CHAPTER 32

Security In the Internet

Solutions to Odd-Numbered Review Questions and Exercises

Review Questions

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)***.

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

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.

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.

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.

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.

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.

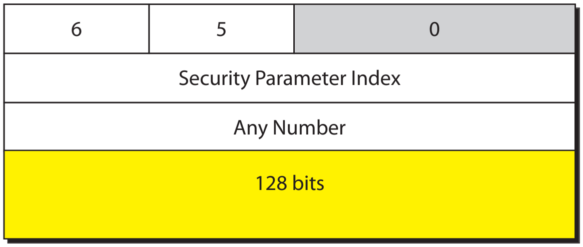
15. A ***firewall*** is a security mechanism that stands between the global Internet and a network. A firewall selectively filters packets.

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

Exercises

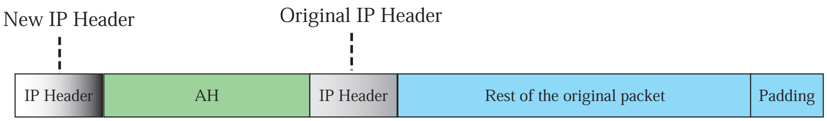
19. The only fields we can fill are the next header (assuming the packet encapsulates TCP) and the length field. The sequence number can be any number. Note that the length field defines the number of 32-bit words minus 2. See Figure 32.1.

Figure 32.1 *Solution to Exercise 19*



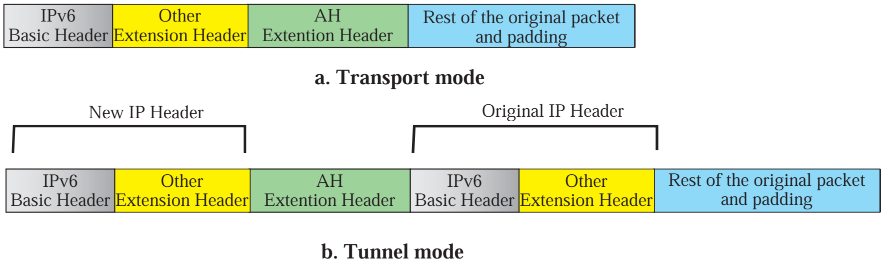
21. See Figure 32.2.

Figure 32.2 *Solution to Exercise 21*



23. See Figure 32.3.

Figure 32.3 *Solution to Exercise 23*



25. ***IPSec*** uses the services of IKE to create a security association that includes session keys. However, this does not start from scratch. Some kind of secret needs to exist between the two parties. In one of the methods used in IKE, the assumption is that

there is a ***shared secret key*** between the two parties. In this case, a ***KDC*** can be used to create this shared secret key.

27. Some ***SSL*** cipher suites need to use shared session keys. However, these session keys are created during hand-shaking. There is no need for a ***KDC***.

29. One of the purposes of ***PGP*** is to free the sender of the message from using a ***KDC***. In PGP, the session key is created and encrypted with the public key established between the sender and the receiver.

31. ***IPSec*** uses IKE to create security parameters. IKE has defined several methods to do so. Each method uses a different set of ciphers to accomplish its task However, the list of ciphers for each method is pre-defined. Although the two parties can choose any of the methods during negotiation, the cipher used for that particular method is predefined. In other words, we can say that IPSec has a list of method suites, but not a cipher suite.