



# ISC2

## Exam Questions SSCP

System Security Certified Practitioner (SSCP)

## About Exambible

*[Your Partner of IT Exam](#)*

## Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### TECHNICAL CONTROLS

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

##### Preventive Technical Controls

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

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

Smart cards. Encryption.

Dial-up access control and callback systems.

##### Preventive Physical Controls

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

Backup files and documentation. Fences.

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

Biometric access controls. Site selection.

Fire extinguishers.

##### Preventive Administrative Controls

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

Security awareness and technical training. Separation of duties.

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

Supervision.

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

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

### NEW QUESTION 2

- (Topic 1)

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 3

- (Topic 1)

Smart cards are an example of which type of control?

- A. Detective control
- B. Administrative control
- C. Technical control
- D. Physical control

**Answer: C**

#### Explanation:

Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control.

Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 245). 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 32).

#### NEW QUESTION 4

- (Topic 1)

Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?

- A. Authentication
- B. Administration
- C. Accounting
- D. Authorization

**Answer:** B

#### Explanation:

Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.

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

also see:

The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A's" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.

Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

#### NEW QUESTION 5

- (Topic 1)

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

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

**Answer:** D

#### Explanation:

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

Telecommunications and Network Security (page 74).

#### NEW QUESTION 6

- (Topic 1)

What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?

- A. Mandatory model
- B. Discretionary model
- C. Lattice model
- D. Rule model

**Answer:** C

#### Explanation:

In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values.

Reference(s) used for this question:

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

#### NEW QUESTION 7

- (Topic 1)

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

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

**Answer:** D

#### Explanation:

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

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

Handwritten signature dynamics

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

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

#### NEW QUESTION 8

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

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

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

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

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

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

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

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

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

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

References:

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

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

**NEW QUESTION 9**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

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

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

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

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

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

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

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

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

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

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

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

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

Strong Property

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

Tranquility principle

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



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

## NEW QUESTION 10

- (Topic 1)

Rule-Based Access Control (RuBAC) access is determined by rules. Such rules would fit within what category of access control ?

- A. Discretionary Access Control (DAC)
- B. Mandatory Access control (MAC)
- C. Non-Discretionary Access Control (NDAC)
- D. Lattice-based Access control

**Answer: C**

### Explanation:

Rule-based access control is a type of non-discretionary access control because this access is determined by rules and the subject does not decide what those rules will be, the rules are uniformly applied to ALL of the users or subjects.

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.

Both Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC) fall within Non Discretionary Access Control (NDAC). If it is not DAC or MAC then it is most likely NDAC.

IT IS NOT ALWAYS BLACK OR WHITE

The different access control models are not totally exclusive of each others. MAC is making use of Rules to be implemented. However with MAC you have requirements above and beyond having simple access rules. The subject would get formal approval from management, the subject must have the proper security clearance, objects must have labels/sensitivity levels attached to them, subjects must have the proper security clearance. If all of this is in place then you have MAC.

BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:

MAC = Mandatory Access Control

Under a mandatory access control environment, the system or security administrator will define what permissions subjects have on objects. The administrator does not dictate user's access but simply configure the proper level of access as dictated by the Data Owner.

The MAC system will look at the Security Clearance of the subject and compare it with the object sensitivity level or classification level. This is what is called the dominance relationship.

The subject must DOMINATE the object sensitivity level. Which means that the subject must have a security clearance equal or higher than the object he is attempting to access.

MAC also introduce the concept of labels. Every objects will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle. Even thou a user has a security clearance of Secret it does not mean he would be able to access any Secret documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belong to one of the categories attached to the object.

If there is no clearance and no labels then IT IS NOT Mandatory Access Control.

Many of the other models can mimic MAC but none of them have labels and a dominance relationship so they are NOT in the MAC category.

NISTR-7316 Says:

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. A variation on this rule called the ??strict \*-property?? requires that information can be written at, but not above, the subject's clearance level. Multilevel security models such as the Bell-La Padula Confidentiality and Biba Integrity models are used to formally specify this kind of MAC policy.

DAC = Discretionary Access Control

DAC is also known as: Identity Based access control system.

The owner of an object is define as the person who created the object. As such the owner has the discretion to grant access to other users on the network. Access will be granted based solely on the identity of those users.

Such system is good for low level of security. One of the major problem is the fact that a user who has access to someone's else file can further share the file with other users without the knowledge or permission of the owner of the file. Very quickly this could become the wild wild west as there is no control on the dissimulation of the information.

RBAC = Role Based Access Control

RBAC is a form of Non-Discretionary access control.

Role Based access control usually maps directly with the different types of jobs performed by employees within a company.

For example there might be 5 security administrator within your company. Instead of creating each of their profile one by one, you would simply create a role and assign the administrators to the role. Once an administrator has been assigned to a role, he will IMPLICITLY inherit the permissions of that role.

RBAC is great tool for environment where there is a a large rotation of employees on a daily basis such as a very large help desk for example.

RBAC or RuBAC = Rule Based Access Control RuBAC is a form of Non-Discretionary access control.

A good example of a Rule Based access control device would be a Firewall. A single set of rules is imposed to all users attempting to connect through the firewall.

NOTE FROM CLEMENT:

Lot of people tend to confuse MAC and Rule Based Access Control.

Mandatory Access Control must make use of LABELS. If there is only rules and no label, it cannot be Mandatory Access Control. This is why they call it Non Discretionary Access control (NDAC).

There are even books out there that are WRONG on this subject. Books are sometimes opiniated and not strictly based on facts.

In MAC subjects must have clearance to access sensitive objects. Objects have labels that contain the classification to indicate the sensitivity of the object and the label also has categories to enforce the need to know.

Today the best example of rule based access control would be a firewall. All rules are imposed globally to any user attempting to connect through the device. This is NOT the case with MAC.

I strongly recommend you read carefully the following document:

NISTIR-7316 at <http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf>

It is one of the best Access Control Study document to prepare for the exam. Usually I tell people not to worry about the hundreds of NIST documents and other reference. This document is an exception. Take some time to read it.

Reference(s) used for this question:

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

NISTIR-7316 at <http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf> and

Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Locations 651-652). Elsevier Science (reference). Kindle Edition.

#### NEW QUESTION 10

- (Topic 1)

What is the most critical characteristic of a biometric identifying system?

- A. Perceived intrusiveness
- B. Storage requirements
- C. Accuracy
- D. Scalability

**Answer: C**

#### Explanation:

Accuracy is the most critical characteristic of a biometric identifying verification system.

Accuracy is measured in terms of false rejection rate (FRR, or type I errors) and false acceptance rate (FAR or type II errors).

The Crossover Error Rate (CER) is the point at which the FRR equals the FAR and has become the most important measure of biometric system accuracy.

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 9).

#### NEW QUESTION 15

- (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 16

- (Topic 1)

In discretionary access environments, which of the following entities is authorized to grant information access to other people?

- A. Manager
- B. Group Leader
- C. Security Manager
- D. Data Owner

**Answer: D**

#### Explanation:

In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.

The following answers are incorrect:

manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

IMPORTANT NOTE:

The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data.

The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

#### NEW QUESTION 18

- (Topic 1)

Controls to keep password sniffing attacks from compromising computer systems include which of the following?

- A. static and recurring passwords.
- B. encryption and recurring passwords.
- C. one-time passwords and encryption.
- D. static and one-time passwords.

**Answer: C**

**Explanation:**

To minimize the chance of passwords being captured one-time passwords would prevent a password sniffing attack because once used it is no longer valid. Encryption will also minimize these types of attacks.

The following answers are correct:

static and recurring passwords. This is incorrect because if there is no encryption then someone password sniffing would be able to capture the password much easier if it never changed.

encryption and recurring passwords. This is incorrect because while encryption helps, recurring passwords do nothing to minimize the risk of passwords being captured.

static and one-time passwords. This is incorrect because while one-time passwords will prevent these types of attacks, static passwords do nothing to minimize the risk of passwords being captured.

**NEW QUESTION 23**

- (Topic 1)

Which one of the following authentication mechanisms creates a problem for mobile users?

- A. Mechanisms based on IP addresses
- B. Mechanism with reusable passwords
- C. one-time password mechanism.
- D. challenge response mechanism.

**Answer: A**

**Explanation:**

Anything based on a fixed IP address would be a problem for mobile users because their location and its associated IP address can change from one time to the next. Many providers will assign a new IP every time the device would be restarted. For example an insurance adjuster using a laptop to file claims online. He goes to a different client each time and the address changes every time he connects to the ISP.

NOTE FROM CLEMENT:

The term MOBILE in this case is synonymous with Road Warriors where a user is constantly traveling and changing location. With smartphone today that may not be an issue but it would be an issue for laptops or WIFI tablets. Within a carrier network the IP will tend to be the same and would change rarely. So this question is more applicable to devices that are not cellular devices but in some cases this issue could affect cellular devices as well.

The following answers are incorrect:

mechanism with reusable password. This is incorrect because reusable password mechanism would not present a problem for mobile users. They are the least secure and change only at specific interval.

one-time password mechanism. This is incorrect because a one-time password mechanism would not present a problem for mobile users. Many are based on a clock and not on the IP address of the user.

challenge response mechanism. This is incorrect because challenge response mechanism would not present a problem for mobile users.

**NEW QUESTION 24**

- (Topic 1)

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

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

**Answer: B**

**Explanation:**

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

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

The other answers are not correct because:

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

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

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

References:

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

**NEW QUESTION 25**

- (Topic 1)

Which of the following biometric devices has the lowest user acceptance level?

- A. Retina Scan
- B. Fingerprint scan
- C. Hand geometry
- D. Signature recognition



**Answer:** A

**Explanation:**

According to the cited reference, of the given options, the Retina scan has the lowest user acceptance level as it is needed for the user to get his eye close to a device and it is not user friendly and very intrusive.  
However, retina scan is the most precise with about one error per 10 millions usage. Look at the 2 tables below. If necessary right click on the image and save it on your desktop for a larger view or visit the web site directly at <https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy> . Biometric Comparison Chart

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

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

Biometric Aspect Descriptions Reference(s) used for this question:

RHODES, Keith A., Chief Technologist, United States General Accounting Office, National Preparedness, Technologies to Secure Federal Buildings, April 2002 (page 10).

and

<https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy>

**NEW QUESTION 28**

- (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 30**

- (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 35**

- (Topic 1)

What is called a password that is the same for each log-on session?

- A. "one-time password"
- B. "two-time password"
- C. static password
- D. dynamic password

**Answer:** C

**Explanation:**

Source: 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 37**

- (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 41**

- (Topic 1)

Which of the following would constitute the best example of a password to use for access to a system by a network administrator?

- A. holiday
- B. Christmas12
- C. Jenny
- D. GyN19Za!

**Answer:** D

**Explanation:**

GyN19Za! would be the the best answer because it contains a mixture of upper and lower case characters, alphabetic and numeric characters, and a special character making it less vulnerable to password attacks.

All of the other answers are incorrect because they are vulnerable to brute force or dictionary attacks. Passwords should not be common words or names. The addition of a number to the end of a common word only marginally strengthens it because a common password attack would also check combinations of words: Christmas23 Christmas123 etc...

**NEW QUESTION 43**

- (Topic 1)

Pin, Password, Passphrases, Tokens, smart cards, and biometric devices are all items that can be used for Authentication. When one of these item listed above in conjunction with a second factor to validate authentication, it provides robust authentication of the individual by practicing which of the following?

- A. Multi-party authentication
- B. Two-factor authentication
- C. Mandatory authentication
- D. Discretionary authentication

**Answer:** B

**Explanation:**

Once an identity is established it must be authenticated. There exist numerous technologies and implementation of authentication methods however they almost all fall under three major areas.

There are three fundamental types of authentication: Authentication by knowledge??something a person knows

Authentication by possession??something a person has

Authentication by characteristic??something a person is Logical controls related to these types are called ??factors.??

Something you know can be a password or PIN, something you have can be a token fob or smart card, and something you are is usually some form of biometrics.

Single-factor authentication is the employment of one of these factors, two-factor authentication is using two of the three factors, and three-factor authentication is the combination of all three factors.

The general term for the use of more than one factor during authentication is multifactor authentication or strong authentication.

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 2367-2379). Auerbach Publications. Kindle Edition.

**NEW QUESTION 44**

- (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 49**

- (Topic 1)

RADIUS incorporates which of the following services?

- A. Authentication server and PIN codes.
- B. Authentication of clients and static passwords generation.
- C. Authentication of clients and dynamic passwords generation.
- D. Authentication server as well as support for Static and Dynamic passwords.

**Answer: D**

**Explanation:**

A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

RADIUS authentication is based on provisions of simple username/password credentials.

These credentials are encrypted

by the client using a shared secret between the client and the RADIUS server. OIG 2007, Page 513

RADIUS incorporates an authentication server and can make uses of both dynamic and static passwords.

Since it uses the PAP and CHAP protocols, it also includes static passwords.

RADIUS is an Internet protocol. RADIUS carries authentication, authorization, and configuration information between a Network Access Server and a shared Authentication Server. RADIUS features and functions are described primarily in the IETF (International Engineering Task Force) document RFC2138.

The term " RADIUS" is an acronym which stands for Remote Authentication Dial In User Service.

The main advantage to using a RADIUS approach to authentication is that it can provide a stronger form of authentication. RADIUS is capable of using a strong, two-factor form of authentication, in which users need to possess both a user ID and a hardware or software token to gain access.

Token-based schemes use dynamic passwords. Every minute or so, the token generates a unique 4-, 6- or 8-digit access number that is synchronized with the security server. To gain entry into the system, the user must generate both this one-time number and provide his or her user ID and password.

Although protocols such as RADIUS cannot protect against theft of an authenticated session via some realtime attacks, such as wiretapping, using unique, unpredictable authentication requests can protect against a wide range of active attacks.

**RADIUS: Key Features and Benefits**

RADIUS supports dynamic passwords and challenge/response passwords. Improved system security due to the fact that passwords are not static.

It is much more difficult for a bogus host to spoof users into giving up their passwords or password-generation algorithms.

RADIUS allows the user to have a single user ID and password for all computers in a network.

Improved usability due to the fact that the user has to remember only one login combination.

RADIUS is able to:

Prevent RADIUS users from logging in via login (or ftp). Require them to log in via login (or ftp)

Require them to login to a specific network access server (NAS); Control access by time of day.

Provides very granular control over the types of logins allowed, on a per-user basis. The time-out interval for failing over from an unresponsive primary RADIUS server to a

backup RADIUS server is site-configurable.

RADIUS gives System Administrator more flexibility in managing which users can login from which hosts or devices.

Stratus Technology Product Brief <http://www.stratus.com/products/vos/openvos/radius.htm>

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 43, 44.

Also check: MILLER, Lawrence & GREGORY, Peter, CISSP for Dummies, 2002, Wiley Publishing, Inc., pages 45-46.

**NEW QUESTION 53**

- (Topic 1)

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

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

**Answer: C**

**Explanation:**

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

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

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

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

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

282

**NEW QUESTION 57**

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

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

accurate.

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

The following are used as performance metrics for biometric systems:

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

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

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

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

template capacity: the maximum number of sets of data which can be stored in the system. Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten

Domains of Computer Security, 2001, John Wiley & Sons, Page 37. and

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

#### NEW QUESTION 60

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

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

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

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

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

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

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

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

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

References:

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

#### NEW QUESTION 64

- (Topic 1)

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

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

**Answer: A**

#### Explanation:

Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. The changing of passwords can also fall between these two extremes.

Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use.

Obviously, the more times a password is used, the more chance there is of it being compromised.

It is recommended to use a passphrase instead of a password. A passphrase is more resistant to attacks. The passphrase is converted into a virtual password by the system. Often time the passphrase will exceed the maximum length supported by the system and it must be truncated into a Virtual Password.

Reference(s) used for this question: <http://www.itl.nist.gov/fipspubs/fip112.htm>

and

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36 & 37.

#### NEW QUESTION 66

- (Topic 1)

In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person.

This raised the necessity of answering 2 questions :

- A. what was the sex of a person and his age
- B. what part of body to be used and how to accomplish identification that is viable
- C. what was the age of a person and his income level



D. what was the tone of the voice of a person and his habits

**Answer:** B

**Explanation:**

Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already taking place. Unique physical attributes or behavior of a person are used for that purpose.

From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

**NEW QUESTION 69**

- (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 74**

- (Topic 1)

A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?

- A. Content-dependent access control
- B. Context-dependent access control
- C. Least privileges access control
- D. Ownership-based access control

**Answer:** A

**Explanation:**

When access control is based on the content of an object, it is considered to be content dependent access control.

Content-dependent access control is based on the content itself. The following answers are incorrect:

context-dependent access control. Is incorrect because this type of control is based on what the context is, facts about the data rather than what the object contains.

least privileges access control. Is incorrect because this is based on the least amount of rights needed to perform their jobs and not based on what is contained in the database. ownership-based access control. Is incorrect because this is based on the owner of the data and not based on what is contained in the database.

References:

OIG CBK Access Control (page 191)

**NEW QUESTION 75**

- (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 78**

- (Topic 1)

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:

- A. specify what users can do



- B. specify which resources they can access
- C. specify how to restrain hackers
- D. specify what operations they can perform on a system.

**Answer:** C

**Explanation:**

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system. Specifying HOW to restrain hackers is not directly linked to access control.

Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 12.

**NEW QUESTION 80**

- (Topic 1)

Who developed one of the first mathematical models of a multilevel-security computer system?

- A. Diffie and Hellman.
- B. Clark and Wilson.
- C. Bell and LaPadula.
- D. Gasser and Lipner.

**Answer:** C

**Explanation:**

In 1973 Bell and LaPadula created the first mathematical model of a multi-level security system.

The following answers are incorrect:

Diffie and Hellman. This is incorrect because Diffie and Hellman was involved with cryptography.

Clark and Wilson. This is incorrect because Bell and LaPadula was the first model. The Clark-Wilson model came later, 1987.

Gasser and Lipner. This is incorrect, it is a distractor. Bell and LaPadula was the first model.

**NEW QUESTION 85**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 89**

- (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 than 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 94

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

In an organization where there are frequent personnel changes, non- discretionary access control (also called Role Based Access Control) is useful because the access controls are based on the individual's role or title within the organization. You can easily configure a new employee access by assigning the user to a role that has been predefined. 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 choices 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 lists 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 95

- (Topic 1)

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

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

**Answer: D**

#### Explanation:

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

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

#### NEW QUESTION 98

- (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 102

- (Topic 1)

Which access control model was proposed for enforcing access control in government and military applications?

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

**Answer:** A

**Explanation:**

The Bell-LaPadula model, mostly concerned with confidentiality, was proposed for enforcing access control in government and military applications. It supports mandatory access control by determining the access rights from the security levels associated with subjects and objects. It also supports discretionary access control by checking access rights from an access matrix. The Biba model, introduced in 1977, the Sutherland model, published in 1986, and the Brewer-Nash model, published in 1989, are concerned with integrity.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 11).

**NEW QUESTION 104**

- (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 106**

- (Topic 1)

What physical characteristic does a retinal scan biometric device measure?

- A. The amount of light reaching the retina
- B. The amount of light reflected by the retina
- C. The pattern of light receptors at the back of the eye
- D. The pattern of blood vessels at the back of the eye

**Answer:** D

**Explanation:**

The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain - the equivalent of film in a camera. Blood vessels used for biometric identification are located along the neural retina, the outermost of retina's four cell layers.

The following answers are incorrect:

The amount of light reaching the retina The amount of light reaching the retina is not used in the biometric scan of the retina.

The amount of light reflected by the retina The amount of light reflected by the retina is not used in the biometric scan of the retina.

The pattern of light receptors at the back of the eye This is a distractor The following reference(s) were/was used to create this question: Reference: Retina Scan Technology.

ISC2 Official Guide to the CBK, 2007 (Page 161)

**NEW QUESTION 109**

- (Topic 1)

The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:

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

**Answer:** C

**Explanation:**

Detective/physical controls usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists.

Source: 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 111**

- (Topic 1)

The following is NOT a security characteristic we need to consider while choosing a biometric identification systems:

- A. data acquisition process
- B. cost
- C. enrollment process
- D. speed and user interface

**Answer:** B

**Explanation:**

Cost is a factor when considering Biometrics but it is not a security characteristic.

All the other answers are incorrect because they are security characteristics related to Biometrics.

data acquisition process can cause a security concern because if the process is not fast and efficient it can discourage individuals from using the process.

enrollment process can cause a security concern because the enrollment process has to be quick and efficient. This process captures data for authentication.

speed and user interface can cause a security concern because this also impacts the users acceptance rate of biometrics. If they are not comfortable with the interface and speed they might sabotage the devices or otherwise attempt to circumvent them.

References:

OIG Access Control (Biometrics) (pgs 165-167)

From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Pages 5-6.

in process of correction

**NEW QUESTION 114**

- (Topic 1)

Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:

A. neither physical attacks nor attacks from malicious code.

B. physical attacks only

C. both physical attacks and attacks from malicious code.

D. physical attacks but not attacks from malicious code.

**Answer: C**

**Explanation:**

Since all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code.

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.

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

**NEW QUESTION 118**

- (Topic 1)

When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?

A. Type I error

B. Type II error

C. Type III error

D. Crossover error

**Answer: B**

**Explanation:**

When the biometric system accepts impostors who should have been rejected, it is called a Type II error or False Acceptance Rate or False Accept Rate.

Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification.

Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual's behavior, as in signature dynamics, but these can change over time and possibly be forged.

Biometric systems that base authentication decisions on physical attributes (iris, retina, fingerprint) provide more accuracy, because physical attributes typically don't change much, absent some disfiguring injury, and are harder to impersonate.

When a biometric system rejects an authorized individual, it is called a Type I error (False Rejection Rate (FRR) or False Reject Rate (FRR)).

When the system accepts impostors who should be rejected, it is called a Type II error (False Acceptance Rate (FAR) or False Accept Rate (FAR)). Type II errors are the most dangerous and thus the most important to avoid.

The goal is to obtain low numbers for each type of error, but When comparing different biometric systems, many different variables are used, but one of the most important metrics is the crossover error rate (CER).

The accuracy of any biometric method is measured in terms of Failed Acceptance Rate (FAR) and Failed Rejection Rate (FRR). Both are expressed as percentages. The FAR is the rate at which attempts by unauthorized users are incorrectly accepted as valid. The FRR is just the opposite. It measures the rate at which authorized users are denied access.

The relationship between FRR (Type I) and FAR (Type II) is depicted in the graphic below. As one rate increases, the other decreases. The Cross-over Error Rate (CER) is sometimes considered a good indicator of the overall accuracy of a biometric system. This

is the point at which the FRR and the FAR have the same value. Solutions with a lower CER are typically more accurate.

See graphic below from Biometria showing this relationship. The Cross-over Error Rate (CER) is also called the Equal Error Rate (EER), the two are synonymous.

C:\Users\MCS\Desktop\1.jpg Cross Over Error Rate

The other answers are incorrect:

Type I error is also called as False Rejection Rate where a valid user is rejected by the system.

Type III error : there is no such error type in biometric system.

Crossover error rate stated in percentage, represents the point at which false rejection equals the false acceptance rate.

Reference(s) used for this question: <http://www.biometria.sk/en/principles-of-biometrics.html>

and

Shon Harris, CISSP All In One (AIO), 6th Edition, Chapter 3, Access Control, Page 188- 189

and

Tech Republic, Reduce Multi\_Factor Authentication Cost

**NEW QUESTION 120**

- (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 121**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

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

Reference:

Official ISC2 Guide to the CISSP, 2007 Edition, page 184 also see:

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

**NEW QUESTION 125**

- (Topic 1)

Access Control techniques do not include which of the following?

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

**Answer:** D

**Explanation:**

Access Control Techniques Discretionary Access Control

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

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

**NEW QUESTION 129**

- (Topic 1)

How can an individual/person best be identified or authenticated to prevent local masquerading attacks?

- A. UserId and password
- B. Smart card and PIN code
- C. Two-factor authentication
- D. Biometrics

**Answer:** D

**Explanation:**

The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric

identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.

Some people are getting thrown off by the term Masquerade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.

A UserId only provides for identification.

A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.

A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.

Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.

Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur.

As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is



because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information. Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost. NOTE FROM CLEMENT:

This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well. I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.

Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.

I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.

The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes.

Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and terrorists. This is how you could use biometric for Identification.

There are always THREE means of authentication, they are: Something you know (Type 1)

Something you have (Type 2)

Something you are (Type 3)

Reference(s) used for this question:

TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) , 2000, CRC Press, Chapter 1, Biometric Identification (page 7).

and

Search Security at <http://searchsecurity.techtarget.com/definition/masquerade>

### NEW QUESTION 133

- (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 135

- (Topic 1)

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

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

**Answer: A**

#### Explanation:

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

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

### NEW QUESTION 136

- (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 137

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

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

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

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

CBK, pp. 329 - 330

AIO3, pp. 302 - 306

#### NEW QUESTION 142

- (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 146

- (Topic 1)

Which of the following is NOT true of the Kerberos protocol?

- A. Only a single login is required per session.
- B. The initial authentication steps are done using public key algorithm.
- C. The KDC is aware of all systems in the network and is trusted by all of them
- D. It performs mutual authentication

**Answer:** B

#### Explanation:

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:

It is secure: it never sends a password unless it is encrypted.

Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.

The concept depends on a trusted third party ?C a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.

It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.

Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS ?C a ticket is a time-limited

cryptographic message ?C giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.

Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication. Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 ??The Kerberos Network Authorization Service (V5)??.

C:\Users\MCS\Desktop\1.jpg Kerberos Authentication Step by Step

Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).

Step 2: The Authorization Server verifies the user??s access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user??s password and sends a message back to the user workstation.

The workstation prompts the user for a password and uses the password to decrypt the incoming message. When decryption succeeds, the user will be able to use the TGT to request a service ticket.

Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.

Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key

?C one encrypted with the client password, and one encrypted by the service password.

Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.

Step 6: If mutual authentication is required, then the server will reply with a server authentication message.

The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above.

To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.

Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.

For more information about Kerberos, see <http://web.mit.edu/kerberos/www/>.

References:

Introduction to Kerberos Authentication from Intel

and

<http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3> and

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

### NEW QUESTION 151

- (Topic 1)

Which of the following models does NOT include data integrity or conflict of interest?

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

**Answer: C**

#### Explanation:

Bell LaPadula model (Bell 1975): The granularity of objects and subjects is not predefined, but the model prescribes simple access rights. Based on simple access restrictions the Bell LaPadula model enforces a discretionary access control policy enhanced with mandatory rules. Applications with rigid confidentiality requirements and without strong integrity requirements may properly be modeled.

These simple rights combined with the mandatory rules of the policy considerably restrict the spectrum of applications which can be appropriately modeled.

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

Also check:

Proceedings of the IFIP TC11 12th International Conference on Information Security, Samos (Greece), May 1996, On Security Models.

### NEW QUESTION 156

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

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

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

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

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

The user sends a request for authentication to the Authentication Server as in Kerberos, except that SESAME is making use of public key cryptography for authentication where the client will present his digital certificate and the request will be signed using a digital signature. The signature is communicated to the authentication server through the preauthentication fields. Upon receipt of this request, the authentication server will verifies the certificate, then validate the signature, and if all is fine the AS will issue a ticket granting ticket (TGT) as in Kerberos. This TGT will be use to communicate with the privilege attribute server (PAS) when access to a resource is needed.

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

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

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

and

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

### NEW QUESTION 157

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

Reference(s) used for this question:

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

**NEW QUESTION 160**

- (Topic 1)

What does the simple security (ss) property mean in the Bell-LaPadula model?

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

**Answer:** A

**Explanation:**

The ss (simple security) property of the Bell-LaPadula access control model states that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).

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

**NEW QUESTION 163**

- (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 166**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

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

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

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

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

**NEW QUESTION 170**

- (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 171**

- (Topic 1)

In Synchronous dynamic password tokens:

- A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
- B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
- C. The unique password is not entered into a system or workstation along with an owner's PIN.
- D. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.

**Answer:** A

**Explanation:**

Synchronous dynamic password tokens:

- The token generates a new password value at fixed time intervals (this password could be the time of day encrypted with a secret key).
- the unique password is entered into a system or workstation along with an owner's PIN.
- The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid time window.

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 173**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

Access Control Techniques Discretionary Access Control

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

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

**NEW QUESTION 176**

- (Topic 1)

Which of the following does not apply to system-generated passwords?

- A. Passwords are harder to remember for users.
- B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
- C. Passwords are more vulnerable to brute force and dictionary attacks.
- D. Passwords are harder to guess for attackers.

**Answer:** C

**Explanation:**

Users tend to choose easier to remember passwords. System-generated passwords can provide stronger, harder to guess passwords. Since they are based on rules provided by the administrator, they can include combinations of uppercase/lowercase letters, numbers and special characters, making them less vulnerable to brute force and dictionary attacks. One danger is that they are also harder to remember for users, who will tend to write them down, making them more vulnerable to anyone having access to the user's desk. Another danger with system-generated passwords is that if the password-generating algorithm gets to be known, the entire system is in jeopardy.

Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 64).

**NEW QUESTION 178**

- (Topic 1)

Which of the following statements pertaining to the Bell-LaPadula is TRUE if you are NOT making use of the strong star property?

- A. It allows "read up."
- B. It addresses covert channels.
- C. It addresses management of access controls.
- D. It allows "write up."

**Answer:** D

**Explanation:**

Bell?CLaPadula Confidentiality Model10 The Bell?CLaPadula model is perhaps the most well-known and significant security model, in addition to being one of the oldest models used in the creation of modern secure computing systems. Like the Trusted Computer System Evaluation Criteria (or TCSEC), it was inspired by



early U.S. Department of Defense security policies and the need to prove that confidentiality could be maintained. In other words, its primary goal is to prevent disclosure as the model system moves from one state (one point in time) to another.

When the strong star property is not being used it means that both the property and the

Simple Security Property rules would be applied.

The Star (\*) property rule of the Bell-LaPadula model says that subjects cannot write down, this would compromise the confidentiality of the information if someone at the secret layer would write the object down to a confidential container for example.

The Simple Security Property rule states that the subject cannot read up which means that a subject at the secret layer would not be able to access objects at Top Secret for example.

You must remember: The model tells you about are NOT allowed to do. Anything else would be allowed. For example within the Bell LaPadula model you would be allowed to write up as it does not compromise the security of the information. In fact it would upgrade it to the point that you could lock yourself out of your own information if you have only a secret security clearance.

The following are incorrect answers because they are all FALSE:

"It allows read up" is incorrect. The "simple security" property forbids read up.

"It addresses covert channels" is incorrect. Covert channels are not addressed by the Bell- LaPadula model.

"It addresses management of access controls" is incorrect. Management of access controls are beyond the scope of the Bell-LaPadula model.

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 17595-17600). Auerbach Publications. Kindle Edition.

#### NEW QUESTION 180

- (Topic 1)

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

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

**Answer: C**

#### Explanation:

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

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

#### NEW QUESTION 185

- (Topic 1)

In biometric identification systems, the parts of the body conveniently available for identification are:

- A. neck and mouth
- B. hands, face, and eyes
- C. feet and hair
- D. voice and neck

**Answer: B**

#### Explanation:

Today implementation of fast, accurate, reliable, and user-acceptable biometric identification systems are already under way. Because most identity authentication takes place when a people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes. From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

#### NEW QUESTION 190

- (Topic 1)

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

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

**Answer: A**

#### Explanation:

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

Reference:

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

#### NEW QUESTION 193

- (Topic 1)

Which security model introduces access to objects only through programs?

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

**Answer: C**

**Explanation:**

In the Clark-Wilson model, the subject no longer has direct access to objects but instead must access them through programs (well-formed transactions).

The Clark-CWilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.

The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.

Clark-CWilson is more clearly applicable to business and industry processes in which the integrity of the information content is paramount at any level of classification.

Integrity goals of Clark-CWilson model:

Prevent unauthorized users from making modification (Only this one is addressed by the Biba model).

Separation of duties prevents authorized users from making improper modifications. Well formed transactions: maintain internal and external consistency i.e. it is a series of operations that are carried out to transfer the data from one consistent state to the other.

The following are incorrect answers:

The Biba model is incorrect. The Biba model is concerned with integrity and controls access to objects based on a comparison of the security level of the subject to that of the object.

The Bell-LaPadula model is incorrect. The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearance level of the subject to the classification level of the object.

The information flow model is incorrect. The information flow model uses a lattice where objects are labelled with security classes and information can flow either upward or at the

same level. It is similar in framework to the Bell-LaPadula model. References:

ISC2 Official Study Guide, Pages 325 - 327 AIO3, pp. 284 - 287

AIOv4 Security Architecture and Design (pages 338 - 342) AIOv5 Security Architecture and Design (pages 341 - 344) Wikipedia at:

[https://en.wikipedia.org/wiki/Clark-Wilson\\_model](https://en.wikipedia.org/wiki/Clark-Wilson_model)

**NEW QUESTION 195**

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

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

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

Changing passwords regularly would not prevent such attack.

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

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

**NEW QUESTION 198**

- (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 203**

- (Topic 1)

Which of the following are additional access control objectives?

- A. Consistency and utility
- B. Reliability and utility
- C. Usefulness and utility
- D. Convenience and utility

**Answer: B**

**Explanation:**

Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system. The additional access control objectives are reliability and utility. These and other related objectives flow from the organizational security policy. This policy is a high-level statement of management intent regarding the control of access to information and the personnel who are authorized to receive that information. Three things that must be considered for the planning and implementation of access control mechanisms are the threats to the system, the system's vulnerability to these threats, and the risk that the threat may materialize.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

#### NEW QUESTION 207

- (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](https://secure.wikimedia.org/wikipedia/en/wiki/Padding_%28cryptography%29#Traffic_analysis)

#### NEW QUESTION 208

- (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 210

- (Topic 1)

What security model is dependent on security labels?

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

**Answer:** C

#### Explanation:

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

the classification or sensitivity of the object. Label-based access control is not defined. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide:

Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

#### NEW QUESTION 211

- (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 213

- (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 218**

- (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 223**

- (Topic 1)

Which of the following questions is less likely to help in assessing physical and environmental protection?

- A. Are entry codes changed periodically?
- B. Are appropriate fire suppression and prevention devices installed and working?
- C. Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
- D. Is physical access to data transmission lines controlled?

**Answer:** C

**Explanation:**

Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical and environmental protection except for the one regarding processes that ensuring that unauthorized individuals cannot access information, which is more a production control.

Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

**NEW QUESTION 226**

.....

## Relate Links

**100% Pass Your SSCP Exam with Exambible Prep Materials**

<https://www.exambible.com/SSCP-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>