CHAPTER 32 : Security In the Internet

Solutions to Selected Review Questions

Review Questions

1. A ***session*** between two systems is an association that can last for a long time; a ***connection*** can be established and broken several times during a session. Some of the security parameters are created during the session establishment and are in effect until the session is terminated. Some of the security parameters must be recreated (or occasionally resumed) for each connection.

2. A ***VPN*** is a technology that allows an organization to use the global Internet yet safely maintain private internal communication.

3. Either ***AH*** or ***ESP*** is needed for IP security. ESP, with greater functionality than AH, was developed after AH was already in use.

4. Two types of firewalls discussed in this chapter are ***packet-filter firewall*** and ***proxy-based firewall***.

5. The ***Handshake Protocol*** establishes a cipher set and provides keys and security parameters. It also authenticates the server to the client and the client to the server, if needed.

6. The ***Encapsulating Security Payload (ESP)*** protocol adds an ***ESP header***, ***ESP trailer***, and the ***digest***. The ESP header contains the security parameter index and the sequence number fields. The ESP trailer contains the padding, the padding length, and the next header fields. Note that the ***digest*** is a field separate from the header or trailer.

7. In ***PGP***, the ***security parameters*** need to be sent with the message because e-mail is a one-time activity, in which the sender and receiver cannot agree on the security parameters to be used before sending the message.

8. The ***Record Protocol*** carries messages from the upper layer. The message is fragmented and optionally compressed; a MAC is added to the compressed message by using the negotiated hash algorithm. The compressed fragment and the MAC are encrypted by using the negotiated encryption algorithm. Finally, the SSL header is added to the encrypted message.

9. ***LANs*** on a fully private internet can communicate through ***routers*** and ***leased lines***.

10. ***IPSec*** needs a set of security parameters before it can be operative. In IPSec, the establishment of the security parameters is done via a mechanism called ***security association (SA)***.

11. The two protocols defined by IPSec for exchanging datagrams are ***Authentication Header (AH)*** and ***Encapsulating Security Payload*** (ESP).

12. A ***firewall*** is a security mechanism that stands between the global Internet and a network. A firewall selectively filters packets.

13. One of the protocols designed to provide security for email is ***Pretty Good Privacy (PGP)***. ***PGP*** is designed to create authenticated and confidential e-mails.

14. The ***Authentication Header (AH)*** protocol adds an ***AH header*** that contains next header, payload length, security parameter index, sequence number, and digest fields. Note that the ***digest*** is part of the AH header.

15. ***SSL*** uses two protocols for this purpose: the ***Handshake Protocol*** and ***ChangeCipherSpecProtocol***.

16. The two dominant protocols for providing security at the transport layer are the ***Secure Sockets Layer (SSL)*** Protocol and the ***Transport Layer Security (TLS)*** Protocol. The latter is actually an IETF version of the former.

17. A set of ***security parameters*** between any two entities is created using the ***security association***. Security association uses three protocols: ***IKE***, ***Oakley***, and ***SKEME*** to create a security association between two parties or a security association database between a group of users.

18. The ***Internet Key Exchange (IKE)*** is a protocol designed to create both inbound and outbound security associations in SADBs. ***IKE*** is a complex protocol based on three other protocols: ***Oakley***, ***SKEME***, and ***ISAKMP***.