Assignment 4

USER AUTHENTICATION PROTOCOLS

TRUE OR FALSE

T F 1. Kerberos provides a trusted third party authentication service that enables clients and servers to establish authenticated communication.

T F 2. Examples of dynamic biometrics include recognition by fingerprint, retina, and face.

T F 3. User authentication is the basis for most types of access control and for user accountability.

T F 4. For network based user authentication the most important methods involve cryptographic keys and something the individual possesses, such as a smart card.

T F 5. There are a variety of problems including dealing with false positives and false negatives, user acceptance, cost, and convenience with respect to biometric authenticators.

T F 6. Any timestamp based procedure must allow for a window of time sufficiently large enough to accommodate network delays yet sufficiently small to minimize the opportunity for attack.

T F 7. An e-mail message should be encrypted such that the mail handling system is not in possession of the decryption key.

T F 8. Because there are no potential delays in the e-mail process timestamps are extremely useful.

T F 9. The operating system cannot enforce access-control policies based on user identity.

T F 10. The security of the Kerberos server should not automatically be assumed but must be guarded carefully by taking precautions such as placing the server in a locked room.

T F 11. Once the server verifies that the user ID in the ticket is the same as the unencrypted user ID in the message it considers the user authenticated and grants the requested service.

Assignment 4

T F 12. It is the ticket that proves the client's identity.

MULTIPLE CHOICE

1. _____ is an authentication service designed for use in a distributed environment.

   A. Kerberos B. PCBC

   C. Toklas D. X.509

2. The _____ approach is unsuitable for a connectionless type of application because it requires the overhead of a handshake before any connectionless transmission, effectively negating the chief characteristic of a connectionless transaction.

   A. timestamp B. backward reply

   C. challenge-response D. replay

3. A common item of authentication information associated with a user is a _____ .

   A. nonce B. timestamp

   C. ticket D. password

4. The overall scheme of Kerberos is that of a trusted third party authentication service that uses a protocol based on a proposal by _____ .

   A. Needham and Schroeder B. Kehn

   C. Denning D. Gong

Assignment 4

5. _____ is a procedure that allows communicating parties to verify that the contents of a received message have not been altered and that the source is authentic.

   A. Identification
   B. Message authentication
   C. Verification
   D. User authentication

6. Presenting an identifier to the security system is the _____ step.

   A. authentication
   B. verification
   C. identification
   D. clarification

7. Presenting or generating authentication information that corroborates the binding between the entity and the identifier is the _____ step.

   A. identification
   B. verification
   C. clarification
   D. authentication

8. The _____ is unsuitable for a connectionless type of application because it requires the overhead of a handshake before any connectionless transmission effectively negating the chief characteristic of a connectionless transaction.

   A. timestamp approach
   B. challenge-response approach
   C. simple replay approach
   D. one-way authentication approach

9. Kerberos relies exclusively on _____ .

   A. symmetric encryption
   B. asymmetric encryption
   C. private key encryption
   D. public key encryption

10. A Kerberos _____ is a set of managed nodes that share the same Kerberos database.

A. realm B. TGS

C. network D. principal

11. In an unprotected network environment any client can apply to any server for service. The obvious security risk of this is _____ .

A. certification B. authentication

C. impersonation D. authorization

12. A service to solve the problem of minimizing the number of times that a user has to enter a password and the risk of an eavesdropper capturing the password and using it is known as the _____ .

A. authentication server B. ticket granting server

C. Kerberos mutual authentication D. PCBC mode

SHORT ANSWER

1. _____ protocols enable communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys.

2. _____ in Greek mythology is a three headed dog with a serpent's tail that guards the entrance of Hades.

3. There are four general means of authenticating a user's identity. They are: something the individual knows, something the individual possesses, something the individual is, and something the individual _____ .

4. To convince the server that a user is authentic, the authentication server creates a _____ that contains the user's ID and network address and the server's ID and sends it back to the client so they can continue the request for service.

5. An authentication process consists of two steps: identification step and _____ step.
6. The first published report on Kerberos listed the following requirements: secure, reliable, scalable and _____ .

7. Examples of something the individual possesses would include cryptographic keys, electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a _____.

8. The _____ is responsible for generating keys to be used for a short time over a connection between two parties and for distributing those keys using the master keys to protect the distribution.

9. A _____ is where an opponent intercepts a message from the sender and replays it later when the timestamp in the message becomes current at the recipient's site.

10. _____ is an authentication service developed as part of Project Athena at MIT.

11. A solution, which eliminates the burden of each server having to confirm the identities of clients who request service, is to use an _____ that knows the passwords of all users and stores these in a centralized database and shares a unique secret key with each server.

12. The ticket granting ticket is encrypted with a secret key known only to the AS and the _____ .

Question 1. When you request a service via Kerberos you are presented with a ticket. What does the ticket contain and how is it used?

Question 2. Does message authentication imply user authentication? Is the opposite true? Explain your answer.

Assignment 4

Question 3. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.
a) John peeks at Alice's password when she is logging in.
b) John logs into Alice's account using Alice's password without Alice knowing about it.
c) There is a process running in Alice's machine, which is updating a database from a remote machine. John interrupts the process, results in inconsistent databases.
d) John copies a file from Alice's account and then deletes the file from Alice's directory.

Question 4. Classify each of the following as a violation of confidentiality, of integrity, of availability, or non-repudiation

a) Alice copies Bob's homework.
b) Alice crashes Bob's operating system.
c) Alice changes the amount on Bob's check from 100 to 1000.
d) Alice does not honor the contract between her and Bob.