ISC2

Exam Questions SSCP

System Security Certified Practitioner (SSCP)

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)
The type of discretionary access control (DAC) that is based on an individual's identity is also called:

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

Answer: A

Explanation:
An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.
DAC is good for low level security environment. The owner of the file decides who has access to the file.
If a user creates a file, he is the owner of that file. An identifier for this user is placed in the file header and/or in an access control matrix within the operating system.
Ownership might also be granted to a specific individual. For example, a manager for a certain department might be made the owner of the files and resources within her department. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources.
This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers , are the owners of the data within their specific department. Being the owner, they can specify who should have access and who should not.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 220). McGraw- Hill . Kindle Edition.

NEW QUESTION 3
- (Topic 1)
Which access control model achieves data integrity through well-formed transactions and separation of duties?

A. Clark-Wilson model
B. Biba model
C. Non-interference model
D. Sutherland model

Answer: A

Explanation:
The Clark-Wilson model differs from other models that are subject- and object- oriented by introducing a third access element programs resulting in what is called an access triple, which prevents unauthorized users from modifying data or programs. The Biba model uses objects and subjects and addresses integrity based on a hierarchical
lattice of integrity levels. The non-interference model is related to the information flow model with restrictions on the information flow. The Sutherland model approaches integrity by focusing on the problem of inference.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 12).
And: KRAUSE, Micki & TIPTON, Harold F., Handbook of Information Security Management, CRC Press, 1997, Domain 1: Access Control.

NEW QUESTION 4
- (Topic 1)
Detective/Technical measures:

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

Answer: A

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

NEW QUESTION 5

- (Topic 1)
Which is the last line of defense in a physical security sense?

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

Answer: A

Explanation:
"Ultimately, people are the last line of defense for your company's assets" (Pastore & Dulaney, 2006, p. 529).
Pastore, M. and Dulaney, E. (2006). CompTIA Security+ study guide: Exam SY0-101. Indianapolis, IN: Sybex.

NEW QUESTION 6
- (Topic 1)
Controlling access to information systems and associated networks is necessary for the preservation of their:

A. Authenticity, confidentiality and availability
B. Confidentiality, integrity, and availability.
C. integrity and availability.
D. authenticity,confidentiality, integrity and availability.

Answer: B

Explanation:
Controlling access to information systems and associated networks is necessary for the preservation of their confidentiality, integrity and availability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

NEW QUESTION 7
- (Topic 1)
Smart cards are an example of which type of control?

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

Answer: C

Explanation:
Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 245). McGraw- Hill. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 32).

NEW QUESTION 8
- (Topic 1)
What refers to legitimate users accessing networked services that would normally be restricted to them?

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

Answer: D

Explanation:
Unauthorized access of restricted network services by the circumvention of security access controls is known as logon abuse. This type of abuse refers to users who may be internal to the network but access resources they would not normally be allowed. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3:
Telecommunications and Network Security (page 74).

NEW QUESTION 9
- (Topic 1)
Which of the following is most affected by denial-of-service (DOS) attacks?

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

Answer: D

Explanation:
Denial of service attacks obviously affect availability of targeted systems. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 61).

NEW QUESTION 10
- (Topic 1)
Which of the following would be used to implement Mandatory Access Control (MAC)?

A. Clark-Wilson Access Control
B. Role-based access control
C. Lattice-based access control
D. User dictated access control

Answer: C

Explanation:
The lattice is a mechanism use to implement Mandatory Access Control (MAC)
Under Mandatory Access Control (MAC) you have: Mandatory Access Control
Under Non Discretionary Access Control (NDAC) you have: Rule-Based Access Control
Role-Based Access Control
Under Discretionary Access Control (DAC) you have: Discretionary Access Control
The Lattice Based Access Control is a type of access control used to implement other access control method. A lattice is an ordered list of elements that has a least upper bound and a most lower bound. The lattice can be used for MAC, DAC, Integrity level, File Permission, and more
For example in the case of MAC, if we look at common government classifications, we have the following:
TOP SECRET
SECRET -----------------------I am the user at secret CONFIDENTIAL
SENSITIVE BUT UNCLASSIFIED UNCLASSIFIED
If you look at the diagram above where I am a user at SECRET it means that I can access document at lower classification but not document at TOP SECRET. The lattice is a list of ORDERED ELEMENT, in this case the ordered elements are classification levels. My least upper bound is SECRET and my most lower bound is UNCLASSIFIED.
However the lattice could also be used for Integrity Levels such as: VERY HIGH
HIGH
MEDIUM ----------I am a user, process, application at the medium level LOW
VERY LOW
In the case of of Integrity levels you have to think about TRUST. Of course if I take for example the the VISTA operating system which is based on Biba then Integrity Levels would be used. As a user having access to the system I cannot tell a process running with administrative privilege what to do. Else any users on the system could take control of the system by getting highly privilege process to do things on their behalf. So no read down would be allowed in this case and this is an example of the Biba model.
Last but not least the lattice could be use for file permissions: RWX
RW ---------User at this level
R
If I am a user with READ and WRITE (RW) access privilege then I cannot execute the file
because I do not have execute permission which is the X under linux and UNIX.
Many people confuse the Lattice Model and many books says MAC = LATTICE, however the lattice can be use for other purposes.
There is also Role Based Access Control (RBAC) that exists out there. It COULD be used to simulate MAC but it is not MAC as it does not make use of Label on objects indicating sensitivity and categories. MAC also require a clearance that dominates the object.
You can get more info about RBAC at:http://csrc.nist.gov/groups/SNS/rbac/faq.html#03 Also note that many book uses the same acronym for Role Based Access Control and Rule
Based Access Control which is RBAC, this can be confusing.
The proper way of writing the acronym for Rule Based Access Control is RuBAC, unfortunately it is not commonly used.
References:
There is a great article on technet that talks about the lattice in VISTA: http://blogs.technet.com/b/steriley/archive/2006/07/21/442870.aspx
also see:
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).
and
http://www.microsoft-watch.com/content/vista/gaging_vistas_integrity.html

NEW QUESTION 10
- (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 11
- (Topic 1)
Which of the following access control techniques best gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure?

A. Access control lists
B. Discretionary access control
C. Role-based access control
D. Non-mandatory access control

Answer: C

Explanation:
Role-based access control (RBAC) gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are given to users in that role. An access control list (ACL) is a table that tells a system which access rights each user has to a particular system object. With discretionary access control, administration is decentralized and owners of resources control other users' access. Non-mandatory access control is not a defined access control technique.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 9).

NEW QUESTION 16
- (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 20
- (Topic 1)
In which of the following model are Subjects and Objects identified and the permissions applied to each subject/object combination are specified. Such a model can be used to quickly summarize what permissions a subject has for various system objects.

A. Access Control Matrix model
B. Take-Grant model
C. Bell-LaPadula model
D. Biba model

Answer: A

Explanation:
An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. Matrices are data structures that programmers implement as table lookups that will be used and enforced by the operating system.
This type of access control is usually an attribute of DAC models. The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs).
Capability Table
A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.
Access control lists (ACLs)
ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access a specific object, and they define what level of authorization is granted. Authorization can be specific to an individual, group, or role. ACLs map values from the access control matrix to the object.
Whereas a capability corresponds to a row in the access control matrix, the ACL corresponds to a column of the matrix.
NOTE: Ensure you are familiar with the terms Capability and ACLs for the purpose of the exam.
Resource(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5264-5267). McGraw-Hill. Kindle Edition.
or
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Page 229 and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1923-1925). Auerbach Publications. Kindle Edition.

NEW QUESTION 21
- (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 23
- (Topic 1)
What is the most critical characteristic of a biometric identifying system?

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

Answer: C

Explanation:
Accuracy is the most critical characteristic of a biometric identifying verification system.
Accuracy is measured in terms of false rejection rate (FRR, or type I errors) and false acceptance rate (FAR or type II errors).
The Crossover Error Rate (CER) is the point at which the FRR equals the FAR and has become the most important measure of biometric system accuracy.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 9).

NEW QUESTION 26
- (Topic 1)
Controls to keep password sniffing attacks from compromising computer systems include which of the following?

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

Answer: C

Explanation:
To minimize the chance of passwords being captured one-time passwords would prevent a password sniffing attack because once used it is no longer valid.
Encryption will also minimize these types of attacks.
The following answers are correct:
static and recurring passwords. This is incorrect because if there is no encryption then someone password sniffing would be able to capture the password much easier if it never changed.
encryption and recurring passwords. This is incorrect because while encryption helps, recurring passwords do nothing to minimize the risk of passwords being captured.
static and one-time passwords. This is incorrect because while one-time passwords will prevent these types of attacks, static passwords do nothing to minimize the risk of passwords being captured.

NEW QUESTION 30
- (Topic 1)
Which of the following is NOT a system-sensing wireless proximity card?

A. magnetically striped card
B. passive device
C. field-powered device
D. transponder

Answer: A

Explanation:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 342.

NEW QUESTION 31
- (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 32
- (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 35
- (Topic 1)
Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is correct?

A. Examples of these types of controls include policies and procedures, securityawareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.
B. Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.
C. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
D. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

Answer: C

Explanation:
Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 36
- (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 40
- (Topic 1)
What does the Clark-Wilson security model focus on?

A. Confidentiality

B. Integrity
C. Accountability
D. Availability

Answer: B

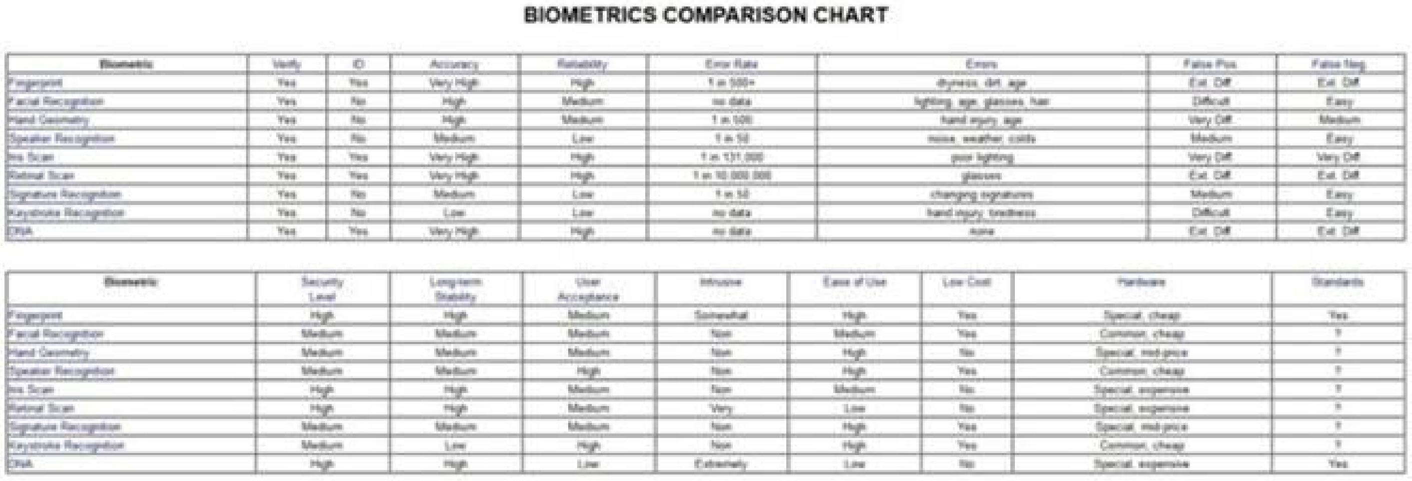
Explanation:
The Clark-Wilson model addresses integrity. It incorporates mechanisms to enforce internal and external consistency, a separation of duty, and a mandatory integrity policy.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION 42
- (Topic 1)
Which of the following biometric devices has the lowest user acceptance level?

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

Answer: A

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

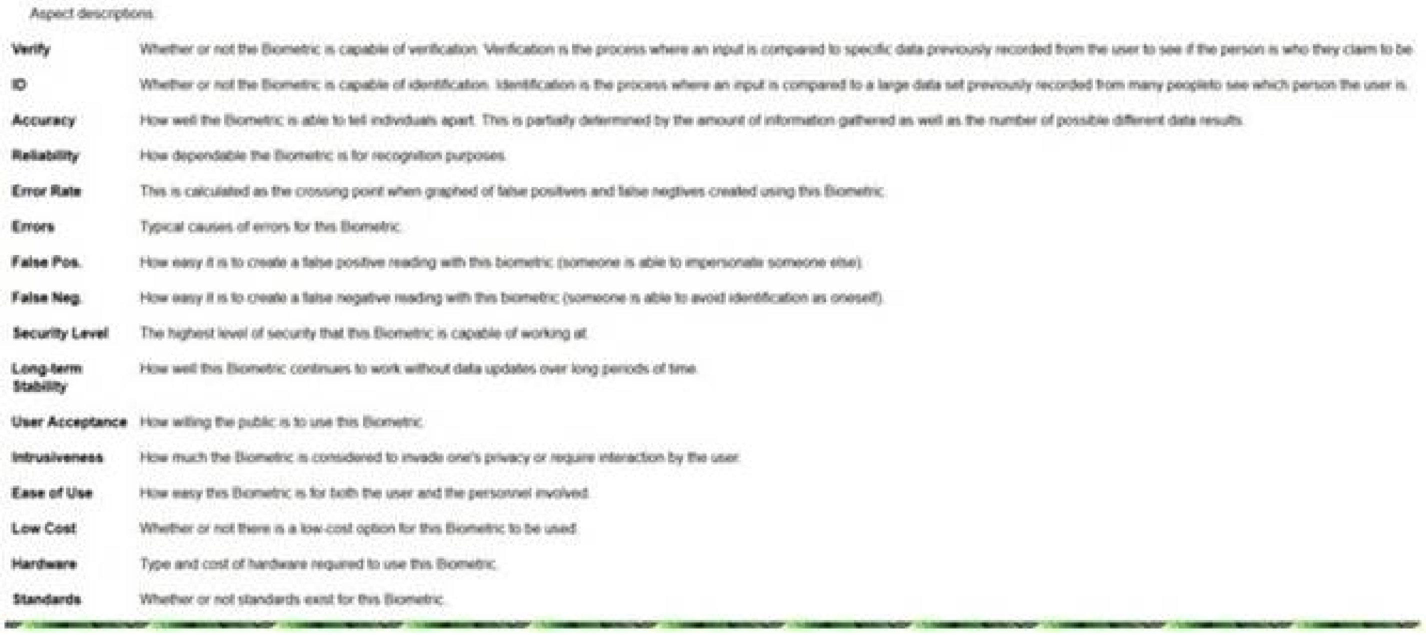


BIOMETRICS COMPARISON CHART

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors	False Pos.	False Neg.
Fingerprint	Yes	Yes	Very High	High	1 in 500+	dryness, dirt, age	Ext. Diff.	Ext. Diff.
Facial Recognition	Yes	No	High	Medium	no data	lighting, age, glasses, hair	Difficult	Easy
Hand Geometry	Yes	No	High	Medium	1 in 500	hand injury, age	Very Diff.	Medium
Speaker Recognition	Yes	No	Medium	Low	1 in 50	noise, weather, colds	Medium	Easy
Iris Scan	Yes	Yes	Very High	High	1 in 131,000	poor lighting	Very Diff.	Very Diff.
Retinal Scan	Yes	Yes	Very High	High	1 in 10,000,000	glasses	Ext. Diff.	Ext. Diff.
Signature Recognition	Yes	No	Medium	Low	1 in 50	changing signatures	Medium	Easy
Keystroke Recognition	Yes	No	Low	Low	no data	hand injury, tiredness	Difficult	Easy
DNA	Yes	Yes	Very High	High	no data	none	Ext. Diff.	Ext. Diff.

Biometric	Security Level	Long-term Stability	User Acceptance	Intrusive	Ease of Use	Low Cost	Hardware	Standards
Fingerprint	High	High	Medium	Somewhat	High	Yes	Special, cheap	Yes
Facial Recognition	Medium	Medium	Medium	Non	Medium	Yes	Common, cheap	?
Hand Geometry	Medium	Medium	Medium	Non	High	No	Special, mid-price	?
Speaker Recognition	Medium	Medium	High	Non	High	Yes	Common, cheap	?
Iris Scan	High	High	Medium	Non	Medium	No	Special, expensive	?
Retinal Scan	High	High	Medium	Very	Low	No	Special, expensive	?
Signature Recognition	Medium	Medium	Medium	Non	High	Yes	Special, mid-price	?
Keystroke Recognition	Medium	Low	High	Non	High	Yes	Common, cheap	?
DNA	High	High	Low	Extremely	Low	No	Special, expensive	Yes

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



Aspect descriptions

Verify	Whether or not the Biometric is capable of verification. Verification is the process where an input is compared to specific data previously recorded from the user to see if the person is who they claim to be.
ID	Whether or not the Biometric is capable of identification. Identification is the process where an input is compared to a large data set previously recorded from many peopleto see which person the user is.
Accuracy	How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results.
Reliability	How dependable the Biometric is for recognition purposes.
Error Rate	This is calculated as the crossing point when graphed of false positives and false negtives created using this Biometric.
Errors	Typical causes of errors for this Biometric.
False Pos.	How easy it is to create a false positive reading with this biometric (someone is able to impersonate someone else).
False Neg.	How easy it is to create a false negative reading with this biometric (someone is able to avoid identification as oneself).
Security Level	The highest level of security that this Biometric is capable of working at.
Long-term Stability	How well this Biometric continues to work without data updates over long periods of time.
User Acceptance	How willing the public is to use this Biometric.
Intrusiveness	How much the Biometric is considered to invade one's privacy or require interaction by the user.
Ease of Use	How easy this Biometric is for both the user and the personnel involved.
Low Cost	Whether or not there is a low-cost option for this Biometric to be used.
Hardware	Type and cost of hardware required to use this Biometric.
Standards	Whether or not standards exist for this Biometric.

C:\Users\MCS\Desktop\1.jpg
Biometric Aspect Descriptions Reference(s) used for this question:
RHODES, Keith A., Chief Technologist, United States General Accounting Office, National Preparedness, Technologies to Secure Federal Buildings, April 2002 (page 10).
and
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy

NEW QUESTION 45
- (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 48
- (Topic 1)
The control measures that are intended to reveal the violations of security policy using software and hardware are associated with:

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

Answer: B

Explanation:
The detective/technical control measures are intended to reveal the violations of security policy using technical means.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION 53
- (Topic 1)
What is called a password that is the same for each log-on session?

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

Answer: C

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

NEW QUESTION 56
- (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 59
- (Topic 1)
Which of the following is the most reliable authentication method for remote access?

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

Answer: B

Explanation:
A Synchronous token generates a one-time password that is only valid for a short period of time. Once the password is used it is no longer valid, and it expires if not entered in the acceptable time frame.
The following answers are incorrect:
Variable callback system. Although variable callback systems are more flexible than fixed callback systems, the system assumes the identity of the individual unless two-factor authentication is also implemented. By itself, this method might allow an attacker access as a trusted user.
Fixed callback system. Authentication provides assurance that someone or something is who or what he/it is supposed to be. Callback systems authenticate a person, but anyone can pretend to be that person. They are tied to a specific place and phone number, which can be spoofed by implementing call-forwarding.
Combination of callback and Caller ID. The caller ID and callback functionality provides greater confidence and auditability of the caller's identity. By disconnecting and calling back only authorized phone numbers, the system has a greater confidence in the location of the call. However, unless combined with strong authentication, any individual at the location could obtain access.
The following reference(s) were/was used to create this question: Shon Harris AIO v3 p. 140, 548
ISC2 OIG 2007 p. 152-153, 126-127

NEW QUESTION 60
- (Topic 1)

What is the main objective of proper separation of duties?

A. To prevent employees from disclosing sensitive information.
B. To ensure access controls are in place.
C. To ensure that no single individual can compromise a system.
D. To ensure that audit trails are not tampered with.

Answer: C

Explanation:
The primary objective of proper separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. A proper separation of duties does not prevent employees from disclosing information, nor does it ensure that access controls are in place or that audit trails are not tampered with. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 12: Operations Security (Page 808).

NEW QUESTION 65
- (Topic 1)
Pin, Password, Passphrases, Tokens, smart cards, and biometric devices are all items that can be used for Authentication. When one of these item listed above in conjunction with a second factor to validate authentication, it provides robust authentication of the individual by practicing which of the following?

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

Answer: B

Explanation:
Once an identity is established it must be authenticated. There exist numerous technologies and implementation of authentication methods however they almost all fall under three major areas.
There are three fundamental types of authentication: Authentication by knowledge—something a person knows
Authentication by possession—something a person has
Authentication by characteristic—something a person is Logical controls related to these types are called “factors.”
Something you know can be a password or PIN, something you have can be a token fob or smart card, and something you are is usually some form of biometrics.
Single-factor authentication is the employment of one of these factors, two-factor authentication is using two of the three factors, and three-factor authentication is the combination of all three factors.
The general term for the use of more than one factor during authentication is multifactor authentication or strong authentication.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 2367-2379). Auerbach Publications. Kindle Edition.

NEW QUESTION 68
- (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 71
- (Topic 1)
Which TCSEC class specifies discretionary protection?

A. B2
B. B1
C. C2
D. C1

Answer: D

Explanation:
C1 involves discretionary protection, C2 involves controlled access protection, B1 involves labeled security protection and B2 involves structured protection.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 72
- (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 76
- (Topic 1)
In the context of Biometric authentication, what is a quick way to compare the accuracy of devices. In general, the device that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

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

Answer: A

Explanation:
equal error rate or crossover error rate (EER or CER): the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
In the context of Biometric Authentication almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher False Reject Rate (FRR).
Conversely, if the sensitivity is decreased, the False Acceptance Rate (FAR) will increase. Thus, to have a valid measure of the system performance, the CrossOver Error Rate (CER) is used.
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value.
false reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
template capacity: the maximum number of sets of data which can be stored in the system. Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten
Domains of Computer Security, 2001, John Wiley & Sons, Page 37. and
Wikipedia at: https://en.wikipedia.org/wiki/Biometrics

NEW QUESTION 78
- (Topic 1)
Which of the following control pairing places emphasis on "soft" mechanisms that support the access control objectives?

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

Answer: B

Explanation:
Soft Control is another way of referring to Administrative control.
Technical and Physical controls are NOT soft control, so any choice listing them was not the best answer.
Preventative/Technical is incorrect because although access control can be technical control, it is commonly not referred to as a "soft" control
Preventative/Administrative is correct because access controls are preventative in nature. it is always best to prevent a negative event, however there are times where controls might fail and you cannot prevent everything. Administrative controls are roles, responsibilities,
policies, etc which are usually paper based. In the administrative category you would find audit, monitoring, and security awareness as well.
Preventative/Physical pairing is incorrect because Access controls with an emphasis on "soft" mechanisms conflict with the basic concept of physical controls, physical controls are usually tangible objects such as fences, gates, door locks, sensors, etc...
Detective/Administrative Pairing is incorrect because access control is a preventative control used to control access, not to detect violations to access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 83
- (Topic 1)
What is called the verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time?

A. Authentication
B. Identification
C. Integrity
D. Confidentiality

Answer: A

Explanation:
Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.
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 87
- (Topic 1)
Identification and authentication are the keystones of most access control systems. Identification establishes:

A. User accountability for the actions on the system.
B. Top management accountability for the actions on the system.
C. EDP department accountability for the actions of users on the system.
D. Authentication for actions on the system

Answer: A

Explanation:
Identification and authentication are the keystones of most access control systems. Identification establishes user accountability for the actions on the system.
The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.
Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three general factors can be used for authentication: something a person knows, something a person has, and something a person is. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.
For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting. Once these steps are completed successfully, the user can access and use network resources; however, it is necessary to track the user's activities and enforce accountability for his actions.
Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase,
cryptographic key, personal identification number (PIN), anatomical attribute, or token.
These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are not done yet. Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.
Although identification, authentication, authorization, and accountability have close and complementary definitions, each has distinct functions that fulfill a specific requirement in the process of access control. A user may be properly identified and authenticated to the network, but he may not have the authorization to access the files on the file server. On the other hand, a user may be authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Access Control ((ISC)2 Press) (Kindle Locations 889-892). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3875-3878). McGraw-Hill. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3833-3848). McGraw-Hill. Kindle Edition.
and
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 90
- (Topic 1)
When submitting a passphrase for authentication, the passphrase is converted into ...

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

Answer: A

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

NEW QUESTION 93

- (Topic 1)
Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?

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

Answer: B

Explanation:
Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit
of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter.
Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 34).

NEW QUESTION 95
- (Topic 1)
Which of the following statements pertaining to access control is false?

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

Answer: B

Explanation:
Access control mechanisms should default to no access to provide the necessary level of security and ensure that no security holes go unnoticed. If access is not explicitly allowed, it should be implicitly denied.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 4: Access Control (page 143).

NEW QUESTION 98
- (Topic 1)
A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?

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

Answer: A

Explanation:
When access control is based on the content of an object, it is considered to be content dependent access control.
Content-dependent access control is based on the content itself. The following answers are incorrect:
context-dependent access control. Is incorrect because this type of control is based on what the context is, facts about the data rather than what the object contains.
least privileges access control. Is incorrect because this is based on the least amount of rights needed to perform their jobs and not based on what is contained in the database. ownership-based access control. Is incorrect because this is based on the owner of the data and and not based on what is contained in the database.
References:
OIG CBK Access Control (page 191)

NEW QUESTION 101
- (Topic 1)
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on :

A. sex of a person
B. physical attributes of a person
C. age of a person
D. voice of a person

Answer: B

Explanation:
Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already under way.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION 103
- (Topic 1)
Which of the following Operation Security controls is intended to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system?

A. Detective Controls
B. Preventative Controls
C. Corrective Controls
D. Directive Controls

Answer: B

Explanation:
In the Operations Security domain, Preventative Controls are designed to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 217.

NEW QUESTION 104
- (Topic 1)
Which of the following floors would be most appropriate to locate information processing facilities in a 6-stories building?

A. Basement
B. Ground floor
C. Third floor
D. Sixth floor

Answer: C

Explanation:
You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well.
Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.
They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation
considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor.
The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center.
So it was easy to come up with the answer by using the process of elimination where the top, the bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 5th Edition, Page 425.

NEW QUESTION 106
- (Topic 1)
Which of the following choices describe a Challenge-response tokens generation?

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

Answer: A

Explanation:
Challenge-response tokens are:
- A workstation or system generates a random challenge string and the owner enters the string into the token along with the proper PIN.
- The token generates a response that is then entered into the workstation or system.
- The authentication mechanism in the workstation or system then determines if the owner should be authenticated.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 136-137).

NEW QUESTION 111
- (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 115
- (Topic 1)
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:

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

Answer: C

Explanation:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered.
These factors include the enrollment time, the throughput rate, and acceptability. Enrollment time is the time it takes to initially "register" with a system by providing samples
of the biometric characteristic to be evaluated. An acceptable enrollment time is around two
minutes.
For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.
In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.
Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

NEW QUESTION 117
- (Topic 1)
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:

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

Answer: C

Explanation:
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.
Specifying HOW to restrain hackers is not directly linked to access control.
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 12.

NEW QUESTION 122
- (Topic 1)
Which of the following questions is less likely to help in assessing physical access controls?

A. Does management regularly review the list of persons with physical access to sensitive facilities?
B. Is the operating system configured to prevent circumvention of the security software and application controls?
C. Are keys or other access devices needed to enter the computer room and media library?
D. Are visitors to sensitive areas signed in and escorted?

Answer: B

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 access controls except for the one regarding operating system configuration, which is a logical access 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 127
- (Topic 1)
What is the primary role of smartcards in a PKI?

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

Answer: D

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

Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance Security
Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from
retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.
Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.
It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:
physical attack of various forms (microprobing, drills, files, solvents, etc.) freezing the device
applying out-of-spec voltages or power surges applying unusual clock signals
inducing software errors using radiation
measuring the precise time and power requirements of certain operations (see power analysis)
Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of- specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.
Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

NEW QUESTION 130
- (Topic 1)
Who developed one of the first mathematical models of a multilevel-security computer system?

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

Answer: C

Explanation:
In 1973 Bell and LaPadula created the first mathematical model of a multi- level security system.
The following answers are incorrect:
Diffie and Hellman. This is incorrect because Diffie and Hellman was involved with cryptography.
Clark and Wilson. This is incorrect because Bell and LaPadula was the first model. The Clark-Wilson model came later, 1987.
Gasser and Lipner. This is incorrect, it is a distractor. Bell and LaPadula was the first model.

NEW QUESTION 135
- (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 140
- (Topic 1)
Which of the following biometric parameters are better suited for authentication use over a long period of time?

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

Answer: A

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

NEW QUESTION 145
- (Topic 1)
What is the name of the first mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?

A. Clark and Wilson Model
B. Harrison-Ruzzo-Ullman Model
C. Rivest and Shamir Model
D. Bell-LaPadula Model

Answer: D

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

NEW QUESTION 150
- (Topic 1)
Which of the following is true about Kerberos?

A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.

Answer: C

Explanation:
Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.
The following answers are incorrect:
It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys
(symmetric ciphers).
It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys.
It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.
References:
MIT http://web.mit.edu/kerberos/
Wikipedi http://en.wikipedia.org/wiki/Kerberos_%28protocol%29
OIG CBK Access Control (pages 181 - 184) AIOv3 Access Control (pages 151 - 155)

NEW QUESTION 153
- (Topic 1)
Which of the following remote access authentication systems is the most robust?

A. TACACS+
B. RADIUS
C. PAP
D. TACACS

Answer: A

Explanation:
TACACS+ is a proprietary Cisco enhancement to TACACS and is more robust than RADIUS. PAP is not a remote access authentication system but a remote node security protocol.
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 122).

NEW QUESTION 155
- (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 160
- (Topic 1)
Why should batch files and scripts be stored in a protected area?

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

Answer: C

Explanation:
Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION 163
- (Topic 1)
Kerberos can prevent which one of the following attacks?

A. tunneling attack.
B. playback (replay) attack.
C. destructive attack.
D. process attack.

Answer: B

Explanation:
Each ticket in Kerberos has a timestamp and are subject to time expiration to
help prevent these types of attacks. The following answers are incorrect:
tunneling attack. This is incorrect because a tunneling attack is an attempt to bypass security and access low-level systems. Kerberos cannot totally prevent these types of attacks.
destructive attack. This is incorrect because depending on the type of destructive attack, Kerberos cannot prevent someone from physically destroying a server.
process attack. This is incorrect because with Kerberos cannot prevent an authorzied individuals from running processes.

NEW QUESTION 168
- (Topic 1)
What does the (star) integrity axiom mean in the Biba model?

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

Answer: D

Explanation:
The (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION 171
- (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 174
- (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 176
- (Topic 1)
What does the simple integrity axiom mean in the Biba model?

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

Answer: B

Explanation:
The simple integrity axiom of the Biba access control model states that a subject at one level of integrity is not permitted to observe an object of a lower integrity (no read down).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION 181
- (Topic 1)

Which of the following is the FIRST step in protecting data's confidentiality?

A. Install a firewall
B. Implement encryption
C. Identify which information is sensitive
D. Review all user access rights

Answer: C

Explanation:
In order to protect the confidentiality of the data. The following answers are incorrect because :
Install a firewall is incorrect as this would come after the information has been identified for sensitivity levels.
Implement encryption is also incorrect as this is one of the mechanisms to protect the data once it has been identified.
Review all user access rights is also incorrect as this is also a protection mechanism for the identified information.
Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 126

NEW QUESTION 184
- (Topic 1)
What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

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

Answer: A

Explanation:
The Answer Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION 185
- (Topic 1)
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

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

Answer: A

Explanation:
RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 186
- (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 188
- (Topic 1)
The following is NOT a security characteristic we need to consider while choosing a biometric identification systems:

A. data acquisition process

B. cost
C. enrollment process
D. speed and user interface

Answer: B

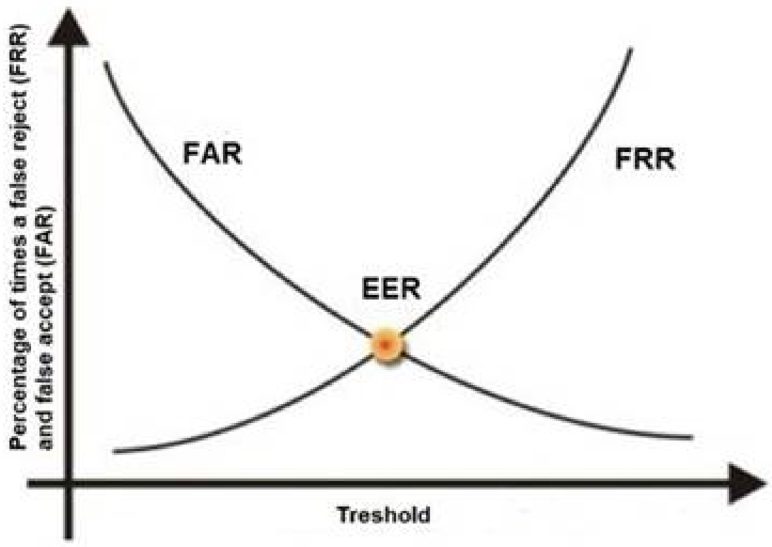
Explanation:
Cost is a factor when considering Biometrics but it is not a security characteristic.
All the other answers are incorrect because they are security characteristics related to Biometrics.
data acquisition process can cause a security concern because if the process is not fast and efficient it can discourage individuals from using the process.
enrollment process can cause a security concern because the enrollment process has to be quick and efficient. This process captures data for authentication.
speed and user interface can cause a security concern because this also impacts the users acceptance rate of biometrics. If they are not comfortable with the interface and speed they might sabotage the devices or otherwise attempt to circumvent them.
References:
OIG Access Control (Biometrics) (pgs 165-167)
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Pages 5-6.
in process of correction

NEW QUESTION 192
- (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 195
- (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 200
- (Topic 1)
Kerberos is vulnerable to replay in which of the following circumstances?

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

Answer: C

Explanation:
Replay can be accomplished on Kerberos if the compromised tickets are used within an allotted time window.
The security depends on careful implementation:enforcing limited lifetimes for authentication credentials minimizes the threat of of replayed credentials, the KDC must be physically secured, and it should be hardened, not permitting any non-kerberos activities.
Reference:
Official ISC2 Guide to the CISSP, 2007 Edition, page 184 also see:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

NEW QUESTION 201
- (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 202
- (Topic 1)
Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

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

Answer: B

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

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

NEW QUESTION 204
- (Topic 1)
Which of the following biometric devices offers the LOWEST CER?

A. Keystroke dynamics
B. Voice verification
C. Iris scan
D. Fingerprint

Answer: C

Explanation:
From most effective (lowest CER) to least effective (highest CER) are: Iris scan, fingerprint, voice verification, keystroke dynamics.
Reference : Shon Harris Aio v3 , Chapter-4 : Access Control , Page : 131
Also see: http://www.sans.org/reading_room/whitepapers/authentication/biometric-selection-body-parts-online_139

NEW QUESTION 205
- (Topic 1)
A confidential number used as an authentication factor to verify a user's identity is called a:

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

Answer: A

Explanation:
PIN Stands for Personal Identification Number, as the name states it is a combination of numbers.
The following answers are incorrect:
User ID This is incorrect because a Userid is not required to be a number and a Userid is only used to establish identity not verify it.
Password. This is incorrect because a password is not required to be a number, it could be any combination of characters.
Challenge. This is incorrect because a challenge is not defined as a number, it could be anything.

NEW QUESTION 209
- (Topic 1)
How can an individual/person best be identified or authenticated to prevent local masquarading attacks?

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

Answer: D

Explanation:
The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric
identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.
Some people are getting thrown off by the term Masquarade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.
A UserId only provides for identification.
A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.
A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.
Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.
Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur.
As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information.
Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.
NOTE FROM CLEMENT:
This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well.
I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.
Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.
I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.
The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In

the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes.
Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and terrorists. This is how you could use biometric for Identification.
There are always THREE means of authentication, they are: Something you know (Type 1)
Something you have (Type 2)
Something you are (Type 3)
Reference(s) used for this question:
TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) , 2000, CRC Press, Chapter 1, Biometric Identification (page 7).
and
Search Security at http://searchsecurity.techtarget.com/definition/masquerade

NEW QUESTION 214
- (Topic 1)
Which authentication technique best protects against hijacking?

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

Answer: B

Explanation:
A continuous authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. This is the best protection against hijacking. Static authentication is the type of authentication provided by traditional password schemes and the strength of the authentication is highly dependent on the difficulty of guessing passwords. The robust authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, and it does not protect against hijacking. Strong authentication refers to a two-factor authentication (like something a user knows and something a user is).
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3: Secured Connections to External Networks (page 51).

NEW QUESTION 219
- (Topic 1)
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:

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

Answer: A

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

NEW QUESTION 224
- (Topic 1)
What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

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

Answer: B

Explanation:
D or "minimal protection" is reserved for systems that were evaluated under the TCSEC but did not meet the requirements for a higher trust level.
A is incorrect. A or "Verified Protectection" is the highest trust level under the TCSEC. E is incorrect. The trust levels are A - D so "E" is not a valid trust level.
F is incorrect. The trust levels are A - D so "F" is not a valid trust level.
CBK, pp. 329 - 330
AIO3, pp. 302 - 306

NEW QUESTION 225
- (Topic 1)
What is Kerberos?

A. A three-headed dog from the egyptian mythology.
B. A trusted third-party authentication protocol.
C. A security model.
D. A remote authentication dial in user server.

Answer: B

Explanation:
Is correct because that is exactly what Kerberos is. The following answers are incorrect:
A three-headed dog from Egyptian mythology. Is incorrect because we are dealing with Information Security and not the Egyptian mythology but the Greek Mythology.
A security model. Is incorrect because Kerberos is an authentication protocol and not just a security model.
A remote authentication dial in user server. Is incorrect because Kerberos is not a remote authentication dial in user server that would be called RADIUS.

NEW QUESTION 228
- (Topic 1)
The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

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

Answer: A

Explanation:
The correct answer is "clipping level". This is the point at which a system decides to take some sort of action when an action repeats a preset number of times. That action may be to log the activity, lock a user account, temporarily close a port, etc.
Example: The most classic example of a clipping level is failed login attempts. If you have a system configured to lock a user's account after three failed login attemts, that is the "clipping level".
The other answers are not correct because:
Acceptance level, forgiveness level, and logging level are nonsensical terms that do not exist (to my knowledge) within network security.
Reference:
Official ISC2 Guide - The term "clipping level" is not in the glossary or index of that book. I cannot find it in the text either. However, I'm quite certain that it would be considered part of the CBK, despite its exclusion from the Official Guide.
All in One Third Edition page: 136 - 137

NEW QUESTION 232
- (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 237
- (Topic 1)
Which access control model is best suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

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

Answer: B

Explanation:
MAC provides high security by regulating access based on the clearance of individual users and sensitivity labels for each object. Clearance levels and sensitivity levels cannot be modified by individual users -- for example, user Joe (SECRET clearance) cannot reclassify the "Presidential Doughnut Recipe" from "SECRET" to "CONFIDENTIAL" so that his friend Jane (CONFIDENTIAL clearance) can read it. The administrator is ultimately responsible for configuring this protection in accordance with security policy and directives from the Data Owner.
DAC is incorrect. In DAC, the data owner is responsible for controlling access to the object. Access control matrix is incorrect. The access control matrix is a way of thinking about the
access control needed by a population of subjects to a population of objects. This access
control can be applied using rules, ACL's, capability tables, etc.
TACACS is incorrect. TACACS is a tool for performing user authentication. References:
CBK, p. 187, Domain 2: Access Control. AIO3, Chapter 4, Access Control.

NEW QUESTION 238
- (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 242
- (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 245
- (Topic 1)
Which of the following best ensures accountability of users for the actions taken within a system or domain?

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

Answer: B

Explanation:
Details:
The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be. After showing proper credentials, a user is authorized access to resources.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

NEW QUESTION 247
- (Topic 1)
Which of the following would be an example of the best password?

A. golf001
B. Elizabeth
C. T1me4g0lF
D. password

Answer: C

Explanation:
The best passwords are those that are both easy to remember and hard to crack using a dictionary attack. The best way to create passwords that fulfil both criteria is to use two small unrelated words or phonemes, ideally with upper and lower case characters, a special character, and/or a number. Shouldn't be used: common names, DOB, spouse, phone numbers, words found in dictionaries or system defaults.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 1.

NEW QUESTION 251
- (Topic 1)
Why do buffer overflows happen? What is the main cause?

A. Because buffers can only hold so much data
B. Because of improper parameter checking within the application
C. Because they are an easy weakness to exploit
D. Because of insufficient system memory

Answer: B

Explanation:

Buffer Overflow attack takes advantage of improper parameter checking within the application. This is the classic form of buffer overflow and occurs because the programmer accepts whatever input the user supplies without checking to make sure that the length of the input is less than the size of the buffer in the program.
The buffer overflow problem is one of the oldest and most common problems in software development and programming, dating back to the introduction of interactive computing. It can result when a program fills up the assigned buffer of memory with more data than its buffer can hold. When the program begins to write beyond the end of the buffer, the program's execution path can be changed, or data can be written into areas used by the operating system itself. This can lead to the insertion of malicious code that can be used to gain administrative privileges on the program or system.
As explained by Gaurab, it can become very complex. At the time of input even if you are checking the length of the input, it has to be check against the buffer size. Consider a case where entry point of data is stored in Buffer1 of Application1 and then you copy it to Buffer2 within Application2 later on, if you are just checking the length of data against Buffer1, it will
not ensure that it will not cause a buffer overflow in Buffer2 of Application2.
A bit of reassurance from the ISC2 book about level of Coding Knowledge needed for the exam:
It should be noted that the CISSP is not required to be an expert programmer or know the inner workings of developing application software code, like the FORTRAN programming language, or how to develop Web applet code using Java. It is not even necessary that the CISSP know detailed security-specific coding practices such as the major divisions of buffer overflow exploits or the reason for preferring str(n)cpy to strcpy in the C language (although all such knowledge is, of course, helpful). Because the CISSP may be the person responsible for ensuring that security is included in such developments, the CISSP should know the basic procedures and concepts involved during the design and development of software programming. That is, in order for the CISSP to monitor the software development process and verify that security is included, the CISSP must understand the fundamental concepts of programming developments and the security strengths and weaknesses of various application development processes.
The following are incorrect answers:
"Because buffers can only hold so much data" is incorrect. This is certainly true but is not the best answer because the finite size of the buffer is not the problem -- the problem is that the programmer did not check the size of the input before moving it into the buffer.
"Because they are an easy weakness to exploit" is incorrect. This answer is sometimes true but is not the best answer because the root cause of the buffer overflow is that the programmer did not check the size of the user input.
"Because of insufficient system memory" is incorrect. This is irrelevant to the occurrence of a buffer overflow.
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 13319-13323). Auerbach Publications. Kindle Edition.

NEW QUESTION 252
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SSCP Practice Exam Features:

* SSCP Questions and Answers Updated Frequently

* SSCP Practice Questions Verified by Expert Senior Certified Staff

* SSCP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SSCP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SSCP Practice Test Here