CHAPTER 30

Internet Security

Exercises

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.

3. SSL provides both entity and message authentications. 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.

5. 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, authentication, and so on); the receiver needs to use those algorithm to be able to read the e-mail.

7. 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.

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