Solution and scheme of Internal Assessment Test III – Nov. 2019

Sub:	Cryptography and Network Security					Sub Code:	15TE71	Branch:	TCE
Date:	16/11/2019	Duration:	90 min's	Max Marks:	50	Sem / Sec:	7th A		OBE

1(a) List the different types of threats and consequences when using the web. Also list the countermeasure to be taken.

	Threats	Consequences	Countermeasures
Integrity	•Modification of user data •Trojan horse browser •Modification of memory •Modification of message traffic in transit	•Loss of information •Compromise of machine •Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	•Eavesdropping on the net •Theft of info from server •Theft of data from client •Info about network configuration •Info about which client talks to server	•Loss of information •Loss of privacy	Encryption, Web proxies
Denial of Service	•Killing of user threads •Flooding machine with bogus requests •Filling up disk or memory •Isolating machine by DNS attacks	•Disruptive •Annoying •Prevent user from getting work done	Difficult to prevent
Authentication	•Impersonation of legitimate users •Data forgery	•Misrepresentation of user •Belief that false information is valid	Cryptographic techniques

A Comparison of Threats on the Web

[5 marks]

1(b) What is the difference between SSL connection and SSL session?

SSL Session: **[2.5 mark]**

i. An SSL session is an association between a client and a server.
ii. Sessions are created by the handshake protocol.
iii. Session defines a set of cryptographic security parameters which can be shared among multiple connections.

Sl. No.	Parameters	Description
1	**Session Identifier**	A byte sequence is chosen by the server to identify an active session state.
2	**Peer certificate**	A certificate X. 509v3 is used to verify the public key belong to user
3	**Compression Method**	The data is compressed prior to the encryption
4	**Cipher Spec**	It specifies the different encryption algorithm such as DES, AES, 3DES and hash Algorithm.
5	**Master Secret**	48 byte secret shared between the client and the server
6	**Is resumable**	It is a flag which indicates whether the session can be used to initiate new connections.

SSL Connection: **[2.5 mark]**

SSL connection is the transport to provide peer to peer relationship. Every connection is associated with one session. Between server and the client there may be multiple connections.

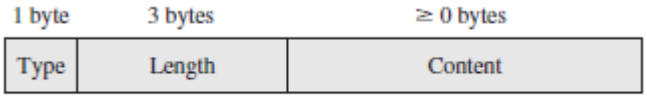
Sl. No.	Parameters	Description
1	**Server and Client**	It is the byte sequences that are chosen by the server and the

	random	client for each connection.
2	**Server write MAC secret**	The secret key used in MAC operation on data sent by the server
3	**Client Write MAC secret**	The secret key used in MAC operation on data sent by the client
4	**Server Write Key**	The encryption key for data encryption done by the server and decryption by the client.
5	**Client Write Key**	The encryption key for data encryption done by the client and decryption by the server.
6	**Initialization vector**	For different modes of operations such as CBC, OFB, CFB the initialize vector is defined for each cipher key during negotiation, which is used for the 1st block exchange. The final cipher text from the block is used as the IV for the next block
7	**Sequence Number**	Each party maintains separate sequence numbers for transmitted and received messages for each connection. The sequence number starts from 0 and increments. It must not exceed $2^{64} - 1$

2. Explain the various phases of SSL handshake protocol with a diagram.

a) <u>HANDSHAKE PROTOCOL:</u> **[Diagram 4 marks +Explain 6 marks]**

- The handshake protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and the keys to be used to protect data sent in an SSL record.
- The handshake protocol is used before any application data is transmitted.
- The handshake protocol consists of a series of messages exchanged by client and server. Each message has 3 fields
    a) Type (1 Byte): one out of 10 messages.
    b) Length (3 Bytes): Length of the message in bytes.
    c) Content (≥ 0 Bytes): Parameters associated with that message.



(c) Handshake Protocol

The SSL Handshake protocol message types are:

Message Type	Parameters
`hello_request`	null
`client_hello`	version, random, session id, cipher suite, compression method
`server_hello`	version, random, session id, cipher suite, compression method
`certificate`	chain of X.509v3 certificates
`server_key_exchange`	parameters, signature
`certificate_request`	type, authorities
`server_done`	null
`certificate_verify`	signature
`client_key_exchange`	parameters, signature
`finished`	hash value

- Handshake is done in 4 phases.

Phase -1: (Establishing security capabilities): This phase is used to initiate a logical connection and to establish the security capabilities that will be associated with it. This exchange is initiated by the client, which sends a client hello message with the following parameters.

a) Version: The Highest SSL version supported by the Client.
b) Client random number: 32 bits timestamp + 28 bytes of random generated by client. It is required to prevent reply attack.
c) Session ID: variable session length, 0 mean new session, else client want to update existing session.
d) Cipher Suite: This is a list that contains the cryptographic algorithm supported by the client in decreasing order of preferences.
e) Compression Method: This is a list of compression method the client can support.

After sending the client hello message, the client waits for the server-hello message, the server hello message has the following parameters.

a) Version: An SSL version. It is the version supported by both client and server.
b) Server random number: 32 byte random number is generated by the server.
c) Session ID: if client id is 0 server put new session id which indicates new session else client id
d) Selected cipher set: encryption algorithm selected by client
e) Selected compression method: compression algorithm selected by client

After phase 1, the client and server know the following:

a) The version of SSL
b) The algorithm for key exchange, message authentication and encryption.
c) The compression method
d) The 2 random numbers for key generation

Phase-2: (Server authentication and key exchange): The server begins this phase by sending its certificates for the authentication. The server may also request certificates from the client. At the end, the server announces that the server hello process is done. The phase 2 has these 4 following steps.

a) Certificate: Server sends the certificate message to authenticate itself.
b) Server key exchange: After the certificate message, the server sends the server key exchange message that includes its contribution to the pre-master secret.
c) Certificate request: The server may request the client to authenticate itself.
d) Server Hello Done: It is a signal to the client that Phase-2 is over and the client needs to start Phase-3.

After phase 2,

a) The server is authenticated to the client.
b) The client knows the public key of the server if required.

Phase-3: (Client authentication and key exchange): Phase-3 is designed to authenticate the client. In this phase, 3 messages can be sent from the client to the server. Those are

a) Certificate: The client sends the certificate message. This message is sent only if the server has requested a certificate in phase-2. If there is a request and the client has no certificate to send, it sends an Alert message (no certificate).
b) Client Key exchange: Client sends key exchange message which includes its contribution to the pre master secret. Depending on the cipher suit selected in phase-1, pre master secret and parameters are sent which is used to calculate for both sides.
c) Certificate verify: If the client sends the certificate declaring its public key, client will definitely have its private key. The proof of the private key can be done by creating a message and signing it with the private key. The server can verify the message with public key already sent to ensure the certificate belong to the client.

After phase 3,

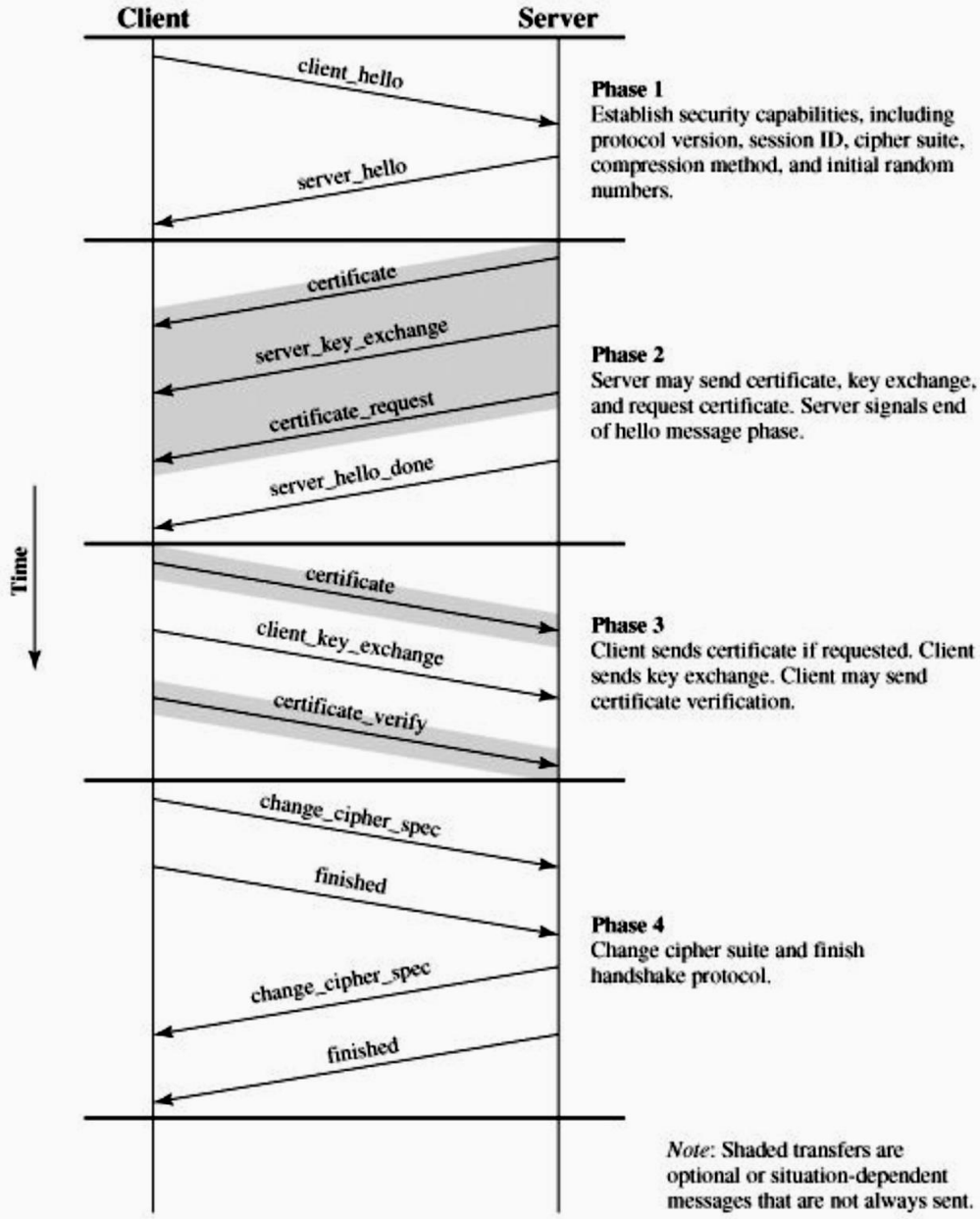
a) The client is authenticated for the server.
b) Both the client and the server know the pre-master secret.

Phase-4: (Finalizing and Finishing): In phase -4, the client and server complete the setting up of a secure connection and finish the handshake protocol. In this phase, 4 messages are exchanged those are

a) Change cipher spec: (sent by client): The client sends change cipher specification message and copies the pending cipher specification into current cipher specification.
b) Finished (sent by client): The finish message is sent by the client; where client announces the end of handshake protocol.
c) Change cipher spec: (sent by server): The server sends change cipher specification message and copies the pending cipher specification into current cipher specification.
d) Finished: (sent by server): The finish message is sent by the server; where server announces the handshaking is totally completed.

After phase 4,

After Phase-4, the client and server are ready to exchange the data.

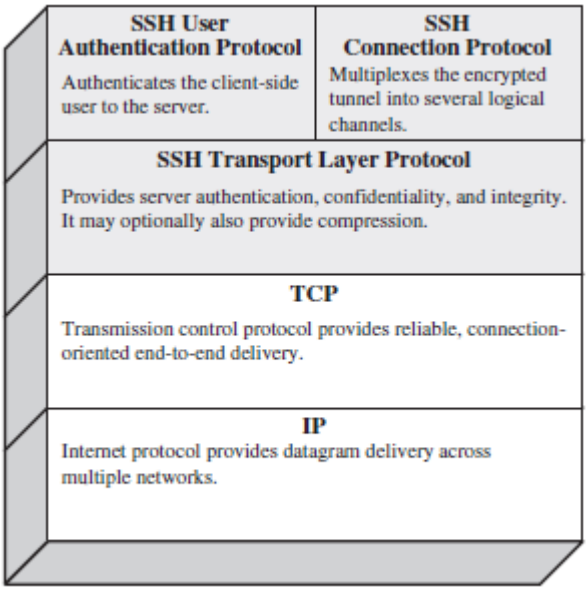


[Figure: Handshake Protocol Action]

3. Define SSH. List and briefly describe the SSH Protocol.

SECURE SHELL (SSH): **[Diagram 4 marks +Explain 6 marks]**

1. Secure Shell (SSH) is a protocol for secure network communications designed to be relatively simple and inexpensive to implement.
2. The initial version, SSH1 was focused on providing a secure remote logon facility to replace TELNET and other remote logon schemes that provided no security.
3. SSH also provides a more general client/server capability and can be used for such network functions as file transfer and e-mail.
4. SSH2 fixes a number of security flaws in the original scheme.
5. SSH client and server applications are available for all most all the operating system.
6. It has become the choice for remote login and X tunneling.
7. SSH is organized as three protocols that run on top of TCP.
    a) Transport Layer Protocol
    b) User Authentication Protocol
    c) Connection Protocol



SSH Protocol Stack

8. Transport Layer Protocol Provides server authentication, data confidentiality, and data integrity. It may optionally provide compression.
9. User Authentication Protocol authenticates the user to the server.
10. Connection Protocol multiplexes multiple logical communications over a single SSH connection.

Transport Layer Protocol:

1. Server authentication occurs at the transport layer. A server may have multiple host keys using different asymmetric encryption algorithms. Multiple hosts may share the same host key. The server host key is used during key exchange to authenticate the identity of the host; the client must have a priori knowledge of the server's public host key. Hence two alternative trust models can be used:
    a) The client has a local database that associates each host name with the corresponding public host key. The difficulty is that the database of name-to-key associations may become burdensome to maintain.
    b) The host name-to-key association is certified by a trusted certification authority (CA). The client only knows the CA root key and can verify the validity of all host keys. This method is easy as only single CA key needs to be securely stored on the client.

2. First client establishes a TCP connection to the server. It is done by the TCP protocol not by the Transport layer protocol. Once the connection is established, the client and server exchange data in terms of packet. Each packet consists of the following format.
    a) Packet length
    b) Padding length
    c) Payload
    d) Random Padding
    e) Message Authentication code

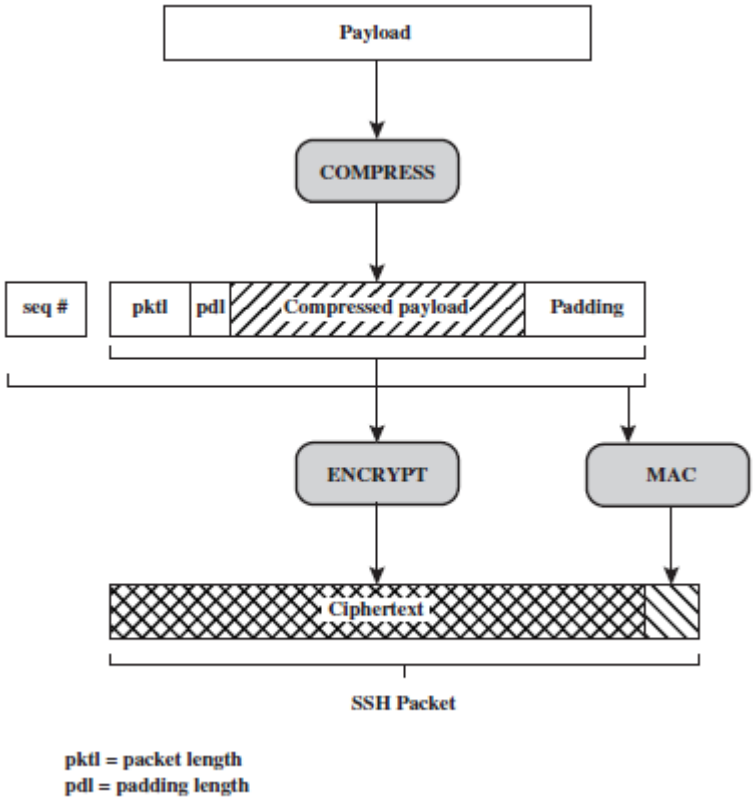


Figure SSH Transport Layer Protocol Packet Formation

User Authentication Protocol: The User Authentication Protocol provides the means by which the client is authenticated to the server.

4. Briefly describe the IEEE 802.11i phase of operation

IEEE 802.11i PHASES OF OPERATION: **[Diagram 4 marks +Explain 6 marks]**

1. The operation of an IEEE 802.11i RSN can be broken into 5 phases.
2. These are the possible communication in a IEEE 802.11 extended service set (ESS).
    a) Two wireless stations (STA) in the BSS communicate via the access point for that BSS.
    b) Two wireless station (STA) in the same adhoc IBSS communicate directly with each other.
    c) Two wireless stations in different BSS communicating via their respective APs across a distributed system.
    d) A wireless station communicating with an end station on a wired network via its AP and the distributed system.
3. IEEE 802.11i security is concerned only with secure communication between the STA and its AP.
4. In case 1, the secure communication is assured if each STA establishes secure communication with the AP.
5. In case 2, The AP functionality is residing inside STA.
6. In case 3, security can't be provided across the distribution system by the IEEE 802.11, but it can be provided with in BSS.
7. In case 4, Security is only provided between the STA and its AP.

8. There are phases of operation for a RSN. The Network component involved are
    a) Wireless stations (STA)
    b) Access Point (AP)
    c) Authentication Server (AS)
    d) End station.
9. The rectangle indicates the exchange of MAC protocol data unit (MPDU).
10. Those 5 Phases are
    a) Discovery
    b) Authentication
    c) Key Generation and distribution
    d) Protected data transfer
    e) Connection Termination

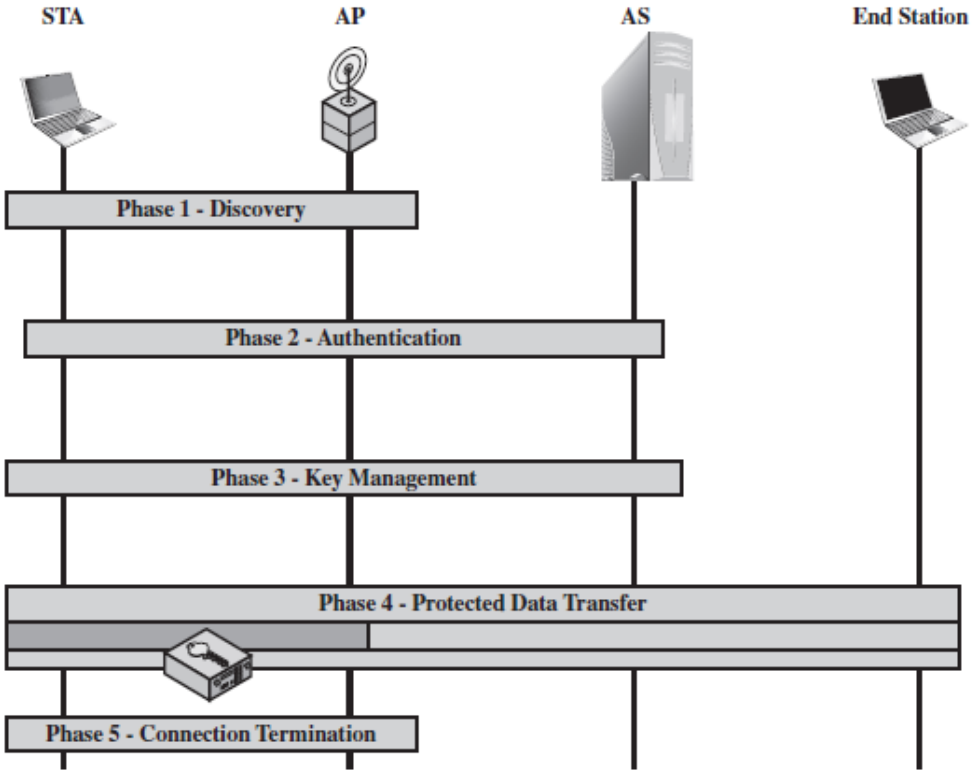


Figure IEEE 802.11i Phases of Operation

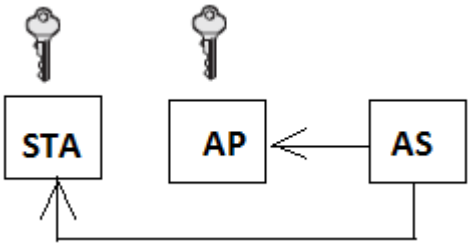
(a) Discovery Phase:

An access point uses messages called Beacon and probe response to advertise its IEEE 802.11i security policy. The STA uses these to identify an AP for the WLAN with which it wants to communicate. The STA associates with the AP and select the cipher suite and authentication mechanism to be used.

(b) Authentication:

- In this phase the wireless station (STA) and the Authentication server (AS) prove their identity to each other. The AP blocks the non-authenticated traffic between STA and the AS until the authentication transaction is successful.
- The Access point doesn't participate in the authentication transaction other than forwarding traffic between STA and SS.

(c) Key Generation and Distribution: The AP and STA perform several operations that cause cryptographic keys to be generated and placed on the AP and STA. Authentication server generates the secret session key and placed securely at AP and STA.



(d) Protected Data Transfer:

- Frames are exchanges between STA and the end station through the AP.
- Here secure data transfer occurs between STA and the AP only.
- Security is not provided end-to-end.
- The security indicates secure data transfer occurs between the STA and AP.

(e) Connection termination: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.

Discovery Phase:

1. The purpose of this phase is for STA and AP to recognize each other, agree on a set of security algorithm and establish an association for the future communication using those security capabilities.
2. The MAC protocol Data unit (MPDU) in discovery phase is
    a) Network and security capability discovery
    b) Open system Authentication
    c) Association: If there is no match, in the capabilities between the AP and the STA, the AP refuses the association request and STA blocks it too and no user traffic goes beyond the AP.

Authentication Phase: Authentication enables mutual authentication between STA and AS.

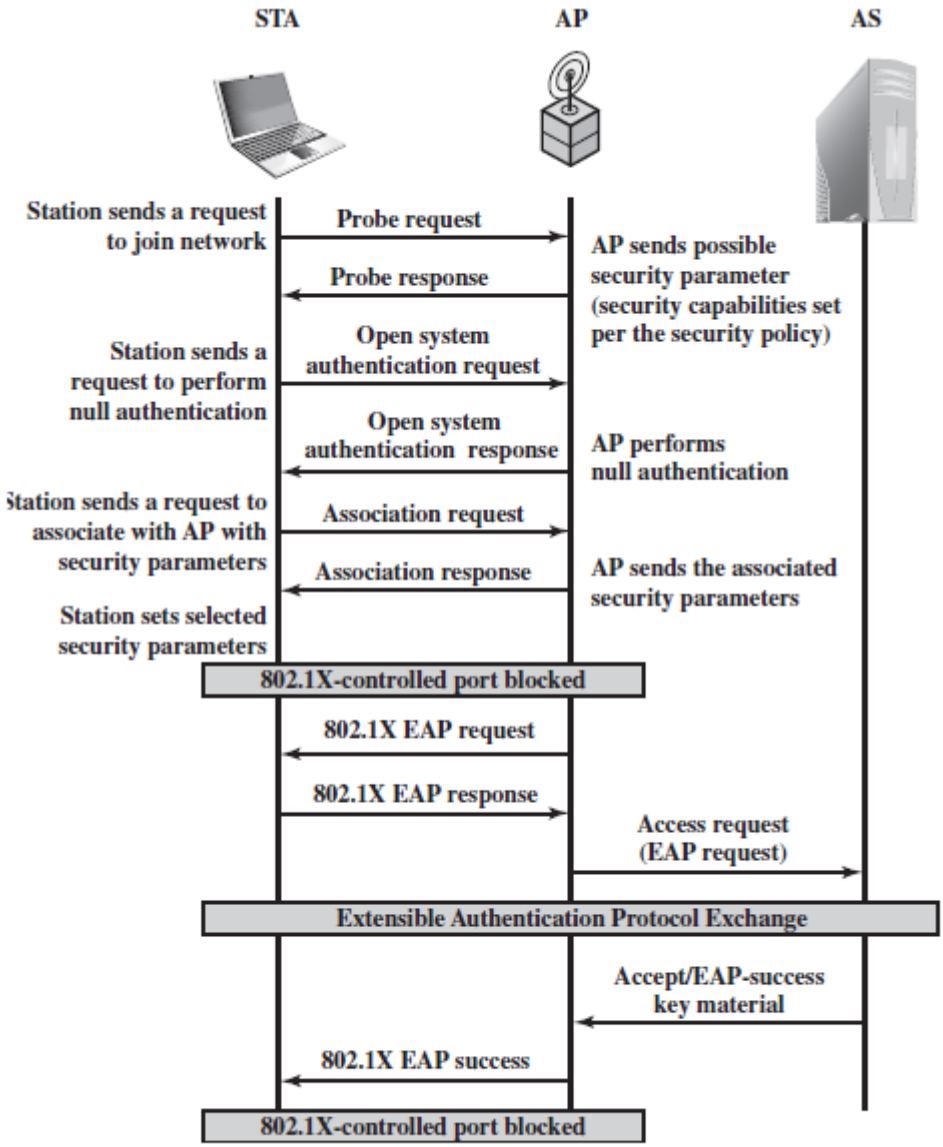


Figure IEEE 802.11i Phases of Operation: Discovery, Authentication, and Association

5. What are the services provided by the PGP? Draw the appropriate diagram to explain it and mention the types of algorithm used for it.

PRETTY GOOD PRIVACY (PGP): **[Services 4 marks + Diagram 4 marks + Types of algorithms used 2 marks]**

1. PGP was invented by Phil Zimmermann in 1991 to provide e-mail with privacy, integrity and authentication.
2. PGP can be used to create a secure e-mail message or to store a file securely for future retrieval.

Notation:

$K_S =$ Session key used in Symmetric encryption scheme
$PR_a =$ Private Key of user A
$PU_a =$ Public Key of user A
$EP =$ Public key Encryption
$DP =$ Public key decryption
$EC =$ Symmetric encryption/ Conventional Encryption.
$DC =$ Symmetric decryption/ Conventional Decryption.
$H =$ Hash function
$|| =$ Concatenation
$Z =$ Compression using ZIP algorithm
$R64 =$ Conversion to radix 64 ASCII Format

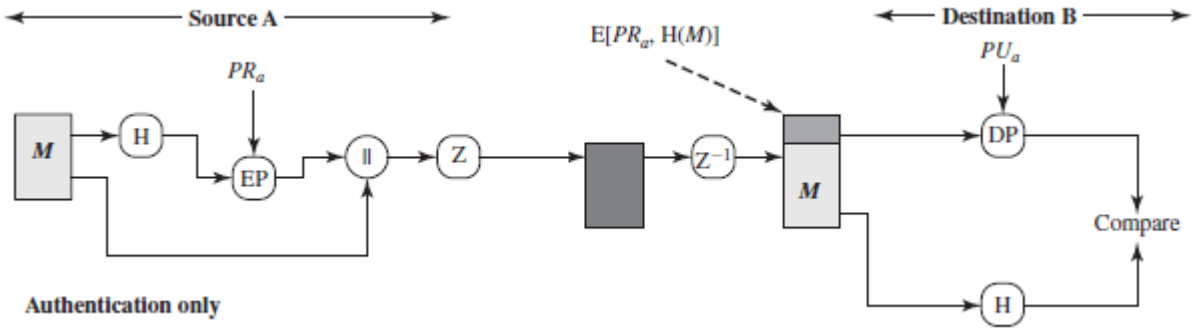
Operational Description: The PGP provides 4 services:

a) Authentication
b) Confidentiality
c) Compression
d) E-mail Compatibility

Table Summary of PGP Services

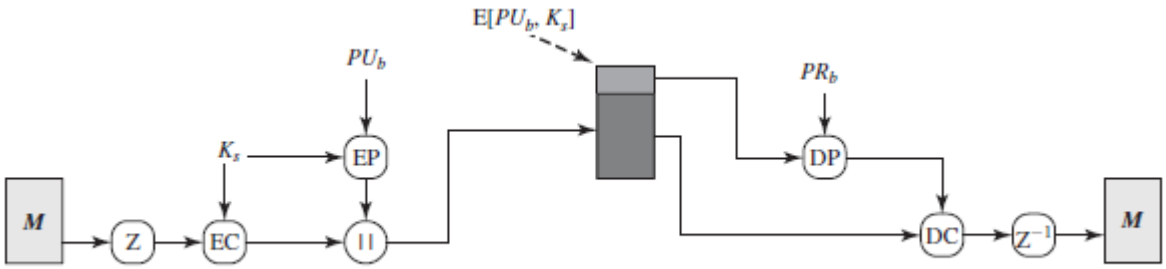
Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

(a) Authentication: The figure shown below express the digital signature service provided by the PGP.



1) The sender creates a message.
2) SHA-1 is used to generate 160-bit hash code of the message.
3) The Hash code is encrypted with RSA/DSS using the sender's private key and the result is appended to the message.
4) The complete message along with hash is then compressed using ZIP.
5) At the receiver the message is unzipped.
6) Then the receiver uses RSA with the Sender's public key to decrypt and recover the hash code.
7) The receiver generated a new hash code for the message and compares it with the decrypted hash code. If the 2 match, the message is accepted.

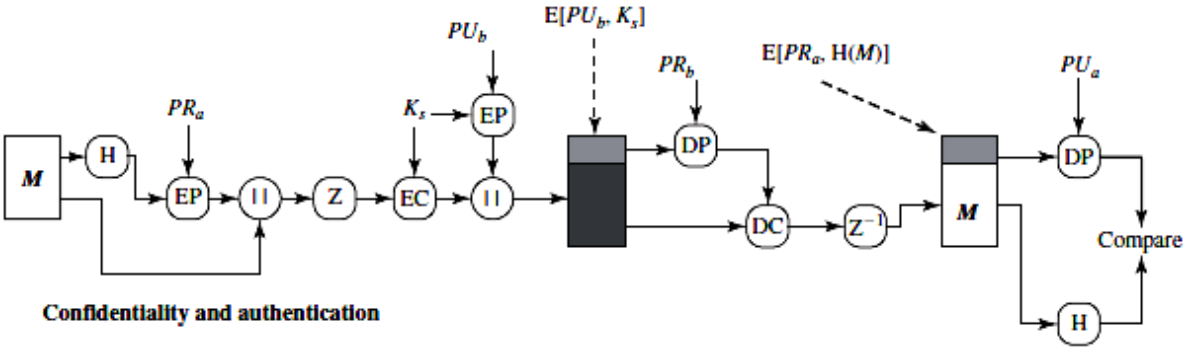
(b) Confidentiality: Another basic service provided by PGP is confidentiality. The figure shown below express the confidentiality services provided by PGP.



Confidentiality only

1) The sender generates a message and a random 128 bit number to be used as a session key.
2) Then the message is compressed.
3) The compressed message is then encrypted using the CAST-128 or IDEA or 3DES with the session key.
4) The session key is encrypted using RSA/ Diffie-Hellman using the recipient's public key and is appended to the message.
5) The receiver uses RSA/Diffie-Hellman to decrypt and recover the session key.
6) The session key is used to decrypt the message.
7) Finally the unzipped to get the actual message.
   - PGP uses a variant of Diffie-Hellman that provides encryption/ decryption known as ElGamal.
   - Symmetric Encryption/Decryption is used because they are eventually faster than public key encryption/decryption.
   - Public key algorithm is used for the session key distribution.

(c) Confidentiality and Authentication: The figure shown below indicates both services operated on the same message.



Confidentiality and authentication

1) First signature is generated and pretended to the message.
2) The Plaintext plus signature is then compressed.
3) The compressed data is encrypted using CAST-128 or IDEA or 3DES using 128 bit session key.
4) The session key is encrypted by using RSA (or ElGamal).
5) The receiver uses either RSA or ElGamal to retrieve the session key.
6) The receiver uses the CAST-128 or IDEA or 3DES decryption algorithm along with the session key.
7) It is then unzipped.
8) The unzipped message is then Processed by the RSA or Diffie- Hellman algorithm with the sender's public key.
9) The receiver generates the new hash by using the SHA-1 and those 2 hashes are compared. If these 2 hashes are equal the message is accepted.

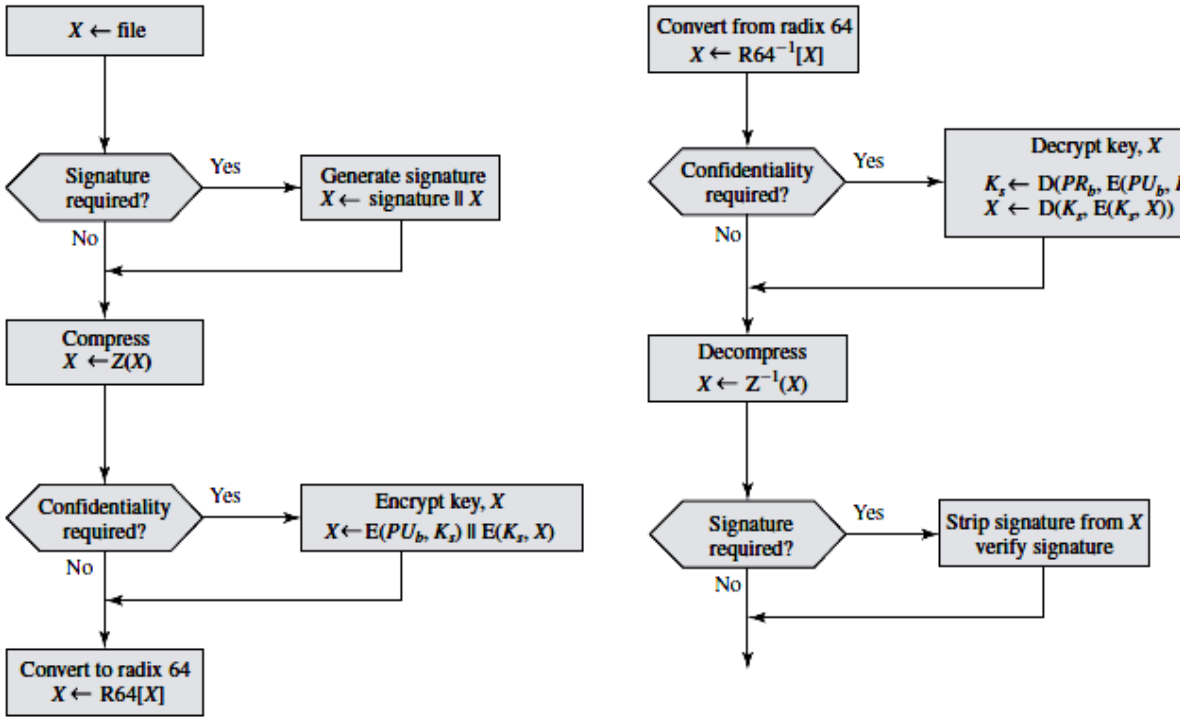
(d) Compression:

1) As a default PGP compresses the message after applying the digital signature but before the encryption
2) It provides the benefit of saving space both for e-mail transmission and for file storage.
3) The compression algorithm is indicated by Z and the decompression algorithm is indicated by Z^{-1}.
4) The signature is generated before compression due to 2 reasons

a) It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. If one signed a compressed document, then it would be necessary either to store the compressed version of the message for future verification or to recompress the message when verification is required.
b) When the compression is applied before signature it may produce different compressed form. Applying hash and signature after compression will create difficulty.

5) Message encryption is applied after compression to strengthen security. Because the compressed message has less redundancy than original plaintext, the cryptanalysis is more difficult.
6) The compression algorithm used is ZIP.

(e) E-mail Compatibility:



(a) Generic transmission diagram (from A)

(b) Generic reception diagram (to B)

Figure Transmission and Reception of PGP Messages

6. (a) What is the difference between transport mode and tunnel mode?

Transport Mode: **[2.5 marks]**

1. Transport mode provides protection for upper layer protocol. That is, transport mode protection extends to the payload.
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. (E.g. a client and a server or 2 workstations).
4. The IP Payload is the data that normally follow in IP header.ESP in transport mode encrypts and optionally authenticates the IP Payload. But not the IP header. AH in transport mode authenticates the IP payload and selected portions of the IP header.

Tunnel Mode: **[2.5 marks]**

1. Tunnel mode provides protection to the entire IP Packet to achieve this after AH or ESP fields are added to the IP Packets. The entire packet plus security fields is treated as the payload of new outer IP packet with new outer IP header.
2. The entire original, inner, packet travels through a tunnel from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Because the original packet is encapsulated, the new, larger packet may have totally different source and destination addresses.

3. Tunnel mode is used when one or both ends use the security gateway such as firewall or router that implements IPsec.
4. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec.
5. **Example how tunnel mode works:**
    a) Host 'A' on a network generates an IP packet with a destination address of host 'B' on other network.
    b) This packet is routed from the originating host to a firewall or secure router at the boundary of A's network. The firewall filters all outgoing packets to determine the need for IPsec processing.
    c) The firewall performs the IPsec processing and encapsulates the packet with an outer IP header. This outer IP header is the IP address of the firewall. Then this packet is routed to B's firewall with intermediate routes examining only the outer IP header.
    d) At B's firewall the outer header is stripped off and the inner packet is delivered to B.
6. ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.
7. AH in tunnel mode authenticates the entire IP packet and selected portion of the outer IP header. Table shown below summarizes the transport and tunnel mode.

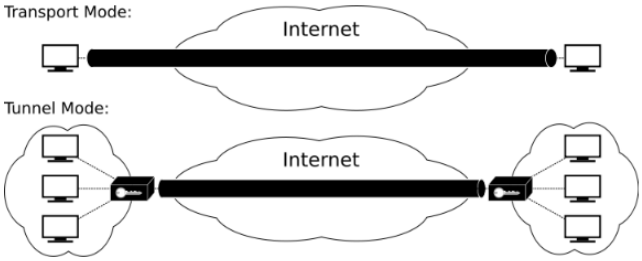


Table Tunnel Mode and Transport Mode Functionality

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

6. (b) What is MIME? Write the header fields defined in MIME?

MULTIPURPOSE INTERNET MAIL EXTENSION: (MIME):[definition 2 marks + Header 3 marks]

1. Multipurpose internet mail extension (MIME) is an extension to the RFC 322.
2. MIME Solves some of the problem appears when simple mail transfer protocol (SMTP) is used.
3. Some of the problems are listed below:
    a) SMTP can't transmit executable files or other binary objects
    b) SMTP can't transmit the text data that includes national language characters.
    c) SMTP server may reject mail message over a certain size.
    d) SMTP gateway translates between ASCII and the character code EBCDIC (Extended Binary Coded Decimal Interchange code); but it don't use consistent mapping results the translation problem.
    e) SMTP doesn't support non-textual data.
    f) Wrapping lines longer than 76 characters.

g) Removal of trailing white spaces

4. MIME intended to resolve these problems.

Five new message header fields are defined, those are

a) MIME version: The parameter value is 1.0 to ensure the standards.

b) Content Type: Describes the data contained in the body with sufficient details.

c) Content Transfer Encoding: Indicate the type of transformation used.

d) Content ID: Used to identify the MIME Entities uniquely.

e) Content Description: A text description of the object with the body, this is useful when the object is not readable (e.g. audio data)

7. What are the different types of security associations explain it with appropriate diagram?

Basic Combinations of Security Associations: **[Explanation 6 marks +Diagram 4 marks]**

a) IPsec architecture lists 4 examples of combinations of SAs.

b) The lower part of each case in the figure represents the physical connectivity of the elements; the upper part represents logical connectivity via one or more nested SAs. Each SA can be either AH or ESP and the mode may be either transport or tunnel.

c) **Case 1**: All security is provided between end systems that implement IPsec. Two end systems for the communication must share the appropriate secret keys. Among the possible combinations are

i. AH in transport mode

ii. ESP in transport mode

iii. ESP followed by AH in transport mode (an ESP SA inside an AH SA)

iv. Any one of a, b, or c inside an AH or ESP in tunnel mode

d) **Case 2:** Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec. This case illustrates simple virtual private network support. Only a single tunnel SA is needed for this case. The tunnel could support AH, ESP, or ESP with the authentication option. Nested tunnels are not required, because the IPsec services apply to the entire inner packet.

e) **Case 3:** This builds on case 2 by adding end-to-end security. Here cases 1 and 2 are allowed. The gateway-to-gateway tunnel provides either authentication, confidentiality, or both. When the gateway-to-gateway tunnel is ESP, it also provides a limited form of traffic confidentiality. Individual hosts can implement any additional IPsec services required.

f) **Case 4:** This provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall. Only tunnel mode is required between the remote host and the firewall. Here one or two SAs may be used between the remote host and the local host.

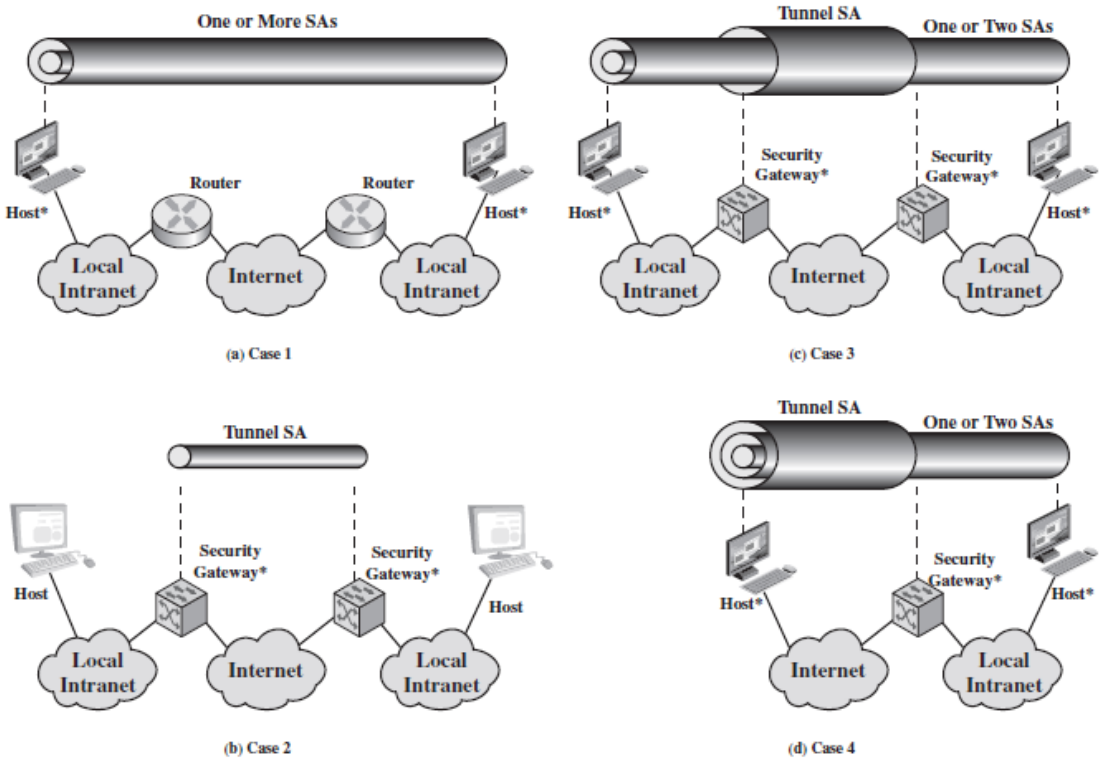


Figure: Basic Combinations of Security Associations

8 (a). Write the application of IPsec with examples.

Application of IPsec: IP sec provides security for the communication across a LAN; across private and public WAN, across Internet. **[5 marks]**

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

b) **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 (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

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

d) **Enhancing electronic commerce security:** Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security.

8. (b) What are the basic approaches to bundling SAs?

Security Association Bundling: Security associations may be combined into **bundles** in two ways: **[5 marks]**

a) **Transport adjacency:** Refers to applying more than one security protocol to the same IP packet without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting won't provide added benefit since the processing is performed at one IPsec instance.

b) **Iterated tunneling:** Refers to the application of multiple layers of security protocols affected through IP tunneling. This approach allows for multiple levels of nesting.