Chapter 3 – User Authentication

TRUE/FALSE QUESTIONS:

T F 1. User authentication is the fundamental building block and the primary line of defense.

T F 2. Identification is the means of establishing the validity of a claimed identity provided by a user.

T F 3. Depending on the details of the overall authentication system, the registration authority issues some sort of electronic credential to the subscriber.

T F 4. Many users choose a password that is too short or too easy to guess.

T F 5. User authentication 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.

T F 6. A good technique for choosing a password is to use the first letter of each word of a phrase.

T F 7. User authentication is the basis for most types of access control and for user accountability.

T F 8. Memory cards store and process data.

T F 9. Depending on the application, user authentication on a biometric system involves either verification or identification.

T F 10. Enrollment creates an association between a user and the user's biometric characteristics.

T F 11. An individual's signature is not unique enough to use in biometric applications.

T F 12. Identifiers should be assigned carefully because authenticated identities are the basis for other security services.

T F 13. A smart card contains an entire microprocessor.

T F 14. Keylogging is a form of host attack.

T F 15. In a biometric scheme some physical characteristic of the individual is mapped into a digital representation.

MULTIPLE CHOICE QUESTIONS:

1. _____ defines user authentication as "the process of verifying an identity claimed by or for a system entity".

   A. RFC 4949 C. RFC 2298

   B. RFC 2493 D. RFC 2328

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

   A. identification step C. verification step

   B. authentication step D. corroboration step

3. Recognition by fingerprint, retina, and face are examples of _____.

   A. face recognition C. dynamic biometrics

   B. static biometrics D. token authentication

4. A _____ is a password guessing program.

   A. password hash C. password cracker

   B. password biometric D. password salt

5. The _____ strategy is when users are told the importance of using hard to guess passwords and provided with guidelines for selecting strong passwords.

   A. reactive password checking C. proactive password checking

   B. computer-generated password D. user education

6. A _____ strategy is one in which the system periodically runs its own password cracker to find guessable passwords.

A. user education
C. proactive password checking
B. reactive password checking
D. computer-generated password

7. The most common means of human-to-human identification are _____.

A. facial characteristics
C. signatures
B. retinal patterns
D. fingerprints

8. _____ systems identify features of the hand, including shape, and lengths and widths of fingers.

A. Signature
C. Hand geometry
B. Fingerprint
D. Palm print

9. Each individual who is to be included in the database of authorized users must first be _____ in the system.

A. verified
C. authenticated
B. identified
D. enrolled

10. To counter threats to remote user authentication, systems generally rely on some form of _____ protocol.

A. eavesdropping
C. Trojan horse
B. challenge-response
D. denial-of-service

11. A _____ is when an adversary attempts to achieve user authentication without access to the remote host or to the intervening communications path.

A. client attack
C. eavesdropping attack
B. host attack
D. Trojan horse attack

12. A _____ is directed at the user file at the host where passwords, token passcodes, or biometric templates are stored.

A. eavesdropping attack
C. denial-of-service attack
B. client attack
D. host attack

13. A _____ attack involves an adversary repeating a previously captured user response.

A. client
C. replay
B. Trojan horse
D. eavesdropping

14. An institution that issues debit cards to cardholders and is responsible for the cardholder's account and authorizing transactions is the _____.

A. cardholder
C. auditor
B. issuer
D. processor

15. _____ allows an issuer to access regional and national networks that connect point of sale devices and bank teller machines worldwide.

A. EFT
C. POS
B. BTM
D. ATF

SHORT ANSWER QUESTIONS:

1. An authentication process consists of the _____ step and the verification step.
2. Voice pattern, handwriting characteristics, and typing rhythm are examples of _____ biometrics.
3. A _____ is a separate file from the user IDs where hashed passwords are kept.
4. With the _____ policy a user is allowed to select their own password, but the system checks to see if the password is allowable.

5. The technique for developing an effective and efficient proactive password checker based on rejecting words on a list is based on the use of a _____ filter.

6. Objects that a user possesses for the purpose of user authentication are called _____

7. Authentication protocols used with smart tokens can be classified into three categories: static, dynamic password generator, and _____.

8. A _____ authentication system attempts to authenticate an individual based on his or her unique physical characteristics.

9. The _____ is the pattern formed by veins beneath the retinal surface.

10. A host generated random number is often called a _____.

11. _____, in the context of passwords, refers to an adversary's attempt to learn the password by observing the user, finding a written copy of the password, or some similar attack that involves the physical proximity of user and adversary.

12. In a _____ attack, an application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric.

13. A _____ attack attempts to disable a user authentication service by flooding the service with numerous authentication attempts.

14. A _____ is an individual to whom a debit card is issued.

15. The _____ step is presenting or generating authentication information that corroborates the binding between the entity and the identifier.

Chapter 3 – User Authentication

Answer Key

TRUE/FALSE QUESTIONS:

1. T
2. T
3. F
4. T
5. F
6. T
7. T
8. F
9. T
10. T
11. F
12. T
13. T
14. F
15. T

Multiple Choice Questions:

1. A
2. C
3. B
4. C
5. D
6. B
7. A
8. C
9. D
10. B
11. A
12. D
13. C
14. B
15. A

Short Answer Questions:

1. identification
2. dynamic
3. shadow password file
4. complex password
5. Bloom
6. tokens
7. challenge-response
8. biometric
9. retinal pattern
10. nonce
11. Eavesdropping
12. Trojan horse
13. denial-of-service
14. cardholder
15. verification