

Exam Questions SSCP

System Security Certified Practitioner (SSCP)

<https://www.2passeasy.com/dumps/SSCP/>



NEW QUESTION 1

- (Topic 1)

Which of the following pairings uses technology to enforce access control policies?

- A. Preventive/Administrative
- B. Preventive/Technical
- C. Preventive/Physical
- D. Detective/Administrative

Answer: B

Explanation:

The preventive/technical pairing uses technology to enforce access control policies.

TECHNICAL CONTROLS

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.

Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

Access control software. Antivirus software. Library control systems. Passwords.

Smart cards. Encryption.

Dial-up access control and callback systems.

Preventive Physical Controls

Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:

Backup files and documentation. Fences.

Security guards. Badge systems. Double door systems. Locks and keys. Backup power.

Biometric access controls. Site selection.

Fire extinguishers.

Preventive Administrative Controls

Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:

Security awareness and technical training. Separation of duties.

Procedures for recruiting and terminating employees. Security policies and procedures.

Supervision.

Disaster recovery, contingency, and emergency plans. User registration for computer access.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 2

- (Topic 1)

Detective/Technical measures:

- A. include intrusion detection systems and automatically-generated violation reports from audit trail information.
- B. do not include intrusion detection systems and automatically-generated violation reports from audit trail information.
- C. include intrusion detection systems but do not include automatically-generated violation reports from audit trail information.
- D. include intrusion detection systems and customised-generated violation reports from audit trail information.

Answer: A

Explanation:

Detective/Technical measures include intrusion detection systems and automatically-generated violation reports from audit trail information. These reports can indicate variations from "normal" operation or detect known signatures of unauthorized access episodes. In order to limit the amount of audit information flagged and reported by automated violation analysis and reporting mechanisms, clipping levels can be set. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION 3

- (Topic 1)

Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is not a component that achieves this type of security?

- A. Administrative control mechanisms
- B. Integrity control mechanisms
- C. Technical control mechanisms
- D. Physical control mechanisms

Answer: B

Explanation:

Integrity Controls Mechanisms are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site: Information security depends on the security and management of the physical space in which computer systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following QUESTION NO: s are covered:

Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response.

Risks, issues and protection strategies: Risk identification and the selection of security protection components.

Perimeter security: Typical physical protection controls.

Facilities management

Facilities management is a complex component of corporate security that ranges from the planning of a secure physical site to the management of the physical information system environment. Facilities management responsibilities include site selection and physical security planning (i.e. facility construction, design and layout, fire and water damage protection, antitheft mechanisms, intrusion detection and security procedures.) Protections must extend to both people and assets. The necessary level of protection depends on the value of the assets and data. CISSP® candidates must learn the concept of critical-path analysis as a means of determining a component's business function criticality relative to the cost of operation and replacement. Furthermore, students need to gain an understanding of the optimal location and physical attributes of a secure facility. Among the QUESTION NO: s covered in this domain are site inspection, location, accessibility and obscurity, considering the area crime rate, and the likelihood of natural hazards such as floods or earthquakes.

This domain also covers the quality of construction material, such as its protective qualities and load capabilities, as well as how to lay out the structure to minimize risk of forcible entry and accidental damage. Regulatory compliance is also touched on, as is preferred proximity to civil protection services, such as fire and police stations. Attention is given to computer and equipment rooms, including their location, configuration (entrance/egress requirements) and their proximity to wiring distribution centers at the site.

Physical risks, issues and protection strategies

An overview of physical security risks includes risk of theft, service interruption, physical damage, compromised system integrity and unauthorized disclosure of information. Interruptions to business can manifest due to loss of power, services, telecommunications connectivity and water supply. These can also seriously compromise electronic security monitoring alarm/response devices. Backup options are also covered in this domain, as is a strategy for quantifying the risk exposure by simple formula.

Investment in preventive security can be costly. Appropriate redundancy of people skills, systems and infrastructure must be based on the criticality of the data and assets to be preserved. Therefore a strategy is presented that helps determine the selection of cost appropriate controls. Among the QUESTION NO: s covered in this domain are regulatory and legal requirements, common standard security protections such as locks and fences, and the importance of establishing service level agreements for maintenance and disaster support. Rounding out the optimization approach are simple calculations for determining mean time between failure and mean time to repair (used to estimate average equipment life expectancy) ?? essential for estimating the cost/benefit of purchasing and maintaining redundant equipment.

As the lifeblood of computer systems, special attention is placed on adequacy, quality and protection of power supplies. CISSP candidates need to understand power supply concepts and terminology, including those for quality (i.e. transient noise vs. clean power); types of interference (EMI and RFI); and types of interruptions such as power excess by spikes and surges, power loss by fault or blackout, and power degradation from sags and brownouts. A simple formula is presented for determining the total cost per hour for backup power. Proving power reliability through testing is recommended and the advantages of three power protection approaches are discussed (standby UPS, power line conditioners and backup sources) including minimum requirements for primary and alternate power provided.

Environmental controls are explored in this domain, including the value of positive pressure water drains and climate monitoring devices used to control temperature, humidity and reduce static electricity. Optimal temperatures and humidity settings are provided.

Recommendations include strict procedures during emergencies, preventing typical risks (such as blocked fans), and the use of antistatic armbands and hygrometers. Positive pressurization for proper ventilation and monitoring for air born contaminants is stressed.

The pros and cons of several detection response systems are deeply explored in this domain. The concept of combustion, the classes of fire and fire extinguisher ratings are detailed. Mechanisms behind smoke-activated, heat-activated and flame-activated devices and Automatic Dial-up alarms are covered, along with their advantages, costs and shortcomings. Types of fire sources are distinguished and the effectiveness of fire suppression methods for each is included. For instance, Halon and its approved replacements are covered, as are the advantages and the inherent risks to equipment of the use of water sprinklers.

Administrative controls

The physical security domain also deals with administrative controls applied to physical sites and assets. The need for skilled personnel, knowledge sharing between them, separation of duties, and appropriate oversight in the care and maintenance of equipment and environments is stressed. A list of management duties including hiring checks, employee maintenance activities and recommended termination procedures is offered. Emergency measures include accountability for evacuation and system shutdown procedures, integration with disaster and business continuity plans, assuring documented procedures are easily available during different types of emergencies, the scheduling of periodic equipment testing, administrative reviews of documentation, procedures and recovery plans, responsibilities delegation, and personnel training and drills.

Perimeter security

Domain nine also covers the devices and techniques used to control access to a space. These include access control devices, surveillance monitoring, intrusion detection and corrective actions. Specifications are provided for optimal external boundary protection, including fence heights and placement, and lighting placement and types. Selection of door types and lock characteristics are covered. Surveillance methods and intrusion-detection methods are explained, including the use of video monitoring, guards, dogs, proximity detection systems, photoelectric/photometric systems, wave pattern devices, passive infrared systems, and sound and motion detectors, and current flow sensitivity devices that specifically address computer theft. Room lock types ?? both preset and cipher locks (and their variations) -- device locks, such as portable laptop locks, lockable server bays, switch control locks and slot locks, port controls, peripheral switch controls and cable trap locks are also covered. Personal access control methods used to identify authorized users for site entry are covered at length, noting social engineering risks such as piggybacking. Wireless proximity devices, both user access and system sensing readers are covered (i.e. transponder based, passive devices and field powered devices) in this domain.

Now that you've been introduced to the key concepts of Domain 9, watch the Domain 9, Physical Security video

Return to the CISSP Essentials Security School main page

See all SearchSecurity.com's resources on CISSP certification training Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 280.

NEW QUESTION 4

- (Topic 1)

Which of the following is implemented through scripts or smart agents that replays the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?

- A. Single Sign-On
- B. Dynamic Sign-On
- C. Smart cards
- D. Kerberos

Answer: A

Explanation:

SSO can be implemented by using scripts that replay the users multiple log- ins against authentication servers to verify a user's identity and to permit access to system services.

Single Sign on was the best answer in this case because it would include Kerberos. When you have two good answers within the 4 choices presented you must select the

BEST one. The high level choice is always the best. When one choice would include the other one that would be the best as well.

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 40.

NEW QUESTION 5

- (Topic 1)

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.

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.

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.

and

CPTED Guide Book

NEW QUESTION 6

- (Topic 1)

What refers to legitimate users accessing networked services that would normally be restricted to them?

- A. Spoofing
- B. Piggybacking
- C. Eavesdropping
- D. Logon abuse

Answer: D

Explanation:

Unauthorized access of restricted network services by the circumvention of security access controls is known as logon abuse. This type of abuse refers to users who may be internal to the network but access resources they would not normally be allowed. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3:

Telecommunications and Network Security (page 74).

NEW QUESTION 7

- (Topic 1)

Which of the following biometric characteristics cannot be used to uniquely authenticate an individual's identity?

- A. Retina scans
- B. Iris scans
- C. Palm scans
- D. Skin scans

Answer: D

Explanation:

The following are typical biometric characteristics that are used to uniquely authenticate an individual's identity:

Fingerprints Retina scans Iris scans Facial scans Palm scans Hand geometry Voice

Handwritten signature dynamics

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 127-131).

NEW QUESTION 8

- (Topic 1)

To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:

- A. Access Rules
- B. Access Matrix
- C. Identification controls
- D. Access terminal

Answer: A

Explanation:

Controlling access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up access rules.

These rules can be classified into three access control models: Mandatory, Discretionary, and Non-Discretionary.

An access matrix is one of the means used to implement access control.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 9

- (Topic 1)

Which of the following is a trusted, third party authentication protocol that was developed under Project Athena at MIT?

- A. Kerberos
- B. SESAME
- C. KryptoKnight
- D. NetSP

Answer: A

Explanation:

Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT.

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.

The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by systems crackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.

Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad

assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure than a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.

Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Kerberos is freely available from MIT, under a copyright permission notice very similar to the one used for the BSD operating and X11 Windowing system. MIT provides Kerberos in source form, so that anyone who wishes to use it may look over the code for themselves and assure themselves that the code is trustworthy. In addition, for those who prefer to rely on a professional supported product, Kerberos is available as a product from many different vendors.

In summary, Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us. At MIT, Kerberos has been invaluable to our Information/Technology architecture.

KryptoKnight is a Peer to Peer authentication protocol incorporated into the NetSP product from IBM.

SESAME is an authentication and access control protocol, that also supports communication confidentiality and integrity. It provides public key based authentication along with the Kerberos style authentication, that uses symmetric key cryptography. Sesame supports the Kerberos protocol and adds some security extensions like public key based authentication and an ECMA-style Privilege Attribute Service. The complete Sesame protocol is a two step process. In the first step, the client successfully authenticates itself to the Authentication Server and obtains a ticket that can be presented to the Privilege Attribute Server. In the second step, the initiator obtains proof of his access rights in the form of Privilege Attributes Certificate (PAC). The PAC is a specific form of Access Control Certificate as defined in the ECMA-219 document. This document describes the extensions to Kerberos for public key based authentication as adopted in Sesame. SESAME, KryptoKnight, and NetSP never took off and the protocols are no longer commonly used.

References:

<http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#whatis> and

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 40.

NEW QUESTION 10

- (Topic 1)

In the Bell-LaPadula model, the Star-property is also called:

- A. The simple security property
- B. The confidentiality property
- C. The confinement property
- D. The tranquility property

Answer: B

Explanation:

The Bell-LaPadula model focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.

In this formal model, the entities in an information system are divided into subjects and objects.

The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby proving that the system satisfies the security objectives of the model.

The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy.

To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.

The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:

The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).

The property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The property is also known as the Confinement property.

The Discretionary Security Property - use an access control matrix to specify the discretionary access control.

The transfer of information from a high-sensitivity document to a lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the property. Untrusted subjects are.

Trusted Subjects must be shown to be trustworthy with regard to the security policy. This security model is directed toward access control and is characterized by the phrase: "no read up, no write down." Compare the Biba model, the Clark-Wilson model and the Chinese Wall.

With Bell-LaPadula, users can create content only at or above their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down). Conversely, users can view content only at or below their own security level (i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).

Strong Property

The Strong Property is an alternative to the Property in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual Property is not present, only a write-to-same level operation. The Strong Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns.

Tranquility principle

The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two

forms to the tranquility principle: the "principle of strong tranquility" states that security levels do not change during the normal operation of the system and the "principle of weak tranquility" states that security levels do not change in a way that violates the rules of a given security policy. Another interpretation of the tranquility principles is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/label will not change during an operation (such as read or write); the weak tranquility principle means that an object's security level/label may change in a way that does not violate the security policy during an operation. Reference(s) used for this question: http://en.wikipedia.org/wiki/Biba_Model http://en.wikipedia.org/wiki/Mandatory_access_control http://en.wikipedia.org/wiki/Discretionary_access_control http://en.wikipedia.org/wiki/Clark-Wilson_model http://en.wikipedia.org/wiki/Brewer_and_Nash_model

NEW QUESTION 10

- (Topic 1)

What does the (star) property mean in the Bell-LaPadula model?

- A. No write up
- B. No read up
- C. No write down
- D. No read down

Answer: C

Explanation:

The (star) property of the Bell-LaPadula access control model states that writing of information by a subject at a higher level of sensitivity to an object at a lower level of sensitivity is not permitted (no write down).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).

Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (page 242, 243).

NEW QUESTION 15

- (Topic 1)

Which of the following questions is less likely to help in assessing identification and authentication controls?

- A. Is a current list maintained and approved of authorized users and their access?
- B. Are passwords changed at least every ninety days or earlier if needed?
- C. Are inactive user identifications disabled after a specified period of time?
- D. Is there a process for reporting incidents?

Answer: D

Explanation:

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. Reporting incidents is more related to incident response capability (operational control) than to identification and authentication (technical control).

Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-30 to A-32).

NEW QUESTION 18

- (Topic 1)

Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

- A. The Take-Grant model
- B. The Biba integrity model
- C. The Clark Wilson integrity model
- D. The Bell-LaPadula integrity model

Answer: C

Explanation:

The Clark Wilson integrity model addresses the three following integrity goals: 1) data is protected from modification by unauthorized users; 2) data is protected from unauthorized modification by authorized users; and 3) data is internally and externally consistent. It also defines a Constrained Data Item (CDI), an Integrity Verification Procedure (IVP), a Transformation Procedure (TP) and an Unconstrained Data item. The Bell-LaPadula and Take-Grant models are not integrity models.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 205).

NEW QUESTION 19

- (Topic 1)

Which of the following access control models is based on sensitivity labels?

- A. Discretionary access control
- B. Mandatory access control
- C. Rule-based access control
- D. Role-based access control

Answer: B

Explanation:

Access decisions are made based on the clearance of the subject and the sensitivity label of the object.

Example: Eve has a "Secret" security clearance and is able to access the "Mugwump Missile Design Profile" because its sensitivity label is "Secret." She is denied

access to the "Presidential Toilet Tissue Formula" because its sensitivity label is "Top Secret."

The other answers are not correct because:

Discretionary Access Control is incorrect because in DAC access to data is determined by the data owner. For example, Joe owns the "Secret Chili Recipe" and grants read access to Charles.

Role Based Access Control is incorrect because in RBAC access decisions are made based on the role held by the user. For example, Jane has the role "Auditor" and that role includes read permission on the "System Audit Log."

Rule Based Access Control is incorrect because it is a form of MAC. A good example would be a Firewall where rules are defined and apply to anyone connecting through the firewall.

References:

All in One third edition, page 164. Official ISC2 Guide page 187.

NEW QUESTION 22

- (Topic 1)

Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is correct?

A. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.

B. Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.

C. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.

D. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

Answer: C

Explanation:

Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 24

- (Topic 1)

What does the Clark-Wilson security model focus on?

A. Confidentiality

B. Integrity

C. Accountability

D. Availability

Answer: B

Explanation:

The Clark-Wilson model addresses integrity. It incorporates mechanisms to enforce internal and external consistency, a separation of duty, and a mandatory integrity policy.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION 25

- (Topic 1)

Which access control model provides upper and lower bounds of access capabilities for a subject?

A. Role-based access control

B. Lattice-based access control

C. Biba access control

D. Content-dependent access control

Answer: B

Explanation:

In the lattice model, users are assigned security clearances and the data is classified. Access decisions are made based on the clearance of the user and the classification of the object. Lattice-based access control is an essential ingredient of formal security models such as Bell-LaPadula, Biba, Chinese Wall, etc.

The bounds concept comes from the formal definition of a lattice as a "partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound." To see the application, consider a file classified as "SECRET" and a user Joe with a security clearance of "TOP SECRET." Under Bell-LaPadula, Joe's "least upper bound" access to the file is "READ" and his least lower bound is "NO WRITE" (star property).

Role-based access control is incorrect. Under RBAC, the access is controlled by the permissions assigned to a role and the specific role assigned to the user.

Biba access control is incorrect. The Biba integrity model is based on a lattice structure but the context of the question disqualifies it as the best answer.

Content-dependent access control is incorrect. In content dependent access control, the actual content of the information determines access as enforced by the arbiter.

References:

CBK, pp. 324-325.

AIO3, pp. 291-293. See particularly Figure 5-19 on p. 293 for an illustration of bounds in action.

NEW QUESTION 29

- (Topic 1)

Which of the following security models does NOT concern itself with the flow of data?

A. The information flow model

B. The Biba model

C. The Bell-LaPadula model

D. The noninterference model

Answer: D

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

The Biba model is incorrect. The Biba model is concerned with integrity and is a complement to the Bell-LaPadula model in that higher levels of integrity are more trusted than lower levels. Access control is based on these integrity levels to assure that read/write operations do not decrease an object's integrity.

References:

CBK, pp 325 - 326

AIO3, pp. 290 - 291

NEW QUESTION 33

- (Topic 1)

Which of the following is most relevant to determining the maximum effective cost of access control?

- A. the value of information that is protected
- B. management's perceptions regarding data importance
- C. budget planning related to base versus incremental spending.
- D. the cost to replace lost data

Answer: A

Explanation:

The cost of access control must be commensurate with the value of the information that is being protected.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION 35

- (Topic 1)

Which access control type has a central authority that determines to what objects the subjects have access to and it is based on role or on the organizational security policy?

- A. Mandatory Access Control
- B. Discretionary Access Control
- C. Non-Discretionary Access Control
- D. Rule-based Access control

Answer: C

Explanation:

Non-Discretionary Access Control includes Role Based Access Control (RBAC) and Rule Based Access Control (RBAC or RuBAC). RBAC being a subset of NDAC, it was easy to eliminate RBAC as it was covered under NDAC already.

Some people think that RBAC is synonymous with NDAC but RuBAC would also fall into this category.

Discretionary Access control is for environment with very low level of security. There is no control on the dissemination of the information. A user who has access to a file can copy the file or further share it with other users.

Rule Based Access Control is when you have ONE set of rules applied uniformly to all users. A good example would be a firewall at the edge of your network. A single rule based is applied against any packets received from the internet.

Mandatory Access Control is a very rigid type of access control. The subject must dominate the object and the subject must have a Need To Know to access the information. Objects have labels that indicate the sensitivity (classification) and there are also categories to enforce the Need To Know (NTK).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 40

- (Topic 1)

Single Sign-on (SSO) is characterized by which of the following advantages?

- A. Convenience
- B. Convenience and centralized administration
- C. Convenience and centralized data administration
- D. Convenience and centralized network administration

Answer: B

Explanation:

Convenience - Using single sign-on users have to type their passwords only once when they first log in to access all the network resources; and Centralized Administration as some single sign-on systems are built around a unified server administration system. This allows a single administrator to add and delete accounts across the entire network from one user interface.

The following answers are incorrect:

Convenience - alone this is not the correct answer.

Centralized Data or Network Administration - these are thrown in to mislead the student. Neither are a benefit to SSO, as these specifically should not be allowed with just an SSO.

References: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, page 35.

TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, page 180.

NEW QUESTION 45

- (Topic 1)

Which of the following is used by RADIUS for communication between clients and servers?

- A. TCP
- B. SSL
- C. UDP
- D. SSH

Answer: C

Explanation:

Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

NEW QUESTION 48

- (Topic 1)

Which of the following would assist the most in Host Based intrusion detection?

- A. audit trails.
- B. access control lists.
- C. security clearances.
- D. host-based authentication.

Answer: A

Explanation:

To assist in Intrusion Detection you would review audit logs for access violations.

The following answers are incorrect:

access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.

security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.

host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not detect intrusions.

NEW QUESTION 53

- (Topic 1)

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

Answer: A

Explanation:

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

NEW QUESTION 57

- (Topic 1)

Which of the following is not a physical control for physical security?

- A. lighting
- B. fences
- C. training
- D. facility construction materials

Answer: C

Explanation:

Some physical controls include fences, lights, locks, and facility construction materials. Some administrative controls include facility selection and construction, facility management, personnel controls, training, and emergency response and procedures.

From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 3rd. Ed., Chapter 6, page 403.

NEW QUESTION 59

- (Topic 1)

The end result of implementing the principle of least privilege means which of the following?

- A. Users would get access to only the info for which they have a need to know
- B. Users can access all systems.
- C. Users get new privileges added when they change positions.
- D. Authorization creep.

Answer: A

Explanation:

The principle of least privilege refers to allowing users to have only the access they need and not anything more. Thus, certain users may have no need to access any of the files on specific systems.

The following answers are incorrect:

Users can access all systems. Although the principle of least privilege limits what access and systems users have authorization to, not all users would have a need to know to access all of the systems. The best answer is still Users would get access to only the info for which they have a need to know as some of the users may not have a need to access a system.

Users get new privileges when they change positions. Although true that a user may indeed require new privileges, this is not a given fact and in actuality a user may require less privileges for a new position. The principle of least privilege would require that the rights required for the position be closely evaluated and where possible rights revoked.

Authorization creep. Authorization creep occurs when users are given additional rights with new positions and responsibilities. The principle of least privilege should actually prevent authorization creep.

The following reference(s) were/was used to create this question: ISC2 OIG 2007 p.101,123

Shon Harris AIO v3 p148, 902-903

NEW QUESTION 64

- (Topic 1)

Which of the following statements relating to the Bell-LaPadula security model is FALSE (assuming the Strong Star property is not being used) ?

- A. A subject is not allowed to read up.
- B. The property restriction can be escaped by temporarily downgrading a high level subject.
- C. A subject is not allowed to read down.
- D. It is restricted to confidentiality.

Answer: C

Explanation:

It is not a property of Bell LaPadula model. The other answers are incorrect because:

A subject is not allowed to read up is a property of the 'simple security rule' of Bell LaPadula model.

The property restriction can be escaped by temporarily downgrading a high level subject can be escaped by temporarily downgrading a high level subject or by identifying a set of trusted objects which are permitted to violate the property as long as it is not in the middle of an operation.

It is restricted to confidentiality as it is a state machine model that enforces the confidentiality aspects of access control.

Reference: Shon Harris AIO v3 , Chapter-5 : Security Models and Architecture , Page:279-282

NEW QUESTION 67

- (Topic 1)

Guards are appropriate whenever the function required by the security program involves which of the following?

- A. The use of discriminating judgment
- B. The use of physical force
- C. The operation of access control devices
- D. The need to detect unauthorized access

Answer: A

Explanation:

The Answer The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.

The following answers are incorrect:

The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force.

The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc. The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.

The following reference(s) were/was used to create this question:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 339).

Source: ISC2 Official Guide to the CBK page 288-289.

NEW QUESTION 69

- (Topic 1)

Which of the following statements pertaining to biometrics is false?

- A. Increased system sensitivity can cause a higher false rejection rate
- B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
- C. False acceptance rate is also known as Type II error.
- D. Biometrics are based on the Type 2 authentication mechanism.

Answer: D

Explanation:

Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based

on the Type 3 authentication mechanism.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).

NEW QUESTION 72

- (Topic 1)

In the context of Biometric authentication, what is a quick way to compare the accuracy of devices. In general, the device that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

- A. the CER is used.
- B. the FRR is used
- C. the FAR is used
- D. the FER is used

Answer: A

Explanation:

equal error rate or crossover error rate (EER or CER): the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

In the context of Biometric Authentication almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher False Reject Rate (FRR). Conversely, if the sensitivity is decreased, the False Acceptance Rate (FAR) will increase. Thus, to have a valid measure of the system performance, the CrossOver Error Rate (CER) is used.

The following are used as performance metrics for biometric systems:

false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value.

false reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

template capacity: the maximum number of sets of data which can be stored in the system. 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 37. and

Wikipedia at: <https://en.wikipedia.org/wiki/Biometrics>

NEW QUESTION 75

- (Topic 1)

What can be defined as a list of subjects along with their access rights that are authorized to access a specific object?

- A. A capability table
- B. An access control list
- C. An access control matrix
- D. A role-based matrix

Answer: B

Explanation:

"It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188

A capability table is incorrect. "Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's possession of a capability (or ticket) for the object." CBK, pp. 191-192. The distinction that makes this an incorrect choice is that access is based on possession of a capability by the subject.

To put it another way, as noted in AIO3 on p. 169, "A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL."

An access control matrix is incorrect. The access control matrix is a way of describing the rules for an access control strategy. The matrix lists the users, groups and roles down the left side and the resources and functions across the top. The cells of the matrix can either indicate that access is allowed or indicate the type of access. CBK pp 317 - 318.

AIO3, p. 169 describes it as a table of subjects and objects specifying the access rights a certain subject possesses pertaining to specific objects.

In either case, the matrix is a way of analyzing the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.

A role-based matrix is incorrect. Again, a matrix of roles vs objects could be used as a tool for thinking about the access control to be applied to a set of objects.

The results of the analysis could then be implemented using RBAC.

References:

CBK, Domain 2: Access Control. AIO3, Chapter 4: Access Control

NEW QUESTION 77

- (Topic 1)

When submitting a passphrase for authentication, the passphrase is converted into ...

- A. a virtual password by the system
- B. a new passphrase by the system
- C. a new passphrase by the encryption technology
- D. a real password by the system which can be used forever

Answer: A

Explanation:

Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. The changing of passwords can also fall between these two extremes.
Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use.
Obviously, the more times a password is used, the more chance there is of it being compromised.
It is recommended to use a passphrase instead of a password. A passphrase is more resistant to attacks. The passphrase is converted into a virtual password by the system. Often time the passphrase will exceed the maximum length supported by the system and it must be truncated into a Virtual Password.
Reference(s) used for this question: <http://www.itl.nist.gov/fipspubs/fip112.htm>
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36 & 37.

NEW QUESTION 82

- (Topic 1)

In the CIA triad, what does the letter A stand for?

- A. Auditability
- B. Accountability
- C. Availability
- D. Authentication

Answer: C

Explanation:

The CIA triad stands for Confidentiality, Integrity and Availability.

NEW QUESTION 86

- (Topic 1)

This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

- A. Checkpoint level
- B. Ceiling level
- C. Clipping level
- D. Threshold level

Answer: C

Explanation:

Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.

The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).

If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.

The following answers are incorrect:

All of the other choices presented were simply detractors. The following reference(s) were used for this question:

Handbook of Information Security Management

NEW QUESTION 88

- (Topic 1)

Which of the following is the WEAKEST authentication mechanism?

- A. Passphrases
- B. Passwords
- C. One-time passwords
- D. Token devices

Answer: B

Explanation:

Most of the time users usually choose passwords which can be guessed, hence passwords is the BEST answer out of the choices listed above.

The following answers are incorrect because:

Passphrases is incorrect as it is more secure than a password because it is longer.

One-time passwords is incorrect as the name states, it is good for only once and cannot be reused.

Token devices is incorrect as this is also a password generator and is an one time password mechanism.

Reference: Shon Harris AIO v3, Chapter-4: Access Control, Page: 139, 142.

NEW QUESTION 91

- (Topic 1)

Which of the following is true about Kerberos?

- A. It utilizes public key cryptography.
- B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.

- C. It depends upon symmetric ciphers.
- D. It is a second party authentication system.

Answer: C

Explanation:

Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.

The following answers are incorrect:

It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers).

It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys.

It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.

References:

MIT <http://web.mit.edu/kerberos/>

Wikipedi http://en.wikipedia.org/wiki/Kerberos_%28protocol%29

OIG CBK Access Control (pages 181 - 184) AIOv3 Access Control (pages 151 - 155)

NEW QUESTION 92

- (Topic 1)

Which type of control is concerned with avoiding occurrences of risks?

- A. Deterrent controls
- B. Detective controls
- C. Preventive controls
- D. Compensating controls

Answer: C

Explanation:

Preventive controls are concerned with avoiding occurrences of risks while deterrent controls are concerned with discouraging violations. Detecting controls identify occurrences and compensating controls are alternative controls, used to compensate weaknesses in other controls. Supervision is an example of compensating control. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 93

- (Topic 1)

What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?

- A. False Rejection Rate (FRR) or Type I Error
- B. False Acceptance Rate (FAR) or Type II Error
- C. Crossover Error Rate (CER)
- D. Failure to enroll rate (FTE or FER)

Answer: C

Explanation:

The percentage at which the False Rejection Rate equals the False Acceptance Rate is called the Crossover Error Rate (CER). Another name for the CER is the Equal Error Rate (EER), any of the two terms could be used.

Equal error rate or crossover error rate (EER or CER)

It is the rate at which both accept and reject errors are equal. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

The other choices were all wrong answers:

The following are used as performance metrics for biometric systems:

false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. This is when an impostor would be accepted by the system.

False reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. This is when a valid company employee would be rejected by the system.

Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

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 38.

and <https://en.wikipedia.org/wiki/Biometrics>

NEW QUESTION 96

- (Topic 1)

Which of the following is not a two-factor authentication mechanism?

- A. Something you have and something you know.
- B. Something you do and a password.
- C. A smartcard and something you are.
- D. Something you know and a password.

Answer: D

Explanation:

Something you know and a password fits within only one of the three ways authentication could be done. A password is an example of something you know, thereby something you know and a password does not constitute a two-factor authentication as both are in the same category of factors.

A two-factor (strong) authentication relies on two different kinds of authentication factors out of a list of three possible choice:

something you know (e.g. a PIN or password),
something you have (e.g. a smart card, token, magnetic card),
something you are is mostly Biometrics (e.g. a fingerprint) or something you do (e.g. signature dynamics).

TIP FROM CLEMENT:

On the real exam you can expect to see synonyms and sometimes sub-categories under the main categories. People are familiar with Pin, Passphrase, Password as subset of Something you know.

However, when people see choices such as Something you do or Something you are they immediately get confused and they do not think of them as subset of Biometrics where you have Biometric implementation based on behavior and physiological attributes. So something you do falls under the Something you are category as a subset.

Something your do would be signing your name or typing text on your keyboard for example.

Strong authentication is simply when you make use of two factors that are within two different categories.

Reference(s) used for this question:

Shon Harris, CISSP All In One, Fifth Edition, pages 158-159

NEW QUESTION 101

- (Topic 1)

In an organization where there are frequent personnel changes, non-discretionary access control using Role Based Access Control (RBAC) is useful because:

- A. people need not use discretion
- B. the access controls are based on the individual's role or title within the organization.
- C. the access controls are not based on the individual's role or title within the organization
- D. the access controls are often based on the individual's role or title within the organization

Answer: B

Explanation:

In an organization where there are frequent personnel changes, non- discretionary access control (also called Role Based Access Control) is useful because the access controls are based on the individual's role or title within the organization. You can easily configure a new employee access by assigning the user to a role that has been predefine. The user will implicitly inherit the permissions of the role by being a member of that role.

These access permissions defined within the role do not need to be changed whenever a new person takes over the role.

Another type of non-discretionary access control model is the Rule Based Access Control (RBAC or RuBAC) where a global set of rule is uniformly applied to all subjects accessing the resources. A good example of RuBAC would be a firewall.

This question is a sneaky one, one of the choice has only one added word to it which is often. Reading questions and their choices very carefully is a must for the real exam. Reading it twice if needed is recommended.

Shon Harris in her book list the following ways of managing RBAC: Role-based access control can be managed in the following ways:

Non-RBAC Users are mapped directly to applications and no roles are used. (No roles being used)

Limited RBAC Users are mapped to multiple roles and mapped directly to other types of applications that do not have role-based access functionality. (A mix of roles for applications that supports roles and explicit access control would be used for applications that do not support roles)

Hybrid RBAC Users are mapped to multiapplication roles with only selected rights assigned to those roles.

Full RBAC Users are mapped to enterprise roles. (Roles are used for all access being granted)

NIST defines RBAC as:

Security administration can be costly and prone to error because administrators usually specify access control lists for each user on the system individually. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier.

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 32.

and

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition McGraw-Hill. and

<http://csrc.nist.gov/groups/SNS/rbac/>

NEW QUESTION 104

- (Topic 1)

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

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 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

NEW QUESTION 105

- (Topic 1)

Why should batch files and scripts be stored in a protected area?

- A. Because of the least privilege concept.
- B. Because they cannot be accessed by operators.
- C. Because they may contain credentials.
- D. Because of the need-to-know concept.

Answer: C

Explanation:

Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.

Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION 108

- (Topic 1)

What does the (star) integrity axiom mean in the Biba model?

- A. No read up
- B. No write down
- C. No read down
- D. No write up

Answer: D

Explanation:

The (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION 111

- (Topic 1)

Which division of the Orange Book deals with discretionary protection (need-to-know)?

- A. D
- B. C
- C. B
- D. A

Answer: B

Explanation:

C deals with discretionary protection. See matrix below:

TNI/TCSEC MATRIX

	A1	B3	B2	B1	C2	C1
DISCRETIONARY ACCESS						
Discretionary Access Control						
Identification and Authentication						
System Integrity						
System Architecture						
Security Testing						
Security Features User's Guide Trusted Facility						
Manual Design Documentation Test Documentation						
CONTROLLED ACCESS						
Protect Audit Trails						
Object Reuse						
MANDATORY ACCESS CONTROL						
Labels						
Mandatory Access Control						
Process isolation in system architecture						
Design Specification & Verification						
Device labels						
Subject Sensitivity Labels						
Trusted Path						
Separation of Administrator and User functions						
Covert Channel Analysis (Only Covert Storage Channel at B2)						
Trusted Facility Management						
Configuration Management						
Trusted Recovery						
Covert Channel Analysis (Both Timing and Covert Channel analysis at B3)						
Security Administrator Role Defined						
Monitor events and notify security personnel						
Trusted Distribution						
Formal Methods						
	A1	B3	B2	B1	C2	C1

C:\Users\MCS\Desktop\1.jpg

TCSEC Matric

The following are incorrect answers:

D is incorrect. D deals with minimal security.

B is incorrect. B deals with mandatory protection. A is incorrect. A deals with verified protection. Reference(s) used for this question:

CBK, p. 329 ?C 330

and

Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

NEW QUESTION 116

- (Topic 1)

Which of the following is NOT a compensating measure for access violations?

- A. Backups
- B. Business continuity planning
- C. Insurance
- D. Security awareness

Answer: D

Explanation:

Security awareness is a preventive measure, not a compensating measure for access violations.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 50).

NEW QUESTION 120

- (Topic 1)

What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

- A. Biometrics
- B. Micrometrics
- C. Macrometrics
- D. MicroBiometrics

Answer: A

Explanation:

The Answer Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION 123

- (Topic 1)

Examples of types of physical access controls include all EXCEPT which of the following?

- A. badges
- B. locks
- C. guards
- D. passwords

Answer: D

Explanation:

Passwords are considered a Preventive/Technical (logical) control. The following answers are incorrect:

badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.

locks Locks are a Preventative Physical control and has no Technical association. guards Guards are a Preventative Physical control and has no Technical association.

The following reference(s) were/was used to create this question:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 35).

NEW QUESTION 126

- (Topic 1)

What does it mean to say that sensitivity labels are "incomparable"?

- A. The number of classification in the two labels is different.
- B. Neither label contains all the classifications of the other.
- C. the number of categories in the two labels are different.
- D. Neither label contains all the categories of the other.

Answer: D

Explanation:

If a category does not exist then you cannot compare it. Incomparable is when you have two disjointed sensitivity labels, that is a category in one of the labels is not in the other label. "Because neither label contains all the categories of the other, the labels can't be compared. They're said to be incomparable"

COMPARABILITY:

The label:

TOP SECRET [VENUS ALPHA]

is "higher" than either of the labels:

SECRET [VENUS ALPHA] TOP SECRET [VENUS]

But you can't really say that the label:

TOP SECRET [VENUS]

is higher than the label:

SECRET [ALPHA]

Because neither label contains all the categories of the other, the labels can't be compared. They're said to be incomparable. In a mandatory access control system, you won't be allowed access to a file whose label is incomparable to your clearance.

The Multilevel Security policy uses an ordering relationship between labels known as the dominance relationship. Intuitively, we think of a label that dominates another as being "higher" than the other. Similarly, we think of a label that is dominated by another as being "lower" than the other. The dominance relationship is used to determine permitted operations and information flows.

DOMINANCE

The dominance relationship is determined by the ordering of the Sensitivity/Clearance component of the label and the intersection of the set of Compartments.

Sample Sensitivity/Clearance ordering are:

Top Secret > Secret > Confidential > Unclassified s3 > s2 > s1 > s0

Formally, for label one to dominate label 2 both of the following must be true: The sensitivity/clearance of label one must be greater than or equal to the sensitivity/clearance of label two.

The intersection of the compartments of label one and label two must equal the compartments of label two.

Additionally:

Two labels are said to be equal if their sensitivity/clearance and set of compartments are exactly equal. Note that dominance includes equality.

One label is said to strictly dominate the other if it dominates the other but is not equal to the other.

Two labels are said to be incomparable if each label has at least one compartment that is not included in the other's set of compartments.

The dominance relationship will produce a partial ordering over all possible MLS labels, resulting in what is known as the MLS Security Lattice.

The following answers are incorrect:

The number of classification in the two labels is different. Is incorrect because the categories are what is being compared, not the classifications.

Neither label contains all the classifications of the other. Is incorrect because the categories are what is being compared, not the classifications.

the number of categories in the two labels is different. Is incorrect because it is possible a category exists more than once in one sensitivity label and does exist in the other so they would be comparable.

Reference(s) used for this question:

OReilly - Computer Systems and Access Control (Chapter 3) <http://www.oreilly.com/catalog/csb/chapter/ch03.html>

and http://rubix.com/cms/mls_dom

NEW QUESTION 130

- (Topic 1)

In the context of access control, locks, gates, guards are examples of which of the following?

- A. Administrative controls
- B. Technical controls
- C. Physical controls
- D. Logical controls

Answer: C

Explanation:

Administrative, technical and physical controls are categories of access control mechanisms.

Logical and Technical controls are synonymous. So both of them could be eliminated as possible choices.

Physical Controls: These are controls to protect the organization's people and physical environment, such as locks, gates, and guards. Physical controls may be called "operational controls" in some contexts.

Physical security covers a broad spectrum of controls to protect the physical assets (primarily the people) in an organization. Physical Controls are sometimes referred to as "operational" controls in some risk management frameworks. These controls range from doors, locks, and windows to environment controls, construction standards, and guards. Typically, physical security is based on the notion of establishing security zones or concentric areas within a facility that require increased security as you get closer to the

valuable assets inside the facility. Security zones are the physical representation of the defense-in-depth principle discussed earlier in this chapter. Typically, security zones are associated with rooms, offices, floors, or smaller elements, such as a cabinet or storage locker. The design of the physical security controls within the facility must take into account the protection of the asset as well as the individuals working in that area.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1301-1303). Auerbach Publications. Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1312-1318). Auerbach Publications. Kindle Edition.

NEW QUESTION 133

- (Topic 1)

Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

- A. Wave pattern motion detectors
- B. Capacitance detectors
- C. Field-powered devices
- D. Audio detectors

Answer: B

Explanation:

Capacitance detectors monitor an electrical field surrounding the object being monitored. They are used for spot protection within a few inches of the object, rather than for overall room security monitoring used by wave detectors. Penetration of this field changes the electrical capacitance of the field enough to generate and alarm. Wave pattern motion detectors generate a frequency wave pattern and send an alarm if the pattern is disturbed as it is reflected back to its receiver. Field-powered devices are a type of personnel access control devices. Audio detectors simply monitor a room for any abnormal sound wave generation and trigger an alarm.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 344).

NEW QUESTION 134

- (Topic 1)

Access Control techniques do not include which of the following?

- A. Rule-Based Access Controls
- B. Role-Based Access Control
- C. Mandatory Access Control
- D. Random Number Based Access Control

Answer: D

Explanation:

Access Control Techniques Discretionary Access Control

Mandatory Access Control Lattice Based Access Control Rule-Based Access Control Role-Based Access Control

Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

NEW QUESTION 136

- (Topic 1)

A confidential number used as an authentication factor to verify a user's identity is called a:

- A. PIN
- B. User ID
- C. Password
- D. Challenge

Answer: A

Explanation:

PIN Stands for Personal Identification Number, as the name states it is a combination of numbers.

The following answers are incorrect:

User ID This is incorrect because a Userid is not required to be a number and a Userid is only used to establish identity not verify it.

Password. This is incorrect because a password is not required to be a number, it could be any combination of characters.

Challenge. This is incorrect because a challenge is not defined as a number, it could be anything.

NEW QUESTION 140

- (Topic 1)

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

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

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).

NEW QUESTION 141

- (Topic 1)

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:

- A. through access control mechanisms that require identification and authentication and through the audit function.
- B. through logical or technical controls involving the restriction of access to systems and the protection of information.
- C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.
- D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Answer: A

Explanation:

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 145

- (Topic 1)

Examples of types of physical access controls include all EXCEPT which of the following?

- A. badges
- B. locks
- C. guards
- D. passwords

Answer: D

Explanation:

Passwords are considered a Preventive/Technical (logical) control. The following answers are incorrect:

badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.

locks Locks are a Preventative Physical control and has no Technical association. guards Guards are a Preventative Physical control and has no Technical association.

The following reference(s) were/was used to create this question:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 35).

NEW QUESTION 147

- (Topic 1)

What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

- A. A
- B. D
- C. E
- D. F

Answer: B

Explanation:

D or "minimal protection" is reserved for systems that were evaluated under the TCSEC but did not meet the requirements for a higher trust level.

A is incorrect. A or "Verified Protection" is the highest trust level under the TCSEC. E is incorrect. The trust levels are A - D so "E" is not a valid trust level.

F is incorrect. The trust levels are A - D so "F" is not a valid trust level.

CBK, pp. 329 - 330

AIO3, pp. 302 - 306

NEW QUESTION 151

- (Topic 1)

Like the Kerberos protocol, SESAME is also subject to which of the following?

- A. timeslot replay
- B. password guessing
- C. symmetric key guessing
- D. asymmetric key guessing

Answer: B

Explanation:

Sesame is an authentication and access control protocol, that also supports communication confidentiality and integrity. It provides public key based authentication along with the Kerberos style authentication, that uses symmetric key cryptography. Sesame supports the Kerberos protocol and adds some security extensions like public key based authentication and an ECMA-style Privilege Attribute Service.

The users under SESAME can authenticate using either symmetric encryption as in Kerberos or Public Key authentication. When using Symmetric Key authentication as in Kerberos, SESAME is also vulnerable to password guessing just like Kerberos would be.

The Symmetric key being used is based on the password used by the user when he logged on the system. If the user has a simple password it could be guessed or compromise. Even thou Kerberos or SESAME may be use, there is still a need to have strong password discipline.

The Basic Mechanism in Sesame for strong authentication is as follow:

The user sends a request for authentication to the Authentication Server as in Kerberos, except that SESAME is making use of public key cryptography for

authentication where the client will present his digital certificate and the request will be signed using a digital signature. The signature is communicated to the authentication server through the preauthentication fields. Upon receipt of this request, the authentication server will verify the certificate, then validate the signature, and if all is fine the AS will issue a ticket granting ticket (TGT) as in Kerberos. This TGT will be used to communicate with the privilege attribute server (PAS) when access to a resource is needed.

Users may authenticate using either a public key pair or a conventional (symmetric) key. If public key cryptography is used, public key data is transported in preauthentication data fields to help establish identity.

Kerberos uses tickets for authenticating subjects to objects and SESAME uses Privileged Attribute Certificates (PAC), which contain the subject's identity, access capabilities for the object, access time period, and lifetime of the PAC. The PAC is digitally signed so that the object can validate that it came from the trusted authentication server, which is referred to as the privilege attribute server (PAS). The PAS holds a similar role as the KDC within Kerberos. After a user successfully authenticates to the authentication service (AS), he is presented with a token to give to the PAS. The PAS then creates a PAC for the user to present to the resource he is trying to access.

Reference(s) used for this question: <http://srg.cs.uiuc.edu/Security/nephilim/Internal/SESAME.txt>

and

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 43.

NEW QUESTION 152

- (Topic 1)

Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are some of the examples of:

- A. Administrative controls
- B. Logical controls
- C. Technical controls
- D. Physical controls

Answer: D

Explanation:

Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are all examples of Physical Security.

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 33.

NEW QUESTION 157

- (Topic 1)

Which of the following is most appropriate to notify an internal user that session monitoring is being conducted?

- A. Logon Banners
- B. Wall poster
- C. Employee Handbook
- D. Written agreement

Answer: D

Explanation:

This is a tricky question, the keyword in the question is Internal users.

There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous/external users.

Internal users should always have a written agreement first, then logon banners serve as a constant reminder.

Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system, who is authorized and unauthorized, and if it is an unauthorized user then he is fully aware of trespassing. Anonymous/External users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.

References 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 50.

and

Shon Harris, CISSP All-in-one, 5th edition, pg 873

NEW QUESTION 160

- (Topic 1)

Which of the following Kerberos components holds all users' and services' cryptographic keys?

- A. The Key Distribution Service
- B. The Authentication Service
- C. The Key Distribution Center
- D. The Key Granting Service

Answer: C

Explanation:

The Key Distribution Center (KDC) holds all users' and services' cryptographic keys. It provides authentication services, as well as key distribution functionality.

The Authentication Service is the part of the KDC that authenticates a principal. The Key Distribution Service and Key Granting Service are distracters and are not defined Kerberos components.

Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION 163

- (Topic 1)

Which of the following is most appropriate to notify an external user that session monitoring is being conducted?

- A. Logon Banners

- B. Wall poster
- C. Employee Handbook
- D. Written agreement

Answer: A

Explanation:

Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system and if it is an unauthorized user then he is fully aware of trespassing.

This is a tricky question, the keyword in the question is External user.

There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous user.

Internal users should always have a written agreement first, then logon banners serve as a constant reminder.

Anonymous users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.

References 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 50.

and

Shon Harris, CISSP All-in-one, 5th edition, pg 873

NEW QUESTION 168

- (Topic 1)

Which access control model is best suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

- A. DAC
- B. MAC
- C. Access control matrix
- D. TACACS

Answer: B

Explanation:

MAC provides high security by regulating access based on the clearance of individual users and sensitivity labels for each object. Clearance levels and sensitivity levels cannot be modified by individual users -- for example, user Joe (SECRET clearance) cannot reclassify the "Presidential Doughnut Recipe" from "SECRET" to "CONFIDENTIAL" so that his friend Jane (CONFIDENTIAL clearance) can read it. The administrator is ultimately responsible for configuring this protection in accordance with security policy and directives from the Data Owner.

DAC is incorrect. In DAC, the data owner is responsible for controlling access to the object. Access control matrix is incorrect. The access control matrix is a way of thinking about the

access control needed by a population of subjects to a population of objects. This access

control can be applied using rules, ACL's, capability tables, etc.

TACACS is incorrect. TACACS is a tool for performing user authentication. References:

CBK, p. 187, Domain 2: Access Control. AIO3, Chapter 4, Access Control.

NEW QUESTION 171

- (Topic 1)

Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?

- A. Preventive/Administrative Pairing
- B. Preventive/Technical Pairing
- C. Preventive/Physical Pairing
- D. Detective/Technical Pairing

Answer: B

Explanation:

Preventive/Technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 172

- (Topic 1)

What is considered the most important type of error to avoid for a biometric access control system?

- A. Type I Error
- B. Type II Error
- C. Combined Error Rate
- D. Crossover Error Rate

Answer: B

Explanation:

When a biometric system is used for access control, the most important error is the false accept or false acceptance rate, or Type II error, where the system would accept an impostor.

A Type I error is known as the false reject or false rejection rate and is not as important in the security context as a type II error rate. A type one is when a valid company employee is rejected by the system and he cannot get access even thou it is a valid user.

The Crossover Error Rate (CER) is the point at which the false rejection rate equals the false acceptance rate if your would create a graph of Type I and Type II errors. The lower the CER the better the device would be.

The Combined Error Rate is a distracter and does not exist.

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 10).

NEW QUESTION 175

- (Topic 1)

Which of the following best ensures accountability of users for the actions taken within a system or domain?

- A. Identification
- B. Authentication
- C. Authorization
- D. Credentials

Answer: B

Explanation:

Details:

The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be. After showing proper credentials, a user is authorized access to resources.

References:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

NEW QUESTION 177

- (Topic 1)

What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?

- A. Authentication
- B. Identification
- C. Authorization
- D. Confidentiality

Answer: B

Explanation:

Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system.

Identification is nothing more than claiming you are somebody. You identify yourself when you speak to someone on the phone that you don't know, and they ask you who they're speaking to. When you say, "I'm Jason", you've just identified yourself.

In the information security world, this is analogous to entering a username. It's not analogous to entering a password. Entering a password is a method for verifying that you are who you identified yourself as.

NOTE: The word "professing" used above means: "to say that you are, do, or feel something when other people doubt what you say". This is exactly what happens when you provide your identifier (identification), you claim to be someone but the system cannot take your word for it, you must further Authenticate to the system to prove who you claim to be.

The following are incorrect answers:

Authentication: is how one proves that they are who they say they are. When you claim to be Jane Smith by logging into a computer system as "jsmith", it's most likely going to ask you for a password. You've claimed to be that person by entering the name into the username field (that's the identification part), but now you have to prove that you are really that person.

Many systems use a password for this, which is based on "something you know", i.e. a secret between you and the system.

Another form of authentication is presenting something you have, such as a driver's license, an RSA token, or a smart card.

You can also authenticate via something you are. This is the foundation for biometrics. When you do this, you first identify yourself and then submit a thumb print, a retina scan, or another form of bio-based authentication.

Once you've successfully authenticated, you have now done two things: you've claimed to be someone, and you've proven that you are that person. The only thing that's left is for the system to determine what you're allowed to do.

Authorization: is what takes place after a person has been both identified and authenticated; it's the step determines what a person can then do on the system. An example in people terms would be someone knocking on your door at night. You say, "Who is it?", and wait for a response. They say, "It's John." in order to identify themselves. You ask them to back up into the light so you can see them through the peephole. They do so, and you authenticate them based on what they look like (biometric). At that point you decide they can come inside the house.

If they had said they were someone you didn't want in your house (identification), and you then verified that it was that person (authentication), the authorization phase would not include access to the inside of the house.

Confidentiality: Is one part of the CIA triad. It prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is a credit card number while shopping online, the merchant needs it to clear the transaction but you do not want your information exposed over the network, you would use a secure link such as SSL, TLS, or some tunneling tool to protect the information from prying eyes between point A and point B. Data encryption is a common method of ensuring confidentiality.

The other parts of the CIA triad are listed below:

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. If an unexpected change occurs, a backup copy must be available to restore the affected data to its correct state.

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, providing a certain measure of redundancy and failover, providing adequate communications bandwidth and preventing the occurrence of bottlenecks, implementing emergency backup power systems, keeping current with all necessary system upgrades, and guarding against malicious actions such as denial-of-service (DoS) attacks.

Reference used for this question:

<http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> <http://www.danielmiessler.com/blog/security-identification-authentication-and-authorization> <http://www.merriam-webster.com/dictionary/profess>

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION 181

- (Topic 1)

Access Control techniques do not include which of the following choices?

- A. Relevant Access Controls
- B. Discretionary Access Control
- C. Mandatory Access Control
- D. Lattice Based Access Control

Answer: A

Explanation:

Access Control Techniques Discretionary Access Control

Mandatory Access Control Lattice Based Access Control Rule-Based Access Control Role-Based Access Control

Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

NEW QUESTION 186

- (Topic 1)

Which access control model is also called Non Discretionary Access Control (NDAC)?

- A. Lattice based access control
- B. Mandatory access control
- C. Role-based access control
- D. Label-based access control

Answer: C

Explanation:

RBAC is sometimes also called non-discretionary access control (NDAC) (as Ferraiolo says "to distinguish it from the policy-based specifics of MAC"). Another model that fits within the NDAC category is Rule-Based Access Control (RuBAC or RBAC). Most of the CISSP books use the same acronym for both models but NIST tend to use a lowercase "u" in between R and B to differentiate the two models.

You can certainly mimic MAC using RBAC but true MAC makes use of Labels which contains the sensitivity of the objects and the categories they belong to. No labels means MAC is not being used.

One of the most fundamental data access control decisions an organization must make is the amount of control it will give system and data owners to specify the level of access users of that data will have. In every organization there is a balancing point between the access controls enforced by organization and system policy and the ability for information owners to determine who can have access based on specific business requirements. The process of translating that balance into a workable access control model can be defined by three general access frameworks:

Discretionary access control Mandatory access control Nondiscretionary access control

A role-based access control (RBAC) model bases the access control authorizations on the roles (or functions) that the user is assigned within an organization. The determination of what roles have access to a resource can be governed by the owner of the data, as with DACs, or applied based on policy, as with MACs.

Access control decisions are based on job function, previously defined and governed by policy, and each role (job function) will have its own access capabilities.

Objects associated with a role will inherit privileges assigned to that role. This is also true for groups of users, allowing administrators to simplify access control strategies by assigning users to groups and groups to roles.

There are several approaches to RBAC. As with many system controls, there are variations on how they can be applied within a computer system.

There are four basic RBAC architectures:

1. Non-RBAC: Non-RBAC is simply a user-granted access to data or an application by traditional mapping, such as with ACLs. There are no formal ??roles?? associated with the mappings, other than any identified by the particular user.
2. Limited RBAC: Limited RBAC is achieved when users are mapped to roles within a single application rather than through an organization-wide role structure. Users in a limited RBAC system are also able to access non-RBAC-based applications or data. For example, a user may be assigned to multiple roles within several applications and, in addition, have direct access to another application or system independent of his or her assigned role. The key attribute of limited RBAC is that the role for that user is defined within an application and not necessarily based on the user??s organizational job function.
3. Hybrid RBAC: Hybrid RBAC introduces the use of a role that is applied to multiple applications or systems based on a user??s specific role within the organization. That role is then applied to applications or systems that subscribe to the organization??s role-based model. However, as the term ??hybrid?? suggests, there are instances where the subject may also be assigned to roles defined solely within specific applications, complimenting (or, perhaps, contradicting) the larger, more encompassing organizational role used by other systems.
4. Full RBAC: Full RBAC systems are controlled by roles defined by the organization??s policy and access control infrastructure and then applied to applications and systems across the enterprise. The applications, systems, and associated data apply permissions based on that enterprise definition, and not one defined by a specific application or system. Be careful not to try to make MAC and DAC opposites of each other -- they are two different access control strategies with RBAC being a third strategy that was defined later to address some of the limitations of MAC and DAC.

The other answers are not correct because:

Mandatory access control is incorrect because though it is by definition not discretionary, it is not called "non-discretionary access control." MAC makes use of label to indicate the sensitivity of the object and it also makes use of categories to implement the need to know.

Label-based access control is incorrect because this is not a name for a type of access control but simply a bogus detractor.

Lattice based access control is not adequate either. A lattice is a series of levels and a subject will be granted an upper and lower bound within the series of levels.

These levels could be sensitivity levels or they could be confidentiality levels or they could be integrity levels.

Reference(s) used for this question: All in One, third edition, page 165.

Ferraiolo, D., Kuhn, D. & Chandramouli, R. (2003). Role-Based Access Control, p. 18.

Ferraiolo, D., Kuhn, D. (1992). Role-Based Access Controls. http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html

Schneider, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 1557-1584). Auerbach Publications. Kindle Edition.

Schneider, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 1474-1477). Auerbach Publications. Kindle Edition.

NEW QUESTION 189

- (Topic 1)

In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?

- A. Access-Accept
- B. Access-Reject
- C. Access-Granted
- D. Access-Challenge

Answer: C

Explanation:

In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier.

Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

NEW QUESTION 192

- (Topic 1)

The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:

- A. you need.
- B. you read.
- C. you are.
- D. you do.

Answer: C

Explanation:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 193

- (Topic 1)

Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?

- A. SESAME
- B. RADIUS
- C. KryptoKnight
- D. TACACS+

Answer: A

Explanation:

Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support.

Reference:

TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 184. ISC OIG Second Edition, Access Controls, Page 111

NEW QUESTION 196

- (Topic 1)

Which access model is most appropriate for companies with a high employee turnover?

- A. Role-based access control
- B. Mandatory access control
- C. Lattice-based access control
- D. Discretionary access control

Answer: A

Explanation:

The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company.

Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitly inherit the permissions of the role or roles they have been assigned to. When they leave the company or change jobs, their role assignment is revoked/changed appropriately.

Mandatory access control is incorrect. While controlling access based on the clearance level of employees and the sensitivity of objects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company.

Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc).

In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324- 325.

Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.

References

All in One, third edition page 165

RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

NEW QUESTION 201

- (Topic 1)

Which TCSEC level is labeled Controlled Access Protection?

- A. C1
- B. C2
- C. C3
- D. B1

Answer: B

Explanation:

C2 is labeled Controlled Access Protection.

The TCSEC defines four divisions: D, C, B and A where division A has the highest security. Each division represents a significant difference in the trust an individual or organization

can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1.

Each division and class expands or modifies as indicated the requirements of the immediately prior division or class.

D ?? Minimal protection

Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division

C ?? Discretionary protection

C1 ?? Discretionary Security Protection Identification and authentication Separation of users and data

Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis

Required System Documentation and user manuals C2 ?? Controlled Access Protection

More finely grained DAC

Individual accountability through login procedures Audit trails

Object reuse Resource isolation

B ?? Mandatory protection

B1 ?? Labeled Security Protection

Informal statement of the security policy model Data sensitivity labels

Mandatory Access Control (MAC) over selected subjects and objects Label exportation capabilities

All discovered flaws must be removed or otherwise mitigated Design specifications and verification

B2 ?? Structured Protection

Security policy model clearly defined and formally documented DAC and MAC enforcement extended to all subjects and objects

Covert storage channels are analyzed for occurrence and bandwidth Carefully structured into protection-critical and non-protection-critical elements Design and implementation enable more comprehensive testing and review Authentication mechanisms are strengthened

Trusted facility management is provided with administrator and operator segregation Strict configuration management controls are imposed

B3 ?? Security Domains

Satisfies reference monitor requirements

Structured to exclude code not essential to security policy enforcement Significant system engineering directed toward minimizing complexity Security administrator role defined

Audit security-relevant events

Automated imminent intrusion detection, notification, and response Trusted system recovery procedures

Covert timing channels are analyzed for occurrence and bandwidth

An example of such a system is the XTS-300, a precursor to the XTS-400 A ?? Verified protection

A1 ?? Verified Design Functionally identical to B3

Formal design and verification techniques including a formal top-level specification Formal management and distribution procedures

An example of such a system is Honeywell's Secure Communications Processor SCOMP, a precursor to the XTS-400

Beyond A1

System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB).

Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications.

Formal Specification and Verification is where the TCB is verified down to the source code level, using formal verification methods where feasible.

Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.

The following are incorrect answers: C1 is Discretionary security

C3 does not exist, it is only a detractor

B1 is called Labeled Security Protection.

Reference(s) used for this question:

HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

and

AI0v4 Security Architecture and Design (pages 357 - 361) AI0v5 Security Architecture and Design (pages 358 - 362)

NEW QUESTION 203

- (Topic 1)

Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

- A. Accountability of biometrics systems
- B. Acceptability of biometrics systems
- C. Availability of biometrics systems
- D. Adaptability of biometrics systems

Answer: B

Explanation:

Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

NEW QUESTION 206

- (Topic 1)

What is a common problem when using vibration detection devices for perimeter control?

- A. They are vulnerable to non-adversarial disturbances.
- B. They can be defeated by electronic means.
- C. Signal amplitude is affected by weather conditions.
- D. They must be buried below the frost line.

Answer: A

Explanation:

Vibration sensors are similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.

Such sensors are prone to false positive. If there is a large truck with heavy equipment driving by it may trigger the sensor. The same with a storm with thunder and lightning, it may trigger the alarm even though there are no adversarial threat or disturbance.

The following are incorrect answers: All of the other choices are incorrect. Reference used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (pp. 495-496).

McGraw-Hill . Kindle Edition.

NEW QUESTION 209

- (Topic 1)

Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

- A. Limiting the local access of operations personnel
- B. Job rotation of operations personnel
- C. Management monitoring of audit logs
- D. Enforcing regular password changes

Answer: A

Explanation:

The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.

Management monitoring of audit logs is a detective control and it would not prevent collusion.

Changing passwords regularly would not prevent such attack.

This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be forced to use collusion to defeat those security mechanisms.

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 212

- (Topic 1)

What are called user interfaces that limit the functions that can be selected by a user?

- A. Constrained user interfaces
- B. Limited user interfaces
- C. Mini user interfaces
- D. Unlimited user interfaces

Answer: A

Explanation:

Constrained user interfaces limit the functions that can be selected by a user.

Another method for controlling access is by restricting users to specific functions based on their role in the system. This is typically implemented by limiting available menus, data views, encryption, or by physically constraining the user interfaces.

This is common on devices such as an automated teller machine (ATM). The advantage of a constrained user interface is that it limits potential avenues of attack and system failure by restricting the processing options that are available to the user.

On an ATM machine, if a user does not have a checking account with the bank he or she will not be shown the "Withdraw money from checking" option.

Likewise, an information system might have an "Add/Remove Users" menu option for administrators, but if a normal, non-administrative user logs in he or she will not even see that menu option. By not even identifying potential options for non-qualifying users, the system limits the potentially harmful execution of unauthorized system or application commands.

Many database management systems have the concept of "views." A database view is an extract of the data stored in the database that is filtered based on predefined user or system criteria. This permits multiple users to access the same database while only having the ability to access data they need (or are allowed to have) and not data for another user. The use of database views is another example of a constrained user interface.

The following were incorrect answers:

All of the other choices presented were bogus answers.

The following reference(s) were used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1989-2002). Auerbach Publications. Kindle Edition.

NEW QUESTION 213

- (Topic 1)

Which of the following access control models requires security clearance for subjects?

- A. Identity-based access control
- B. Role-based access control
- C. Discretionary access control
- D. Mandatory access control

Answer: D

Explanation:

With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance.

Identity-based access control is a type of discretionary access control. A role-based access control is a type of non-discretionary access control.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION 216

- (Topic 1)

What security model is dependent on security labels?

- A. Discretionary access control
- B. Label-based access control
- C. Mandatory access control
- D. Non-discretionary access control

Answer: C

Explanation:

With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and

the classification or sensitivity of the object. Label-based access control is not defined. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION 221

- (Topic 1)

What is the difference between Access Control Lists (ACLs) and Capability Tables?

- A. Access control lists are related/attached to a subject whereas capability tables are related/attached to an object.
- B. Access control lists are related/attached to an object whereas capability tables are related/attached to a subject.
- C. Capability tables are used for objects whereas access control lists are used for users.
- D. They are basically the same.

Answer: B

Explanation:

Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's possession of a capability (or ticket) for the object. It is a row within the matrix.

To put it another way, A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.

CLEMENT NOTE:

If we wish to express this very simply:

Capabilities are attached to a subject and it describes what access the subject has to each of the objects on the row that matches with the subject within the matrix.

It is a row within the matrix.

ACL's are attached to objects, it describes who has access to the object and what type of access they have. It is a column within the matrix.

The following are incorrect answers:

"Access control lists are subject-based whereas capability tables are object-based" is incorrect.

"Capability tables are used for objects whereas access control lists are used for users" is incorrect.

"They are basically the same" is incorrect. References used for this question:

CBK, pp. 191 - 192

AIO3 p. 169

NEW QUESTION 222

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SSCP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SSCP Product From:

<https://www.2passeasy.com/dumps/SSCP/>

Money Back Guarantee

SSCP Practice Exam Features:

- * SSCP Questions and Answers Updated Frequently
- * SSCP Practice Questions Verified by Expert Senior Certified Staff
- * SSCP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SSCP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year