**Quiz #1 Answers**

**CECS 378 – Spring 2021 Cappel**

**Chapter 1 – Computer Systems Overview**

**TRUE/FALSE QUESTIONS:**

T F 1. Threats are attacks carried out.

T F 2. Computer security is protection of the integrity, availability, and confidentiality of

information system resources.

T F 3. Data integrity assures that information and programs are changed only in a specified

and authorized manner.

T F 4. Availability assures that systems works promptly and service is not denied to

authorized users.

T F 5. The “A” in the CIA triad stands for “authenticity”.

T F 6. The more critical a component or service, the higher the level of availability required.

T F 7. Computer security is essentially a battle of wits between a perpetrator who tries to find

holes and the administrator who tries to close them.

T F 8. Security mechanisms typically do not involve more than one particular algorithm or

protocol.

T F 9. Many security administrators view strong security as an impediment to efficient and

user-friendly operation of an information system.

T F 10. In the context of security our concern is with the vulnerabilities of system resources.

T F 11. Hardware is the most vulnerable to attack and the least susceptible to automated

controls.

T F 12. Contingency planning is a functional area that primarily requires computer security

technical measures.

T F 13. X.800 architecture was developed as an international standard and focuses on security

in the context of networks and communications.

T F 14. The first step in devising security services and mechanisms is to develop a security

policy.

T F 15. Assurance is the process of examining a computer product or system with respect to

certain criteria.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_\_\_\_\_ assures that individual’s control or influence what information related to them may be

collected and stored and by whom and to whom that information may be disclosed.

A. Availability B. System Integrity

C. Privacy D. Data Integrity

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

A. System Integrity B. Data Integrity

C. Availability D. Confidentiality

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

A. confidentiality B. integrity

C. authenticity D. availability

4. A \_\_\_\_\_\_\_\_ level breach of security could be expected to have a severe or catastrophic adverse effect on

organizational operations, organizational assets, or individuals.

A. low B. normal

C. moderate D. high

5. A flaw or weakness in a system’s design, implementation, or operation and management that could be

exploited to violate the system’s security policy is a(n) \_\_\_\_\_\_\_\_\_\_.

A. countermeasure B. vulnerability

C. adversary D. risk

6. 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 is a(n) \_\_\_\_\_\_\_\_\_\_.

A. risk B. asset

C. attack D. vulnerability

7. A(n) \_\_\_\_\_\_\_\_\_\_ is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an

attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and

reporting it so that correct action can be taken.

A. attack B. countermeasure

C. adversary D. protocol

8. A(n) \_\_\_\_\_\_\_\_\_ is an attempt to learn or make use of information from the system that does not affect

system resources.

A. passive attack B. inside attack

C. outside attack D. active attack

9. Masquerade, falsification, and repudiation are threat actions that cause \_\_\_\_\_\_\_\_\_\_ threat consequences.

A. unauthorized disclosure B. deception

C. disruption D. usurpation

10. A threat action in which sensitive data are directly released to an unauthorized entity is \_\_\_\_\_\_\_\_\_\_.

A. corruption B. disruption

C. intrusion D. exposure

11. An example of \_\_\_\_\_\_\_\_\_\_ is an attempt by an unauthorized user to gain access to a system by posing as

an authorized user.

A. masquerade B. interception

C. repudiation D. inference

12. The \_\_\_\_\_\_\_\_\_ prevents or inhibits the normal use or management of communications facilities.

A. passive attack B. traffic encryption

C. denial of service D. masquerade

13. A \_\_\_\_\_\_\_\_\_\_ is any action that compromises the security of information owned by an organization.

A. security mechanism B. security attack

C. security policy D. security service

14. The assurance that data received are exactly as sent by an authorized entity is \_\_\_\_\_\_\_\_\_\_.

A. authentication B. data confidentiality

C. access control D. data integrity

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

A. Traffic padding B. Traffic routing

C. Traffic control D. Traffic integrity

**SHORT ANSWER QUESTIONS:**

1. Computer Security is 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. Confidentiality, Integrity, and Availability form what is often referred to as the CIA Triad.

3. A loss of availability is the disruption of access to or use of information or an information system.

1. In the United States, student grade information is an asset whose confidentiality is regulated by the

FERPA (Family Educational Rights and Privacy Act.

1. A(n) attack is a threat that is carried out and, if successful, leads to an undesirable violation of security, or threat consequence.
2. A(n) countermeasure is any means taken to deal with a security attack.
3. Misappropriation and misuse are attacks that result in usurpation threat consequences.
4. The assets of a computer system can be categorized as hardware, software, communication lines and

networks, and data.

1. Release of message contents and traffic analysis are two types of passive attacks.
2. Replay, masquerade, modification of messages, and denial of service are example of active attacks.
3. Establishing, maintaining, and implementing plans for emergency response, backup operations, and

post disaster recovery for organizational information systems to ensure the availability of critical

information resources and continuity of operations in emergency situations is a contingency plan.

1. A(n) risk assessment is periodically assessing the risk to organizational operations, organizational

assets, and individuals, resulting from the operation of organizational information systems and the

associated processing, storage, or transmission or organizational information.

1. The OSI security architecture focuses on security attacks, mechanisms, and services.
2. A digital signature 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.

1. Security implementation involves four complementary courses of action: prevention, detection,

response, and recovery.