CHAPTER 32

PRACTICE SET

Questions

Q32-1. 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.

Q32-2. Two types of firewalls discussed in this chapter are *packet-filter firewall* and *proxy-based firewall*.

Q32-3. The two protocols defined by IPSec for exchanging datagrams are *Authentication Header (AH)* and *Encapsulating Security Payload (ESP)*.

Q32-4. 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.

Q32-5. 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)*.

Q32-6. LANs on a fully private internet can communicate through routers and leased lines.

Q32-7. 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.

Q32-8. 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.

Q32-9. 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.

Q32-10. 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.

Q32-11. A *firewall* is a security mechanism that stands between the global Internet and a network. A firewall selectively filters packets.

Q32-12. SSL uses two protocols for this purpose: the *Handshake Protocol* and *ChangeCipherSpec Protocol*.

Q32-13. A *VPN* is a virtual network that uses VPN technology.The technology allows an organization to use the global Internet yet safely maintain private internal communication.

Q32-14. 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.

Q32-15. 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.

Q32-16. Either AH or ESP is needed for IP security. ESP, with greater functionality than AH, was developed after AH was already in use.

Q32-17. 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.

Q32-18. 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.

Problems

P32-1. In e-mail communication, there is no virtual connection between the two parties. Each e-mail is a unidirectional communication between the sender and receiver. This means that there cannot be entity authentication in PGP or in S/ MIME. When we talk about authentication in PGP or S/MIME, we mean message authentication.

P32-2. One advantage of PGP is the way it creates a web of trust among a group of people that need to continuously exchange e-mails between themselves. The disadvantage is that it takes a long time for someone out of the group to obtain the trust of the group. The advantage of S/MIME is that anyone in the world can send a secure e-mail to anyone else in the world as long as the sender can hold the certificate to prove its identity. The disadvantage is that the senders need to get these certificates. In other words, PGP and S/MIME are designed for two different purposes: PGP is convenient for e-mail exchange inside a group; S/MIME is convenient for e-mail exchange between any two persons in the world.

P32-3. When IPSec is used in the transport mode, two parties need to first create cryptographic secrets between themselves before exchanging secure data. This cannot be done using the connectionless service provided by IP. The two parties need to create a virtual connection-oriented service between themselves over the services provided by IP. This is done using the Security Association (SA) described in the text.

P32-4. SSL provides both entity and message authentication. Two entities are authenticated for each other using the handshake protocol. The record protocol provides message authentication when it encapsulates messages from the application layer.

P32-5. Although it is possible to create an SA permanently, it is strongly discouraged because of the leak of security parameters. With the passage of time, Eve may find the secrets between Alice and Bob and misuse them.

P32-6. Alice creates the session key. She uses the session key to encrypt the message. She encrypts the session key with Bob's public key. Alice sends the encrypted message and the encrypted session key to Bob.

P32-7. The handshake protocol in SSL should start its function after the three-way handshaking in TCP because the handshaking protocol in SSL does not create a connection; it uses the connection established by TCP to exchange security parameters.

P32-8. Alice uses an *authenticatedData* object. She randomly creates a session key. She then encrypts the session key with Bob's public key. Alice now creates a MAC from the message hash and the secret key. Alice now sends the MAC, her public-key certificate (in case Bob needs to respond), the name of the algorithm used for creating the MAC, and the encrypted session key used to create the MAC. Alice also sends the message. The whole is referred to as the *authenticatedData.* (See Figure 32.31 in the book.)

P32-9. Alice creates a message digest from the content. Alice then sends the digest, the hash algorithm, and the content. The whole is referred to as *digestedData* object.

P32-10. SSL cannot be used with UDP because UDP does not create a connection-oriented service, which is required for the operation of SSL. SSL can be used with a connection-oriented transport-layer protocol such as TCP.

P32-11. Alice creates a message digest and signs it with her private key. She then sends the message and the signed digest.

P32-12. IPSec provides both message authentication and entity authentication (see Table 10.1 in the text). At the beginning of each association, two parties are authenticated for each other based on their IP addresses. During data exchange, each packet is also authenticated.

P32-13. Alice uses an *envelopedData*. She creates a random number as the session key. She then encrypts the session key with Bob's public key. The message is encrypted with the session key.

P32-14. Both parties that use PGP or S/MIME need to agree about the list of predefined cryptography algorithms. The sender of the e-mail defines the algorithms used for each purpose (confidentiality, integrity, and message authentication); the receiver needs to use those algorithms to be able to read the e-mail.

P32-15. An SA provides two services for IPSec: it creates a virtual connection and establishes security parameters between the two parties. The first service is not needed in the case of SSL because SSL runs over TCP, which is a connection-oriented protocol. The second service of SA is provided by the handshake protocol in SSL.

P32-16. Only applications that can create a session can use the service of SSL/TLS. There is no session in an e-mail. Alice sends an e-mail to Bob without creating a session.