**Chapter 15:** **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 means by which a user provides a

claimed identity to the system.

T F 4. Identity federation is in essence an extension of identity

management to multiple security domains.

T F 5. User authentication is the basis for most types of access control

and for user accountability.

T F 6. For network based user authentication the most important

methods involve cryptographic keys and something the individual

possesses, such as a smart card.

T F 7. 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 8. 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 9. An e-mail message should be encrypted such that the mail

handling system is not in possession of the decryption key.

T F 10. Because there are no potential delays in the e-mail process

timestamps are extremely useful.

T F 11. The operating system cannot enforce access-control policies

based on user identity.

T F 12. 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 13. Once the server verifies that the user ID in the ticket is the same as

the unecrypted user ID in the message it considers the user

authenticated and grants the requested service.

T F 14. It is the ticket that proves the client's identity.

T F 15. Identity providers may also assign attributes to users, such as

roles, access permissions, and employee information.

**MULTIPLE CHOICE**

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

A. Kerberos B. PCBC

C. Toklas D. X.509

1. 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

1. A common item of authentication information associated with a user is a \_\_\_\_\_\_\_\_\_\_\_ .

A. nonce B. timestamp

C. ticket D. password

1. 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

1. \_\_\_\_\_\_\_\_ 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

1. Presenting an identifier to the security system is the \_\_\_\_\_\_\_\_\_\_ step.

A. authentication B. verification

C. identification D. clarification

1. 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

1. 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

1. Kerberos relies exclusively on \_\_\_\_\_\_\_\_\_\_ .

A. symmetric encryption B. asymmetric encryption

C. private key encryption D. public key encryption

1. A Kerberos \_\_\_\_\_\_\_\_\_\_ is a set of managed nodes that share the same Kerberos database.

A. realm B. TGS

C. network D. principal

1. 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

1. 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

1. A centralized, automated approach to provide enterprise-wide access to resources by employees and other authorized individuals with a focus of defining an identity for each user, associating attributes with the identity, and enforcing a means by which a user can verify identity is \_\_\_\_\_\_\_\_\_\_ .

A. enterprise management B. identity management

C. federated identity management D. realm management

1. \_\_\_\_\_\_\_\_\_\_ is an extension of identity management to multiple security domains such as autonomous internal business units, external business partners and other third party applications and services with the goal of sharing digital identities so that a user can be authenticated a single time and then access applications and resources across multiple domains.

A. Identity federation B. Kerberos

C. Attribute service D. Data security management

1. The principal underlying standard for federated identity is the \_\_\_\_\_\_\_\_\_\_ which defines the exchange of security information between online business partners.

A. OSAIS B. SAML

C. RBAC D. SFIL

**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. \_\_\_\_\_\_\_\_\_\_\_\_ is a centralized, automated approach to provide enterprise wide access to resources by employees and other authorized individuals.
7. The first published report on Kerberos listed the following requirements: secure, reliable, scalable and \_\_\_\_\_\_\_\_\_\_ .
8. 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 \_\_\_\_\_\_\_\_\_\_ .
9. 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.
10. A \_\_\_\_\_\_\_\_\_\_ attack 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.
11. \_\_\_\_\_\_\_\_\_\_ is an authentication service developed as part of Project Athena at MIT.
12. 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.
13. The ticket granting ticket is encrypted with a secret key known only to the AS and the \_\_\_\_\_\_\_\_\_\_ .
14. Intended to provide an integrity check as part of the encryption operation, encryption in Kerberos Version 4 makes use of a nonstandard mode of DES known as \_\_\_\_\_\_\_\_\_\_\_\_. It has been demonstrated that this mode is vulnerable to an attack involving the interchange of ciphertext blocks.
15. A concept dealing with the use of a common identity management scheme across multiple enterprises and numerous applications and refers to the agreements, standards, and technologies that enable the portability of identities, identity attributes, and entitlements across multiple enterprises and numerous applications and supporting many thousands, even millions, of users is \_\_\_\_\_\_\_\_\_ .