

Exam Questions SSCP

System Security Certified Practitioner (SSCP)

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



NEW QUESTION 1

- (Topic 1)

Which is the last line of defense in a physical security sense?

- A. people
- B. interior barriers
- C. exterior barriers
- D. perimeter barriers

Answer: A

Explanation:

"Ultimately, people are the last line of defense for your company's assets" (Pastore & Dulaney, 2006, p. 529).

Pastore, M. and Dulaney, E. (2006). CompTIA Security+ study guide: Exam SY0-101. Indianapolis, IN: Sybex.

NEW QUESTION 2

- (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 3

- (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 4

- (Topic 1)

Which of the following is most affected by denial-of-service (DOS) attacks?

- A. Confidentiality
- B. Integrity
- C. Accountability
- D. Availability

Answer: D

Explanation:

Denial of service attacks obviously affect availability of targeted systems. 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 61).

NEW QUESTION 5

- (Topic 1)

Which of the following centralized access control mechanisms is the least appropriate for mobile workers accessing the corporate network over analog lines?

- A. TACACS
- B. Call-back
- C. CHAP
- D. RADIUS

Answer: B

Explanation:

Call-back allows for a distant user connecting into a system to be called back at a number already listed in a database of trusted users. The disadvantage of this system is that the user must be at a fixed location whose phone number is known to the authentication server. Being mobile workers, users are accessing the system from multiple

locations, making call-back inappropriate for them.

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 44).

NEW QUESTION 6

- (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 7

- (Topic 1)

Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?

- A. Using a TACACS+ server.
- B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
- C. Setting modem ring count to at least 5.
- D. Only attaching modems to non-networked hosts.

Answer: B

Explanation:

Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.

The use of a TACACS+ Server by itself cannot eliminate hacking.

Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.

Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

NEW QUESTION 8

- (Topic 1)

Which access control type has a central authority that determine 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 include Role Based Access Control (RBAC) and Rule Based Access Control (RBAC or RuBAC). RABC 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 is 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 9

- (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 10

- (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 10

- (Topic 1)

The control measures that are intended to reveal the violations of security policy using software and hardware are associated with:

- A. Preventive/physical
- B. Detective/technical
- C. Detective/physical
- D. Detective/administrative

Answer: B

Explanation:

The detective/technical control measures are intended to reveal the violations of security policy using technical means.

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 15

- (Topic 1)

Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?

- A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
- B. The initial logon process is cumbersome to discourage potential intruders.
- C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
- D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems

Answer: A

Explanation:

Single Sign-On is a distributed Access Control methodology where an individual only has to authenticate once and would have access to all primary and secondary network domains. The individual would not be required to re-authenticate when they needed additional resources. The security issue that this creates is if a fraudster is able to compromise those credential they too would have access to all the resources that account has access to.

All the other answers are incorrect as they are distractors.

NEW QUESTION 18

- (Topic 1)

Which security model is based on the military classification of data and people with clearances?

- A. Brewer-Nash model
- B. Clark-Wilson model
- C. Bell-LaPadula model
- D. Biba model

Answer: C

Explanation:

The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model. The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity.

Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION 22

- (Topic 1)

Which of the following is the most reliable authentication method for remote access?

- A. Variable callback system
- B. Synchronous token
- C. Fixed callback system
- D. Combination of callback and caller ID

Answer: B

Explanation:

A Synchronous token generates a one-time password that is only valid for a short period of time. Once the password is used it is no longer valid, and it expires if not entered in the acceptable time frame.

The following answers are incorrect:

Variable callback system. Although variable callback systems are more flexible than fixed callback systems, the system assumes the identity of the individual unless two-factor authentication is also implemented. By itself, this method might allow an attacker access as a trusted user.

Fixed callback system. Authentication provides assurance that someone or something is who or what he/it is supposed to be. Callback systems authenticate a person, but anyone can pretend to be that person. They are tied to a specific place and phone number, which can be spoofed by implementing call-forwarding.

Combination of callback and Caller ID. The caller ID and callback functionality provides greater confidence and auditability of the caller's identity. By disconnecting and calling back only authorized phone numbers, the system has a greater confidence in the location of the call. However, unless combined with strong authentication, any individual at the location could obtain access.

The following reference(s) were/was used to create this question: Shon Harris AIO v3 p. 140, 548

ISC2 OIG 2007 p. 152-153, 126-127

NEW QUESTION 26

- (Topic 1)

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

- A. you need.
- B. non-trivial
- C. you are.
- D. you can get.

Answer: C

Explanation:

This is more commonly known as biometrics and is one of the most accurate ways to authenticate an individual.

The rest of the answers are incorrect because they not one of the three recognized forms for Authentication.

NEW QUESTION 28

- (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 32

- (Topic 1)

Which of the following control pairings include: organizational policies and procedures, pre- employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?

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

Answer: A

Explanation:

The Answer: Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.

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 35

- (Topic 1)

Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?

- A. Dynamic authentication
- B. Continuous authentication
- C. Encrypted authentication
- D. Robust authentication

Answer: B

Explanation:

Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit

of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter.

Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 34).

NEW QUESTION 38

- (Topic 1)

Which of the following statements pertaining to access control is false?

- A. Users should only access data on a need-to-know basis.
- B. If access is not explicitly denied, it should be implicitly allowed.
- C. Access rights should be granted based on the level of trust a company has on a subject.
- D. Roles can be an efficient way to assign rights to a type of user who performs certain tasks.

Answer: B

Explanation:

Access control mechanisms should default to no access to provide the necessary level of security and ensure that no security holes go unnoticed. If access is not explicitly allowed, it should be implicitly denied.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 4: Access Control (page 143).

NEW QUESTION 41

- (Topic 1)

How would nonrepudiation be best classified as?

- A. A preventive control
- B. A logical control
- C. A corrective control
- D. A compensating control

Answer: A

Explanation:

Systems accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Because the mechanisms implemented in nonrepudiation prevent the ability to successfully repudiate an action, it can be considered as a preventive control.

Source: STONEBURNER, Gary, NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology, December 2001, page 7.

NEW QUESTION 42

- (Topic 1)

A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:

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

Answer: C

Explanation:

A central authority determines what subjects can have access to certain objects based on the organizational security policy.

The key focal point of this question is the 'central authority' that determines access rights. Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as:

"MAC Policy means that Access Control Policy Decisions are made by a CENTRAL

AUTHORITY. Which seems to indicate there could be two good answers to this question.

However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy.

Within the same document it is also mentioned: "In general, all access control policies other than DAC are grouped in the category of non- discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action."

Under NDAC you have two choices:

Rule Based Access control and Role Base Access Control

MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC.

This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control.

The following are incorrect answers: MANDATORY ACCESS CONTROL

In Mandatory Access Control the labels of the object and the clearance of the subject

determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed.

The need for a MAC mechanism arises when the security policy of a system dictates that:

* 1. Protection decisions must not be decided by the object owner.

* 2. The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the “simple security rule,” or “no read up.”

Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the “*-property” (pronounced

“star property”) or “no write down.” The *-property is required to maintain system security in an automated environment.

DISCRETIONARY ACCESS CONTROL

In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority.

DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file.

DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons: First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann's file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann's file without Ann's knowledge.

Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann's files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows:

Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system.

No restrictions apply to the usage of information when the user has received it.

The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization's security requirements.

ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy.

RULE BASED ACCESS CONTROL

In Rule-based Access Control a central authority could in fact determine what subjects can

have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer.

RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC.

“Rule-based access” is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices.

Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control—for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be re configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting. Some provisions of access control systems have rule-based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.

References used for this question: <http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf> and

AIO v3 p162-167 and OIG (2007) p.186-191

also

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 44

- (Topic 1)

Which of the following choices describe a Challenge-response tokens generation?

- A. A workstation or system that generates a random challenge string that the user enters into the token when prompted along with the proper PIN.
- B. A workstation or system that generates a random login id that the user enters when prompted along with the proper PIN.
- C. A special hardware device that is used to generate random text in a cryptography system.
- D. The authentication mechanism in the workstation or system does not determine if the owner should be authenticated.

Answer: A

Explanation:

Challenge-response tokens are:

- A workstation or system generates a random challenge string and the owner enters the string into the token along with the proper PIN.
- The token generates a response that is then entered into the workstation or system.
- The authentication mechanism in the workstation or system then determines if the owner should be authenticated.

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

Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 136-137).

NEW QUESTION 48

- (Topic 1)

In addition to the accuracy of the biometric systems, there are other factors that must also be considered:

- A. These factors include the enrollment time and the throughput rate, but not acceptability.
- B. These factors do not include the enrollment time, the throughput rate, and acceptability.
- C. These factors include the enrollment time, the throughput rate, and acceptability.
- D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.

Answer: C

Explanation:

In addition to the accuracy of the biometric systems, there are other factors that must also be considered.

These factors include the enrollment time, the throughput rate, and acceptability. Enrollment time is the time it takes to initially "register" with a system by providing samples

of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes.

For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.

In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.

Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.

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

NEW QUESTION 49

- (Topic 1)

Which of the following biometric parameters are better suited for authentication use over a long period of time?

- A. Iris pattern
- B. Voice pattern
- C. Signature dynamics
- D. Retina pattern

Answer: A

Explanation:

The iris pattern is considered lifelong. Unique features of the iris are: freckles, rings, rifts, pits, striations, fibers, filaments, furrows, vasculature and coronas. Voice, signature and retina patterns are more likely to change over time, thus are not as suitable for authentication over a long period of time without needing re-enrollment. Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 1 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

NEW QUESTION 54

- (Topic 1)

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 a biometric authentication system, the system becomes increasingly selective and has the possibility of generating:

- A. Lower False Rejection Rate (FRR)
- B. Higher False Rejection Rate (FRR)
- C. Higher False Acceptance Rate (FAR)
- D. It will not affect either FAR or FRR

Answer: B

Explanation:

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 a biometric authentication system, the system becomes increasingly selective and has a higher False Rejection Rate (FRR).

Conversely, if the sensitivity is decreased, the False Acceptance Rate (FRR) will increase. Thus, to have a valid measure of the system performance, the Cross Over Error (CER) rate is used. The Crossover Error Rate (CER) is the point at which the false rejection rates and the false acceptance rates are equal. The lower the value of the CER, the more accurate the system.

There are three categories of biometric accuracy measurement (all represented as percentages):

False Reject Rate (a Type I Error): When authorized users are falsely rejected as unidentified or unverified.

False Accept Rate (a Type II Error): When unauthorized persons or imposters are falsely accepted as authentic.

Crossover Error Rate (CER): The point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.

NOTE:

Within the ISC2 book they make use of the term Accept or Acceptance and also Reject or Rejection when referring to the type of errors within biometrics. Below we make use of Acceptance and Rejection throughout the text for consistency. However, on the real exam you could see either of the terms.

Performance of biometrics

Different metrics can be used to rate the performance of a biometric factor, solution or application. The most common performance metrics are the False Acceptance Rate FAR and the False Rejection Rate FRR.

When using a biometric application for the first time the user needs to enroll to the system. The system requests fingerprints, a voice recording or another biometric factor from the

operator, this input is registered in the database as a template which is linked internally to a user ID. The next time when the user wants to authenticate or identify himself, the biometric input provided by the user is compared to the template(s) in the database by a matching algorithm which responds with acceptance (match) or rejection (no match).

FAR and FRR

The FAR or False Acceptance rate is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a valid template. The FAR is normally expressed as a percentage, following the FAR definition this is the percentage of invalid inputs which are incorrectly accepted.

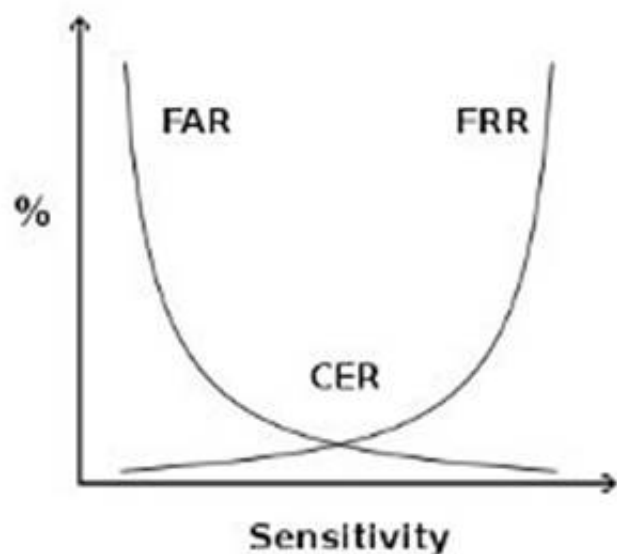
The FRR or False Rejection Rate is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input provided by the user with a stored template. The FRR is normally expressed as a percentage, following the FRR definition this is the percentage of valid inputs which are incorrectly rejected.

FAR and FRR are very much dependent on the biometric factor that is used and on the technical implementation of the biometric solution. Furthermore the FRR is strongly person dependent, a personal FRR can be determined for each individual.

Take this into account when determining the FRR of a biometric solution, one person is insufficient to establish an overall FRR for a solution. Also FRR might increase due to environmental conditions or incorrect use, for example when using dirty fingers on a fingerprint reader. Mostly the FRR lowers when a user gains more experience in how to use the biometric device or software.

FAR and FRR are key metrics for biometric solutions, some biometric devices or software even allow to tune them so that the system more quickly matches or rejects. Both FRR and FAR are important, but for most applications one of them is considered most important. Two examples to illustrate this:

When biometrics are used for logical or physical access control, the objective of the application is to disallow access to unauthorized individuals under all circumstances. It is clear that a very low FAR is needed for such an application, even if it comes at the price of a higher FRR. When surveillance cameras are used to screen a crowd of people for missing children, the objective of the application is to identify any missing children that come up on the screen. When the identification of those children is automated using a face recognition software, this software has to be set up with a low FRR. As such a higher number of matches will be false positives, but these can be reviewed quickly by surveillance personnel. False Acceptance Rate is also called False Match Rate, and False Rejection Rate is sometimes referred to as False Non-Match Rate. crossover error rate



crossover error rate

Above see a graphical representation of FAR and FRR errors on a graph, indicating the CER

CER

The Crossover Error Rate or CER is illustrated on the graph above. It is the rate where both FAR and FRR are equal.

The matching algorithm in a biometric software or device uses a (configurable) threshold which determines how close to a template the input must be for it to be considered a match. This threshold value is in some cases referred to as sensitivity, it is marked on the X axis of the plot. When you reduce this threshold there will be more false acceptance errors (higher FAR) and less false rejection errors (lower FRR), a higher threshold will lead to lower FAR and higher FRR.

Speed

Most manufacturers of biometric devices and softwares can give clear numbers on the time it takes to enroll as well on the time for an individual to be authenticated or identified using their application. If speed is important then take your time to consider this, 5 seconds might seem a short time on paper or when testing a device but if hundreds of people will use the device multiple times a day the cumulative loss of time might be significant.

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 2723-2731). Auerbach Publications. Kindle Edition.

and

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

and

http://www.biometric-solutions.com/index.php?story=performance_biometrics

NEW QUESTION 55

- (Topic 1)

What are the components of an object's sensitivity label?

- A. A Classification Set and a single Compartment.
- B. A single classification and a single compartment.
- C. A Classification Set and user credentials.
- D. A single classification and a Compartment Set.

Answer: D

Explanation:

Both are the components of a sensitivity label. The following are incorrect:

A Classification Set and a single Compartment. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classification and it is not a "single compartment" but a Compartment Set.

A single classification and a single compartment. Is incorrect because while there only is one classification, it is not a "single compartment" but a Compartment Set.

A Classification Set and user credentials. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classification and it is not "user credential" but a Compartment Set. The user would have their own sensitivity label.

NEW QUESTION 58

- (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 59

- (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 64

- (Topic 1)

Which of the following would be true about Static password tokens?

- A. The owner identity is authenticated by the token
- B. The owner will never be authenticated by the token.
- C. The owner will authenticate himself to the system.
- D. The token does not authenticates the token owner but the system.

Answer: A

Explanation:

Password Tokens

Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.

Static Password Tokens:

The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.

Synchronous Dynamic Password Tokens:

This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.

Asynchronous Dynamic Password Tokens:

The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).

Challenge Response Tokens:

This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.

Reference(s) used for this question: <http://www.informit.com/guides/content.aspx?g=security&seqNum=146>

and

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

NEW QUESTION 65

- (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 69

- (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 acces 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 70

- (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

AI03, pp. 290 - 291

AI0v4 Security Architecture and Design (page 345)

AI0v5 Security Architecture and Design (pages 347 - 348)

https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models#Noninterference_Models

NEW QUESTION 72

- (Topic 1)

What is called a sequence of characters that is usually longer than the allotted number for a password?

- A. passphrase
- B. cognitive phrase
- C. anticipated phrase
- D. Real phrase

Answer: A

Explanation:

A passphrase is a sequence of characters that is usually longer than the allotted number for a password.

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

NEW QUESTION 74

- (Topic 1)

What does the simple integrity axiom mean in the Biba model?

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

Answer: B

Explanation:

The simple integrity axiom of the Biba access control model states that a subject at one level of integrity is not permitted to observe an object of a lower integrity (no read 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 205).

NEW QUESTION 78

- (Topic 1)

Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

- A. Extensible Authentication Protocol
- B. Challenge Handshake Authentication Protocol
- C. Remote Authentication Dial-In User Service
- D. Multilevel Authentication Protocol.

Answer: A

Explanation:

RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 79

- (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 81

- (Topic 1)

Which of the following statements pertaining to Kerberos is TRUE?

- A. Kerberos does not address availability
- B. Kerberos does not address integrity
- C. Kerberos does not make use of Symmetric Keys
- D. Kerberos cannot address confidentiality of information

Answer: A

Explanation:

The question was asking for a TRUE statement and the only correct statement is "Kerberos does not address availability".

Kerberos addresses the confidentiality and integrity of information. It does not directly address availability.

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 42).

NEW QUESTION 83

- (Topic 1)

What is the main focus of the Bell-LaPadula security model?

- A. Accountability
- B. Integrity
- C. Confidentiality
- D. Availability

Answer: C

Explanation:

The Bell-LaPadula model is a formal model dealing with confidentiality.

The Bell-LaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott Bell and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g. "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").

The Bell-LaPadula model focuses on data confidentiality and controlled 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 inductively 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 computer network 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 of an access matrix to specify the discretionary access control.

The following are incorrect answers:

Accountability is incorrect. Accountability requires that actions be traceable to the user that performed them and is not addressed by the Bell-LaPadula model.

Integrity is incorrect. Integrity is addressed in the Biba model rather than Bell-Lapadula. Availability is incorrect. Availability is concerned with assuring that data/services are available to authorized users as specified in service level objectives and is not addressed by the Bell-Lapadula model.

References: CBK, pp. 325-326

AI03, pp. 279 - 284

AI0v4 Security Architecture and Design (pages 333 - 336) AI0v5 Security Architecture and Design (pages 336 - 338)

Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

NEW QUESTION 86

- (Topic 1)

What security model implies a central authority that define rules and sometimes global rules, dictating what subjects can have access to what objects?

- A. Flow Model
- B. Discretionary access control
- C. Mandatory access control
- D. Non-discretionary access control

Answer: D

Explanation:

As a security administrator you might configure user profiles so that users cannot change the system's time, alter system configuration files, access a command prompt, or install unapproved applications. This type of access control is referred to as nondiscretionary, meaning that access decisions are not made at the discretion of the user. Nondiscretionary access controls are put into place by an authoritative entity (usually a security administrator) with the goal of protecting the organization's most critical assets.

Non-discretionary access control is when a central authority determines what subjects can have access to what objects based on the organizational security policy. Centralized access control is not an existing security model.

Both, Rule Based Access Control (RuBAC or RBAC) and Role Based Access Controls (RBAC) falls into this category.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 221). McGraw- Hill. Kindle Edition.

and

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 91

- (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 $s_3 > s_2 > s_1 > s_0$

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:

O'Reilly - 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 93

- (Topic 1)

Sensitivity labels are an example of what application control type?

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

Answer: A

Explanation:

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

The incorrect answers are:

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

Compensating administrative controls - There no such application control. Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups. Sources:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 264).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

NEW QUESTION 96

- (Topic 1)

What is called the percentage of valid subjects that are falsely rejected by a Biometric Authentication system?

- A. False Rejection Rate (FRR) or Type I Error
- B. False Acceptance Rate (FAR) or Type II Error
- C. Crossover Error Rate (CER)
- D. True Rejection Rate (TRR) or Type III Error

Answer: A

Explanation:

The percentage of valid subjects that are falsely rejected is called the False Rejection Rate (FRR) or Type I Error.

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

NEW QUESTION 99

- (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 100

- (Topic 1)

What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?

- A. Central station alarm
- B. Proprietary alarm
- C. A remote station alarm
- D. An auxiliary station alarm

Answer: D

Explanation:

Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station.

Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.

Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings. Each of the buildings in the same vicinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions.

A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service. This is the most popular type of implementation and the owner of the premise must pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf.

A remote system differs from an auxiliary system in that it does not use the municipal fire of police alarm circuits.

Reference(s) used for this question:

ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211).

and

Great presentation J.T.A. Stone on SlideShare

NEW QUESTION 103

- (Topic 1)

The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:

- A. 100 subjects per minute.
- B. 25 subjects per minute.
- C. 10 subjects per minute.
- D. 50 subjects per minute.

Answer: C

Explanation:

The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system.

Acceptable throughput rates are in the range of 10 subjects per minute.

Things that may impact the throughput rate for some types of biometric systems may include:

A concern with retina scanning systems may be the exchange of body fluids on the eyepiece.

Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

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

NEW QUESTION 106

- (Topic 1)

Which authentication technique best protects against hijacking?

- A. Static authentication
- B. Continuous authentication
- C. Robust authentication
- D. Strong authentication

Answer: B

Explanation:

A continuous authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. This is the best protection against hijacking. Static authentication is the type of authentication provided by traditional password schemes and the strength of the authentication is highly dependent on the difficulty of guessing passwords. The robust authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, and it does not protect against hijacking. Strong authentication refers to a two-factor authentication (like something a user knows and something a user is).

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3: Secured Connections to External Networks (page 51).

NEW QUESTION 107

- (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 110

- (Topic 1)

Which of the following is NOT an advantage that TACACS+ has over TACACS?

- A. Event logging
- B. Use of two-factor password authentication
- C. User has the ability to change his password
- D. Ability for security tokens to be resynchronized

Answer: A

Explanation:

Although TACACS+ provides better audit trails, event logging is a service that is provided with TACACS.

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 121).

NEW QUESTION 112

- (Topic 1)

The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

- A. clipping level
- B. acceptance level
- C. forgiveness level
- D. logging level

Answer: A

Explanation:

The correct answer is "clipping level". This is the point at which a system decides to take some sort of action when an action repeats a preset number of times. That action may be to log the activity, lock a user account, temporarily close a port, etc.

Example: The most classic example of a clipping level is failed login attempts. If you have a system configured to lock a user's account after three failed login

attempts, that is the "clipping level".

The other answers are not correct because:

Acceptance level, forgiveness level, and logging level are nonsensical terms that do not exist (to my knowledge) within network security.

Reference:

Official ISC2 Guide - The term "clipping level" is not in the glossary or index of that book. I cannot find it in the text either. However, I'm quite certain that it would be considered part of the CBK, despite its exclusion from the Official Guide.

All in One Third Edition page: 136 - 137

NEW QUESTION 113

- (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 118

- (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 120

- (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 122

- (Topic 1)

Which type of attack involves impersonating a user or a system?

- A. Smurfing attack
- B. Spoofing attack

- C. Spamming attack
- D. Sniffing attack

Answer: B

Explanation:

A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network.

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 77).

NEW QUESTION 123

- (Topic 1)

Which of the following statements pertaining to using Kerberos without any extension is false?

- A. A client can be impersonated by password-guessing.
- B. Kerberos is mostly a third-party authentication protocol.
- C. Kerberos uses public key cryptography.
- D. Kerberos provides robust authentication.

Answer: C

Explanation:

Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network.

Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.

Here is a nice overview of HOW Kerberos is implement as described in RFC 4556:

* 1. Introduction

The Kerberos V5 protocol [RFC4120] involves use of a trusted third party known as the Key Distribution Center (KDC) to negotiate shared session keys between clients and services and provide mutual authentication between them.

The corner-stones of Kerberos V5 are the Ticket and the Authenticator. A Ticket encapsulates a symmetric key (the ticket session key) in an envelope (a public message) intended for a specific service. The contents of the Ticket are encrypted with a symmetric key shared between the service principal and the issuing KDC. The encrypted part of the Ticket contains the client principal name, among other items. An Authenticator is a record that can be shown to have been recently generated using the ticket session key in the associated Ticket. The ticket session key is known by the client who requested the ticket. The contents of the Authenticator are encrypted with the associated ticket session key. The encrypted part of an Authenticator contains a timestamp and the client principal name, among other items.

As shown in Figure 1, below, the Kerberos V5 protocol consists of the following message exchanges between the client and the KDC, and the client and the application service:

The Authentication Service (AS) Exchange

The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket

(TGT). The AS-REQ message and the AS-REP message are the request and the reply message, respectively, between the client and the AS.

The Ticket Granting Service (TGS) Exchange

The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos

ticket-granting server (TGS). The TGS-REQ message and the TGS-REP message are the request and the reply message respectively between the client and the TGS.

The Client/Server Authentication Protocol (AP) Exchange

The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the

client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session-specific symmetric keys.

Usually, the AS and TGS are integrated in a single device also known as the KDC.

```

+-----+
+----->| KDC |
AS-REQ / +-----| |
// +-----+
// ^|
/|AS-REP / |
|| / TGS-REQ + TGS-REP
| | /
| | /
| | / +-----+
| | /
| | /
| | /
| v / v
++-----+-----+ +-----+
| Client +----->| Application | |
| | AP-REQ | Server |
| |<-----| |
+-----+ AP-REP +-----+
  
```

Figure 1: The Message Exchanges in the Kerberos V5 Protocol

In the AS exchange, the KDC reply contains the ticket session key, among other items, that is encrypted using a key (the AS reply key) shared between the client and the KDC. The AS reply key is typically derived from the client's password for human users. Therefore, for human users, the attack resistance strength of the Kerberos protocol is no stronger than the strength of their passwords.

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 40).

And

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 147-151).

and <http://www.ietf.org/rfc/rfc4556.txt>

NEW QUESTION 127

- (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 128

- (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 happen 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 informaiton 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 131

- (Topic 1)

In Mandatory Access Control, sensitivity labels attached to object contain what information?

- A. The item's classification
- B. The item's classification and category set
- C. The item's category
- D. The items's need to know

Answer: B

Explanation:

A Sensitivity label must contain at least one classification and one category set.

Category set and Compartment set are synonyms, they mean the same thing. The sensitivity label must contain at least one Classification and at least one Category. It is common in some environments for a single item to belong to multiple categories. The list of all the categories to which an item belongs is called a compartment set or category set.

The following answers are incorrect:

the item's classification. Is incorrect because you need a category set as well.

the item's category. Is incorrect because category set and classification would be both be required.

The item's need to know. Is incorrect because there is no such thing. The need to know is indicated by the categories the object belongs to. This is NOT the best answer.

Reference(s) used for this question:

OIG CBK, Access Control (pages 186 - 188)

AIO, 3rd Edition, Access Control (pages 162 - 163) AIO, 4th Edition, Access Control, pp 212-214.

Wikipedia - http://en.wikipedia.org/wiki/Mandatory_Access_Control

NEW QUESTION 136

- (Topic 1)

Which of the following logical access exposures INVOLVES CHANGING data before, or as it is entered into the computer?

- A. Data diddling
- B. Salami techniques
- C. Trojan horses
- D. Viruses

Answer: A

Explanation:

It involves changing data before , or as it is entered into the computer or in

other words , it refers to the alteration of the existing data. The other answers are incorrect because :

Salami techniques : A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed.

Trojan horses: A Trojan Horse is a program that is disguised as another program. Viruses:A Virus is a small application , or a string of code , that infects applications.

Reference: Shon Harris , AIO v3

Chapter - 11: Application and System Development, Page : 875-880 Chapter - 10: Law, Investigation and Ethics , Page : 758-759

NEW QUESTION 138

- (Topic 1)

Which of the following protects a password from eavesdroppers and supports the encryption of communication?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Challenge Handshake Identification Protocol (CHIP)
- C. Challenge Handshake Encryption Protocol (CHEP)
- D. Challenge Handshake Substitution Protocol (CHSP)

Answer: A

Explanation:

CHAP: A protocol that uses a three way hanbdshake The server sends the client a challenge which includes a random value(a nonce) to thwart replay attacks. The client responds with the MD5 hash of the nonce and the password.

The authentication is successful if the client's response is the one that the server expected. Reference: Page 450, OIG 2007.

CHAP protects the password from eavesdroppers and supports the encryption of communication.

Reference: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

NEW QUESTION 140

- (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
AIOv4 Security Architecture and Design (pages 357 - 361) AIOv5 Security Architecture and Design (pages 358 - 362)

NEW QUESTION 145

- (Topic 1)

The Computer Security Policy Model the Orange Book is based on is which of the following?

- A. Bell-LaPadula
- B. Data Encryption Standard
- C. Kerberos
- D. Tempest

Answer: A

Explanation:

The Computer Security Policy Model Orange Book is based on the Bell-LaPadula Model. Orange Book Glossary.
The Data Encryption Standard (DES) is a cryptographic algorithm. National Information Security Glossary.
TEMPEST is related to limiting the electromagnetic emanations from electronic equipment. Reference: U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

NEW QUESTION 150

- (Topic 1)

Password management falls into which control category?

- A. Compensating
- B. Detective
- C. Preventive
- D. Technical

Answer: C

Explanation:

Password management is an example of preventive control. Proper passwords prevent unauthorized users from accessing a system.
There are literally hundreds of different access approaches, control methods, and technologies, both in the physical world and in the virtual electronic world. Each method addresses a different type of access control or a specific access need.
For example, access control solutions may incorporate identification and authentication mechanisms, filters, rules, rights, logging and monitoring, policy, and a plethora of other controls. However, despite the diversity of access control methods, all access control systems can be categorized into seven primary categories.
The seven main categories of access control are:
* 1. Directive: Controls designed to specify acceptable rules of behavior within an organization
* 2. Deterrent: Controls designed to discourage people from violating security directives
* 3. Preventive: Controls implemented to prevent a security incident or information breach
* 4. Compensating: Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
* 5. Detective: Controls designed to signal a warning when a security control has been breached
* 6. Corrective: Controls implemented to remedy circumstance, mitigate damage, or restore controls
* 7. Recovery: Controls implemented to restore conditions to normal after a security incident
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 1156-1176). Auerbach Publications. Kindle Edition.

NEW QUESTION 153

- (Topic 1)

An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):

- A. active attack
- B. outside attack
- C. inside attack
- D. passive attack

Answer: C

Explanation:

An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 155

- (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 156

- (Topic 1)

Which of the following are not Remote Access concerns?

- A. Justification for remote access
- B. Auditing of activities
- C. Regular review of access privileges
- D. Access badges

Answer: D

Explanation:

Access badges are more relevant to physical security rather than remote access.

"Justification for remote access" is incorrect. Justification for remote access is a relevant concern.

"Auditing of activities" is incorrect. Auditing of activities is an important aspect to assure that malicious or unauthorized activities are not occurring.

"Regular review of access privileges" is incorrect. Regular review of remote access privileges is an important management responsibility.

References:

AIO3, pp. 547 - 548

NEW QUESTION 160

- (Topic 1)

An alternative to using passwords for authentication in logical or technical access control is:

- A. manage without passwords
- B. biometrics
- C. not there
- D. use of them for physical access control

Answer: B

Explanation:

An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism-something you are.

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

NEW QUESTION 161

- (Topic 1)

Which of the following is NOT a technique used to perform a penetration test?

- A. traffic padding
- B. scanning and probing
- C. war dialing
- D. sniffing

Answer: A

Explanation:

Traffic padding is a countermeasure to traffic analysis.

Even if perfect cryptographic routines are used, the attacker can gain knowledge of the amount of traffic that was generated. The attacker might not know what Alice and Bob were talking about, but can know that they were talking and how much they talked. In certain circumstances this can be very bad. Consider for example when a military is organising a secret attack against another nation: it may suffice to alert the other nation for them to know merely that there is a lot of secret activity going on.

As another example, when encrypting Voice Over IP streams that use variable bit rate encoding, the number of bits per unit of time is not obscured, and this can be exploited to guess spoken phrases.

Padding messages is a way to make it harder to do traffic analysis. Normally, a number of random bits are appended to the end of the message with an indication at the end how much this random data is. The randomness should have a minimum value of 0, a maximum number of N and an even distribution between the two extremes. Note, that increasing 0 does not help, only increasing N helps, though that also means that a lower percentage of the channel will be used to transmit real data. Also note, that since the cryptographic routine is assumed to be uncrackable (otherwise the padding length itself is crackable), it does not help to put the padding anywhere else, e.g. at the beginning, in the middle, or in a sporadic manner.

The other answers are all techniques used to do Penetration Testing. References:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 233, 238.

and https://secure.wikimedia.org/wikipedia/en/wiki/Padding_%28cryptography%29#Traffic_analysis

NEW QUESTION 166

- (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 168

- (Topic 1)

Which of the following is NOT a factor related to Access Control?

- A. integrity
- B. authenticity
- C. confidentiality
- D. availability

Answer: B

Explanation:

These factors cover the integrity, confidentiality, and availability components of information system security.

Integrity is important in access control as it relates to ensuring only authorized subjects can make changes to objects.

Authenticity is different from authentication. Authenticity pertains to something being authentic, not necessarily having a direct correlation to access control.

Confidentiality is pertinent to access control in that the access to sensitive information is controlled to protect confidentiality.

availability is protected by access controls in that if an attacket attempts to disrupt availability they would first need access.

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 172

- (Topic 1)

Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

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

Answer: A

Explanation:

B level is the first Mandatory Access Control Level.

First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.

Reference 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 17920-17926). Auerbach Publications. Kindle Edition.

and
THE source for all TCSEC "level" questions: <http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt> (paragraph 3 for this one)

NEW QUESTION 175

- (Topic 1)

Which of the following classes is defined in the TCSEC (Orange Book) as discretionary protection?

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

Answer: A

Explanation:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 197.

Also: THE source for all TCSEC "level" questions: <http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt>

NEW QUESTION 180

- (Topic 1)

Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?

- A. Degaussing
- B. Parity Bit Manipulation
- C. Zeroization
- D. Buffer overflow

Answer: A

Explanation:

A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.

The following answers are incorrect: Parity Bit Manipulation. Parity has to do with disk lerror detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the information that was sent.

Zeroization. Zeroization involves overwriting data to sanitize it. It is time-consuming and not foolproof. The potential of restoration of data does exist with this method.

Buffer overflow. This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.

The following reference(s) were/was used to create this question: Shon Harris AIO v3. pg 908

Reference: What is degaussing.

NEW QUESTION 181

- (Topic 1)

What can be defined as a table of subjects and objects indicating what actions individual subjects can take upon individual objects?

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

Answer: C

Explanation:

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 capacity table" is incorrect.

This answer is a trap for the unwary -- it sounds a little like "capability table" but is just there to distract you.

"An access control list" is incorrect.

"It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188 Access control lists (ACL) could be used to implement the rules identified by an access control matrix but is different from the matrix itself.

"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.

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."

Again, a capability table could be used to implement the rules identified by an access control matrix but is different from the matrix itself.

References:

CBK pp. 191-192, 317-318

AIO3, p. 169

NEW QUESTION 186

.....

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