ISC2

Exam Questions SSCP

System Security Certified Practitioner (SSCP)

NEW QUESTION 1
- (Topic 1)
Which of the following pairings uses technology to enforce access control policies?

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

Answer: B

Explanation:
The preventive/technical pairing uses technology to enforce access control policies.
TECHNICAL CONTROLS
Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.
Preventive Technical Controls
Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:
Access control software. Antivirus software. Library control systems. Passwords.
Smart cards. Encryption.
Dial-up access control and callback systems.
Preventive Physical Controls
Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:
Backup files and documentation. Fences.
Security guards. Badge systems. Double door systems. Locks and keys. Backup power.
Biometric access controls. Site selection.
Fire extinguishers.
Preventive Administrative Controls
Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:
Security awareness and technical training. Separation of duties.
Procedures for recruiting and terminating employees. Security policies and procedures.
Supervision.
Disaster recovery, contingency, and emergency plans. User registration for computer access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 2
- (Topic 1)
Detective/Technical measures:

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

Answer: A

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

NEW QUESTION 3
- (Topic 1)
Smart cards are an example of which type of control?

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

Answer: C

Explanation:
Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 245). McGraw- Hill. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 32).

NEW QUESTION 4
- (Topic 1)
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:

A. concern that the laser beam may cause eye damage
B. the iris pattern changes as a person grows older.
C. there is a relatively high rate of false accepts.
D. the optical unit must be positioned so that the sun does not shine into the aperture.

Answer: D

Explanation:
Because the optical unit utilizes a camera and infrared light to create the images, sun light can impact the aperture so it must not be positioned in direct light of any type. Because the subject does not need to have direct contact with the optical reader, direct light can impact the reader.
An Iris recognition is a form of biometrics that is based on the uniqueness of a subject's iris. A camera like device records the patterns of the iris creating what is known as Iriscode.
It is the unique patterns of the iris that allow it to be one of the most accurate forms of biometric identification of an individual. Unlike other types of biometics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resoulution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject's identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.
Reference(s) used for this question: AIO, 3rd edition, Access Control, p 134. AIO, 4th edition, Access Control, p 182.
Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition The following answers are incorrect:
concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue.
the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the question would have been about long term problems then it could have been the best choice. Recent research has shown that Irises actually do change over time: http://www.nature.com/news/ageing- eyes-hinder-biometric-scans-1.10722
there is a relatively high rate of false accepts. Since the advent of the Iriscode there is a very low rate of false accepts, in fact the algorithm used has never had a false match. This all depends on the quality of the equipment used but because of the uniqueness of the iris even when comparing identical twins, iris patterns are unique.

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

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

Answer: B

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

NEW QUESTION 6
- (Topic 1)
Which of the following is a trusted, third party authentication protocol that was developed under Project Athena at MIT?

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

Answer: A

Explanation:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT.
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.
The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by systems crackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.
Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad
assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure then a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.
Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its

identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.
Kerberos is freely available from MIT, under a copyright permission notice very similar to the one used for the BSD operating and X11 Windowing system. MIT provides Kerberos in source form, so that anyone who wishes to use it may look over the code for themselves and assure themselves that the code is trustworthy. In addition, for those who prefer to rely on a professional supported product, Kerberos is available as a product from many different vendors.
In summary, Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us. At MIT, Kerberos has been invaluable to our Information/Technology architecture.
KryptoKnight is a Peer to Peer authentication protocol incorporated into the NetSP product from IBM.
SESAME is an authentication and access control protocol, that also supports communication confidentiality and integrity. It provides public key based authentication along with the Kerberos style authentication, that uses symmetric key cryptography. Sesame supports the Kerberos protocol and adds some security extensions like public key based authentication and an ECMA-style Privilege Attribute Service. The complete Sesame protocol is a two step process. In the first step, the client successfully authenticates itself to the Authentication Server and obtains a ticket that can be presented to the Privilege Attribute Server. In the second step, the initiator obtains proof of his access rights in the form of Privilege Attributes Certificate (PAC). The PAC is a specific form of Access Control Certificate as defined in the ECMA-219 document. This document describes the extensions to Kerberos for public key based authentication as adopted in Sesame.
SESAME, KryptoKnight, and NetSP never took off and the protocols are no longer commonly used.
References:
http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#whatis and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 40.

NEW QUESTION 7
- (Topic 1)
Which of the following is an example of a passive attack?

A. Denying services to legitimate users
B. Shoulder surfing
C. Brute-force password cracking
D. Smurfing

Answer: B

Explanation:
Shoulder surfing is a form of a passive attack involving stealing passwords, personal identification numbers or other confidential information by looking over someone's shoulder. All other forms of attack are active attacks, where a threat makes a modification to the system in an attempt to take advantage of a vulnerability.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 3: Security Management Practices (page 63).

NEW QUESTION 8
- (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 9
- (Topic 1)
Which of the following centralized access control mechanisms is the least appropriate for mobile workers accessing the corporate network over analog lines?

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

Answer: B

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

NEW QUESTION 10
- (Topic 1)
What is the most critical characteristic of a biometric identifying system?

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

Answer: C

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

NEW QUESTION 10
- (Topic 1)
In discretionary access environments, which of the following entities is authorized to grant information access to other people?

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

Answer: D

Explanation:
In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.
The following answers are incorrect:
manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
IMPORTANT NOTE:
The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data.
The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based
on their identity.

NEW QUESTION 13
- (Topic 1)
A network-based vulnerability assessment is a type of test also referred to as:

A. An active vulnerability assessment.
B. A routing vulnerability assessment.

C. A host-based vulnerability assessment.
D. A passive vulnerability assessment.

Answer: A

Explanation:
A network-based vulnerability assessment tool/system either re-enacts system attacks, noting and recording responses to the attacks, or probes different targets to infer weaknesses from their responses.
Since the assessment is actively attacking or scanning targeted systems, network-based vulnerability assessment systems are also called active vulnerability systems.
There are mostly two main types of test:
PASSIVE: You don't send any packet or interact with the remote target. You make use of public database and other techniques to gather information about your target.
ACTIVE: You do send packets to your target, you attempt to stimulate response which will help you in gathering information about hosts that are alive, services runnings, port state, and more.
See example below of both types of attacks:
Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system. Passive attacks are hard to detect, so in most cases methods are put in place to try to prevent them rather than to detect and stop them.
Altering messages , modifying system files, and masquerading as another individual are acts that are considered active attacks because the attacker is actually doing something instead of sitting back and gathering data. Passive attacks are usually used to gain information prior to carrying out an active attack.
IMPORTANT NOTE:
On the commercial vendors will sometimes use different names for different types of scans. However, the exam is product agnostic. They do not use vendor terms but general terms. Experience could trick you into selecting the wrong choice sometimes. See feedback from Jason below:
"I am a system security analyst. It is my daily duty to perform system vulnerability analysis. We use Nessus and Retina (among other tools) to perform our network based vulnerability scanning. Both commercially available tools refer to a network based vulnerability scan as a "credentialed" scan. Without credentials, the scan tool cannot login to the system being scanned, and as such will only receive a port scan to see what ports are open and exploitable"
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 865). McGraw- Hill. Kindle Edition.
and
DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 97).

NEW QUESTION 18
- (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 21
- (Topic 1)
Which of the following statements pertaining to biometrics is FALSE?

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

Answer: C

Explanation:
As this is not a characteristic of Biometrics this is the rigth choice for this question. This is one of the three basic way authentication can be performed and it is not related to Biometrics. Example of something you know would be a password or PIN for example.
Please make a note of the negative 'FALSE' within the question. This question may seem tricky to some of you but you would be amazed at how many people cannot deal with negative questions. There will be a few negative questions within the real exam, just like this one the keyword NOT or FALSE will be in Uppercase to clearly indicate that it is negative.
Biometrics verifies an individual’s identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of performing authentication (one to one matching) or identification (a one to many matching).
A biometric system scans an attribute or behavior of a person and compares it to a template store within an authentication server datbase, such template would be created in an earlier enrollment process. Because this system inspects the grooves of a person’s fingerprint, the pattern of someone’s retina, or the pitches of someone’s voice, it has to be extremely sensitive.
The system must perform accurate and repeatable measurements of anatomical or physiological characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so that these false positives and false negatives occur infrequently and the results are as accurate as possible.
There are two types of failures in biometric identification:
False Rejection also called False Rejection Rate (FRR) — The system fail to recognize a legitimate user. While it could be argued that this has the effect of keeping the protected area extra secure, it is an intolerable frustration to legitimate users who are refused access because the scanner does not recognize them.
False Acceptance or False Acceptance Rate (FAR) — This is an erroneous recognition, either by confusing one user with another or by accepting an imposter as a legitimate user.
Physiological Examples:
Unique Physical Attributes:

Fingerprint (Most commonly accepted) Hand Geometry
Retina Scan (Most accurate but most intrusive) Iris Scan
Vascular Scan Behavioral Examples:
Repeated Actions Keystroke Dynamics
(Dwell time (the time a key is pressed) and Flight time (the time between "key up" and the next "key down").
Signature Dynamics
(Stroke and pressure points)
EXAM TIP:
Retina scan devices are the most accurate but also the most invasive biometrics system available today. The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option. Unfortunately, the cost of the proprietary hardware as well the stigma of users thinking it is potentially harmful to the eye makes retinal scanning a bad fit for most situations.
Remember for the exam that fingerprints are the most commonly accepted type of biometrics system.
The other answers are incorrect:
'Users can be authenticated based on behavior.' is incorrect as this choice is TRUE as it pertains to BIOMETRICS.
Biometrics systems makes use of unique physical characteristics or behavior of users.
'User can be authenticated based on unique physical attributes.' is also incorrect as this choice is also TRUE as it pertains to BIOMETRICS. Biometrics systems makes use of unique physical characteristics or behavior of users.
'A biometric system's accuracy is determined by its crossover error rate (CER)' is also incorrect as this is TRUE as it also pertains to BIOMETRICS. The CER is the point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of
the CER, the more accurate the system.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25353-25356). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25297-25303). Auerbach Publications. Kindle Edition.

NEW QUESTION 23
- (Topic 1)
Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

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

Answer: C

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

NEW QUESTION 26
- (Topic 1)
Single Sign-on (SSO) is characterized by which of the following advantages?

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

Answer: B

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

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

NEW QUESTION 30
- (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 35
- (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 38
- (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 42
- (Topic 1)
Which of the following would constitute the best example of a password to use for access to a system by a network administrator?

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

Answer: D

Explanation:
GyN19Za! would be the the best answer because it contains a mixture of upper and lower case characters, alphabetic and numeric characters, and a special character making it less vulnerable to password attacks.
All of the other answers are incorrect because they are vulnerable to brute force or dictionary attacks. Passwords should not be common words or names. The addition of a number to the end of a common word only marginally strengthens it because a common password attack would also check combinations of words: Christmas23 Christmas123 etc...

NEW QUESTION 43

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

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

Answer: B

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

NEW QUESTION 48
- (Topic 1)
The three classic ways of authenticating yourself to the computer security software are by something you know, by something you have, and by something:

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

Answer: C

Explanation:
This is more commonly known as biometrics and is one of the most accurate ways to authenticate an individual.
The rest of the answers are incorrect because they not one of the three recognized forms for Authentication.

NEW QUESTION 53
- (Topic 1)
RADIUS incorporates which of the following services?

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

Answer: D

Explanation:
A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to
designated RADIUS servers, and then acting on the response which is returned.
RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.
RADIUS authentication is based on provisions of simple username/password credentials.
These credentials are encrypted
by the client using a shared secret between the client and the RADIUS server. OIG 2007, Page 513
RADIUS incorporates an authentication server and can make uses of both dynamic and static passwords.
Since it uses the PAP and CHAP protocols, it also incluses static passwords.
RADIUS is an Internet protocol. RADIUS carries authentication, authorization, and configuration information between a Network Access Server and a shared Authentication Server. RADIUS features and functions are described primarily in the IETF (International Engineering Task Force) document RFC2138.
The term " RADIUS" is an acronym which stands for Remote Authentication Dial In User Service.
The main advantage to using a RADIUS approach to authentication is that it can provide a stronger form of authentication. RADIUS is capable of using a strong, two-factor form of authentication, in which users need to possess both a user ID and a hardware or software token to gain access.
Token-based schemes use dynamic passwords. Every minute or so, the token generates a unique 4-, 6- or 8-digit access number that is synchronized with the security server. To gain entry into the system, the user must generate both this one-time number and provide his or her user ID and password.
Although protocols such as RADIUS cannot protect against theft of an authenticated session via some realtime attacks, such as wiretapping, using unique, unpredictable authentication requests can protect against a wide range of active attacks.
RADIUS: Key Features and Benefits Features Benefits
RADIUS supports dynamic passwords and challenge/response passwords. Improved system security due to the fact that passwords are not static.
It is much more difficult for a bogus host to spoof users into giving up their passwords or password-generation algorithms.
RADIUS allows the user to have a single user ID and password for all computers in a network.
Improved usability due to the fact that the user has to remember only one login combination.
RADIUS is able to:
Prevent RADIUS users from logging in via login (or ftp). Require them to log in via login (or ftp)
Require them to login to a specific network access server (NAS); Control access by time of day.
Provides very granular control over the types of logins allowed, on a per-user basis. The time-out interval for failing over from an unresponsive primary RADIUS server to a
backup RADIUS server is site-configurable.

RADIUS gives System Administrator more flexibility in managing which users can login from which hosts or devices.
Stratus Technology Product Brief http://www.stratus.com/products/vos/openvos/radius.htm
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 43, 44.
Also check: MILLER, Lawrence & GREGORY, Peter, CISSP for Dummies, 2002, Wiley Publishing, Inc., pages 45-46.

NEW QUESTION 56
- (Topic 1)
Which of the following control pairings include: organizational policies and procedures, pre- employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?

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

Answer: A

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

NEW QUESTION 61
- (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 64
- (Topic 1)
Which of the following statements relating to the Bell-LaPadula security model is FALSE (assuming the Strong Star property is not being used) ?

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

Answer: C

Explanation:
It is not a property of Bell LaPadula model. The other answers are incorrect because:
A subject is not allowed to read up is a property of the 'simple security rule' of Bell LaPadula model.
The property restriction can be escaped by temporarily downgrading a high level subject can be escaped by temporarily downgrading a high level subject or by identifying a set of trusted objects which are permitted to violate the property as long as it is not in the middle of an operation.
It is restricted to confidentiality as it is a state machine model that enforces the confidentiality aspects of access control.
Reference: Shon Harris AIO v3 , Chapter-5 : Security Models and Architecture , Page:279-
282

NEW QUESTION 67
- (Topic 1)
For maximum security design, what type of fence is most effective and cost-effective method (Foot are being used as measurement unit below)?

A. 3' to 4' high
B. 6' to 7' high
C. 8' high and above with strands of barbed wire
D. Double fencing

Answer: D

Explanation:
The most commonly used fence is the chain linked fence and it is the most affordable. The standard is a six-foot high fence with two-inch mesh square openings. The material should consist of nine-gauge vinyl or galvanized metal. Nine-gauge is a typical fence material installed in residential areas.
Additionally, it is recommended to place barbed wire strands angled out from the top of the fence at a 45° angle and away from the protected area with three strands running across the top. This will provide for a seven-foot fence. There are several variations of the use of “top guards” using V-shaped barbed wire or the use of concertina wire as an enhancement, which has been a replacement for more traditional three strand barbed wire “top guards.”
The fence should be fastened to ridged metal posts set in concrete every six feet with additional bracing at the corners and gate openings. The bottom of the fence should be stabilized against intruders crawling under by attaching posts along the bottom to keep the fence from being pushed or pulled up from the bottom. If the

soil is sandy, the bottom edge of the fence should be installed below ground level.
For maximum security design, the use of double fencing with rolls of concertina wire positioned between the two fences is the most effective deterrent and cost-efficient method. In this design, an intruder is required to use an extensive array of ladders and equipment to breach the fences.
Most fencing is largely a psychological deterrent and a boundary marker rather than a barrier, because in most cases such fences can be rather easily penetrated unless added security measures are taken to enhance the security of the fence. Sensors attached to the fence to provide electronic monitoring of cutting or scaling the fence can be used.
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 24416-24431). Auerbach Publications. Kindle Edition.

NEW QUESTION 70
- (Topic 1)
What can be defined as a list of subjects along with their access rights that are authorized to access a specific object?

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

Answer: B

Explanation:
"It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188
A capability table is incorrect. "Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object." CBK, pp. 191-192. The distinction that makes this an incorrect choice is that access is based on posession of a capability by the subject.
To put it another way, as noted in AIO3 on p. 169, "A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL."
An access control matrix is incorrect. The access control matrix is a way of describing the rules for an access control strategy. The matrix lists the users, groups and roles down the left side and the resources and functions across the top. The cells of the matrix can either indicate that access is allowed or indicate the type of access. CBK pp 317 - 318.
AIO3, p. 169 describes it as a table if subjects and objects specifying the access rights a certain subject possesses pertaining to specific objects.
In either case, the matrix is a way of analyzing the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.
A role-based matrix is incorrect. Again, a matrix of roles vs objects could be used as a tool for thinking about the access control to be applied to a set of objects. The results of the analysis could then be implemented using RBAC.
References:
CBK, Domain 2: Access Control. AIO3, Chapter 4: Access Control

NEW QUESTION 74
- (Topic 1)
Which of the following is not a security goal for remote access?

A. Reliable authentication of users and systems
B. Protection of confidential data
C. Easy to manage access control to systems and network resources
D. Automated login for remote users

Answer: D

Explanation:
An automated login function for remote users would imply a weak authentication, thus certainly not a security goal.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition, volume 2, 2001, CRC Press, Chapter 5: An Introduction to Secure Remote Access (page 100).

NEW QUESTION 75
- (Topic 1)
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessity of answering 2 questions :

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

Answer: B

Explanation:
Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already taking place. Unique physical attributes or behavior of a person are used for that purpose.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION 76
- (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 81
- (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 84
- (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 89
- (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 90
- (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 94
- (Topic 1)
A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:

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

Answer: C

Explanation:
A central authority determines what subjects can have access to certain objects based on the organizational security policy.
The key focal point of this question is the 'central authority' that determines access rights. Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as:
"MAC Policy means that Access Control Policy Decisions are made by a CENTRAL
AUTHORITY. Which seems to indicate there could be two good answers to this question.
However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy.
Within the same document it is also mentioned: "In general, all access control policies other than DAC are grouped in the category of non- discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action."
Under NDAC you have two choices:
Rule Based Access control and Role Base Access Control
MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC.
This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control.
The following are incorrect answers: MANDATORY ACCESS CONTROL
In Mandatory Access Control the labels of the object and the clearance of the subject
determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed.
The need for a MAC mechanism arises when the security policy of a system dictates that:
* 1. Protection decisions must not be decided by the object owner.
* 2. The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).
Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the “simple security rule,” or “no read up.”
Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the “*-property” (pronounced
“star property”) or “no write down.” The *-property is required to maintain system security in an automated environment.
DISCRETIONARY ACCESS CONTROL
In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority.
DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file.
DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons: First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann’s file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann’s file without Ann’s knowledge.
Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann’s files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows:
Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system.
No restrictions apply to the usage of information when the user has received it.
The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization’s security requirements.
ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy.
RULE BASED ACCESS CONTROL
In Rule-based Access Control a central authority could in fact determine what subjects can
have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer.
RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC. “Rule-based access” is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices. Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control—for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as

domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be re configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting. Some provisions of access control systems have rule- based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.
References used for this question: http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf and
AIO v3 p162-167 and OIG (2007) p.186-191
also
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 96
- (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 97
- (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 98
- (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 103
- (Topic 1)
In biometrics, "one-to-many" search against database of stored biometric images is done in:

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

Answer: B

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

NEW QUESTION 104
- (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 109
- (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 114
- (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).

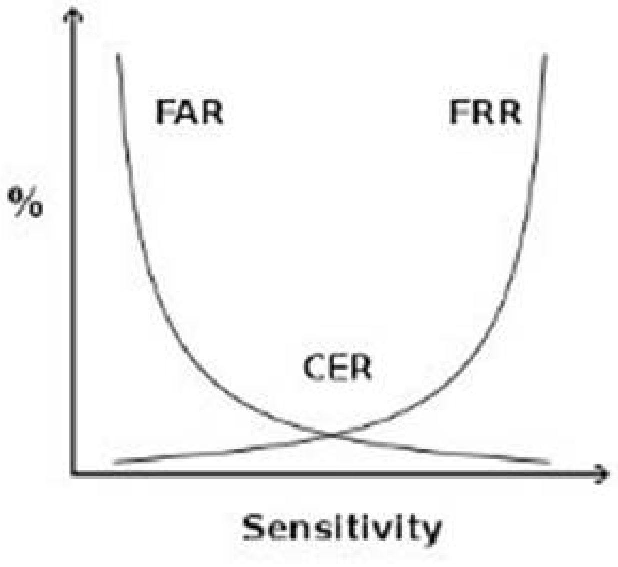
NEW QUESTION 116
- (Topic 1)
Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in a biometric authentication system, the system becomes increasingly selective and has the possibility of generating:

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

Answer: B

Explanation:
Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in a biometric authentication system, the system becomes increasingly selective and has a higher False Rejection Rate (FRR).
Conversely, if the sensitivity is decreased, the False Acceptance Rate (FRR) will increase. Thus, to have a valid measure of the system performance, the Cross Over Error (CER) rate is used. The Crossover Error Rate (CER) is the point at which the false rejection rates and the false acceptance rates are equal. The lower the value of the CER, the more accurate the system.
There are three categories of biometric accuracy measurement (all represented as percentages):
False Reject Rate (a Type I Error): When authorized users are falsely rejected as unidentified or unverified.
False Accept Rate (a Type II Error): When unauthorized persons or imposters are falsely accepted as authentic.
Crossover Error Rate (CER): The point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.
NOTE:
Within the ISC2 book they make use of the term Accept or Acceptance and also Reject or Rejection when referring to the type of errors within biometrics. Below we make use of Acceptance and Rejection throughout the text for conistency. However, on the real exam you could see either of the terms.
Performance of biometrics
Different metrics can be used to rate the performance of a biometric factor, solution or application. The most common performance metrics are the False Acceptance Rate FAR and the False Rejection Rate FRR.
When using a biometric application for the first time the user needs to enroll to the system. The system requests fingerprints, a voice recording or another biometric factor from the
operator, this input is registered in the database as a template which is linked internally to a user ID. The next time when the user wants to authenticate or identify himself, the biometric input provided by the user is compared to the template(s) in the database by a matching algorithm which responds with acceptance (match) or rejection (no match).
FAR and FRR
The FAR or False Acceptance rate is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a valid template. The FAR is normally expressed as a percentage, following the FAR definition this is the percentage of invalid inputs which are incorrectly accepted.
The FRR or False Rejection Rate is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input provided by the user with a stored template. The FRR is normally expressed as a percentage, following the FRR definition this is the percentage of valid inputs which are incorrectly rejected.
FAR and FRR are very much dependent on the biometric factor that is used and on the technical implementation of the biometric solution. Furthermore the FRR is strongly person dependent, a personal FRR can be determined for each individual.
Take this into account when determining the FRR of a biometric solution, one person is insufficient to establish an overall FRR for a solution. Also FRR might

increase due to environmental conditions or incorrect use, for example when using dirty fingers on a fingerprint reader. Mostly the FRR lowers when a user gains more experience in how to use the biometric device or software.
FAR and FRR are key metrics for biometric solutions, some biometric devices or software even allow to tune them so that the system more quickly matches or rejects. Both FRR and FAR are important, but for most applications one of them is considered most important. Two examples to illustrate this:
When biometrics are used for logical or physical access control, the objective of the application is to disallow access to unauthorized individuals under all circumstances. It is clear that a very low FAR is needed for such an application, even if it comes at the price of a higher FRR.
When surveillance cameras are used to screen a crowd of people for missing children, the objective of the application is to identify any missing children that come up on the screen. When the identification of those children is automated using a face recognition software, this software has to be set up with a low FRR. As such a higher number of matches will be false positives, but these can be reviewed quickly by surveillance personnel.
False Acceptance Rate is also called False Match Rate, and False Rejection Rate is sometimes referred to as False Non-Match Rate.
crossover error rate



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

NEW QUESTION 117
- (Topic 1)
What are the components of an object's sensitivity label?

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

Answer: D

Explanation:
Both are the components of a sensitivity label. The following are incorrect:
A Classification Set and a single Compartment. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classifcation and it is not a "single compartment" but a Compartment Set.
A single classification and a single compartment. Is incorrect because while there only is one classifcation, it is not a "single compartment" but a Compartment Set.
A Classification Set and user credentials. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classifcation and it is not "user credential" but a Compartment Set. The user would have their own sensitivity label.

NEW QUESTION 121
- (Topic 1)
Who first described the DoD multilevel military security policy in abstract, formal terms?

A. David Bell and Leonard LaPadula
B. Rivest, Shamir and Adleman
C. Whitfield Diffie and Martin Hellman
D. David Clark and David Wilson

Answer: A

Explanation:
It was David Bell and Leonard LaPadula who, in 1973, first described the DoD multilevel military security policy in abstract, formal terms. The Bell-LaPadula is a

Mandatory Access Control (MAC) model concerned with confidentiality. Rivest, Shamir and Adleman (RSA) developed the RSA encryption algorithm. Whitfield Diffie and Martin Hellman published the Diffie-Hellman key agreement algorithm in 1976. David Clark and David Wilson developed the Clark-Wilson integrity model, more appropriate for security in commercial activities.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (pages 78,109).

NEW QUESTION 126
- (Topic 1)
Which of the following is the WEAKEST authentication mechanism?

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

Answer: B

Explanation:
Most of the time users usually choose passwords which can be guessed , hence passwords is the BEST answer out of the choices listed above.
The following answers are incorrect because :
Passphrases is incorrect as it is more secure than a password because it is longer.
One-time passwords is incorrect as the name states , it is good for only once and cannot be reused.
Token devices is incorrect as this is also a password generator and is an one time
password mechanism.
Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 139 , 142.

NEW QUESTION 131
- (Topic 1)
Which of the following is not a two-factor authentication mechanism?

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

Answer: D

Explanation:
Something you know and a password fits within only one of the three ways authentication could be done. A password is an example of something you know, thereby something you know and a password does not constitute a two-factor authentication as both are in the same category of factors.
A two-factor (strong) authentication relies on two different kinds of authentication factors out of a list of three possible choice:
something you know (e.g. a PIN or password),
something you have (e.g. a smart card, token, magnetic card),
something you are is mostly Biometrics (e.g. a fingerprint) or something you do (e.g. signature dynamics).
TIP FROM CLEMENT:
On the real exam you can expect to see synonyms and sometimes sub-categories under the main categories. People are familiar with Pin, Passphrase, Password as subset of Something you know.
However, when people see choices such as Something you do or Something you are they immediately get confused and they do not think of them as subset of Biometrics where you have Biometric implementation based on behavior and physilogical attributes. So something you do falls under the Something you are category as a subset.
Something your do would be signing your name or typing text on your keyboard for example.
Strong authentication is simply when you make use of two factors that are within two different categories.
Reference(s) used for this question:
Shon Harris, CISSP All In One, Fifth Edition, pages 158-159

NEW QUESTION 132
- (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 133
- (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 134
- (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 136
- (Topic 1)
Which of the following access control models requires defining classification for objects?

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

Answer: D

Explanation:
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and classification of objects.
The Following answers were incorrect:
Identity-based Access Control is a type of Discretionary Access Control (DAC), they are synonymous.
Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC or RBAC) are types of Non Discretionary Access Control (NDAC).
Tip:
When you have two answers that are synonymous they are not the right choice for sure.
There is only one access control model that makes use of Label, Clearances, and Categories, it is Mandatory Access Control, none of the other one makes use of those items.
Reference(s) used for this question:
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 140
- (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 143
- (Topic 1)
Which of the following is NOT part of the Kerberos authentication protocol?

A. Symmetric key cryptography
B. Authentication service (AS)
C. Principals
D. Public Key

Answer: D

Explanation:
There is no such component within kerberos environment. Kerberos uses only symmetric encryption and does not make use of any public key component.
The other answers are incorrect because :
Symmetric key cryptography is a part of Kerberos as the KDC holds all the users' and
services' secret keys.
Authentication service (AS) : KDC (Key Distribution Center) provides an authentication service
Principals : Key Distribution Center provides services to principals , which can be users , applications or network services.
References: Shon Harris , AIO v3 , Chapter - 4: Access Control , Pages : 152-155.

NEW QUESTION 144
- (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 145
- (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 148
- (Topic 1)
What is called the percentage of valid subjects that are falsely rejected by a Biometric Authentication system?

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

Answer: A

Explanation:
The percentage of valid subjects that are falsely rejected is called the False Rejection Rate (FRR) or Type I Error.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION 149
- (Topic 1)
Access Control techniques do not include which of the following?

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

Answer: D

Explanation:
Access Control Techniques Discretionary Access Control
Mandatory Access Control Lattice Based Access Control Rule-Based Access Control Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

NEW QUESTION 150
- (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 152
- (Topic 1)
The throughput rate is the rate at which individuals, once enrolled, can be processed and
identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:

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

Answer: C

Explanation:
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system.
Acceptable throughput rates are in the range of 10 subjects per minute.
Things that may impact the throughput rate for some types of biometric systems may include:
A concern with retina scanning systems may be the exchange of body fluids on the eyepiece.
Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION 157
- (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 159
- (Topic 1)
Which of the following is the LEAST user accepted biometric device?

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

Answer: C

Explanation:
The biometric device that is least user accepted is the retina scan, where a system scans the blood-vessel pattern on the backside of the eyeball. When using this device, an individual has to place their eye up to a device, and may require a puff of air to be blown into the eye. The iris scan only needs for an individual to glance at a camera that could be placed above a door.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 4: Access Control (page 131).

NEW QUESTION 161
- (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 162
- (Topic 1)
Which of the following access control models introduces user security clearance and data classification?

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

Answer: D

Explanation:
The mandatory access control model is based on a security label system. Users are given a security clearance and data is classified. The classification is stored in the security labels of the resources. Classification labels specify the level of trust a user must have to access a certain file.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 4: Access Control (Page 154).

NEW QUESTION 163
- (Topic 1)
Which of the following models does NOT include data integrity or conflict of interest?

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

Answer: C

Explanation:
Bell LaPadula model (Bell 1975): The granularity of objects and subjects is not predefined, but the model prescribes simple access rights. Based on simple access restrictions the Bell LaPadula model enforces a discretionary access control policy enhanced with mandatory rules. Applications with rigid confidentiality requirements and without strong integrity requirements may properly be modeled.
These simple rights combined with the mandatory rules of the policy considerably restrict the spectrum of applications which can be appropriately modeled.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
Also check:
Proceedings of the IFIP TC11 12th International Conference on Information Security, Samos (Greece), May 1996, On Security Models.

NEW QUESTION 167
- (Topic 1)
Which of the following is most appropriate to notify an internal user that session monitoring is being conducted?

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

Answer: D

Explanation:
This is a tricky question, the keyword in the question is Internal users.
There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous/external users.
Internal users should always have a written agreement first, then logon banners serve as a constant reminder.
Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system, who is authorized and unauthorized, and if it is an unauthorized user then he is fully aware of trespassing. Anonymous/External users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 50.
and
Shon Harris, CISSP All-in-one, 5th edition, pg 873

NEW QUESTION 168
- (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 173
- (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 174
- (Topic 1)
Which one of the following factors is NOT one on which Authentication is based?

A. Type 1. Something you know, such as a PIN or password
B. Type 2. Something you have, such as an ATM card or smart card
C. Type 3. Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan
D. Type 4. Something you are, such as a system administrator or security administrator

Answer: D

Explanation:
Authentication is based on the following three factor types:
Type 1. Something you know, such as a PIN or password
Type 2. Something you have, such as an ATM card or smart card

Type 3. Something you are (Unique physical characteristic), such as a fingerprint or retina scan
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 132-133).

NEW QUESTION 175
- (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 180
- (Topic 1)
In Synchronous dynamic password tokens:

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

Answer: A

Explanation:
Synchronous dynamic password tokens:
- The token generates a new password value at fixed time intervals (this password could be the time of day encrypted with a secret key).
- the unique password is entered into a system or workstation along with an owner's PIN.
- The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid time window.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION 183
- (Topic 1)
Which of the following does not apply to system-generated passwords?

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

Answer: C

Explanation:
Users tend to choose easier to remember passwords. System-generated
passwords can provide stronger, harder to guess passwords. Since they are based on rules provided by the administrator, they can include combinations of uppercase/lowercase letters, numbers and special characters, making them less vulnerable to brute force and dictionary attacks. One danger is that they are also harder to remember for users, who will tend to write them down, making them more vulnerable to anyone having access to the user's desk. Another danger with system-generated passwords is that if the password- generating algorithm gets to be known, the entire system is in jeopardy.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 64).

NEW QUESTION 186
- (Topic 1)
What is the Biba security model concerned with?

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

Answer: D

Explanation:
The Biba security model addresses the integrity of data being threatened when subjects at lower security levels are able to write to objects at higher security levels and when subjects can read data at lower levels.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (Page 244).

NEW QUESTION 191
- (Topic 1)
Which of the following statements pertaining to the Bell-LaPadula is TRUE if you are NOT making use of the strong star property?

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

Answer: D

Explanation:
Bell–LaPadula Confidentiality Model10 The Bell–LaPadula model is perhaps the most well-known and significant security model, in addition to being one of the oldest models used in the creation of modern secure computing systems. Like the Trusted Computer System Evaluation Criteria (or TCSEC), it was inspired by early U.S. Department of Defense security policies and the need to prove that confidentiality could be maintained. In other words, its primary goal is to prevent disclosure as the model system moves from one state (one point in time) to another.
When the strong star property is not being used it means that both the property and the
Simple Security Property rules would be applied.
The Star (*) property rule of the Bell-LaPadula model says that subjects cannot write down, this would compromise the confidentiality of the information if someone at the secret layer would write the object down to a confidential container for example.
The Simple Security Property rule states that the subject cannot read up which means that a subject at the secret layer would not be able to access objects at Top Secret for example.
You must remember: The model tells you about are NOT allowed to do. Anything else would be allowed. For example within the Bell LaPadula model you would be allowed to write up as it does not compromise the security of the information. In fact it would upgrade it to the point that you could lock yourself out of your own information if you have only a secret security clearance.
The following are incorrect answers because they are all FALSE:
"It allows read up" is incorrect. The "simple security" property forbids read up.
"It addresses covert channels" is incorrect. Covert channels are not addressed by the Bell- LaPadula model.
"It addresses management of access controls" is incorrect. Management of access controls are beyond the scope of the Bell-LaPadula model.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17595-17600). Auerbach Publications. Kindle Edition.

NEW QUESTION 196
- (Topic 1)
Which of the following logical access exposures INVOLVES CHANGING data before, or as it is entered into the computer?

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

Answer: A

Explanation:
It involves changing data before , or as it is entered into the computer or in
other words , it refers to the alteration of the existing data. The other answers are incorrect because :
Salami techniques : A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed.
Trojan horses: A Trojan Horse is a program that is disguised as another program. Viruses:A Virus is a small application , or a string of code , that infects applications.
Reference: Shon Harris , AIO v3
Chapter - 11: Application and System Development, Page : 875-880 Chapter - 10: Law, Investigation and Ethics , Page : 758-759

NEW QUESTION 201
- (Topic 1)
Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

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

Answer: B

Explanation:
Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

NEW QUESTION 204
- (Topic 1)
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

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

Answer: A

Explanation:
The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.
Management monitoring of audit logs is a detective control and it would not prevent collusion.
Changing passwords regularly would not prevent such attack.
This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 205
- (Topic 1)
The Computer Security Policy Model the Orange Book is based on is which of the following?

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

Answer: A

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

NEW QUESTION 208
......