec usage

1) An organisation maintain LANs at dispersed location. Non secure IP traffic is conducted at each LAN

2) For traffic offsite, through some sort of private or public WAN, IPsec protocal are used.

3) These protocol operate in networking devices, such as router or firewall that connect each LAN to outside world.



② Explain benefits and routing application of IPsec

→ Benefits of IPsec

1) When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.

2) IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

3) IPspec is below the transport layer and so it is transparent to application

4) IPsec can be transparent to end users.

5) IPsec can provide security for individual user if needed

Routing applications:

1) A router advertisement comes from an authorized router.

2) A neighbor advertisment comes from an authorized router.

3) A redirect message comes from the router to which the initial IP packet was sent

4) A routing update is not forged.

5 Explain transport and tunnel mode. IPsec.

→ Transport mode

1) Transport mode provides protection primarily for upper layers protocols

2) Transport mode protection extends to the payload of an IP packet.

3) Transport mode is used for end to end communication between two hosts.

4) When a host runs AH or ESP over IPv4, the payload is the data that normally follow the IP header.

5) For IPv6, the payload is the data that normally follow both the IP header and any IPv6 extensions headers that are present, with the possible exception of destination options headers, which may be included in the protection.

6) ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.

7) AH in transport mode authenticates the IP payload and selected portions of the IP header.

Tunnel mode:

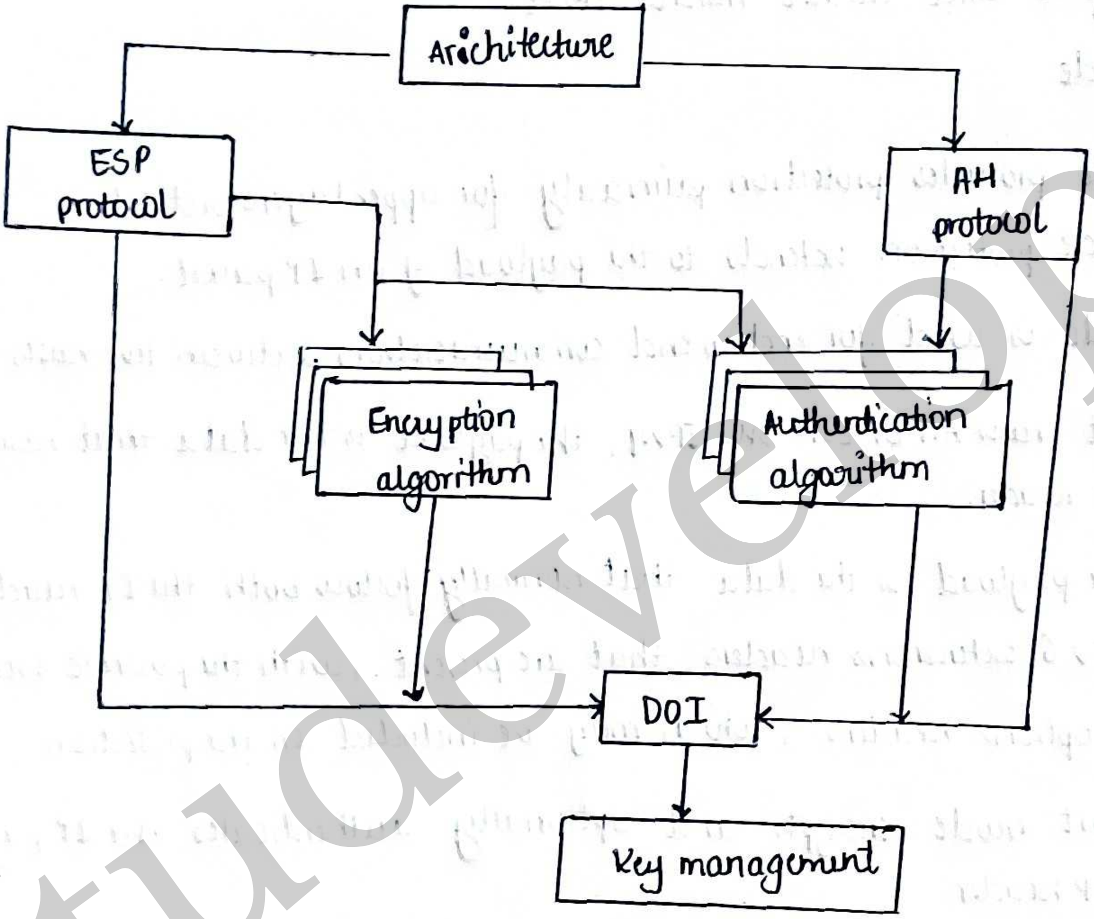
1) Tunnel mode provide protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to IP packet, the entire packet plus security fields is treated as the payload of new outer IP packet with a new outer IP header.

2) The entire original, inner, packet travels through a tunnel from one point of an IP network to another.

3) Because the original packet is encapsulated, the new larger packet may have totally different source and destination addresses, adding to the security

4) Tunnel mode is used when one or both ends of a security association (SA) are security gateway, such as fire wall or router that implement IPsec.

④ Explain IP security architecture



IP sec document: IP sec encompasses three functional areas: authentication, ~~condi~~ confidentiality and key management.

The document can be categorized into following group.

1) Architecture: Covers general concepts, security requirements, definations and mechanism defining IPsec technology.

2) Encapsulating Security payload: ESP consist of an encapsulating header and trailer used to provide encryption or combined encryption.

3) Authentication Header: AH is an extension header to provide message authentication.

4) Padding (0 - 255 bytes): If an encryption algorithm requires the plaintext to be multiple of some number of bytes, the padding field is used to expand the plaintext to required length.

The ESP format requires that the ~~payload~~ Pad length and Next header files be right aligned within a 32 bit word.

5) Pad length: Indicates the number of pad bytes immediately preceding this field

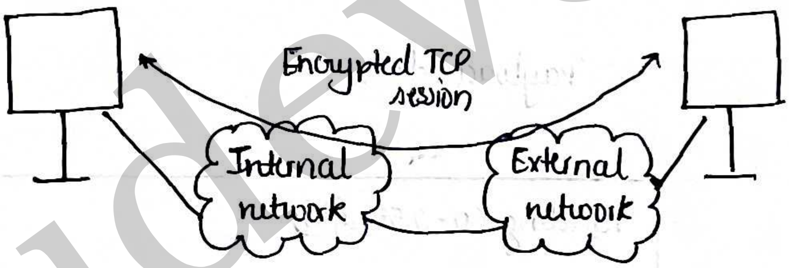
6) Next header: Identifies the type of data contained in the payload data field by identifying the first header in payload.

7) Authentication data variable: A variable length field that contains Integrity check value computed over the ESP packet minus the authentication data field.

⑥ Explain transport mode ESP and tunnel mode ESP

→

Transport mode ESP



1) Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP

2) The IPv6, ESP is viewed as an end to end payload; that is, it is not examined or processed by immediate routers.

3) Therefore, ESP header appears after the IPv6 base header and the hop-by-hop routing and fragment extension headers.

4) Encryption algorithm: A set of document that describe how various encryption algorithm are used in ESP.

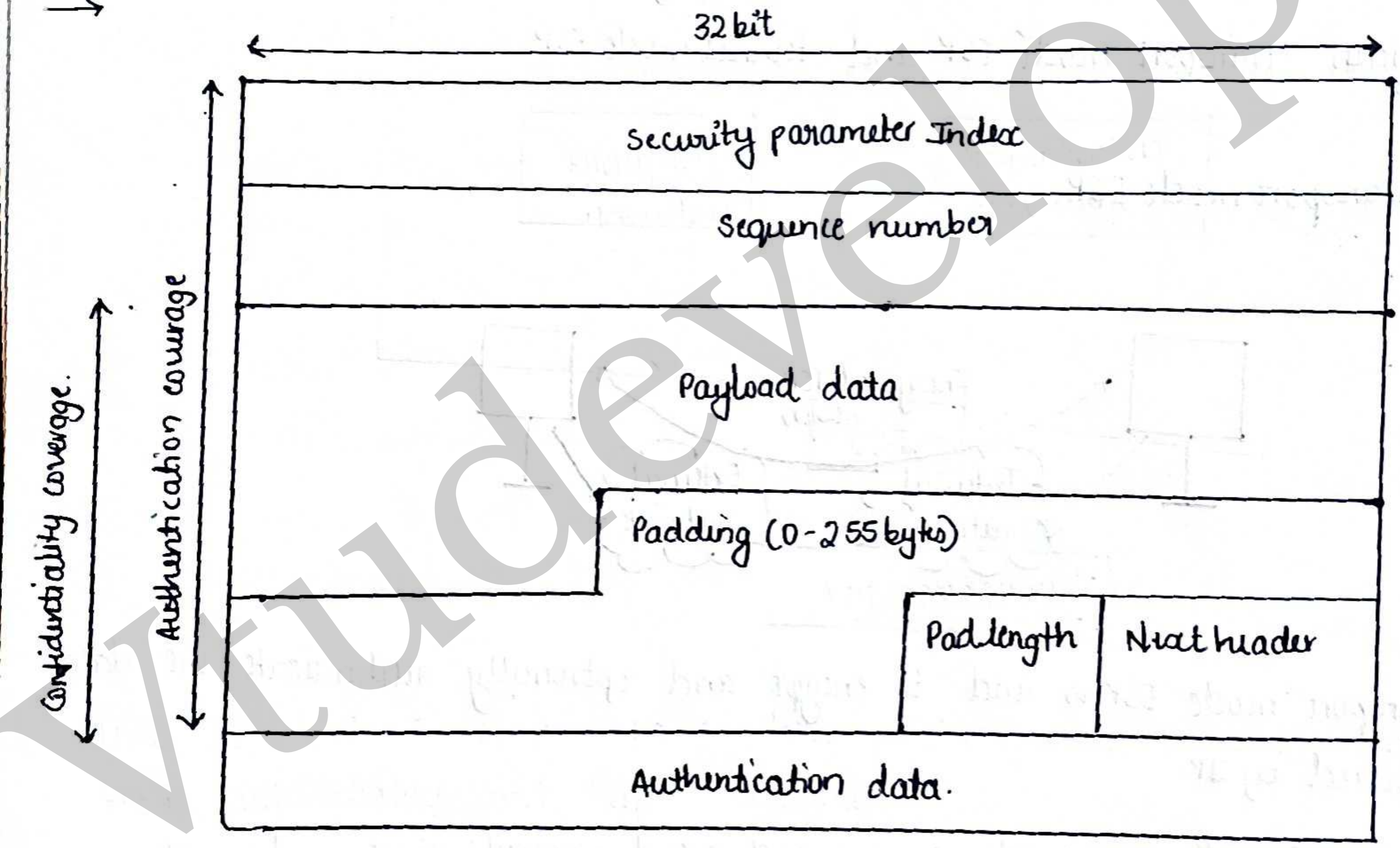
5) Authentication algorithm: A set of document that describe how various authentication algorithm are used for AH and for the authentication option of ESP.

6) Key Management: document that describe key management scheme.

7) Domain of Interpretation: contain values needed for the other document to relate each other.

(5) Explain ESP format with neat diagram.

→



1) Security parameter index: Identifies security association.

2) Sequence numbers: A monotonically increasing counter value, this provides an anti replay function

3) Payload data: This ~~a~~ is a transport level segment or IP packet that is protected by encryption.