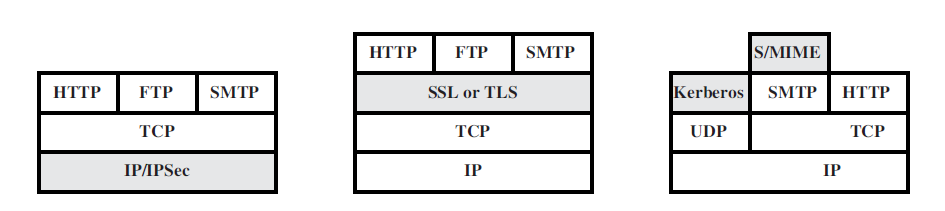
**Unit 4**

1. **Secure Socket Layer Protocol**



1. In the above figure from left to right, the correct order of the shaded levels are  
a) Network level, Application level, Transport level  
b) Application level, Network level, Transport level  
c) Transport level, Application level, Network level  
d) Network level, Transport level, Application level

Answer: d  
Explanation: IP/IPSec is the Network level, SSL or TLS is the Transport Level, Kerberos and S/MIME are the Application level.

2. In the above figure, which of the above shaded block is transparent to end users and applications?  
a) IP/IPSec  
b) SSL  
c) Kerberos  
d) S/MIME

Answer: a  
Explanation: IP/IPSec is the Network layer which is transparent to end users and applications.

3. In terms of Web Security Threats, “Impersonation of another user” is a Passive Attack.  
a) True  
b) False

Answer: b  
Explanation: Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a website that is supposed to be restricted. Active attacks include impersonating another user, altering messages in transit between client and server, altering information on a website.

4. Which one of the following is not a higher –layer SSL protocol?  
a) Alert Protocol  
b) Handshake Protocol  
c) Alarm Protocol  
d) Change Cipher Spec Protocol

Answer: c  
Explanation: Three higher –layer protocols are defined as part of SSL: The Handshake Protocol, The Change Cipher Spec Protocol and The Alert Protocol.

5. In the SSL Protocol, each upper layer message if fragmented into a maximum of \_\_\_\_\_\_\_\_\_\_ bytes.  
a) 216  
b) 232  
c) 214  
d) 212

Answer: c  
Explanation: In the fragmentation process we obtain blocks of 2^14 bytes which is compressed in the next step.

6. The full form of SSL is  
a) Serial Session Layer  
b) Secure Socket Layer  
c) Session Secure Layer  
d) Series Socket Layer

Answer: b  
Explanation: SSL stands for Secure Sockets Layer.

7. Which protocol is used to convey SSL related alerts to the peer entity?  
a) Alert Protocol  
b) Handshake Protocol  
c) Upper-Layer Protocol  
d) Change Cipher Spec Protocol

Answer: a  
Explanation: The Alert protocol is used to convey SSL related alerts to the peer entity.

8. Which protocol consists of only 1 bit?  
a) Alert Protocol  
b) Handshake Protocol  
c) Upper-Layer Protocol  
d) Change Cipher Spec Protocol

Answer: d  
Explanation: The change cipher spec protocol is bit long.

9. Which protocol is used for the purpose of copying the pending state into the current state?  
a) Alert Protocol  
b) Handshake Protocol  
c) Upper-Layer Protocol  
d) Change Cipher Spec Protocol

Answer: d  
Explanation: The Change Cipher Spec Protocol is used for this action.

10. In the alert protocol the first byte takes the value 1 or 2 which corresponds to \_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_ respectively.  
a) Select, Alarm  
b) Alert, Alarm  
c) Warning, Alarm  
d) Warning, Fatal

Answer: d  
Explanation: The first byte takes the value warning(1) or fatal(2) to convey the severity of the message.

**2. Pretty good privacy (PGP), S/MIMIE, SET**

1. Pretty good privacy (PGP) security system uses  
a) Public key cryptosystem  
b) Private key cryptosystem  
c) Public & Private key cryptosystem  
d) None of the mentioned

Answer: c  
Explanation: PGP uses many encryption techniques such as private key cryptosystem and also public key cryptosystem.

2. Data compression includes  
a) Removal of redundant character  
b) Uniform distribution of characters  
c) Removal of redundant character & Uniform distribution of characters  
d) None of the mentioned

Answer: c  
Explanation: Data compression removes redundant character strings in a file and produces a more uniform distribution of characters.

3. PGP offers \_\_\_\_\_ block ciphers for message encryption.  
a) Triple-DES  
b) CAST  
c) IDEA  
d) All of the mentioned

Answer: d  
Explanation: Pretty good privacy security system offers three block ciphers for message encryption – Triple-DES, IDEA and CAST.

4. What is the key size allowed in PGP?  
a) 1024-1056  
b) 1024-4056  
c) 1024-4096  
d) 1024-2048

Answer: c  
Explanation: Pretty good privacy security system allows 1024 to 4096 bits of key size.

5. Which of the following is not a secured mail transferring methodology?  
a) POP3  
b) SSMTP  
c) Mail using PGP  
d) S/MIME

Answer: a  
Explanation: POP (Post Office Protocol) is a simple protocol which fetches the updated mail stored for you by the server. S/MIME (Secure/Multipurpose Internet Mail Extensions), SSMTP (Secure-Simple Mail Transfer Protocol), and PGP (Pretty Good Privacy) are examples of protocols and methods for secure mailing.

6. HTTPS is abbreviated as \_\_\_\_\_\_\_\_\_  
a) Hypertexts Transfer Protocol Secured  
b) Secured Hyper Text Transfer Protocol  
c) Hyperlinked Text Transfer Protocol Secured  
d) Hyper Text Transfer Protocol Secure

Answer: d  
Explanation: Hyper Text Transfer Protocol Secure (HTTPS) is a security protocol which maintains security when data is sent from browser to server and vice versa. It denotes that all communication setup between the browser and the server is encrypted.

7. SSL primarily focuses on \_\_\_\_\_\_\_  
a) integrity and authenticity  
b) integrity and non-repudiation  
c) authenticity and privacy  
d) confidentiality and integrity

Answer: a  
Explanation: SSL primarily focuses on maintaining the integrity of the data. Also, it maintains authenticity which helps the customers feel secure to communicate over the internet.

8. In SSL, what is used for authenticating a message?  
a) MAC (Message Access Code)  
b) MAC (Message Authentication Code)  
c) MAC (Machine Authentication Code)  
d) MAC (Machine Access Code)

Answer: b  
Explanation: For authenticating in SSL, a short message known as MAC (Message Authentication Code) is used for authenticating a message; where both the sender & the receiver need to implement the same key in order to start communicating.

9. \_\_\_\_\_\_\_\_\_\_ is used for encrypting data at network level.  
a) IPSec  
b) HTTPS  
c) SMTP  
d) S/MIME

Answer: a  
Explanation: IPSec (Secure Internet Protocol) is used for securing data at the network level by using 3 different protocols. These are Encapsulating Secure Payload (ESP), Authentication Header, and Internet Key Exchange (IKE).

10. S/MIME is abbreviated as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
a) Secure/Multimedia Internet Mailing Extensions  
b) Secure/Multipurpose Internet Mailing Extensions  
c) Secure/Multimedia Internet Mail Extensions  
d) Secure/Multipurpose Internet Mail Extensions

Answer: d  
Explanation: Secure/Multipurpose Internet Mail Extensions is the most popular protocol used to send encrypted messages that are digitally signed. In this protocol, the encryption is done with a digital sign in them.

11. S/MIME stands for \_\_\_\_\_\_\_\_\_\_\_\_.

a. standard multipurpose internet mail extensions.

b. secure multipurpose internet mail extensions.

c. secure multipurpose international mail extensions.

d. standard multipurpose international mail extensions.

Answer: B.

12. \_\_\_\_\_\_\_\_\_ uniquely identifies the MIME entities uniquely with reference to multiple

contexts.

a. Content description.

b. Content -id.

c. Content type.

d. Content transfer encoding.

Answer: B.

13. The processed S/MIME along with security related data is called as \_\_\_\_\_\_\_\_.

a. public key cryptography standard.

b. private key cryptography standard.

c. S/MIME.

d. MIME.

Answer: A.

14. In S/MIME,MLA stands for \_\_\_\_\_\_\_\_\_\_.

a. mailing list agent.

b. multipurpose list agent.

c. mail lock agent.

d. message link agent.

Answer: A.

15. The cryptography algorithms used in S/MIME are \_\_\_\_\_\_\_\_\_.

a. IDEA.

b. RC4.

c. RSA,DES-3.

d. RC5.

Answer: C.

16. The \_\_\_\_\_\_\_\_\_\_ acts as financial institutions who provides a payment card to a card

holder.

a. payment gateway.

b. card holder.

c. acquirer.

d. issuer.

Answer: D.

17. Who will be responsible for processing the payment from the customer’s account to

the merchant account?

a. Acquirer.

b. Merchant.

c. Issuer.

d. Payment gateway.

Answer: D.

18. The cardholder combines the PIMD and OIMD and hashes them together to form

\_\_\_\_\_\_\_\_.

a. OPMD.

b. POMD.

c. MD.

d. DS.

Answer: B.

19. Which process will ensure that the issues of the credit card is an approved

transactions?

a. Payment capture.

b. Payment authorization.

c. Purchase request.

d. Purchase reply.

Answer: B.

20. \_\_\_\_\_\_\_\_\_ is used for hiding the payment information from the merchant.

a. SET.

b. SSL.

c. SHTTP.

d. TSP.

Answer: A.

**3.IPSEC**

1. IPSec is designed to provide security at the \_\_\_\_\_\_\_\_\_  
a) Transport layer  
b) Network layer  
c) Application layer  
d) Session layer

Answer: b  
Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. In the TCP/IP model, it provides security at the IP layer i.e. the network layer.

2. In tunnel mode, IPSec protects the \_\_\_\_\_\_  
a) Entire IP packet  
b) IP header  
c) IP payload  
d) IP trailer

Answer: a  
Explanation: In the tunnel mode, IPSec adds control bits into the packets to encrypt the entire packet between the IPSec endpoints. Using encryption, it provides secure communication between the two endpoints.

3. Which component is included in IP security?  
a) Authentication Header (AH)  
b) Encapsulating Security Payload (ESP)  
c) Internet key Exchange (IKE)  
d) All of the mentioned

Answer: d  
Explanation: AH ensures that there is no retransmission of data from an unauthorized source, and protects against data tampering. ESP provides with content protection and ensures that there is integrity and confidentiality for the message. IKE is used to make sure that only the intended sender and receiver can access the message.

4. Pretty good privacy (PGP) is used in \_\_\_\_\_\_  
a) Browser security  
b) Email security  
c) FTP security  
d) WiFi security

Answer: b  
Explanation: PGP is an encryption method used in e-mail security to encrypt and decrypt the content of an e-mail transmitted over the internet. It makes sure that the message cannot be stolen by other unauthorized users.

5. PGP encrypts data by using a block cipher called \_\_\_\_\_\_  
a) International data encryption algorithm  
b) Private data encryption algorithm  
c) Internet data encryption algorithm  
d) Local data encryption algorithm

Answer: a  
Explanation: The IDEA was designed in 1991 by Xuejia Lai and James Massey. Before IDEA, PGP used the cipher method BassOmatic.

**VPN**

1. A \_\_\_\_\_\_\_\_\_\_\_ is an extension of an enterprise’s private intranet across a public network such as the internet, creating a secure private connection.  
a) VNP  
b) VPN  
c) VSN  
d) VSPN

Answer: b  
Explanation: VPN provides enhanced security and online anonymity to users on the internet. It is also used to unblock websites that are unavailable in certain regions.

2. When were VPNs introduced into the commercial world?  
a) Early 80’s  
b) Late 80’s  
c) Early 90’s  
d) Late 90’s

Answer: d  
Explanation: VPNs were first introduced in the year 1996. Then as the internet started to get popularized, the need for connection security increased. VPN was a great solution to this, and that’s when VPNs were implemented in the commercial world.

3. What protocol is NOT used in the operation of a VPN?  
a) PPTP  
b) IPsec  
c) YMUM  
d) L2TP

Answer: c  
Explanation: PPTP is a tunneling protocol which was initially used for the creation of VPNs. IPSec is used in encrypting the traffic flowing in the VPN. L2TP is used to tunnel all the L2 traffic on the VPN.

4. Which of the following statements is NOT true concerning VPNs?  
a) Financially rewarding compared to leased lines  
b) Allows remote workers to access corporate data  
c) Allows LAN-to-LAN connectivity over public networks  
d) Is the backbone of the Internet

Answer: d  
Explanation: VPNs are not the backbone of the Internet as they are just a method to create private intranets on the internet. They are used for enhancing the connection security for the users.

5. Traffic in a VPN is NOT \_\_\_\_\_\_\_\_\_\_\_\_  
a) Invisible from public networks  
b) Logically separated from other traffic  
c) Accessible from unauthorized public networks  
d) Restricted to a single protocol in IPsec

Answer: c  
Explanation: Traffic in a VPN is not accessible from any unauthorized public networks because it is secured with the masking IP address. This provides the benefit of access to blocked resources to the users.

6. VPNs are financially speaking \_\_\_\_\_\_\_\_\_\_  
a) Always more expensive than leased lines  
b) Always cheaper than leased lines  
c) Usually cheaper than leased lines  
d) Usually more expensive than leased lines

7. Which layer 3 protocols can be transmitted over an L2TP VPN?  
a) Only IP  
b) Only IPX  
c) Only ICMP  
d) IP and IPX

Answer: d  
Explanation: L2TP stands for Layer 2 Tunneling Protocol. It is used to tunnel all the L2 traffic on an IP network and is able to transmit network layer’s IP and IPX protocol data.

8. ESP (Encapsulating Security Protocol) is defined in which of the following standards?  
a) IPsec  
b) PPTP  
c) PPP  
d) L2TP

Answer: a  
Explanation: ESP is a security component of IPSec. ESP provides content protection and ensures that there is integrity and confidentiality of the message. The other security components of IPSec are Authentication Header and Internet Key Exchange.

9. L2F was developed by which company?  
a) Microsoft  
b) Cisco  
c) Blizzard Entertainment  
d) IETF

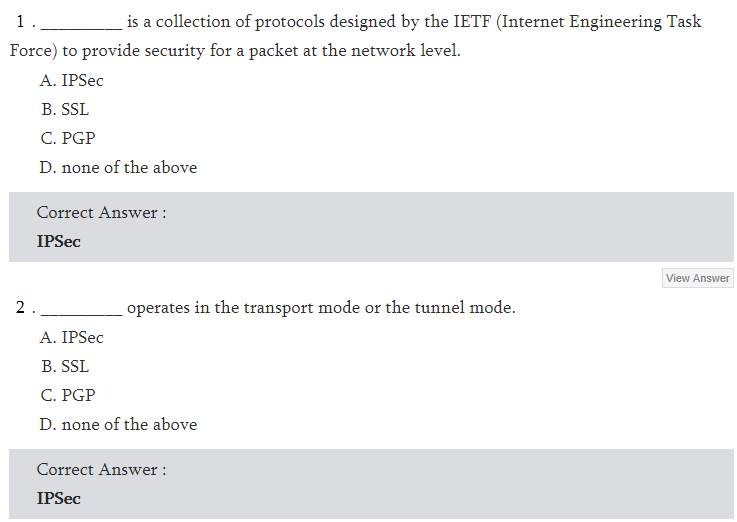
Answer: b  
Explanation: L2F stands for Layer 2 Forwarding protocol. It was designed by Cisco to tunnel PPP traffic, helping create VPNs over the internet.

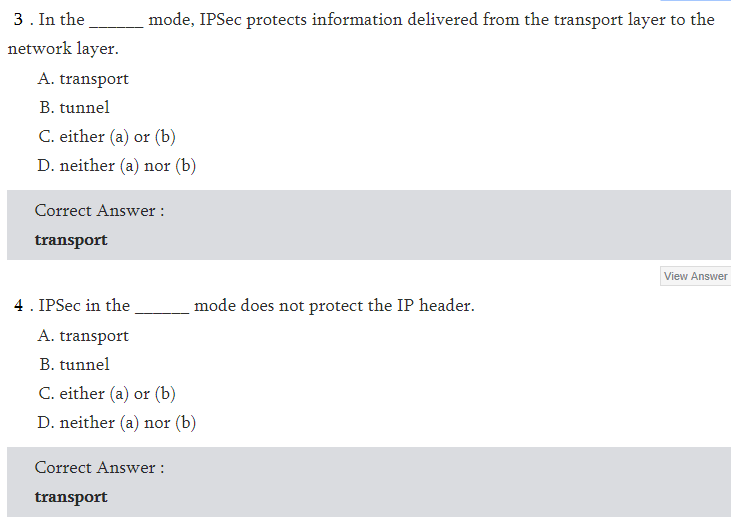
10. Which layer of the OSI reference model does PPTP work at?  
a) Layer 1  
b) Layer 2  
c) Layer 3  
d) Layer 4

Answer: b  
Explanation: PPTP stands for Point-to-Point Tunneling Protocol. PPTP is a tunneling protocol that was primitively used to create VPNs. It is no longer used for VPNs due to the lack of security it provides.

11. Which layer of the OSI reference model does IPsec work at?  
a) Layer 1  
b) Layer 2  
c) Layer 3  
d) Layer 4

Answer: c  
Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. It operates in the network layer.





“I