Cryptography and Network Security: Principles and Practice, 6th Edition, by William Stallings

CHAPTER 1: OVERVIEW

TRUE OR FALSE

T F 1. The OSI security architecture provides a systematic framework for defining security attacks, mechanisms, and services.

T F 2. Security attacks are classified as either passive or aggressive.

T F 3. Authentication protocols and encryption algorithms are examples of security mechanisms.

T F 4. The more critical a component or service, the higher the level of required availability.

T F 5. Security services include access control, data confidentiality and data integrity, but do not include authentication.

T F 6. The field of network and Internet security consists of measures to deter, prevent, detect and correct security violations that involve the transmission of information.

T F 7. Patient allergy information is an example of an asset with a high requirement for integrity.

T F 8. The OSI security architecture was not developed as an international standard, therefore causing an obstacle for computer and communication vendors when developing security features.

T F 9. Data origin authentication does not provide protection against the modification of data units.

T F 10. The emphasis in dealing with active attacks is on prevention rather than detection.

T F 11. The connection- oriented integrity service addresses both message stream modification and denial of service.

T F 12. All the techniques for providing security have two components: a security- related transformation on the information to be sent and some secret information shared by the two principals.

T F 13. Information access threats intercept or modify data on behalf of users who should not have access to that data.

T F 14. The data integrity service inserts bits into gaps in a data stream to frustrate traffic analysis attempts.

T F 15. Symmetric encryption is used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords.

MULTIPLE CHOICE

1. _____ is the most common method used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.

   A) Symmetric encryption B) Data integrity algorithms

   C) Asymmetric encryption D) Authentication protocols

2. A common technique for masking contents of messages or other information traffic so that opponents can not extract the information from the message is _____ .

   A) integrity B) encryption

   C) analysis D) masquerade

3. _____ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

   A) Disruption B) Replay

   C) Service denial D) Masquerade

4. The three concepts that form what is often referred to as the CIA triad are _____ . These three concepts embody the fundamental security objectives for both data and for information and computing services.

   A) confidentiality, integrity and availability

   B) communication, integrity and authentication

   C) confidentiality, integrity, access control

   D) communication, information and authenticity

5. A loss of _____ is the unauthorized disclosure of information.

   A) authenticity B) confidentiality

   C) reliability D) integrity

6. Verifying that users are who they say they are and that each input arriving at the system came from a trusted source is _____ .

   A) authenticity B) credibility

   C) accountability D) integrity

7. A _____ level breach of security could cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.

   A) catastrophic B) moderate

   C) low D) high

8. A _____ is any action that compromises the security of information owned by an organization.

   A) security attack B) security service

   C) security alert D) security mechanism

9. A _____ takes place when one entity pretends to be a different entity.

A) replay B) masquerade

C) service denial D) passive attack

10. _____ is the protection of transmitted data from passive attacks.

A) Access control B) Data control

C) Nonrepudiation D) Confidentiality

11. A(n) _____ service is one that protects a system to ensure its availability and addresses the security concerns raised by denial- of- service attacks.

A) replay B) availability

C) masquerade D) integrity

12. _____ threats exploit service flaws in computers to inhibit use by legitimate users.

A) Information access B) Reliability

C) Passive D) Service

13. A(n) _____ is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.

A) threat B) attack

C) risk D) attack vector

14. The protection of the information that might be derived from observation of traffic flows is _____ .

A) connectionless confidentiality B) connection confidentiality

C) traffic- flow confidentiality D) selective- field confidentiality

15. Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery is a(n) _____ .

A) security audit trail B) digital signature

C) encipherment D) authentication exchange

SHORT ANSWER

1. A _____ is any process, or a device incorporating such a process, that is designed to detect, prevent, or recover from a security attack. Examples are encryption algorithms, digital signatures and authentication protocols.

2. An _____ attack attempts to alter system resources or affect their operation.

3. "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources" is the definition of _____ .

4. A loss of _____ is the disruption of access to or use of information or an information system.

5. Irreversible _____ mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

6. In the United States, the release of student grade information is regulated by the _____ .

7. A loss of _____ is the unauthorized modification or destruction of information.

8. A _____ attack attempts to learn or make use of information from the system but does not affect system resources.

9. The _____ service is concerned with assuring the recipient that the message is from the source that it claims to be from. This service must also assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Cryptography and Network Security: Principles and Practice, 6th Edition, by William Stallings

10. Two specific authentication services defined in X.800 are peer entity authentication and _____ authentication.

11. In the context of network security, _____ is the ability to limit and control the access to host systems and applications via communications links.

12. _____ prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message and when a message is received, the sender can prove that the alleged receiver in fact received the message.

13. Viruses and worms are two examples of _____ attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network.

14. An _____ is an assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

15. _____ is the use of a trusted third party to assure certain properties of a data exchange.