CHAPTER 32 (corrisponde al cap. 30 italiano)

Security In the Internet

Solutions to 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)***.
2. 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.
3. The two protocols defined by IPSec for exchanging datagrams are ***Authentication Header (AH)*** and ***Encapsulating Security Payload*** (ESP).
4. 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.
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.
6. Either ***AH*** or ***ESP*** is needed for IP security. ESP, with greater functionality than AH, was developed after AH was already in use.
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.
8. 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***
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

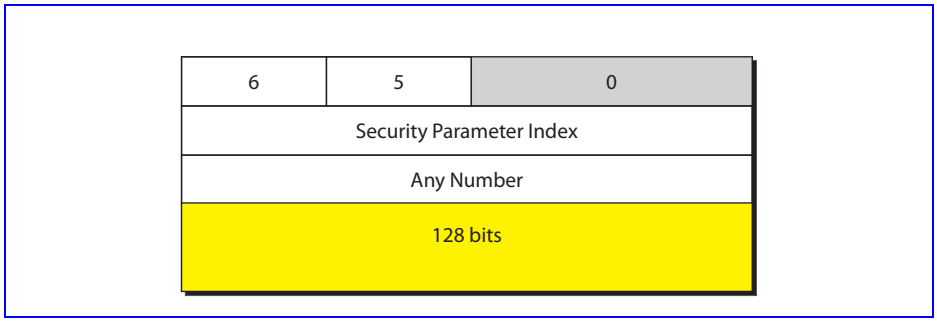
effect until the session is terminated. Some of the security parameters must be recreated (or occasionally resumed) for each connection.

10. ***SSL*** uses two protocols for this purpose: the ***Handshake Protocol*** and ***ChangeCipherSpec Protocol***.
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.
12. 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.
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.
14. 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.
15. A ***firewall*** is a security mechanism that stands between the global Internet and a network. A firewall selectively filters packets.
16. Two types of firewalls discussed in this chapter are ***packet-filter firewall*** and ***proxy-based firewall***.
17. A ***VPN*** is a technology that allows an organization to use the global Internet yet safely maintain private internal communication.
18. ***LANs*** on a fully private internet can communicate through ***routers*** and ***leased lines***.

Exercises

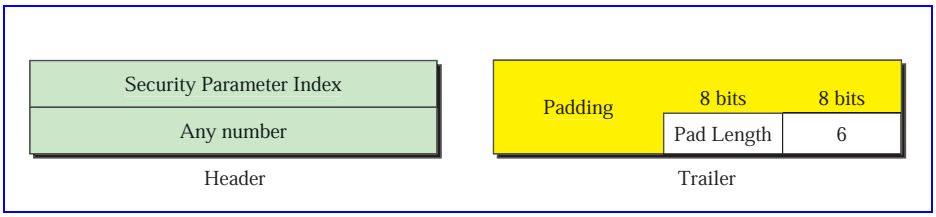
19. The only fields we can fill are the next header (assuming the packet encapsulates TCP) and the length field. The sequence number can be any number. Note that the length field defines the number of 32-bit words minus 2. See Figure 32.1.

Figure 32.1 *Solution to Exercise 19*



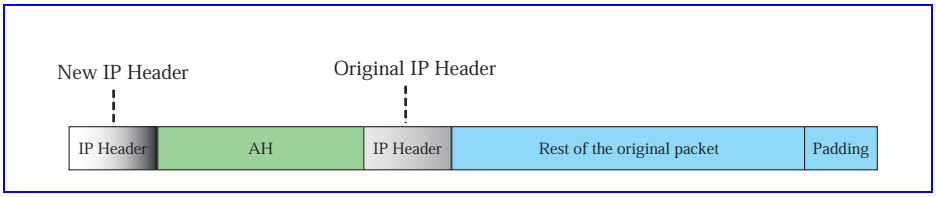
20. The only field we can fill is the next field assuming the packet carries a TCP segment. See Figure 32.2.

Figure 32.2 *Solution to Exercise 20*



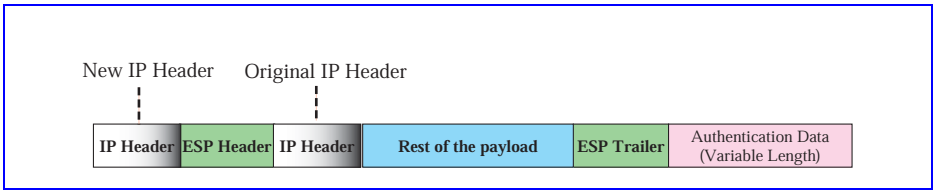
21. See Figure 32.3.

Figure 32.3 *Solution to Exercise 21*



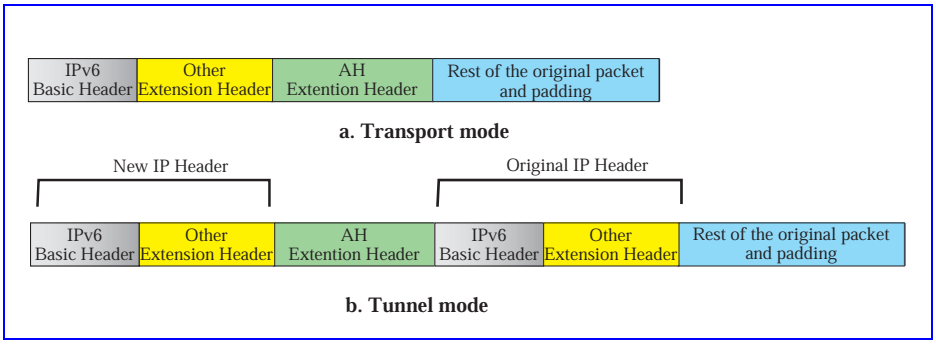
22. See Figure 32.4.

Figure 32.4 *Solution to Exercise 22*



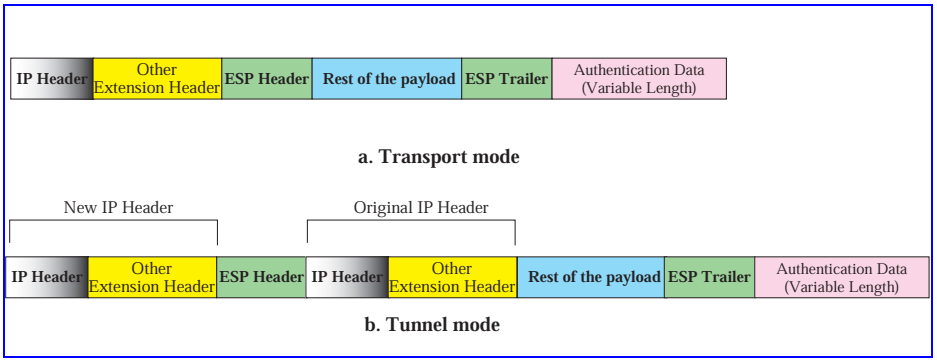
23. See Figure 32.5.

Figure 32.5 *Solution to Exercise 23*



24. See Figure 32.6.

Figure 32.6 *Solution to Exercise 24*



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.
26. ***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 most methods used by IKE, the assumption is that there are some ***public keys*** established between the two parties. In this case, a ***CA*** can be used to create certified public keys.
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***.
28. Some protocols used for key-exchange and authentication require that there should be ***established certified public keys*** between the two parties. An ***AC*** can be used for this purpose.
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.
30. Although ***PGP*** needs to use certified public keys for its operation, it normally does not use the services of a ***CA***. The ***web of trust*** created between the group of people provides the public and private key rings.
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.
32. ***PGP*** creates security parameters for each message sent. Although the sender of the message can choose an encryption/decryption algorithm from the predefined list of these algorithms and the sender can choose an authentication algorithm from

another predefined list of algorithms, we cannot say that PGP is using a ciphersuite in the sense that SSL uses a cipher suite. In SSL, a suite defines a package that contains all the protocols involved; in PGP a sender can choose any protocol from either list and combine them.