CHAPTER 31 : Network Security

Solutions to Selected Review Questions

Review Questions

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

2. The ***Kerberos authentication server (AS)*** registers each user and grants each user a user identity and a password. The AS issues a session key for use between the sender and the ticket-granting server (TGS).

3. The ***N^2*** problem refers to the large number of keys needed for symmetric key cryptography. For ***N*** people, ***$(N \times (N-1))/2$*** keys are needed, which is proportional to N^2.

4. ***X.509*** is a protocol that describes the certificate in a structural way.

5. A ***nonce*** is a large random number that is used ***only once*** to help distinguish a fresh authentication request from a repeated one.

6. The ***Kerberos TGS*** issues a ticket for the real server and provides the session key between the sender and the receiver.

7. A ***frequently-changed password*** is more secure than a ***fixed password*** but less secure than a ***one-time password.*** However, a one-time password needs more effort from the system and the user. The system needs to check if the password is fresh every time the user tries to use the password. The user needs to be careful not to use the pervious one. A more frequently changed password can be used as an alternative. One solution is that the system initializes the process of changing the password by sending the new password, through a secure channel, and challenging the user to be sure that the right user has received the new password.

8. One way to prevent a ***guessing attack*** on a password is to use long passwords. For example, it is more difficult to guess a 10-digit password than a 4-digit one. Banks recommend that a customer not use a short PIN (a type of password). In particular, they recommend not using an easily-guessed number such as the birth year. Banks also request a change in the PIN when a stolen bank card is reported and replaced by a new one.

9. A ***long password*** is more immune to guessing than a ***short password***. However, a long password is difficult to remember; it is often written somewhere. This may make it easier for the adversary to steal it.

10. Both the ***Needham-Schroeder*** and the ***Otway-Rees*** protocols use a ***KDC*** for user authentication.