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

**TRUE OR FALSE**

T F 1. The OSI security architecture focuses on security attacks,

mechanisms, and services.

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

T F 3. Cybersecurity strives to ensure the attainment and maintenance of

the security properties of the organization and users’ assets against relevant security risks in the cyberspace environment.

T F 4. Information security and network security are subsets of

cybersecurity.

T F 5. Data authenticity assures that private or confidential information is

not made available or disclosed to unauthorized individuals.

T F 6. The OSI security architecture focuses on security attacks,

mechanisms, and services.

T F 7. An active attack attempts to alter system resources or affect their

operation.

T F 8. Authentication exchange is the use of a trusted third party to

assure certain properties of a data exchange.

T F 9. A loss of integrity is the unauthorized modification or destruction

of information.

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. The denial of service prevents or inhibits the normal use or

management of communication facilities.

T F 13. Integrity can apply to a stream of messages, a single message, or

selected fields within a message.

T F 14. Passive attacks are very easy to detect because they involve

alteration of the data.

T F 15. Security services implement security policies and are

implemented by security mechanisms.

**MULTIPLE CHOICE**

1. ­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_ is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyberspace environment and organization and users’ assets.

A) Access control B) Data authenticity

C) Cybersecurity D) Authentication

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. \_\_\_\_\_\_\_\_\_ is a branch of mathematics that deals with the transformation of data.

A) Cryptography B) Modularity

C) Encapsulation D) Encryption

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 \_\_\_\_\_\_\_\_\_ is a value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data’s origin and integrity.

A) key exchange B) digital signature

C) message authentication code D) notarization

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. Two types of \_\_\_\_\_\_\_\_\_\_ attacks are the release of message contents and

traffic analysis.

A) information B) eavesdropping

C) service D) passive

1. A(n) \_\_\_\_\_\_\_\_\_\_ is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

A) threat B) attack

C) risk D) attack vector

1. A \_\_\_\_\_\_\_\_\_\_ is a hardware and/or software capability that limits access between a network and device attached to the network, in accordance with a specific security policy.

A) trust model B) cryptographic algorithm

C) firewall D) router

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. The general security objectives of cybersecurity comprise the following: availability; integrity, which may include data authenticity and nonrepudiation; and \_\_\_\_\_\_\_\_\_\_ .
2. A \_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
3. An \_\_\_\_\_\_\_\_\_\_\_ is any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
4. A \_\_\_\_\_\_\_\_\_\_ attack attempts to learn or make use of information from the system but does not affect system resources.
5. The emphasis in dealing with \_\_\_\_\_\_\_\_\_\_ attacks is on prevention rather than detection.
6. Active attacks can be subdivided into four categories: replay, \_\_\_\_\_\_\_\_\_\_ , modification of messages, and denial of service.
7. \_\_\_\_\_\_\_\_\_\_ prevents either sender or receiver from denying a transmitted message.
8. \_\_\_\_\_\_\_\_\_\_ is the property of a system, or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.
9. \_\_\_\_\_\_\_\_\_\_ is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
10. Digital \_\_\_\_\_\_\_\_\_\_ is 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.
11. Cryptographic algorithms can be divided into three categories: keyless, \_\_\_\_\_\_\_\_\_\_ , and two-key.
12. A \_\_\_\_\_\_\_\_\_\_ number generator produces a deterministic sequence of numbers or bits that has the appearance of being a truly random sequence.
13. Encryption algorithms that use a single key are referred to as \_\_\_\_\_\_\_\_\_\_\_ encryption algorithms.
14. \_\_\_\_\_\_\_\_\_\_ is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.
15. \_\_\_\_\_\_\_\_\_\_ is a characteristic of an entity that reflects the degree to which that entity is deserving of trust.