USN

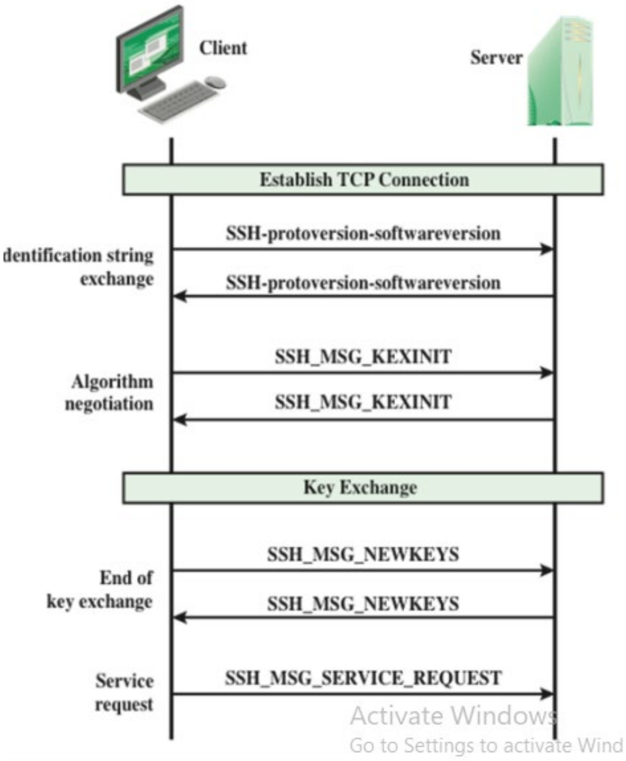
Internal Assessment Test 2 – April 2024

Sub:	Network Security				Sub Code:	18EC821	Branch:	ECE
Date:	13-04-2024	Duration:	90 min's	Max Marks:	50	Sem / Sec:	8 – A, B, C, D	OBE

	Answer any FIVE FULL Questions	MARKS	CO	RBT
1.	Explain with the help of neat diagrams the SSH Transport Layer Protocol Packet Exchange.	[10]	CO2	L2
2.	Infer with the help of neat diagrams: The SSH Connection Protocol.	[10]	CO2	L2
3.	Explain typical scenario of IPsec usage with relevant diagrams and mention the applications of IPsec.	[10]	CO3	L2
4.	List and explain the IPsec documents and IPsec services.	[10]	CO3	L1
5.	Explain with the help of neat diagrams the IP Traffic Processing.	[10]	CO3	L2
6.	Interpret the Encapsulating Security Payload (ESP) format.	[10]	CO3	L2
7.	Identify several approaches in Authentication Plus Confidentiality with reference to IPsec	[10]	CO3	L3
8.	With the help of neat diagram explain the basic combination of security association.	[10]	CO3	L3

Solution

Q1.



Once the connection is established, the client and server exchange data.

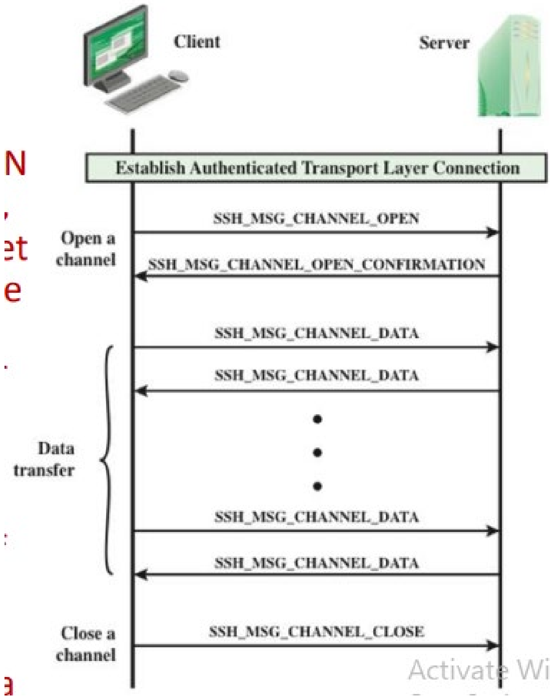
- The first step, the identification string exchange, begins with the client sending a packet with an identification string.
- Next comes algorithm negotiation. Each side sends an SSH_MSG_KEXINIT containing lists of supported algorithms in the order of preference to the sender. There is one list for each type of cryptographic algorithm. The algorithms include key exchange, encryption, MAC algorithm, and compression algorithm.
- The next step is key exchange. The specification allows for alternative methods of key exchange, but at present, only two versions of Diffie-Hellman key exchange are specified.
- The final step is service request. The client sends an SSH_MSG_SERVICE_REQUEST packet to request either the User Authentication or the Connection Protocol. Subsequent to this, all data is exchanged as the payload of an SSH Transport Layer packet, protected by encryption and MAC.

Q2. The SSH Connection Protocol runs on top of the SSH Transport Layer Protocol and assumes that a secure authentication connection is in use – The secure authentication connection, referred to as a tunnel, is used by the Connection Protocol to multiplex a number of logical channels

- Channel mechanism – All types of communication using SSH are supported using separate channels – Either side may open a channel – For each channel, each side associates a unique channel number –

Channels are flow controlled using a window mechanism – No data may be sent to a channel until a message is received to indicate that window space is available – The life of a channel progresses through three stages: opening a channel, data transfer, and closing a channel

• When either side wishes to open a new channel, it allocates a local number for the channel and then sends a message SSH_MSG_CHANNEL_OPEN consists channel type, sender channel, window size and packet size.



• If the remote side is able to open the channel, it returns a SSH_MSG_CHANNEL_OPEN_CONFIRMATION message, which includes the sender channel number, the recipient channel number, and window and packet size values for incoming traffic. Otherwise, the remote side returns a SSH_MSG_CHANNEL_OPEN_FAILURE message with a reason code indicating the reason for failure.

• Once a channel is open, data transfer is performed using a SSH_MSG_CHANNEL_DATA message, which includes the recipient channel number and a block of data. These messages, in both directions, may continue as long as the channel is open.

• When either side wishes to close a channel, it sends a SSH_MSG_CHANNEL_CLOSE message, which includes the recipient channel number.

Four channel types are recognized in the SSH Connection Protocol specification: Session, X11, Forwarded-TCPIP, Direct-TCPIP

One of the most useful features of SSH

• Provides the ability to convert any insecure TCP connection into a secure SSH connection (also referred to as SSH tunneling)

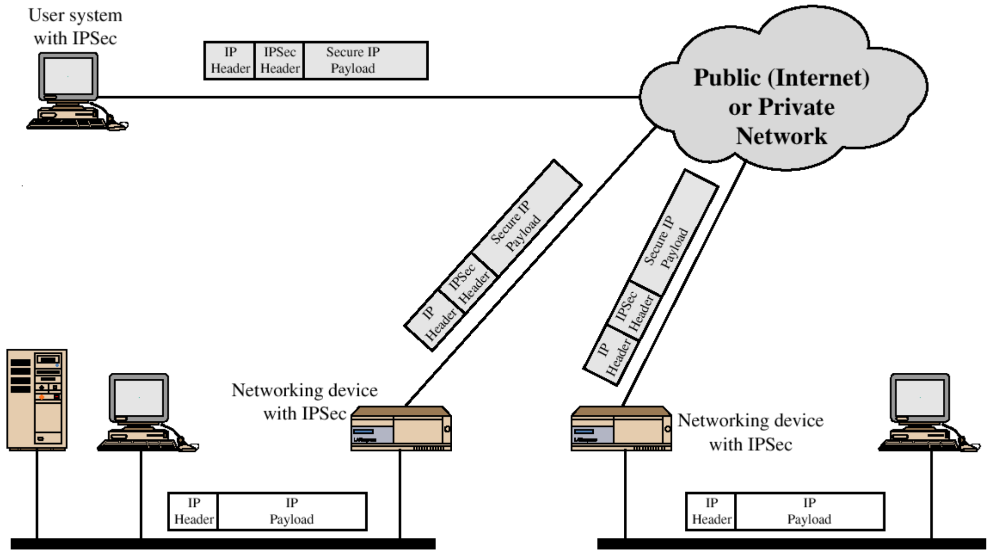
• Incoming TCP traffic is delivered to the appropriate application on the basis of the port number (a port is an identifier of a user of TCP)

• An application may employ multiple port numbers

• For example, for the Simple Mail Transfer Protocol (SMTP)

Q3. IPSec is not a single protocol. Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms to provide security appropriate for the communication

- Applications of IPSec
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establishing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security



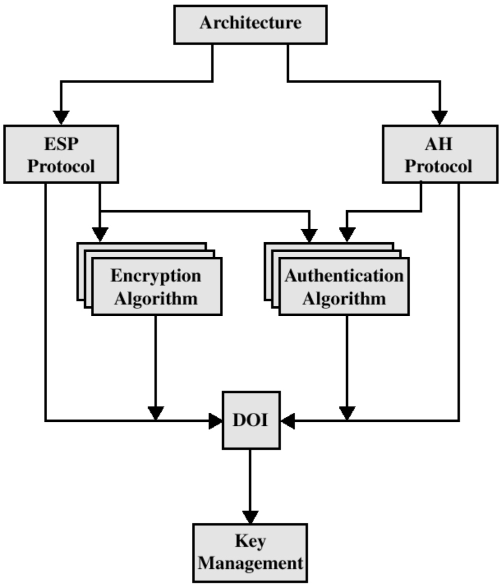
Benefits of IPSec

  - in a firewall/router provides strong security to all traffic crossing the perimeter
  - in a firewall/router is resistant to bypass
  - is below transport layer, hence transparent to applications
  - can be transparent to end users
  - can provide security for individual users
  - secures routing architecture
- IPsec plays a Vital role in routing architecture of internetworking.
  - IPSec can assure that: A router or neighbor advertisement comes from an authorized router
    - A redirect message comes from the router to which the initial packet was sent
    - A routing update is not forged
- A method for establishing a security association (SA) that **authenticates users**, **negotiates the encryption method** and **exchanges the secret key**. IKE is used in the IPsec protocol. Derived from the ISAKMP framework for key exchange and the Oakley and SKEME key exchange techniques, IKE uses public key cryptography to provide the secure transmission of the secret key to the recipient so that the encrypted data may be decrypted at the other end

Q.4 **IPSec Services**

- Access Control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiality

IP document Overview:



Security association is a one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it.

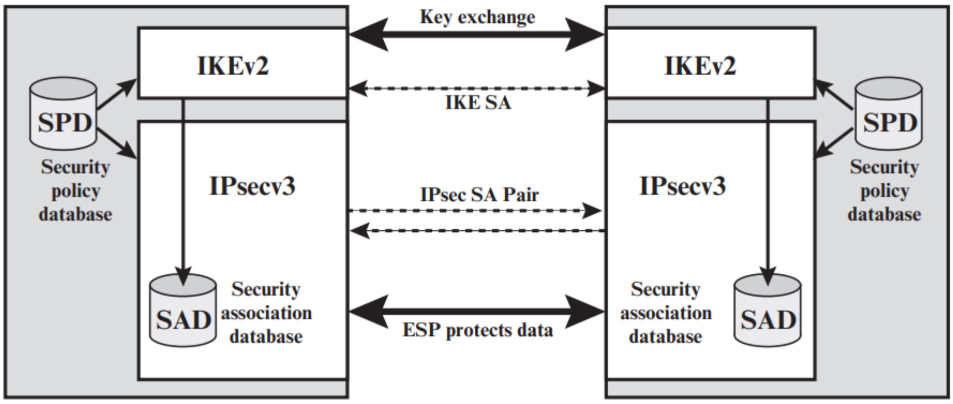


Figure 20.2 IPsec Architecture

- SA Identified by three parameters:
  - Security Parameter Index (SPI)
  - IP Destination address
  - Security Protocol Identified
- Security Association Database that defines the parameters associated with each SA.
- The means by which IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPsec) Is the nominal Security Policy Database (SPD).

Sl No.	Parameters entry in SAD	Parameters entry in SPD
1	Security Parameter Index	Remote IP Address
2	Sequence Number Counter	Local IP Address
3	Sequence Counter Overflow	Next Layer Protocol
4	Anti Replay Window	Name
5	AH Info	Local port
6	ESP Info	Remote port
7	Life time of this SA	
8	Ipsec Protocol mode and Path MTU	

- Q5: When IPsec is implemented, each outbound IP packet is processed by the IPsec logic before transmission,
- Each inbound packet is processed by the IPsec logic after reception and before passing the packet contents on to the next higher layer (e.g., TCP or UDP)
- Two situations in turn
  - Outbound Packet Processing
  - Inbound Packet Processing
- A block of data from a higher layer, such as TCP, is passed down to the IP layer and an IP packet is formed.
  - IPsec searches the SPD for a match to this packet.
  - If no match is found, then the packet is discarded and an error message is generated.
  - If a match is found, further processing is determined. If the policy for this packet is DISCARD, then the packet is discarded. For Bypass no processing.
  - If the policy is PROTECT, then a search is made of the SAD for a matching entry.
  - The matching entry in the SAD determines the processing for this packet.

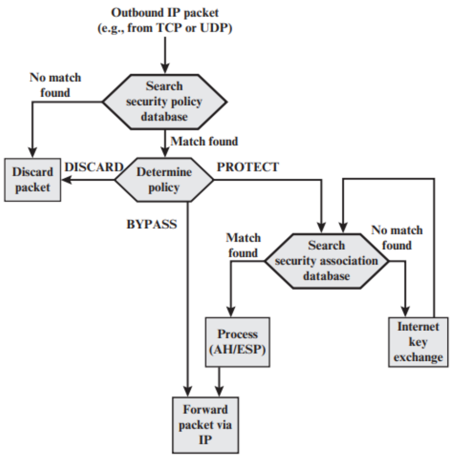


Figure 20.3 Processing Model for Outbound Packets

- An incoming IP packet triggers the IPsec processing. The following steps occur:
  - IPsec determines whether this is an unsecured IP packet or one that has ESP or AH headers/trailers, by examining the IP Protocol field (IPv4) or Next Header field (IPv6)
  - If the packet is unsecured, IPsec searches the SPD for a match to this packet. If the first matching entry has a policy of BYPASS, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP. If the first matching entry has policy of PROTECT or DISCARD, or if there is no matching entry, the packet is discarded.
  - For a secured packet, IPsec searches the SAD. If no match is found, the packet is discarded. Otherwise, IPsec applies the appropriate ESP or AH processing. Then, the IP header is processed and stripped off and the packet body is delivered to the next higher layer, such as TCP

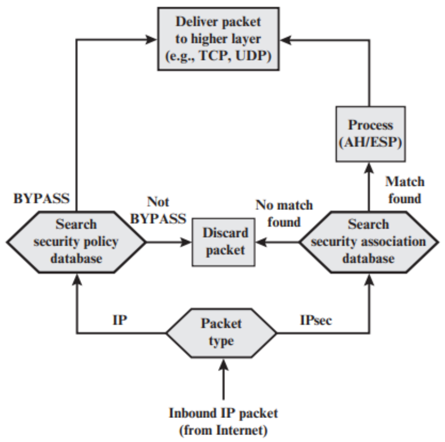


Figure 20.4 Processing Model for Inbound Packets

Q 6.

- ESP provides confidentiality services
- Encryption:
- Three-key triple DES
- RC5
- IDEA
- Three-key triple IDEA
- CAST
- Blowfish
- Authentication:
- HMAC-MD5-96
- HMAC-SHA-1-96

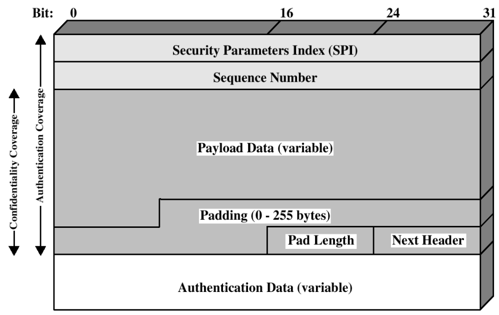


Figure 6.7 IPSec ESP Format

Encryption and Authentication Algorithms

- The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service.
- If the algorithm used to encrypt the payload requires cryptographic synchronization data, such as an initialization vector (IV), then these data may be carried explicitly at the beginning of the Payload Data field.
- The ICV field is optional. It is present only if the integrity service is selected and is provided by either a separate integrity algorithm or a combined mode algorithm that uses an ICV.
- The ICV is computed after the encryption is performed. This order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver prior to decrypting the packet, hence potentially reducing the impact of denial of service (DoS) attacks.
- It also allows for the possibility of parallel processing of packets at the receiver, i.e., decryption can take place in parallel with integrity checking
- The Padding field serves several purposes:
    - If an encryption algorithm requires the plaintext to be a multiple of some number of bytes (e.g., the multiple of a single block for a block cipher), the Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length.
    - The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word. Equivalently, the ciphertext must be an integer multiple of 32 bits. The Padding field is used to assure this alignment.
    - Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload.

Q7

Identify several approaches in Authentication Plus Confidentiality with reference to IPsec
With the help of neat diagram explain the basic combination of security association.