TT

TEXTBOOK TESTBANKS

Test Bank for Security in Computing 6th Pfleeger

TEST BANK SAMPLE PREVIEW

PUBLISHER

Pearson

COPYRIGHT

2024

RESOURCE TYPE

Test Bank

ISBN

9780137891252

Pfleeger, Pfleeger and Coles-Kemp: Security in Computing 6th Ed.
Multiple-Choice Quiz

Chapter 1 (Introduction)

1. Which of the following is considered an asset in computer security?

A) Computer hardware
B) Operating system
C) Email messages
D) All of the above

Answer: D) All of the above

Explanation: In computer security, assets refer to items of value needing protection. Computer hardware, such as the device and associated components, is considered an asset. Software assets include the operating system, utilities, device handlers, and applications like word processors, media players, and email handlers. Furthermore, data items stored on the computer, such as email messages, photos, papers, projects, and contact information, are also considered assets. Therefore, all options listed in the question (computer hardware, operating system, and email messages) are assets in computer security.

2. Which of the following factors affect the value of an asset?

A) Replacement cost and timing
B) User's perspective and storage capacity
C) Paper and ink cost and owner's identity
D) Protection level and availability

Answer: A) Replacement cost and timing

Explanation: The value of an asset depends on factors such as replacement cost and timing. The replacement cost refers to the effort or expense required to replace the asset if lost or damaged. Assets like computer data can be difficult or impossible to replace, while items like DVDs can be easily replaced. Furthermore, the timing also affects asset value. For example, plans for a company's new product line are highly valuable before the release, but their value decreases significantly once the product is released.

3. Which of the following is a security property that falls under the C-I-A triad?

A) Auditability
B) Accountability
C) Availability
D) Authentication

Answer: C) Availability

Explanation: The C-I-A triad refers to confidentiality, integrity, and availability, which are the three fundamental security properties. Availability is one of the aspects that make a computer valuable. It represents the ability of a system to be accessible and operational when needed. Therefore, option C correctly identifies availability as a security property falling under the C-I-A triad.

4. What is the nature of threats in the computer world and in life in general?

A) They are limited and predictable
B) They are limitless and largely unpredictable
C) They are only caused by natural disasters
D) They can be completely protected against

Answer: B) They are limitless and largely unpredictable

Explanation: The number and kinds of threats in the computer world and life, in general, are practically unlimited and largely unpredictable. The causes of harm are limitless and reflect the unpredictable nature of events like natural disasters, accidents, health issues, and random acts of violence. Due to the many possible causes of harm, it is impossible to protect ourselves or our computers entirely against all of them.

5. Which of the following factors is necessary for an attack to succeed?

A) Method, opportunity, and motive
B) Method, vulnerability, and motive
C) Opportunity, vulnerability, and motive
D) Method, opportunity, and vulnerability

Answer: A) Method, opportunity, and motive

Explanation: For an attack to succeed, the attacker must have three things: method, opportunity, and motive. Method refers to the skills, knowledge, tools, and resources needed to perpetrate the attack. Opportunity is the time and access required to execute the attack. Motive refers to the reason or incentive for wanting to carry out the attack. Without any of these factors, the attack will fail.

6. Which of the following is NOT a way to deal with harm in the context of security controls?

A) Prevent it
B) Deter it
C) Recover from its effects
D) Enhance physical security

Answer: D) Enhance physical security

Explanation: There are various ways to deal with harm, including preventing it, deterring it, mitigating its impact, detecting it, and recovering from its effects. Enhancing physical security, such as building castles or fortresses, is provided as an example to understand traditional ways of enhancing security but is not mentioned as one of the ways to deal with harm in the context of security controls.

7. Which class of controls uses tangible elements to stop or block an attack?

A) Physical controls
B) Procedural controls
C) Technical controls
D) Logical controls

Answer: A) Physical controls

Explanation: Physical controls use something tangible, such as walls, fences, locks, guards, and fire extinguishers, to stop or block an attack. These controls rely on physical elements to provide security measures.

8. What is the advantage of using overlapping controls or defense in depth?

A) They are more cost-effective
B) They work in different ways with different results
C) They require fewer resources to implement
D) They eliminate the need for other classes of controls

Answer: B) They work in different ways with different results

Explanation: It can be effective to use overlapping controls or defense in depth, employing more than one control or more than one class of control to achieve protection. The advantage of this approach is that different controls work in different ways, providing complementary layers of security and increasing the overall effectiveness of the security measures.

Chapter 2 (Toolbox: Authentication, Access Control, and Cryptography)

9. What is the difference between identification and authentication?

A) Identification proves an asserted identity, while authentication asserts who a person is.
B) Identification confirms an asserted identity, while authentication proves who a person is.
C) Identification asserts who a person is, while authentication is proves an asserted identity.
D) Identification and authentication refer to the same process.

Answer: C) Identification asserts who a person is, while authentication proves an asserted identity.

Explanation: Identification is the act of asserting who a person is, while authentication is the act of proving that the asserted identity is correct. Identification is about stating or claiming an identity, while authentication involves providing evidence or proof to verify that the claimed identity is valid.

10. Why is authentication necessary even if someone's identity is public?

A) Authentication prevents anyone from claiming a public identity.
B) Authentication protects the privacy of a person's identity.
C) Authentication ensures that the claimed public identity is valid.
D) Authentication is a legal requirement for public identities.

Answer: C) Authentication ensures that the claimed public identity is valid.

Explanation: If someone's identity is public, anyone can claim to be that person. Therefore, authentication becomes necessary to distinguish between genuine individuals and impostors. Authentication provides the means to prove that the claimed public identity is valid, establishing trust and confidence in the identity's authenticity.

11. What is the main limitation of passwords as protection devices?

A) They contain a small number of bits of information.
B) Attackers easily guess them.
C) They can be cracked using specialized software.
D) They are vulnerable to brute force attacks.

Answer: A) They contain a small number of bits of information.

Explanation: Passwords are limited as protection devices because they only contain a relatively small number of bits of information. This limitation means that passwords have a limited complexity and can be easily guessed or cracked by attackers, especially if users choose weak and easily guessable passwords. Increasing the complexity and length of passwords can improve their security, but the fundamental limitation of limited bits of information still exists.

12. How does using numerals and special characters in passwords affect brute force search time?

A) It significantly increases the search time for brute force attacks.
B) It does not impact the search time for brute force attacks.
C) It slightly lengthens the search time for brute force attacks.
D) It makes brute force attacks impossible.