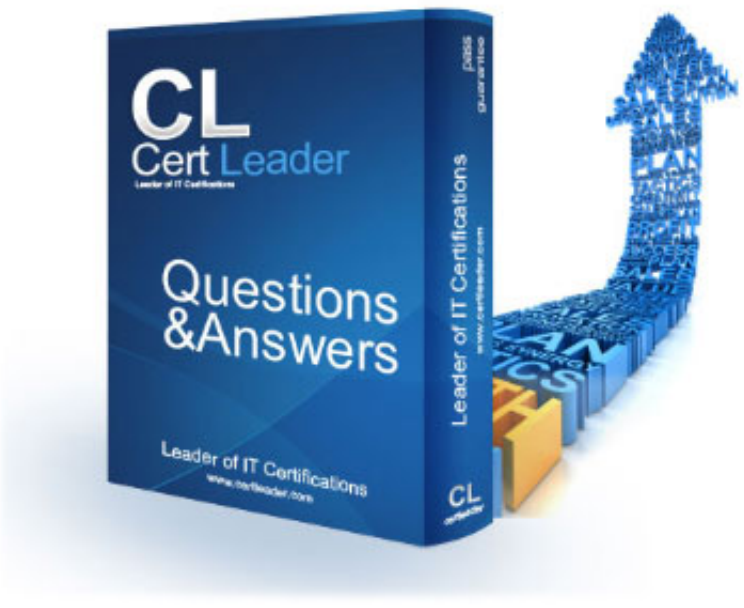
SSCP Dumps

System Security Certified Practitioner (SSCP)

https://www.certleader.com/SSCP-dumps.html



NEW QUESTION 1
- (Topic 1)
The Terminal Access Controller Access Control System (TACACS) employs which of the following?

A. a user ID and static password for network access
B. a user ID and dynamic password for network access
C. a user ID and symmetric password for network access
D. a user ID and asymmetric password for network access

Answer: A

Explanation:
For networked applications, the Terminal Access Controller Access Control System (TACACS) employs a user ID and a static password for network access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

NEW QUESTION 2
- (Topic 1)
What is the main concern with single sign-on?

A. Maximum unauthorized access would be possible if a password is disclosed.
B. The security administrator's workload would increase.
C. The users' password would be too hard to remember.
D. User access rights would be increased.

Answer: A

Explanation:
A major concern with Single Sign-On (SSO) is that if a user's ID and password are compromised, the intruder would have access to all the systems that the user was authorized for.
The following answers are incorrect:
The security administrator's workload would increase. Is incorrect because the security administrator's workload would decrease and not increase. The admin would not be responsible for maintaining multiple user accounts just the one.
The users' password would be too hard to remember. Is incorrect because the users would have less passwords to remember.
User access rights would be increased. Is incorrect because the user access rights would not be any different than if they had to log into systems manually.

NEW QUESTION 3
- (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 4
- (Topic 1)
To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:

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

Answer: A

Explanation:
Controlling access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up access rules.
These rules can be classified into three access control models: Mandatory, Discretionary, and Non-Discretionary.
An access matrix is one of the means used to implement access control.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 5
- (Topic 1)
Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access?

A. Smart cards
B. Single Sign-On (SSO)
C. Symmetric Ciphers
D. Public Key Infrastructure (PKI)

Answer: B

Explanation:
The advantages of SSO include having the ability to use stronger passwords, easier administration as far as changing or deleting the passwords, minimize the risks of orphan accounts, and requiring less time to access resources.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

NEW QUESTION 6
- (Topic 1)
In the Bell-LaPadula model, the Star-property is also called:

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

Answer: B

Explanation:
The Bell-LaPadula model focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.
In this formal model, the entities in an information system are divided into subjects and objects.
The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby proving that the system satisfies the security objectives of the model.
The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions.
A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy.
To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.
The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:
The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).
The property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The property is also known as the Confinement property.
The Discretionary Security Property - use an access control matrix to specify the discretionary access control.
The transfer of information from a high-sensitivity document to a lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the property. Untrusted subjects are.
Trusted Subjects must be shown to be trustworthy with regard to the security policy. This security model is directed toward access control and is characterized by the phrase: "no read up, no write down." Compare the Biba model, the Clark-Wilson model and the Chinese Wall.
With Bell-LaPadula, users can create content only at or above their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down). Conversely, users can view content only at or below their own security level
(i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).
Strong Property
The Strong Property is an alternative to the Property in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual Property is not present, only a write-to-same level operation. The Strong Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns.
Tranquility principle
The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle: the "principle of strong tranquility" states that security levels do not change during the normal operation of the system and the "principle of weak tranquility" states that security levels do not change in a way that violates the rules of a given security policy.
Another interpretation of the tranquility principles is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/label will not change during an operation (such as read or write); the weak tranquility principle means that an object's security level/label may change in a way that does not violate the security policy during an operation.
Reference(s) used for this question: http://en.wikipedia.org/wiki/Biba_Model
http://en.wikipedia.org/wiki/Mandatory_access_control http://en.wikipedia.org/wiki/Discretionary_access_control http://en.wikipedia.org/wiki/Clark-Wilson_model
http://en.wikipedia.org/wiki/Brewer_and_Nash_model

NEW QUESTION 7
- (Topic 1)
Which of the following centralized access control mechanisms is the least appropriate for mobile workers accessing the corporate network over analog lines?

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

Answer: B

Explanation:
Call-back allows for a distant user connecting into a system to be called back at a number already listed in a database of trusted users. The disadvantage of this system is that the user must be at a fixed location whose phone number is known to the authentication server. Being mobile workers, users are accessing the system from multiple
locations, making call-back inappropriate for them.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 44).

NEW QUESTION 8
- (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 dissimination 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 9
- (Topic 1)
Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

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

D. The Bell-LaPadula integrity model

Answer: C

Explanation:
The Clark Wilson integrity model addresses the three following integrity goals: 1) data is protected from modification by unauthorized users; 2) data is protected from unauthorized modification by authorized users; and 3) data is internally and externally consistent. It also defines a Constrained Data Item (CDI), an Integrity Verification Procedure (IVP), a Transformation Procedure (TP) and an Unconstrained Data item. The Bell-LaPadula and Take-Grant models are not integrity models.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 205).

NEW QUESTION 10
- (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 contantly 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 10
- (Topic 1)
Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?

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

Answer: B

Explanation:
Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.
The use of a TACACS+ Server by itself cannot eliminate hacking.
Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.
Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

NEW QUESTION 12
- (Topic 1)
Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

A. plan for implementing workstation locking mechanisms.
B. plan for protecting the modem pool.
C. plan for providing the user with his account usage information.
D. plan for considering proper authentication options.

Answer: D

Explanation:
Before a LAN is connected to the Internet, you need to determine what the
access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.
The following answers are incorrect:
plan for implementing workstation locking mechanisms. This is incorrect because locking the workstations have no impact on the LAN or Internet access.
plan for protecting the modem pool. This is incorrect because protecting the modem pool has no impact on the LAN or Internet access, it just protects the modem.
plan for providing the user with his account usage information. This is incorrect because the question asks what should be done first. While important your primary concern should be focused on security.

NEW QUESTION 14

- (Topic 1)
Which of the following statements pertaining to biometrics is FALSE?

A. User can be authenticated based on behavior.
B. User can be authenticated based on unique physical attributes.
C. User can be authenticated by what he knows.
D. A biometric system's accuracy is determined by its crossover error rate (CER).

Answer: C

Explanation:
As this is not a characteristic of Biometrics this is the rigth choice for this question. This is one of the three basic way authentication can be performed and it is not related to Biometrics. Example of something you know would be a password or PIN for example.
Please make a note of the negative 'FALSE' within the question. This question may seem tricky to some of you but you would be amazed at how many people cannot deal with negative questions. There will be a few negative questions within the real exam, just like this one the keyword NOT or FALSE will be in Uppercase to clearly indicate that it is negative.
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 performing authentication (one to one matching) or identification (a one to many matching).
A biometric system scans an attribute or behavior of a person and compares it to a template store within an authentication server datbase, such template would be created in an earlier enrollment process. Because this system inspects the grooves of a person??s fingerprint, the pattern of someone??s retina, or the pitches of someone??s voice, it has to be extremely sensitive.
The system must perform accurate and repeatable measurements of anatomical or physiological characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so that these false positives and false negatives occur infrequently and the results are as accurate as possible.
There are two types of failures in biometric identification:
False Rejection also called False Rejection Rate (FRR) ?? The system fail to recognize a legitimate user. While it could be argued that this has the effect of keeping the protected area extra secure, it is an intolerable frustration to legitimate users who are refused access because the scanner does not recognize them.
False Acceptance or False Acceptance Rate (FAR) ?? This is an erroneous recognition, either by confusing one user with another or by accepting an imposter as a legitimate user.
Physiological Examples:
Unique Physical Attributes:
Fingerprint (Most commonly accepted) Hand Geometry
Retina Scan (Most accurate but most intrusive) Iris Scan
Vascular Scan Behavioral Examples:
Repeated Actions Keystroke Dynamics
(Dwell time (the time a key is pressed) and Flight time (the time between "key up" and the next "key down").
Signature Dynamics
(Stroke and pressure points)
EXAM TIP:
Retina scan devices are the most accurate but also the most invasive biometrics system available today. The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option. Unfortunately, the cost of the proprietary hardware as well the stigma of users thinking it is potentially harmful to the eye makes retinal scanning a bad fit for most situations.
Remember for the exam that fingerprints are the most commonly accepted type of biometrics system.
The other answers are incorrect:
'Users can be authenticated based on behavior.' is incorrect as this choice is TRUE as it pertains to BIOMETRICS.
Biometrics systems makes use of unique physical characteristics or behavior of users.
'User can be authenticated based on unique physical attributes.' is also incorrect as this choice is also TRUE as it pertains to BIOMETRICS. Biometrics systems makes use of unique physical characteristics or behavior of users.
'A biometric system's accuracy is determined by its crossover error rate (CER)' is also incorrect as this is TRUE as it also pertains to BIOMETRICS. The CER is the point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of
the CER, the more accurate the system.
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 25353-25356). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25297-25303). Auerbach Publications. Kindle Edition.

NEW QUESTION 17
- (Topic 1)
Which of the following security models does NOT concern itself with the flow of data?

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

Answer: D

Explanation:
The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.
The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned with confidentiality and bases access control decsions on the classfication of objects and the clearences of subjects.
The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes.
The Biba model is incorrect. The Biba model is concerned with integrity and is a complement to the Bell-LaPadula model in that higher levels of integrity are more trusted than lower levels. Access control us based on these integrity levels to assure that read/write operations do not decrease an object's integrity.
References:
CBK, pp 325 - 326
AIO3, pp. 290 - 291

NEW QUESTION 21
- (Topic 1)
Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

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

Answer: C

Explanation:
The original TACACS, developed in the early ARPANet days, had very limited functionality and used the UDP transport. In the early 1990s, the protocol was extended to include additional functionality and the transport changed to TCP.
TACACS is defined in RFC 1492, and uses (either TCP or UDP) port 49 by default. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. TACACSD uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back.
TACACS+
TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP).
Since TCP is connection oriented
protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet loss, timeout etc. since it rides on UDP which is connectionless.
RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore it is vulnerable to different types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.
RADIUS and TACACS + are client/ server protocols, which means the server portion cannot send unsolicited commands to the client portion. The server portion can only speak when spoken to. Diameter is a peer-based protocol that allows either end to initiate communication. This functionality allows the Diameter server to send a message to the access server to request the user to provide another authentication credential if she is attempting to access a secure resource.
Reference(s) used for this question: http://en.wikipedia.org/wiki/TACACS
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 239). McGraw- Hill. Kindle Edition.

NEW QUESTION 26
- (Topic 1)
Which of the following is most relevant to determining the maximum effective cost of access control?

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

Answer: A

Explanation:
The cost of access control must be commensurate with the value of the information that is being protected.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION 30
- (Topic 1)
Which access control type has a central authority that determine to what objects the subjects have access to and it is based on role or on the organizational security policy?

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

Answer: C

Explanation:
Non Discretionary Access Control include Role Based Access Control (RBAC) and Rule Based Access Control (RBAC or RuBAC). RABC being a subset of NDAC, it was easy to eliminate RBAC as it was covered under NDAC already.
Some people think that RBAC is synonymous with NDAC but RuBAC would also fall into this category.
Discretionary Access control is for environment with very low level of security. There is no control on the dissemination of the information. A user who has access to a file can copy the file or further share it with other users.
Rule Based Access Control is when you have ONE set of rules applied uniformly to all users. A good example would be a firewall at the edge of your network. A single rule based is applied against any packets received from the internet.
Mandatory Access Control is a very rigid type of access control. The subject must dominate the object and the subject must have a Need To Know to access the information. Objects have labels that indicate the sensitivity (classification) and there is also categories to enforce the Need To Know (NTK).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 31
- (Topic 1)
Single Sign-on (SSO) is characterized by which of the following advantages?

A. Convenience

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

Answer: B

Explanation:
Convenience -Using single sign-on users have to type their passwords only once when they first log in to access all the network resources; and Centralized Administration as some single sign-on systems are built around a unified server administration system. This allows a single administrator to add and delete accounts across the entire network from one user interface.
The following answers are incorrect:
Convenience - alone this is not the correct answer.
Centralized Data or Network Administration - these are thrown in to mislead the student. Neither are a benefit to SSO, as these specifically should not be allowed with just an SSO.
References: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, page 35.
TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, page 180.

NEW QUESTION 32
- (Topic 1)
What is the PRIMARY use of a password?

A. Allow access to files.
B. Identify the user.
C. Authenticate the user.
D. Segregate various user's accesses.

Answer: C

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

NEW QUESTION 36
- (Topic 1)
Which of the following would assist the most in Host Based intrusion detection?

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

Answer: A

Explanation:
To assist in Intrusion Detection you would review audit logs for access violations.
The following answers are incorrect:
access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.
security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.
host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

NEW QUESTION 38
- (Topic 1)
Which security model is based on the military classification of data and people with clearances?

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

Answer: C

Explanation:
The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model. The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION 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 46
- (Topic 1)
The end result of implementing the principle of least privilege means which of the following?

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

Answer: A

Explanation:
The principle of least privilege refers to allowing users to have only the access they need and not anything more. Thus, certain users may have no need to access any of the files on specific systems.
The following answers are incorrect:
Users can access all systems. Although the principle of least privilege limits what access and systems users have authorization to, not all users would have a need to know to access all of the systems. The best answer is still Users would get access to only the info for which they have a need to know as some of the users may not have a need to access a system.
Users get new privileges when they change positions. Although true that a user may indeed require new privileges, this is not a given fact and in actuality a user may require less privileges for a new position. The principle of least privilege would require that the rights required for the position be closely evaluated and where possible rights revoked.
Authorization creep. Authorization creep occurs when users are given additional rights with new positions and responsibilities. The principle of least privilege should actually prevent authorization creep.
The following reference(s) were/was used to create this question: ISC2 OIG 2007 p.101,123
Shon Harris AIO v3 p148, 902-903

NEW QUESTION 51
- (Topic 1)
Which of the following control pairings include: organizational policies and procedures, pre- employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?

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

Answer: A

Explanation:
The Answer: Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 56
- (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)
Which of the following statements pertaining to biometrics is false?

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

Answer: D

Explanation:
Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based on the Type 3 authentication mechanism.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).

NEW QUESTION 62
- (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 63
- (Topic 1)
A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:

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

Answer: C

Explanation:
A central authority determines what subjects can have access to certain objects based on the organizational security policy.
The key focal point of this question is the 'central authority' that determines access rights. Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as:
"MAC Policy means that Access Control Policy Decisions are made by a CENTRAL
AUTHORITY. Which seems to indicate there could be two good answers to this question.
However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy.
Within the same document it is also mentioned: "In general, all access control policies other than DAC are grouped in the category of non- discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action."
Under NDAC you have two choices:
Rule Based Access control and Role Base Access Control
MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC.
This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control.
The following are incorrect answers: MANDATORY ACCESS CONTROL
In Mandatory Access Control the labels of the object and the clearance of the subject
determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed.
The need for a MAC mechanism arises when the security policy of a system dictates that:
1. Protection decisions must not be decided by the object owner.
2. The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).
Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the ??simple security rule,?? or ??no read up.??
Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the ??*-property?? (pronounced
??star property??) or ??no write down.?? The *-property is required to maintain system security in an automated environment.
DISCRETIONARY ACCESS CONTROL
In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority.
DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file.
DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons:
First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann??s file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann??s file without Ann??s knowledge.
Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann??s files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows:
Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system.
No restrictions apply to the usage of information when the user has received it.

The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization??s security requirements.
ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy.
RULE BASED ACCESS CONTROL
In Rule-based Access Control a central authority could in fact determine what subjects can
have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer.
RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC. ??Rule-based access?? is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices. Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control??for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be re configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting. Some provisions of access control systems have rule- based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.
References used for this question: http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf and
AIO v3 p162-167 and OIG (2007) p.186-191
also
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 66
- (Topic 1)
This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

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

Answer: C

Explanation:
Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.
The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).
If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.
The following answers are incorrect:
All of the other choices presented were simply detractors. The following reference(s) were used for this question:
Handbook of Information Security Management

NEW QUESTION 67
- (Topic 1)
In biometrics, "one-to-many" search against database of stored biometric images is done in:

A. Authentication
B. Identification
C. Identities
D. Identity-based access control

Answer: B

Explanation:
In biometrics, identification is a "one-to-many" search of an individual's characteristics from a database of stored images.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION 69
- (Topic 1)
Which of the following is an example of discretionary access control?

A. Identity-based access control

B. Task-based access control
C. Role-based access control
D. Rule-based access control

Answer: A

Explanation:
An identity-based access control is an example of discretionary access control that is based on an individual's identity. Identity-based access control (IBAC) is access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.
Rule Based Access Control (RuBAC) and Role Based Access Control (RBAC) are
examples of non-discretionary access controls.
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.
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.
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 dissimination 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.
Source: 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
http://itlaw.wikia.com/wiki/Identity-based_access_control

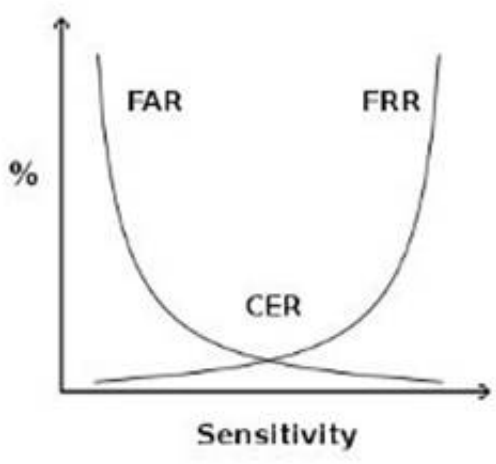
NEW QUESTION 70
- (Topic 1)
Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in a biometric authentication system, the system becomes increasingly selective and has the possibility of generating:

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

Answer: B

Explanation:
Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in a biometric authentication system, the system becomes increasingly selective and has a higher False Rejection Rate (FRR).
Conversely, if the sensitivity is decreased, the False Acceptance Rate (FRR) will increase. Thus, to have a valid measure of the system performance, the Cross Over Error (CER) rate is used. The Crossover Error Rate (CER) is the point at which the false rejection rates and the false acceptance rates are equal. The lower the value of the CER, the more accurate the system.
There are three categories of biometric accuracy measurement (all represented as percentages):
False Reject Rate (a Type I Error): When authorized users are falsely rejected as unidentified or unverified.
False Accept Rate (a Type II Error): When unauthorized persons or imposters are falsely accepted as authentic.
Crossover Error Rate (CER): The point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.
NOTE:
Within the ISC2 book they make use of the term Accept or Acceptance and also Reject or Rejection when referring to the type of errors within biometrics. Below we make use of Acceptance and Rejection throughout the text for conistency. However, on the real exam you could see either of the terms.
Performance of biometrics
Different metrics can be used to rate the performance of a biometric factor, solution or application. The most common performance metrics are the False

Acceptance Rate FAR and the False Rejection Rate FRR.
When using a biometric application for the first time the user needs to enroll to the system. The system requests fingerprints, a voice recording or another biometric factor from the
operator, this input is registered in the database as a template which is linked internally to a user ID. The next time when the user wants to authenticate or identify himself, the biometric input provided by the user is compared to the template(s) in the database by a matching algorithm which responds with acceptance (match) or rejection (no match).
FAR and FRR
The FAR or False Acceptance rate is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a valid template. The FAR is normally expressed as a percentage, following the FAR definition this is the percentage of invalid inputs which are incorrectly accepted.
The FRR or False Rejection Rate is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input provided by the user with a stored template. The FRR is normally expressed as a percentage, following the FRR definition this is the percentage of valid inputs which are incorrectly rejected.
FAR and FRR are very much dependent on the biometric factor that is used and on the technical implementation of the biometric solution. Furthermore the FRR is strongly person dependent, a personal FRR can be determined for each individual.
Take this into account when determining the FRR of a biometric solution, one person is insufficient to establish an overall FRR for a solution. Also FRR might increase due to environmental conditions or incorrect use, for example when using dirty fingers on a fingerprint reader. Mostly the FRR lowers when a user gains more experience in how to use the biometric device or software.
FAR and FRR are key metrics for biometric solutions, some biometric devices or software even allow to tune them so that the system more quickly matches or rejects. Both FRR and FAR are important, but for most applications one of them is considered most important. Two examples to illustrate this:
When biometrics are used for logical or physical access control, the objective of the application is to disallow access to unauthorized individuals under all circumstances. It is clear that a very low FAR is needed for such an application, even if it comes at the price of a higher FRR.
When surveillance cameras are used to screen a crowd of people for missing children, the objective of the application is to identify any missing children that come up on the screen. When the identification of those children is automated using a face recognition software, this software has to be set up with a low FRR. As such a higher number of matches will be false positives, but these can be reviewed quickly by surveillance personnel.
False Acceptance Rate is also called False Match Rate, and False Rejection Rate is sometimes referred to as False Non-Match Rate.
crossover error rate



crossover error rate
Above see a graphical representation of FAR and FRR errors on a graph, indicating the CER
CER
The Crossover Error Rate or CER is illustrated on the graph above. It is the rate where both FAR and FRR are equal.
The matching algorithm in a biometric software or device uses a (configurable) threshold which determines how close to a template the input must be for it to be considered a match. This threshold value is in some cases referred to as sensitivity, it is marked on the X axis of the plot. When you reduce this threshold there will be more false acceptance errors (higher FAR) and less false rejection errors (lower FRR), a higher threshold will lead to lower FAR and higher FRR.
Speed
Most manufacturers of biometric devices and softwares can give clear numbers on the time it takes to enroll as well on the time for an individual to be authenticated or identified using their application. If speed is important then take your time to consider this, 5 seconds might seem a short time on paper or when testing a device but if hundreds of people will use the device multiple times a day the cumulative loss of time might be significant.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third
Edition ((ISC)2 Press) (Kindle Locations 2723-2731). Auerbach Publications. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.
and
http://www.biometric-solutions.com/index.php?story=performance_biometrics

NEW QUESTION 75
- (Topic 1)
What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?

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

Answer: C

Explanation:
The percentage at which the False Rejection Rate equals the False Acceptance Rate is called the Crossover Error Rate (CER). Another name for the CER is the Equal Error Rate (EER), any of the two terms could be used.
Equal error rate or crossover error rate (EER or CER)
It is the rate at which both accept and reject errors are equal. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
The other choices were all wrong answers:
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. This is when an impostor would be accepted by the system.

False reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. This is when a valid company employee would be rejected by the system.
Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.
and https://en.wikipedia.org/wiki/Biometrics

NEW QUESTION 78
- (Topic 1)
Which of the following would be true about Static password tokens?

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

Answer: A

Explanation:
Password Tokens
Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.
Static Password Tokens:
The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.
Synchronous Dynamic Password Tokens:
This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.
Asynchronous Dynamic Password Tokens:
The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).
Challenge Response Tokens:
This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.
Reference(s) used for this question: http://www.informit.com/guides/content.aspx?g=security&seqNum=146
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION 82
- (Topic 1)
In an organization where there are frequent personnel changes, non-discretionary access control using Role Based Access Control (RBAC) is useful because:

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

Answer: B

Explanation:
In an organization where there are frequent personnel changes, non- discretionary access control (also called Role Based Access Control) is useful because the access controls are based on the individual's role or title within the organization. You can easily configure a new employee acces by assigning the user to a role that has been predefine. The user will implicitly inherit the permissions of the role by being a member of that role.
These access permissions defined within the role do not need to be changed whenever a new person takes over the role.
Another type of non-discretionary access control model is the Rule Based Access Control (RBAC or RuBAC) where a global set of rule is uniformly applied to all subjects accessing the resources. A good example of RuBAC would be a firewall.
This question is a sneaky one, one of the choice has only one added word to it which is often. Reading questions and their choices very carefully is a must for the real exam. Reading it twice if needed is recommended.
Shon Harris in her book list the following ways of managing RBAC: Role-based access control can be managed in the following ways:
Non-RBAC Users are mapped directly to applications and no roles are used. (No roles being used)
Limited RBAC Users are mapped to multiple roles and mapped directly to other types of
applications that do not have role-based access functionality. (A mix of roles for applications that supports roles and explicit access control would be used for applications that do not support roles)
Hybrid RBAC Users are mapped to multiapplication roles with only selected rights assigned to those roles.
Full RBAC Users are mapped to enterprise roles. (Roles are used for all access being granted)
NIST defines RBAC as:
Security administration can be costly and prone to error because administrators usually specify access control lists for each user on the system individually. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition McGraw-Hill. and
http://csrc.nist.gov/groups/SNS/rbac/

NEW QUESTION 84
- (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 88
- (Topic 1)
Which of the following is not a logical control when implementing logical access security?

A. access profiles.
B. userids.
C. employee badges.
D. passwords.

Answer: C

Explanation:
Employee badges are considered Physical so would not be a logical control. The following answers are incorrect:
userids. Is incorrect because userids are a type of logical control.
access profiles. Is incorrect because access profiles are a type of logical control. passwords. Is incorrect because passwords are a type of logical control.

NEW QUESTION 91
- (Topic 1)
This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill. What best describes this scenario?

A. Excessive Rights
B. Excessive Access
C. Excessive Permissions
D. Excessive Privileges

Answer: D

Explanation:
Even thou all 4 terms are very close to each other, the best choice is Excessive Privileges which would include the other three choices presented.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 645.
and

NEW QUESTION 92
- (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 93
- (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 96
- (Topic 1)
Which of the following statements pertaining to Kerberos is TRUE?

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

Answer: A

Explanation:
The question was asking for a TRUE statement and the only correct statement is "Kerberos does not address availability".
Kerberos addresses the confidentiality and integrity of information. It does not directly address availability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control
systems (page 42).

NEW QUESTION 99
- (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.

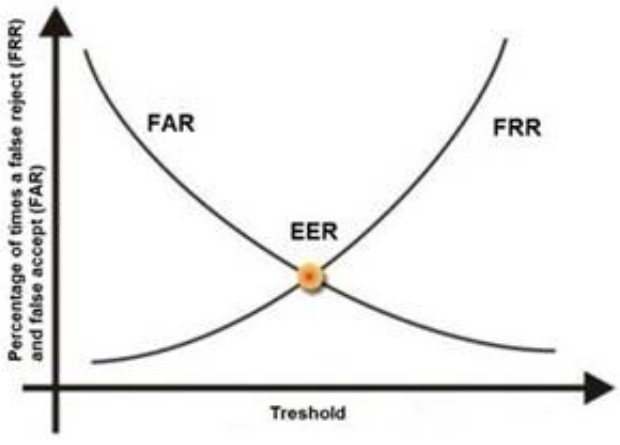
NEW QUESTION 102
- (Topic 1)
When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?

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 106
- (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 111
- (Topic 1)
What does it mean to say that sensitivity labels are "incomparable"?

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

Answer: D

Explanation:
If a category does not exist then you cannot compare it. Incomparable is when you have two disjointed sensitivity labels, that is a category in one of the labels is not in the other label. "Because neither label contains all the categories of the other, the labels can't be compared. They're said to be incomparable"
COMPARABILITY:
The label:
TOP SECRET [VENUS ALPHA]
is "higher" than either of the labels:
SECRET [VENUS ALPHA] TOP SECRET [VENUS]
But you can't really say that the label:
TOP SECRET [VENUS]
is higher than the label:
SECRET [ALPHA]
Because neither label contains all the categories of the other, the labels can't be compared. They're said to be incomparable. In a mandatory access control system, you won't be allowed access to a file whose label is incomparable to your clearance.
The Multilevel Security policy uses an ordering relationship between labels known as the dominance relationship. Intuitively, we think of a label that dominates another as being "higher" than the other. Similarly, we think of a label that is dominated by another as being "lower" than the other. The dominance relationship is used to determine permitted operations and information flows.
DOMINANCE
The dominance relationship is determined by the ordering of the Sensitivity/Clearance component of the label and the intersection of the set of Compartments.

Sample Sensitivity/Clearance ordering are:
Top Secret > Secret > Confidential > Unclassified s3 > s2 > s1 > s0
Formally, for label one to dominate label 2 both of the following must be true: The sensitivity/clearance of label one must be greater than or equal to the sensitivity/clearance of label two.
The intersection of the compartments of label one and label two must equal the compartments of label two.
Additionally:
Two labels are said to be equal if their sensitivity/clearance and set of compartments are exactly equal. Note that dominance includes equality.
One label is said to strictly dominate the other if it dominates the other but is not equal to the other.
Two labels are said to be incomparable if each label has at least one compartment that is not included in the other's set of compartments.
The dominance relationship will produce a partial ordering over all possible MLS labels, resulting in what is known as the MLS Security Lattice.
The following answers are incorrect:
The number of classification in the two labels is different. Is incorrect because the categories are what is being compared, not the classifications.
Neither label contains all the classifications of the other. Is incorrect because the categories are what is being compared, not the classifications.
the number of categories in the two labels is different. Is incorrect because it is possibe a category exists more than once in one sensitivity label and does exist in the other so they would be comparable.
Reference(s) used for this question:
OReilly - Computer Systems and Access Control (Chapter 3) http://www.oreilly.com/catalog/csb/chapter/ch03.html
and http://rubix.com/cms/mls_dom

NEW QUESTION 114
- (Topic 1)
Sensitivity labels are an example of what application control type?

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

Answer: A

Explanation:
Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.
The incorrect answers are:
Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.
Compensating administrative controls - There no such application control. Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups. Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 264).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

NEW QUESTION 119
- (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 122
- (Topic 1)
In non-discretionary access control using Role Based Access Control (RBAC), a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:

A. The societies role in the organization
B. The individual's role in the organization
C. The group-dynamics as they relate to the individual's role in the organization
D. The group-dynamics as they relate to the master-slave role in the organization

Answer: B

Explanation:
In Non-Discretionary Access Control, when Role Based Access Control is being used, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization.
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 124
- (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 privilage 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 126
- (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 128
- (Topic 1)
Which of the following Kerberos components holds all users' and services' cryptographic keys?

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

Answer: C

Explanation:
The Key Distribution Center (KDC) holds all users' and services' cryptographic keys. It provides authentication services, as well as key distribution functionality. The Authentication Service is the part of the KDC that authenticates a principal. The Key Distribution Service and Key Granting Service are distracters and are not defined Kerberos components.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION 129
- (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 130
- (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 133
- (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 136
- (Topic 1)
Which of the following protects a password from eavesdroppers and supports the encryption of communication?

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

Answer: A

Explanation:
CHAP: A protocol that uses a three way hanbdshake The server sends the client a challenge which includes a random value(a nonce) to thwart replay attacks. The client responds with the MD5 hash of the nonce and the password.
The authentication is successful if the client's response is the one that the server expected. Reference: Page 450, OIG 2007.
CHAP protects the password from eavesdroppers and supports the encryption of communication.
Reference: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

NEW QUESTION 139
- (Topic 1)
Which TCSEC level is labeled Controlled Access Protection?

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

Answer: B

Explanation:
C2 is labeled Controlled Access Protection.
The TCSEC defines four divisions: D, C, B and A where division A has the highest security. Each division represents a significant difference in the trust an individual or organization
can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and

A1.
Each division and class expands or modifies as indicated the requirements of the immediately prior division or class.
D ?? Minimal protection
Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division
C ?? Discretionary protection
C1 ?? Discretionary Security Protection Identification and authentication Separation of users and data
Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis
Required System Documentation and user manuals C2 ?? Controlled Access Protection
More finely grained DAC
Individual accountability through login procedures Audit trails
Object reuse Resource isolation
B ?? Mandatory protection
B1 ?? Labeled Security Protection
Informal statement of the security policy model Data sensitivity labels
Mandatory Access Control (MAC) over selected subjects and objects Label exportation capabilities
All discovered flaws must be removed or otherwise mitigated Design specifications and verification
B2 ?? Structured Protection
Security policy model clearly defined and formally documented DAC and MAC enforcement extended to all subjects and objects
Covert storage channels are analyzed for occurrence and bandwidth Carefully structured into protection-critical and non-protection-critical elements Design and implementation enable more comprehensive testing and review Authentication mechanisms are strengthened
Trusted facility management is provided with administrator and operator segregation Strict configuration management controls are imposed
B3 ?? Security Domains
Satisfies reference monitor requirements
Structured to exclude code not essential to security policy enforcement Significant system engineering directed toward minimizing complexity Security administrator role defined
Audit security-relevant events
Automated imminent intrusion detection, notification, and response Trusted system recovery procedures
Covert timing channels are analyzed for occurrence and bandwidth
An example of such a system is the XTS-300, a precursor to the XTS-400 A ?? Verified protection
A1 ?? Verified Design Functionally identical to B3
Formal design and verification techniques including a formal top-level specification Formal management and distribution procedures
An example of such a system is Honeywell's Secure Communications Processor SCOMP, a precursor to the XTS-400
Beyond A1
System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB).
Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications.
Formal Specification and Verification is where the TCB is verified down to the source code level, using formal verification methods where feasible.
Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.
The following are incorrect answers: C1 is Discretionary security
C3 does not exists, it is only a detractor
B1 is called Labeled Security Protection.
Reference(s) used for this question:
HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.
and
AIOv4 Security Architecture and Design (pages 357 - 361) AIOv5 Security Architecture and Design (pages 358 - 362)

NEW QUESTION 142
- (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-LaPdaula model is incorrect. The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearence 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

NEW QUESTION 147
- (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 force to use collusion to defeat those security mechanism.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 150
- (Topic 1)
What are called user interfaces that limit the functions that can be selected by a user?

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

Answer: A

Explanation:
Constrained user interfaces limit the functions that can be selected by a user.
Another method for controlling access is by restricting users to specific functions based on their role in the system. This is typically implemented by limiting available menus, data views, encryption, or by physically constraining the user interfaces.
This is common on devices such as an automated teller machine (ATM). The advantage of a constrained user interface is that it limits potential avenues of attack and system failure by restricting the processing options that are available to the user.
On an ATM machine, if a user does not have a checking account with the bank he or she will not be shown the ??Withdraw money from checking?? option. Likewise, an information system might have an ??Add/Remove Users?? menu option for administrators, but if a normal, non-administrative user logs in he or she will not even see that menu option. By not even identifying potential options for non-qualifying users, the system limits the potentially harmful execution of unauthorized system or application commands.
Many database management systems have the concept of ??views.?? A database view is an extract of the data stored in the database that is filtered based on predefined user or system criteria. This permits multiple users to access the same database while only having the ability to access data they need (or are allowed to have) and not data for another user. The use of database views is another example of a constrained user interface.
The following were incorrect answers:
All of the other choices presented were bogus answers.
The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1989-2002). Auerbach Publications. Kindle Edition.

NEW QUESTION 153
- (Topic 1)
The primary service provided by Kerberos is which of the following?

A. non-repudiation
B. confidentiality
C. authentication
D. authorization

Answer: C

Explanation:
The Answer authentication. Kerberos is an authentication service. It can use single-factor or multi-factor authentication methods.
The following answers are incorrect:
non-repudiation. Since Kerberos deals primarily with symmetric cryptography, it does not help with non-repudiation.
confidentiality. Once the client is authenticated by Kerberos and obtains its session key and ticket, it may use them to assure confidentiality of its communication with a server; however, that is not a Kerberos service as such.
authorization. Although Kerberos tickets may include some authorization information, the meaning of the authorization fields is not standardized in the Kerberos specifications, and authorization is not a primary Kerberos service.
The following reference(s) were/was used to create this question:
ISC2 OIG,2007 p. 179-184
Shon Harris AIO v.3 152-155

NEW QUESTION 157
- (Topic 1)
Which type of control is concerned with restoring controls?

A. Compensating controls
B. Corrective controls
C. Detective controls

D. Preventive controls

Answer: B

Explanation:
Corrective controls are concerned with remedying circumstances and restoring controls.
Detective controls are concerned with investigating what happen after the fact such as logs and video surveillance tapes for example.
Compensating controls are alternative controls, used to compensate weaknesses in other controls.
Preventive controls are concerned with avoiding occurrences of risks. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 159
- (Topic 1)
Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

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

Answer: A

Explanation:
B level is the first Mandatory Access Control Level.
First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition.
and
THE source for all TCSEC "level" questions: http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt (paragraph 3 for this one)

NEW QUESTION 160
- (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 infromation that was sent.
Zeroization. Zeroization involves overwrting 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 165
- (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 169
- (Topic 1)

A timely review of system access audit records would be an example of which of the basic security functions?

A. avoidance.
B. deterrence.
C. prevention.
D. detection.

Answer: D

Explanation:
By reviewing system logs you can detect events that have occured.
The following answers are incorrect:
avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.
deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.
prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

NEW QUESTION 171
- (Topic 1)
Which of the following is needed for System Accountability?

A. Audit mechanisms.
B. Documented design as laid out in the Common Criteria.
C. Authorization.
D. Formal verification of system design.

Answer: A

Explanation:
Is a means of being able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.
Accountability is the ability to identify users and to be able to track user actions. The following answers are incorrect:
Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.
Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.
Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.
References:
OIG CBK Glossary (page 778)

NEW QUESTION 174
- (Topic 1)
How should a doorway of a manned facility with automatic locks be configured?

A. It should be configured to be fail-secure.
B. It should be configured to be fail-safe.
C. It should have a door delay cipher lock.
D. It should not allow piggybacking.

Answer: B

Explanation:
Access controls are meant to protect facilities and computers as well as people.
In some situations, the objectives of physical access controls and the protection of people's lives may come into conflict. In theses situations, a person's life always takes precedence.
Many physical security controls make entry into and out of a facility hard, if not impossible. However, special consideration needs to be taken when this could affect lives. In an information processing facility, different types of locks can be used and piggybacking should be prevented, but the issue here with automatic locks is that they can either be configured as fail-safe or fail-secure.
Since there should only be one access door to an information processing facility, the
automatic lock to the only door to a man-operated room must be configured to allow people out in case of emergency, hence to be fail-safe (sometimes called fail-open), meaning that upon fire alarm activation or electric power failure, the locking device unlocks. This is because the solenoid that maintains power to the lock to keep it in a locked state fails and thus opens or unlocks the electronic lock.
Fail Secure works just the other way. The lock device is in a locked or secure state with no power applied. Upon authorized entry, a solinoid unlocks the lock temporarily. Thus in a Fail Secure lock, loss of power of fire alarm activation causes the lock to remain in a secure mode.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 451). McGraw- Hill. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20249-20251). Auerbach Publications. Kindle Edition.

NEW QUESTION 179
- (Topic 2)
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system is referred to as?

A. Confidentiality
B. Availability
C. Integrity
D. Reliability

Answer: B

Explanation:
An company security program must:
1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability;
2) protect informationcommensurate with the level of risk and magnitude ofharmresulting fromloss, misuse, unauthorized access, or modification.
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.
The following are incorrect answers:
Confidentiality - The information requires protection from unauthorized disclosure and only the INTENDED recipient should have access to the meaning of the data either in storage or in transit.
Integrity - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:
Authenticity ?CA third party must be able to verify that the content of a message has not been changed in transit.
Non-repudiation ?C The origin or the receipt of a specific message must be verifiable by a third party.
Accountability - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
Reference used for this question:
RFC 2828
and
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (page 5).

NEW QUESTION 181
- (Topic 2)
Which of the following is BEST defined as a physical control?

A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms

Answer: B

Explanation:
Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
The following answers are incorrect answers:
Monitoring of system activity is considered to be administrative control.
Identification and authentication methods are considered to be a technical control. Logical access control mechanisms is also considered to be a technical control.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 1280-1282). McGraw-Hill. Kindle Edition.

NEW QUESTION 183
- (Topic 2)
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?

A. Estimating the cost of the changes requested
B. Recreating and analyzing the problem
C. Determining the interface that is presented to the user
D. Establishing the priorities of requests

Answer: D

Explanation:
Change control sub-phase includes Recreating and analyzing the problem, Determining the interface that is presented to the user, and Establishing the priorities of requests.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).

NEW QUESTION 188
- (Topic 2)
Which of the following should NOT be performed by an operator?

A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow

Answer: C

Explanation:
Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.
System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system??s security policy. As such, use of these
privileges should be monitored through audit logs.
Some of the privileges and responsibilities assigned to operators include:
Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.
Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.
Volume mounting: This allows the desired application access to the system and its data. Controlling job flow: Operators can initiate, pause, or terminate programs.

This may allow
an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation
of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.
Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.
Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.
Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.
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 19367-19395). Auerbach Publications. Kindle Edition.

NEW QUESTION 193
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SSCP Exam with Our Prep Materials Via below:

https://www.certleader.com/SSCP-dumps.html