**Chapter 1: COMPUTER AND NETWORK SECURITY CONCEPTS**

**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. Thanks to years of research and development, it is now possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions.

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. An attack tree is a branching hierarchical data structure that

 represents a set of potential techniques for exploiting security vulnerabilities.

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

1. 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

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

1. \_\_\_\_\_\_\_\_\_ refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.

A) Layering B) Modularity

C) Encapsulation D) Open design

1. A loss of \_\_\_\_\_\_\_\_\_\_ is the unauthorized disclosure of information.

A) authenticity B) confidentiality

C) reliability D) integrity

1. 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

1. 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

1. 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

1. A \_\_\_\_\_\_\_\_\_\_ takes place when one entity pretends to be a different entity.

A) replay B) masquerade

C) service denial D) passive attack

1. \_\_\_\_\_\_\_\_\_\_ is the protection of transmitted data from passive attacks.

A) Access control B) Data control

C) Nonrepudiation D) Confidentiality

1. 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

1. \_\_\_\_\_\_\_\_\_\_ threats exploit service flaws in computers to inhibit use by legitimate users.

A) Information access B) Reliability

C) Passive D) Service

1. 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

1. 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

1. 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. An \_\_\_\_\_\_\_\_\_ is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.

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.