**Chapter 1: introduction**

**TRUE OR FALSE**

T F 1. With the introduction of the computer the need for automated

 tools for protecting files and other information stored on the

 computer became evident.

T F 2. There is a natural tendency on the part of users and system

 managers to perceive little benefit from security investment until a

 security failure occurs.

T F 3. There are clear boundaries between network security and internet

 security.

T F 4. The CIA triad embodies the fundamental security objectives for

 both data and for information and computing services.

T F 5. In developing a particular security mechanism or algorithm one

 must always consider potential attacks on those security features.

T F 6. A loss of confidentiality is the unauthorized modification or

 destruction of information.

T F 7. Patient allergy information is an example of an asset with a

 moderate requirement for integrity.

T F 8. The more critical a component or service, the higher the level of

 availability required.

T F 9. Data origin authentication provides protection against the

 duplication or modification of data units.

T F 10. The emphasis in dealing with passive attacks is on prevention

 rather than detection.

T F 11. Data integrity is the protection of data from unauthorized

 disclosure.

T F 12. Information access threats exploit service flaws in computers to

 inhibit use by legitimate users.

T F 13. Viruses and worms are two examples of software attacks.

T F 14. A connection-oriented integrity service deals with individual

 messages without regard to any larger context and generally

 provides protection against message modification only.

T F 15. Pervasive security mechanisms are not specific to any particular

 OSI security service or protocol layer.

**MULTIPLE CHOICE**

1. \_\_\_\_\_\_\_\_\_ security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information.

A. Computer B. Internet

C. Intranet D. Network

1. \_\_\_\_\_\_\_\_\_\_ is verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

A. Authenticity B. Accountability

C. Integrity   D. Confidentiality

1. \_\_\_\_\_\_\_\_\_\_ assures that systems work promptly and service is not denied to authorized users.

A. Integrity   B. Availability

C. System integrity   D. Data confidentiality

1. \_\_\_\_\_\_\_\_\_\_ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

A. Data confidentiality   B. Availability

C. System integrity   D. Privacy

1. The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity is \_\_\_\_\_\_\_\_\_ .

A. accountability   B. authenticity

C. privacy   D. integrity

1. \_\_\_\_\_\_\_\_\_\_ attacks attempt to alter system resources or affect their operation.

A. Active   B. Release of message content

C. Passive   D. Traffic analysis

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

A. passive attack   B. masquerade

C. modification of message   D. replay

1. X.800 defines \_\_\_\_\_\_\_\_\_ as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

A. replay   B. integrity

C. authenticity   D. security service

1. \_\_\_\_\_\_\_\_\_ is a professional membership society with worldwide organizational and individual membership that provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the IETF and the IAB.

A. ITU-T   B. ISO

C. FIPS   D. ISOC

1. The protection of data from unauthorized disclosure is \_\_\_\_\_\_\_\_\_ .

A. access control   B. authentication

C. data confidentiality   D. nonrepudiation

1. \_\_\_\_\_\_\_\_\_\_ is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation.

A. ISO   B. NIST

C. ITU-T   D. ISOC

1. The prevention of unauthorized use of a resource is \_\_\_\_\_\_\_\_\_\_ .

A. access control   B. authentication

C. data confidentiality   D. nonrepudiation

1. The \_\_\_\_\_\_\_\_\_\_ service addresses the security concerns raised by denial-of-service attacks.

A. event detection   B. integrity

C. availability   D. routing control

1. \_\_\_\_\_\_\_\_\_ is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

A. Notarization   B. Authentication exchange

C. Routing control   D. Traffic padding

1. \_\_\_\_\_\_\_\_\_ is a variety of mechanisms used to assure the integrity of a data unit or stream of data units.

A. Data integrity   B. Authentication exchange

C. Trusted functionality   D. Event detection

**SHORT ANSWER**

1. \_\_\_\_\_\_\_\_\_ is defined as "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".

2. Three key objectives that are at the heart of computer security are: confidentiality, availability, and \_\_\_\_\_\_\_\_\_ .

3. An intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is an \_\_\_\_\_\_\_\_\_\_ .

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

5. \_\_\_\_\_\_\_\_\_\_ is the use of mathematical algorithms to transform data into a form that is not readily intelligible, in which the transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

6. Student grade information is an asset whose confidentiality is considered to be highly important by students and, in the United States, the release of such information is regulated by the \_\_\_\_\_\_\_\_\_\_.

7. A possible danger that might exploit a vulnerability, a \_\_\_\_\_\_\_\_\_ 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.

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

9. The common technique for masking contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message is \_\_\_\_\_\_\_\_\_ .

10. Active attacks can be subdivided into four categories: replay, modification of messages, denial of service, and \_\_\_\_\_\_\_\_\_\_ .

11.  X.800 divides security services into five categories: authentication, access control, nonrepudiation, data integrity and \_\_\_\_\_\_\_\_\_\_ .

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

13. The \_\_\_\_\_\_\_\_\_\_ is a worldwide federation of national standards bodies that promote the development of standardization and related activities with a view to facilitating the international exchange of goods and services and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity.

14. \_\_\_\_\_\_\_\_\_\_ prevents either sender or receiver from denying a transmitted message; 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.

15. A \_\_\_\_\_\_\_\_\_\_ 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.

**Chapter 1: introduction**

**TRUE OR FALSE**

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

**MULTIPLE CHOICE**

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

**SHORT ANSWER**

1. Computer Security
2. integrity
3. attack
4. availability
5. Encipherment
6. Family Educational Rights and Privacy Act (FERPA)
7. threat
8. passive
9. encryption
10. masquerade
11. data confidentiality
12. access control
13. International Organization for Standardization (ISO)
14. Nonrepudiation
15. digital signature