CHAPTER 32

PRACTICE SET

Questions

Q32-1. 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)*.

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

Q32-5. 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.

Q32-7. 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.

Q32-9. 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.

Q32-11. 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.

Q32-13. 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.

Q32-15. A *firewall* is a security mechanism that stands between the global Internet and a network. A firewall selectively filters packets.

Q32-17. 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.

Problems

P32-1. 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.

P32-3. 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.

P32-5. 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.

P32-7. 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.

P32-9. Alice creates a message digest and signs it with her private key. She then sends the message and the signed digest.

P32-11. 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.

P32-13. 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.

P32-15. 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.