

**[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)**

Which of the following is addressed by Kerberos?

- A. Confidentiality and Integrity
- B. Authentication and Availability
- C. Validation and Integrity
- D. Auditability and Integrity

**Correct Answer: A**

**Explanation:**

Kerberos addresses the confidentiality and integrity of information. It also addresses primarily authentication but does not directly address availability.

Reference(s) used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

<https://www.ietf.org/rfc/rfc4120.txt>

<http://learn-networking.com/network-security/how-kerberos-authentication-works>

**QUESTION 64**

Kerberos is vulnerable to replay in which of the following circumstances?

- A. When a private key is compromised within an allotted time window.
- B. When a public key is compromised within an allotted time window.
- C. When a ticket is compromised within an allotted time window.
- D. When the KSD is compromised within an allotted time window.

**Correct Answer: C**

**Explanation:**

Replay can be accomplished on Kerberos if the compromised tickets are used within an allotted time window.

The security depends on careful implementation:enforcing limited lifetimes for authentication credentials minimizes the threat of of replayed credentials, the KDC must be physically secured, and it should be hardened, not permitting any non-kerberos activities.

Reference:

Official ISC2 Guide to the CISSP, 2007 Edition, page 184

also see:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

**QUESTION 65**

Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?

- A. Discretionary Access Control
- B. Mandatory Access Control
- C. Sensitive Access Control
- D. Role-based Access Control

**Correct Answer: A**

**Explanation:**

**[SSCP Exam Dumps](#)   [SSCP PDF Dumps](#)   [SSCP VCE Dumps](#)   [SSCP Q&As](#)**

**<https://www.ensurepass.com/SSCP.html>**

## [Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

Data owners decide who has access to resources based only on the identity of the person accessing the resource.

The following answers are incorrect:

Mandatory Access Control: users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes and access decisions are based on security labels.

Sensitive Access Control: There is no such access control in the context of the above question.

Role-based Access Control: uses a centrally administered set of controls to determine how subjects and objects interact, also called as non discretionary access control.

In a mandatory access control (MAC) model, users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes. This model is much more structured and strict and is based on a security label system. Users are given a security clearance (secret, top secret, confidential, and so on), and data is classified in the same way. The clearance and classification data is stored in the security labels, which are bound to the specific subjects and objects. When the system makes a decision about fulfilling a request to access an object, it is based on the clearance of the subject, the classification of the object, and the security policy of the system. The rules for how subjects access objects are made by the security officer, configured by the administrator, enforced by the operating system, and supported by security technologies.

Reference:

Shon Harris, AIO v3, Chapter-4: Access Control, Page: 163-165

### **QUESTION 66**

Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?

- A. The Bell-LaPadula model
- B. The information flow model
- C. The noninterference model
- D. The Clark-Wilson model

**Correct Answer: C**

**Explanation:**

The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users. By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.

The model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level. It is not concerned with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it can not change the state for the entity at the lower level. The model also addresses the inference attack that occurs when some one has access to some type of information and can infer(guess) something that he does not have the clearance level or authority to know.

The following are incorrect answers:

The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned only with confidentiality and bases access control decisions on the classification of objects and the

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

## [Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

clearances of subjects.

The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes. Information will be allowed to flow only in accordance with the security policy.

The Clark-Wilson model is incorrect. The Clark-Wilson model is concerned with change control and assuring that all modifications to objects preserve integrity by means of well- formed transactions and usage of an access triple (subject - interface - object).

References:

CBK, pp 325 - 326

AIO3, pp. 290 - 291

AIOv4 Security Architecture and Design (page 345)

AIOv5 Security Architecture and Design (pages 347 - 348)

[https://en.wikibooks.org/wiki/Security\\_Architecture\\_and\\_Design/Security\\_Models#Noninterference\\_Models](https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models#Noninterference_Models)

### **QUESTION 67**

Which of the following is the LEAST user accepted biometric device?

- A. Fingerprint
- B. Iris scan
- C. Retina scan
- D. Voice verification

**Correct Answer: C**

**Explanation:**

The biometric device that is least user accepted is the retina scan, where a system scans the blood-vessel pattern on the backside of the eyeball. When using this device, an individual has to place their eye up to a device, and may require a puff of air to be blown into the eye. The iris scan only needs for an individual to glance at a camera that could be placed above a door.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 4: Access Control (page 131).

### **QUESTION 68**

Crime Prevention Through Environmental Design (CPTED) is a discipline that:

- A. Outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.
- B. Outlines how the proper design of the logical environment can reduce crime by directly affecting human behavior.
- C. Outlines how the proper design of the detective control environment can reduce crime by directly affecting human behavior.
- D. Outlines how the proper design of the administrative control environment can reduce crime by directly affecting human behavior.

**Correct Answer: A**

**Explanation:**

Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance about lost and crime prevention through proper facility construction and environmental components and procedures.

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

CPTED concepts were developed in the 1960s. They have been expanded upon and have matured as our environments and crime types have evolved. CPTED has been used not just to develop corporate physical security programs, but also for large-scale activities such as development of neighborhoods, towns, and cities. It addresses landscaping, entrances, facility and neighborhood layouts, lighting, road placement, and traffic circulation patterns. It looks at microenvironments, such as offices and rest-rooms, and macroenvironments, like campuses and cities.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 435). McGraw- Hill. Kindle Edition.  
CPTED Guide Book

#### **QUESTION 69**

Another type of access control is lattice-based access control. In this type of control a lattice model is applied. How is this type of access control concept applied?

- A. The pair of elements is the subject and object, and the subject has an upper bound equal or higher than the upper bound of the object being accessed.
- B. The pair of elements is the subject and object, and the subject has an upper bound lower then the upper bound of the object being accessed.
- C. The pair of elements is the subject and object, and the subject has no special upper or lower bound needed within the lattice.
- D. The pair of elements is the subject and object, and the subject has no access rights in relation to an object.

**Correct Answer: A**

#### **Explanation:**

To apply this concept to access control, the pair of elements is the subject and object, and the subject has to have an upper bound equal or higher than the object being accessed.

WIKIPEDIA has a great explanation as well:

In computer security, lattice-based access control (LBAC) is a complex access control based on the interaction between any combination of objects (such as resources, computers, and applications) and subjects (such as individuals, groups or organizations). In this type of label-based mandatory access control model, a lattice is used to define the levels of security that an object may have and that a subject may have access to. The subject is only allowed to access an object if the security level of the subject is greater than or equal to that of the object.

Reference(s) used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.  
[http://en.wikipedia.org/wiki/Lattice-based\\_access\\_control](http://en.wikipedia.org/wiki/Lattice-based_access_control)

#### **QUESTION 70**

Sensitivity labels are an example of what application control type?

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

## [Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

- A. Preventive security controls
- B. Detective security controls
- C. Compensating administrative controls
- D. Preventive accuracy controls

**Correct Answer: A**

**Explanation:**

Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.

The incorrect answers are:

Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.

Compensating administrative controls - There no such application control.

Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups.

Sources:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 264).

KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

### **QUESTION 71**

What is the primary role of smartcards in a PKI?

- A. Transparent renewal of user keys
- B. Easy distribution of the certificates between the users
- C. Fast hardware encryption of the raw data
- D. Tamper resistant, mobile storage and application of private keys of the users

**Correct Answer: D**

**Explanation:**

Reference:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 139; SNYDER, J., What is a SMART CARD?.

Wikipedia has a nice definition at: [http://en.wikipedia.org/wiki/Tamper\\_resistance](http://en.wikipedia.org/wiki/Tamper_resistance)

Security

Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.

Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>