CHAPTER 15

Key Management

(Solution to Odd-Numbered Problems)

Review Questions

1. The following shows the main duties.

a. KDC establishes a shared secret key between itself and each newly joined member.

b. KDC accepts requests from members who wants to establish a session key between themselves and other members.

c. KDC checks the willingness of members for establishing session keys.

d. KDC creates a session key and sends it to two parties who want to use it.

3. Kerberos is a popular authentication protocol, and at the same time a KDC. Three servers are involved in the Kerberos protocol: an authentication server (AS), a ticket-granting server (TGS), and a real (data) server that provides services to others. AS is the KDC. TGS issues a ticket for the real server (Bob) and provides the session key. The real server provides services.

5. Man-in-the-middle attack is an attack on the Diffie-Hellman protocol, in which Eve can fool Alice and Bob by creating two keys: one between herself and Alice, and another between herself and Bob.

7. A certification authority (CA), is a federal or state organization that binds a public key to an entity and issues a certificate.

9. Public-Key Infrastructure (PKI), created by the Internet Engineering Task Force, is a model for creating, distributing, and revoking certificates based on the X.509.

Exercises

11. In this case, Alice can access the ticket, change the session key, and send the altered session key to Bob. In other words, Alice can create the session key instead KDC; the role of KDC in authentication is totally deleted in this case.

13.

a. Alice is authenticated by KDC, because only Alice can decrypt the message sent in step 2.

b. KDC is an authorized and well-know entity. The whole assumption is that Alice trusts KDC.

c. KDC is an authorized and well-know entity. The whole assumption is that Bob also trusts KDC.

d. Alice is authenticated to KDC. KDC is authenticated to Bob. Therefore, Alice is authenticated to Bob.

e. Bob is authenticated to KDC. KDC is authenticated to Alice. Therefore, Bob is authenticated to Alice.

15. There is one flaw in the Needham Schroeder protocol (discovered by Denning and Sacco), which is often referred to as *known-session-key attack*. Eve records the exchanges in a session between Alice and Bob. If is somehow successful to obtain the session key, K_{AB}, Eve now launches a new session starting with the third exchange; she resends the ticket to Bob. Bob responds by sending a new nonce, R_B. Eve can decrypt this message (she knows the session key) and obtain R_B. Eve now responds using $R_B - 1$. A session has been created between Bob and Eve. The flaw in the protocol is that there is not a nonce that glues the five exchanges in the session. The first nonce, R_A, is active only for the first two messages; the second nonce, R_B, is active only for the last two messages. Eve can partially replay the second part of the these messages. In Otway-Rees protocol, a third nonce, R, is used to be active during all four exchanges. Eve cannot replay only part of the message.

17.

a. $K = g^{xy} \bmod p = 7^{3 \times 5} \bmod 23 = \mathbf{14}$

b. $R_1 = g^x \bmod p = 7^3 \bmod 23 = 21$ $R_2 = g^y \bmod p = 7^5 \bmod 23 = 17$. Note that $K = {R_2}^x \bmod 23 = 17^3 \bmod 23 = {R_1}^y \bmod 23 = 21^5 \bmod 23 = \mathbf{14}$.

19. Appendix J gives us the first primitive root for a prime less than 1000. According to this appendix, the first primitive root of 53 is $g = 2$. Note that the number of primitive roots are $\phi(\phi(53)) = 24$. We can also find other primitive roots for 53 using one of the procedures given in the literature. The fastest one is when we know the prime factors of $\phi(p) = p - 1$. In this case, g is a primitive root if $g^{(p-1)/q} \bmod p \neq 1$ for all q's where q is a prime factor of $p - 1$. In this case,

$$\phi(p) = \phi(53) = 52 = 2^2 \times 13 \quad \rightarrow \quad q = 2 \text{ and } q = 13$$

We need to check the powers of 52/13 = 4 and 52/2 = 26. We give the proof for the first three primitives.

a. The first primitive is $g = 2$ because $2^4 \bmod 53 = 16 \neq \mathbf{1}$ and $2^{26} \bmod 53 = 52 \neq \mathbf{1}$.

b. The second primitive is $g = 3$ because $3^4 \bmod 53 = 28 \neq \mathbf{1}$ and $3^{26} \bmod 53 = 52 \neq \mathbf{1}$.

c. The third primitive is $g = 5$ because $5^4 \bmod 53 = 42 \neq \mathbf{1}$ and $5^{26} \bmod 53 = 52 \neq \mathbf{1}$.

21. The root certificate offered by some browsers are not hundred percent trustworthy because we are not sure if the browser actually check the validity of this certificates. The browsers belongs to private companies that their certificates are not necessarily endorsed by governmental authorities.