1. An authentication process consists of the identification step and the verification step.

2. Voice pattern, handwriting characteristics, and typing rhythm are examples of dynamic biometrics.

3. A shadow password file is a separate file from the user IDs where hashed passwords are kept.

4. With the proactive password checking strategy 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 bloom filter.

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

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

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

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

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

11. Eavesdropping, 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 Trojan Horse 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 denial-of-service attack attempts to disable a user authentication service by flooding the service with numerous authentication attempts.

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

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