

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)

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 3

- (Topic 1)

What is the main concern with single sign-on?

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

Answer: A

Explanation:

A major concern with Single Sign-On (SSO) is that if a user's ID and password are compromised, the intruder would have access to all the systems that the user was authorized for.

The following answers are incorrect:

The security administrator's workload would increase. Is incorrect because the security administrator's workload would decrease and not increase. The admin would not be responsible for maintaining multiple user accounts just the one.

The users' password would be too hard to remember. Is incorrect because the users would have less passwords to remember.

User access rights would be increased. Is incorrect because the user access rights would not be any different than if they had to log into systems manually.

NEW QUESTION 4

- (Topic 1)

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

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

Answer: C

Explanation:

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

Reference(s) used for this question:

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

NEW QUESTION 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 than a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.

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

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

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

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

SESAME is an authentication and access control protocol, that also supports communication confidentiality and integrity. It provides public key based authentication along with the Kerberos style authentication, that uses symmetric key cryptography. Sesame supports the Kerberos protocol and adds some security extensions like public key based authentication and an ECMA-style Privilege Attribute Service. The complete Sesame protocol is a two step process. In the first step, the client successfully authenticates itself to the Authentication Server and obtains a ticket that can be presented to the Privilege Attribute Server. In

the second step, the initiator obtains proof of his access rights in the form of Privilege Attributes Certificate (PAC). The PAC is a specific form of Access Control Certificate as defined in the ECMA-219 document. This document describes the extensions to Kerberos for public key based authentication as adopted in Sesame. SESAME, KryptoKnight, and NetSP never took off and the protocols are no longer commonly used.

References:

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

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 8

- (Topic 1)

In which of the following model are Subjects and Objects identified and the permissions applied to each subject/object combination are specified. Such a model can be used to quickly summarize what permissions a subject has for various system objects.

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

Answer: A

Explanation:

An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. Matrices are data structures that programmers implement as table lookups that will be used and enforced by the operating system.

This type of access control is usually an attribute of DAC models. The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs). Capability Table

A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.

Access control lists (ACLs)

ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access a specific object, and they define what level of authorization is granted. Authorization can be specific to an individual, group, or role. ACLs map values from the access control matrix to the object.

Whereas a capability corresponds to a row in the access control matrix, the ACL corresponds to a column of the matrix.

NOTE: Ensure you are familiar with the terms Capability and ACLs for the purpose of the exam.

Resource(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5264-5267). McGraw-Hill. Kindle Edition.

or

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Page 229 and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1923-1925). Auerbach Publications. Kindle Edition.

NEW QUESTION 9

- (Topic 1)

What does the (star) property mean in the Bell-LaPadula model?

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

Answer: C

Explanation:

The (star) property of the Bell-LaPadula access control model states that writing of information by a subject at a higher level of sensitivity to an object at a lower level of sensitivity is not permitted (no write down).

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

Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (page 242, 243).

NEW QUESTION 10

- (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)

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

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

Answer: C

Explanation:

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

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

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

IT IS NOT ALWAYS BLACK OR WHITE

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

BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:

MAC = Mandatory Access Control

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

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

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

MAC also introduce the concept of labels. Every objects will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle. Even thou a user has a security clearance of Secret it does not mean he would be able to access any Secret

documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belong to one of the categories attached to the object.

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

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

NISTR-7316 Says:

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the “simple security rule,” or “no read up.” Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the “*-property” (pronounced “star property”) or “no write down.” The *- property is required to maintain system security in an automated environment. A variation on this rule called the “strict *-property” requires that information can be written at, but not above, the subject’s clearance level. Multilevel security models such as the Bell-La Padula Confidentiality and Biba Integrity models are used to formally specify this kind of MAC policy.

DAC = Discretionary Access Control

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

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

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

RBAC = Role Based Access Control

RBAC is a form of Non-Discretionary access control.

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

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

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

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

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

NOTE FROM CLEMENT:

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

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

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

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

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

I strongly recommend you read carefully the following document:

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

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

Reference(s) used for this question:

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

and

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

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

NEW QUESTION 13

- (Topic 1)

Which of the following questions is less likely to help in assessing identification and authentication controls?

- A. Is a current list maintained and approved of authorized users and their access?
- B. Are passwords changed at least every ninety days or earlier if needed?
- C. Are inactive user identifications disabled after a specified period of time?
- D. Is there a process for reporting incidents?

Answer: D

Explanation:

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. Reporting incidents is more related to incident response capability (operational control) than to identification and authentication (technical control).

Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-30 to A-32).

NEW QUESTION 14

- (Topic 1)

In biometrics, the "one-to-one" search used to verify claim to an identity made by a person is considered:

- A. Authentication
- B. Identification
- C. Auditing
- D. Authorization

Answer: A

Explanation:

Biometric devices can be use for either IDENTIFICATION or AUTHENTICATION

ONE TO ONE is for AUTHENTICATION

This means that you as a user would provide some biometric credential such as your fingerprint. Then they will compare the template that you have provided with the one stored in the Database. If the two are exactly the same that prove that you are who you pretend to be.

ONE TO MANY is for IDENTIFICATION

A good example of this would be within airport. Many airports today have facial recognition cameras, as you walk through the airport it will take a picture of your

face and then compare the template (your face) with a database full of templates and see if there is a match between your template and the ones stored in the Database. This is for IDENTIFICATION of a person.

Some additional clarification or comments that might be helpful are: Biometrics establish authentication using specific information and comparing results to expected data. It does not perform well for identification purposes such as scanning for a person's face in a moving crowd for example.

Identification methods could include: username, user ID, account number, PIN, certificate, token, smart card, biometric device or badge.

Auditing is a process of logging or tracking what was done after the identity and authentication process is completed.

Authorization is the rights the subject is given and is performed after the identity is established.

Reference OIG (2007) p148, 167

Authentication in biometrics is a "one-to-one" search to verify claim to an identity made by a person.

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 15

- (Topic 1)

Which of the following is NOT a system-sensing wireless proximity card?

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

Answer: A

Explanation:

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

NEW QUESTION 16

- (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)

Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

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

Answer: D

Explanation:

Before a LAN is connected to the Internet, you need to determine what the access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.

The following answers are incorrect:

plan for implementing workstation locking mechanisms. This is incorrect because locking the workstations have no impact on the LAN or Internet access.

plan for protecting the modem pool. This is incorrect because protecting the modem pool has no impact on the LAN or Internet access, it just protects the modem.

plan for providing the user with his account usage information. This is incorrect because the question asks what should be done first. While important your primary concern should be focused on security.

NEW QUESTION 25

- (Topic 1)

Which access control model provides upper and lower bounds of access capabilities for a subject?

- A. Role-based access control
- B. Lattice-based access control
- C. Biba access control
- D. Content-dependent access control

Answer: B

Explanation:

In the lattice model, users are assigned security clearances and the data is classified. Access decisions are made based on the clearance of the user and the classification of the object. Lattice-based access control is an essential ingredient of formal security models such as Bell-LaPadula, Biba, Chinese Wall, etc.

The bounds concept comes from the formal definition of a lattice as a "partially ordered set for which every pair of elements has a greatest lower bound and a least

upper bound." To see the application, consider a file classified as "SECRET" and a user Joe with a security clearance of "TOP SECRET." Under Bell-LaPadula, Joe's "least upper bound" access to the file is "READ" and his least lower bound is "NO WRITE" (star property).
Role-based access control is incorrect. Under RBAC, the access is controlled by the permissions assigned to a role and the specific role assigned to the user.
Biba access control is incorrect. The Biba integrity model is based on a lattice structure but the context of the question disqualifies it as the best answer.
Content-dependent access control is incorrect. In content dependent access control, the actual content of the information determines access as enforced by the arbiter.
References:
CBK, pp. 324-325.
AIO3, pp. 291-293. See particularly Figure 5-19 on p. 293 for an illustration of bounds in action.

NEW QUESTION 30

- (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 right 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 database, 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 35

- (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 36

- (Topic 1)

Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?

- A. Discretionary Access Control
- B. Mandatory Access Control
- C. Sensitive Access Control
- D. Role-based Access Control

Answer: A

Explanation:

Data owners decide who has access to resources based only on the identity of the person accessing the resource.

The following answers are incorrect :

Mandatory Access Control : users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes and access decisions are based on security labels.

Sensitive Access Control : There is no such access control in the context of the above question.

Role-based Access Control : uses a centrally administered set of controls to determine how subjects and objects interact , also called as non discretionary access control.

In a mandatory access control (MAC) model, users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes. This model is much more structured and strict and is based on a security label system. Users are given a security clearance (secret, top secret, confidential, and so on), and data is classified in the same way. The clearance and classification data is stored in the security labels, which are bound to the specific subjects and objects. When the system makes a decision about fulfilling a request to access an object, it is based on the clearance of the subject, the classification of the object, and the security policy of the system. The rules for how subjects access objects are made by the security officer, configured by the administrator, enforced by the operating system, and supported by security technologies

Reference : Shon Harris , AIO v3 , Chapter-4 : Access Control , Page : 163-165

NEW QUESTION 41

- (Topic 1)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 42

- (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 43

- (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 46

- (Topic 1)

The end result of implementing the principle of least privilege means which of the following?

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

Answer: A

Explanation:

The principle of least privilege refers to allowing users to have only the access they need and not anything more. Thus, certain users may have no need to access any of the files on specific systems.

The following answers are incorrect:

Users can access all systems. Although the principle of least privilege limits what access and systems users have authorization to, not all users would have a need to know to access all of the systems. The best answer is still Users would get access to only the info for which they have a need to know as some of the users may not have a need to access a system.

Users get new privileges when they change positions. Although true that a user may indeed require new privileges, this is not a given fact and in actuality a user may require less privileges for a new position. The principle of least privilege would require that the rights required for the position be closely evaluated and where possible rights revoked.

Authorization creep. Authorization creep occurs when users are given additional rights with new positions and responsibilities. The principle of least privilege should actually prevent authorization creep.

The following reference(s) were/was used to create this question: ISC2 OIG 2007 p.101,123

Shon Harris AIO v3 p148, 902-903

NEW QUESTION 48

- (Topic 1)

RADIUS incorporates which of the following services?

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

Answer: D

Explanation:

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

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

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

These credentials are encrypted

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

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

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

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

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

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

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

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

RADIUS: Key Features and Benefits 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/opencvos/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 52

- (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 53

- (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 54

- (Topic 1)

What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources?

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

Answer: C

Explanation:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION 57

- (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 60

- (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 63

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 65

- (Topic 1)

How would nonrepudiation be best classified as?

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

Answer: A

Explanation:

Systems accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Because the mechanisms implemented in nonrepudiation prevent the ability to successfully repudiate an action, it can be considered as a preventive control.
Source: STONEBURNER, Gary, NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology, December 2001, page 7.

NEW QUESTION 69

- (Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 72

- (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 76

- (Topic 1)

Which of the following questions is less likely to help in assessing physical access controls?

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

Answer: B

Explanation:

Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical access controls except for the one regarding operating system configuration, which is a logical access control. Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

NEW QUESTION 80

- (Topic 1)

What is the primary role of smartcards in a PKI?

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

Answer: D

Explanation:

Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 139; SNYDER, J., What is a SMART CARD?. Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance_Security Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures. Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip. It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including: physical attack of various forms (microprobing, drills, files, solvents, etc.) freezing the device applying out-of-spec voltages or power surges applying unusual clock signals inducing software errors using radiation measuring the precise time and power requirements of certain operations (see power analysis) Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of- specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled. Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

NEW QUESTION 82

- (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 84

- (Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 85

- (Topic 1)

Which of the following is true about Kerberos?

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

Answer: C

Explanation:

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

NEW QUESTION 90

- (Topic 1)

What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?

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

Answer: C

Explanation:

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

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

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.
and <https://en.wikipedia.org/wiki/Biometrics>

NEW QUESTION 92

- (Topic 1)

Which of the following is not a two-factor authentication mechanism?

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

Answer: D

Explanation:

Something you know and a password fits within only one of the three ways authentication could be done. A password is an example of something you know, thereby something you know and a password does not constitute a two-factor authentication as both are in the same category of factors.

A two-factor (strong) authentication relies on two different kinds of authentication factors out of a list of three possible choice:

something you know (e.g. a PIN or password),

something you have (e.g. a smart card, token, magnetic card),

something you are is mostly Biometrics (e.g. a fingerprint) or something you do (e.g. signature dynamics).

TIP FROM CLEMENT:

On the real exam you can expect to see synonyms and sometimes sub-categories under the main categories. People are familiar with Pin, Passphrase, Password as subset of Something you know.

However, when people see choices such as Something you do or Something you are they immediately get confused and they do not think of them as subset of Biometrics where you have Biometric implementation based on behavior and physiological attributes. So something you do falls under the Something you are category as a subset.

Something your do would be signing your name or typing text on your keyboard for example.

Strong authentication is simply when you make use of two factors that are within two different categories.

Reference(s) used for this question:

Shon Harris, CISSP All In One, Fifth Edition, pages 158-159

NEW QUESTION 95

- (Topic 1)

Kerberos can prevent which one of the following attacks?

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

Answer: B

Explanation:

Each ticket in Kerberos has a timestamp and are subject to time expiration to

help prevent these types of attacks. The following answers are incorrect:

tunneling attack. This is incorrect because a tunneling attack is an attempt to bypass security and access low-level systems. Kerberos cannot totally prevent these types of attacks.

destructive attack. This is incorrect because depending on the type of destructive attack, Kerberos cannot prevent someone from physically destroying a server.

process attack. This is incorrect because with Kerberos cannot prevent an authorized individuals from running processes.

NEW QUESTION 100

- (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 105

- (Topic 1)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 109

- (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 113

- (Topic 1)

Which of the following is NOT a compensating measure for access violations?

- A. Backups
- B. Business continuity planning
- C. Insurance
- D. Security awareness

Answer: D

Explanation:

Security awareness is a preventive measure, not a compensating measure for access violations.

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 50).

NEW QUESTION 116

- (Topic 1)

Which of the following statements pertaining to Kerberos is TRUE?

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

Answer: A

Explanation:

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

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

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 42).

NEW QUESTION 121

- (Topic 1)

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

- A. Type I error
- B. Type II error
- C. Type III error
- D. Crossover error

Answer: B

Explanation:

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

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

Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual's behavior, as in signature dynamics, but these can change over time and possibly be forged. Biometric systems that base authentication decisions on physical attributes (iris, retina, fingerprint) provide more accuracy, because physical attributes typically don't change much, absent some disfiguring injury, and are harder to impersonate.

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

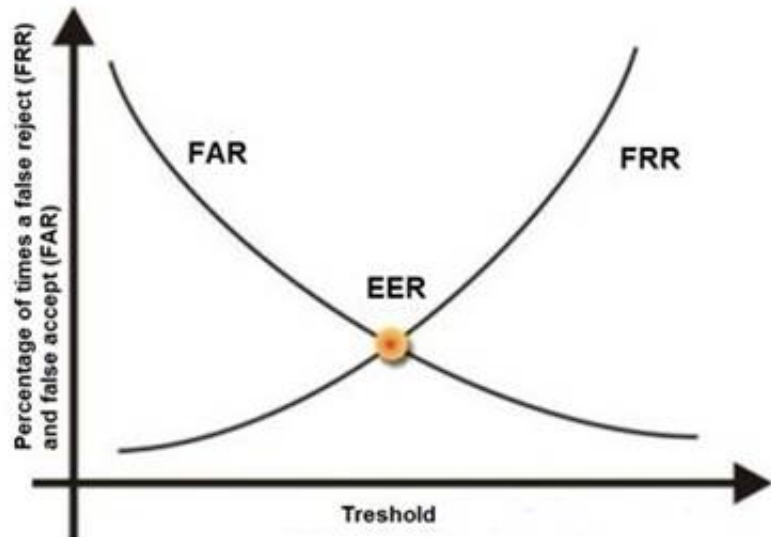
When the system accepts impostors who should be rejected, it is called a Type II error (False Acceptance Rate (FAR) or False Accept Rate (FAR)). Type II errors are the most dangerous and thus the most important to avoid.

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

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

The relationship between FRR (Type I) and FAR (Type II) is depicted in the graphic below . As one rate increases, the other decreases. The Cross-over Error Rate (CER) is sometimes considered a good indicator of the overall accuracy of a biometric system. This is the point at which the FRR and the FAR have the same value. Solutions with a lower CER are typically more accurate.

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



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

The other answers are incorrect:

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

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

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

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

and

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

and

Tech Republic, Reduce Multi_Factor Authentication Cost

NEW QUESTION 126

- (Topic 1)

Which of the following is true of two-factor authentication?

- A. It uses the RSA public-key signature based on integers with large prime factors.
- B. It requires two measurements of hand geometry.
- C. It does not use single sign-on technology.
- D. It relies on two independent proofs of identity.

Answer: D

Explanation:

The Answer It relies on two independent proofs of identity. Two-factor authentication refers to using two independent proofs of identity, such as something the user has (e.g. a token card) and something the user knows (a password). Two-factor authentication may be used with single sign-on.

The following answers are incorrect: It requires two measurements of hand geometry. Measuring hand geometry twice does not yield two independent proofs.

It uses the RSA public-key signature based on integers with large prime factors. RSA encryption uses integers with exactly two prime factors, but the term "two-factor authentication" is not used in that context.

It does not use single sign-on technology. This is a detractor. The following reference(s) were/was used to create this question:

Shon Harris AIO v.3 p.129

ISC2 OIG, 2007 p. 126

NEW QUESTION 130

- (Topic 1)

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

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

Answer: C

Explanation:

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

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

The Bell-LaPadula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. In this formal model, the entities in an information system are divided into subjects and objects.

The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby

inductively proving that the system satisfies the security objectives of the model. The Bell–LaPadula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.

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

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

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

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

The following are incorrect answers:

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

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

References: CBK, pp. 325-326
AIO3, pp. 279 - 284
AIOv4 Security Architecture and Design (pages 333 - 336) AIOv5 Security Architecture and Design (pages 336 - 338)
Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

NEW QUESTION 134

- (Topic 1)

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

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

Answer: C

Explanation:

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

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

Reference:

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

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

NEW QUESTION 136

- (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 140

- (Topic 1)

Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

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

Answer: B

Explanation:

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

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

NEW QUESTION 141

- (Topic 1)

What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to

both the local police/fire station and the appropriate headquarters?

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

Answer: D

Explanation:

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

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

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

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

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

Reference(s) used for this question:

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

and

Great presentation J.T.A. Stone on SlideShare

NEW QUESTION 142

- (Topic 1)

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

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

Answer: D

Explanation:

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

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

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

A UserId only provides for identification.

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

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

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

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

As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information.

Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.

NOTE FROM CLEMENT:

This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well.

I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.

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

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

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

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

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

Something you have (Type 2)

Something you are (Type 3)

Reference(s) used for this question:

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

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

NEW QUESTION 143

- (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 148

- (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 153

- (Topic 1)

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

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

Answer: B

Explanation:

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

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

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

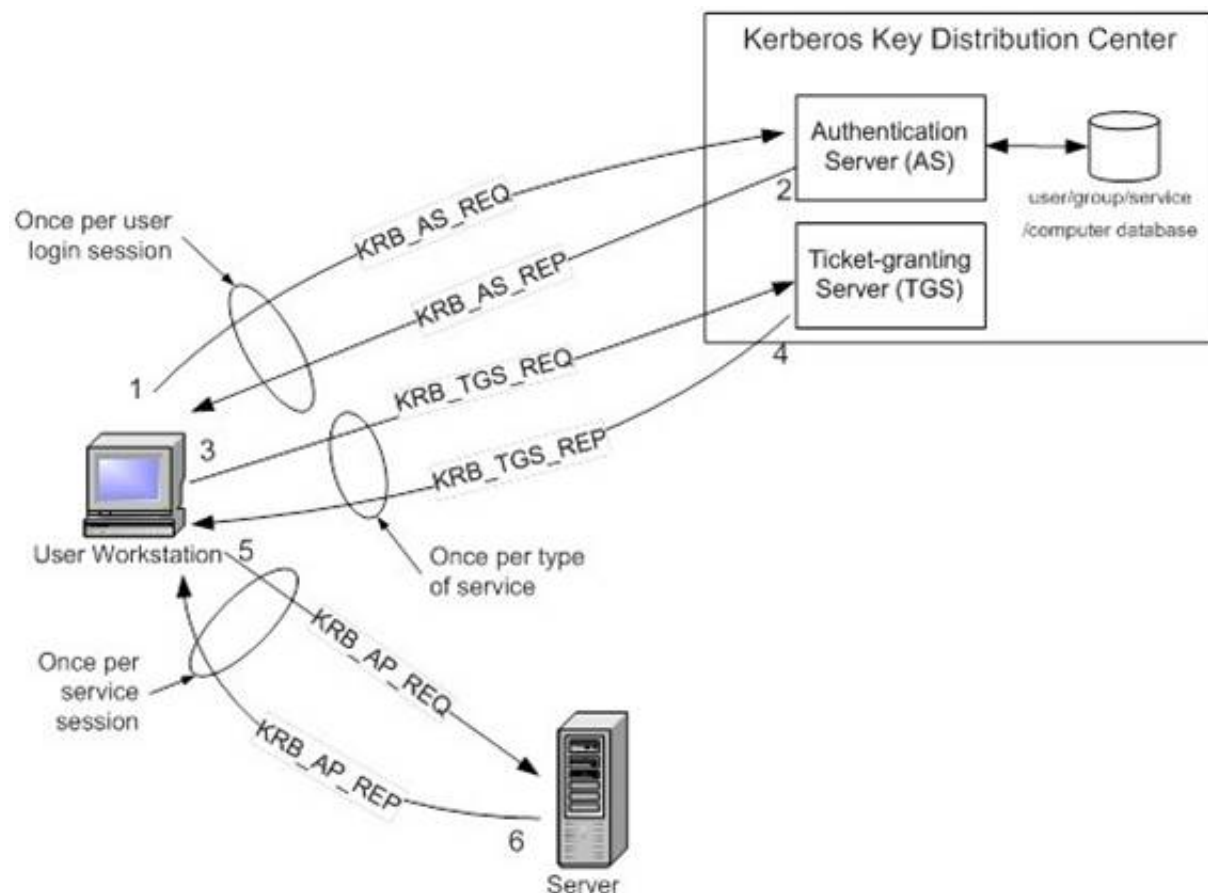
The concept depends on a trusted third party – a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.

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

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

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

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



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

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

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

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

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

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

– one encrypted with the client password, and one encrypted by the service password.

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

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

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

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

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

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

References:

Introduction to Kerberos Authentication from Intel
and

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

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

NEW QUESTION 157

- (Topic 1)

What is Kerberos?

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

Answer: B

Explanation:

Is correct because that is exactly what Kerberos is. The following answers are incorrect:

A three-headed dog from Egyptian mythology. Is incorrect because we are dealing with Information Security and not the Egyptian mythology but the Greek Mythology.

A security model. Is incorrect because Kerberos is an authentication protocol and not just a security model.

A remote authentication dial in user server. Is incorrect because Kerberos is not a remote authentication dial in user server that would be called RADIUS.

NEW QUESTION 160

- (Topic 1)

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

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

Answer: B

Explanation:

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

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

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

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

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

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

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

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

and

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

NEW QUESTION 163

- (Topic 1)

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

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

Answer: A

Explanation:

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

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

The other answers are not correct because:

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

Reference:

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

All in One Third Edition page: 136 - 137

NEW QUESTION 166

- (Topic 1)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 168

- (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 173

- (Topic 1)

Which of the following best ensures accountability of users for the actions taken within a system or domain?

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

Answer: B

Explanation:

Details:

The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be. After showing proper credentials, a user is authorized access to resources.

References:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

NEW QUESTION 174

- (Topic 1)

What kind of certificate is used to validate a user identity?

- A. Public key certificate
- B. Attribute certificate
- C. Root certificate
- D. Code signing certificate

Answer: A

Explanation:

In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. The permission can be delegated.

Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process.

A real life example of this can be found in the mobile software deployments by large service providers and are typically applied to platforms such as Microsoft Smartphone (and related), Symbian OS, J2ME, and others.

In each of these systems a mobile communications service provider may customize the mobile terminal client distribution (ie. the mobile phone operating system or application environment) to include one or more root certificates each associated with a set of capabilities or permissions such as "update firmware", "access address book", "use radio interface", and the most basic one, "install and execute". When a developer wishes to enable distribution and execution in one of these controlled environments they must acquire a certificate from an appropriate CA, typically a large commercial CA, and in the process they usually have their identity verified using out-of-band mechanisms such as a combination of phone call, validation of their legal entity through government and commercial databases, etc., similar to the high assurance SSL certificate vetting process, though often there are additional specific requirements imposed on would-be developers/publishers. Once the identity has been validated they are issued an identity certificate they can use to sign their software; generally the software signed by the developer or publisher's identity certificate is not distributed but rather it is submitted to processor to possibly test or profile the content before generating an authorization certificate which is unique to the particular software release. That certificate is then used with an ephemeral asymmetric key-pair to sign the software as the last step of preparation for distribution. There are many advantages to separating the identity and authorization certificates especially relating to risk mitigation of new content being accepted into the system and key management as well as recovery from errant software which can be used as attack vectors.

References:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 540.

http://en.wikipedia.org/wiki/Attribute_certificate http://en.wikipedia.org/wiki/Public_key_certificate

NEW QUESTION 179

- (Topic 1)

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

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

Answer: A

Explanation:

Access Control Techniques Discretionary Access Control

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

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

NEW QUESTION 184

- (Topic 1)

There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?

- A. public keys
- B. private keys
- C. public-key certificates
- D. private-key certificates

Answer: C

Explanation:

A Kerberos ticket is issued by a trusted third party. It is an encrypted data structure that includes the service encryption key. In that sense it is similar to a public-key certificate. However, the ticket is not the key.

The following answers are incorrect:

public keys. Kerberos tickets are not shared out publicly, so they are not like a PKI public key.

private keys. Although a Kerberos ticket is not shared publicly, it is not a private key. Private keys are associated with Asymmetric crypto system which is not used by Kerberos. Kerberos uses only the Symmetric crypto system.

private key certificates. This is a detractor. There is no such thing as a private key certificate.

NEW QUESTION 187

- (Topic 1)

Which access control model is also called Non Discretionary Access Control (NDAC)?

- A. Lattice based access control
- B. Mandatory access control
- C. Role-based access control
- D. Label-based access control

Answer: C

Explanation:

RBAC is sometimes also called non-discretionary access control (NDAC) (as Ferraiolo says "to distinguish it from the policy-based specifics of MAC"). Another model that fits within the NDAC category is Rule-Based Access Control (RuBAC or RBAC). Most of the CISSP books use the same acronym for both models but NIST tend to use a lowercase "u" in between R and B to differentiate the two models.

You can certainly mimic MAC using RBAC but true MAC makes use of Labels which contains the sensitivity of the objects and the categories they belong to. No labels means MAC is not being used.

One of the most fundamental data access control decisions an organization must make is the amount of control it will give system and data owners to specify the level of access users of that data will have. In every organization there is a balancing point between the access controls enforced by organization and system policy and the ability for information owners to determine who can have access based on specific business requirements. The process of translating that balance into a workable access control model can be defined by three general access frameworks:

Discretionary access control Mandatory access control Nondiscretionary access control

A role-based access control (RBAC) model bases the access control authorizations on the roles (or functions) that the user is assigned within an organization. The determination of what roles have access to a resource can be governed by the owner of the data, as with DACs, or applied based on policy, as with MACs.

Access control decisions are based on job function, previously defined and governed by policy, and each role (job function) will have its own access capabilities.

Objects associated with a role will inherit privileges assigned to that role. This is also true for groups of users, allowing administrators to simplify access control strategies by assigning users to groups and groups to roles.

There are several approaches to RBAC. As with many system controls, there are variations on how they can be applied within a computer system.

There are four basic RBAC architectures:

* 1. Non-RBAC: Non-RBAC is simply a user-granted access to data or an application by traditional mapping, such as with ACLs. There are no formal "roles" associated with the mappings, other than any identified by the particular user.

* 2. Limited RBAC: Limited RBAC is achieved when users are mapped to roles within a single application rather than through an organization-wide role structure.

Users in a limited RBAC system are also able to access non-RBAC-based applications or data. For example, a user may be assigned to multiple roles within several applications and, in addition, have direct access to another application or system independent of his or her assigned role. The key attribute of limited RBAC is that the role for that user is defined within an application and not necessarily based on the user's organizational job function.

* 3. Hybrid RBAC: Hybrid RBAC introduces the use of a role that is applied to multiple applications or systems based on a user's specific role within the organization. That role is then applied to applications or systems that subscribe to the organization's role-based model. However, as the term "hybrid" suggests, there are instances where the subject may also be assigned to roles defined solely within specific applications, complimenting (or, perhaps, contradicting) the larger, more encompassing organizational role used by other systems.

* 4. Full RBAC: Full RBAC systems are controlled by roles defined by the organization's policy and access control infrastructure and then applied to applications and systems across the enterprise. The applications, systems, and associated data apply permissions based on that enterprise definition, and not one defined by a specific application or system. Be careful not to try to make MAC and DAC opposites of each other -- they are two different access control strategies with RBAC being a third strategy that was defined later to address some of the limitations of MAC and DAC.

The other answers are not correct because:

Mandatory access control is incorrect because though it is by definition not discretionary, it is not called "non-discretionary access control." MAC makes use of label to indicate the sensitivity of the object and it also makes use of categories to implement the need to know.

Label-based access control is incorrect because this is not a name for a type of access control but simply a bogus detractor.

Lattice based access control is not adequate either. A lattice is a series of levels and a subject will be granted an upper and lower bound within the series of levels. These levels could be sensitivity levels or they could be confidentiality levels or they could be integrity levels.

Reference(s) used for this question: All in One, third edition, page 165.

Ferraiolo, D., Kuhn, D. & Chandramouli, R. (2003). Role-Based Access Control, p. 18.

Ferraiolo, D., Kuhn, D. (1992). Role-Based Access Controls. http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 1557-1584). Auerbach Publications. Kindle Edition.

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 1474-1477). Auerbach Publications. Kindle Edition.

NEW QUESTION 190

- (Topic 1)

Which access control model would a lattice-based access control model be an example of?

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

Answer: A

Explanation:

In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.

TIPS FROM CLEMENT

Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.

Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it: FIRST: The Lattice

A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.

SECOND: DAC (Discretionary Access Control)

Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.

THIRD: MAC (Mandatory Access Control)

All of the following are forms of Mandatory Access Control: Mandatory Access control (MAC) (Implemented using the lattice)

You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity level and the categories the object belongs to. The categories are used to implement the Need to Know.

All of the following are forms of Non Discretionary Access Control:

Role Based Access Control (RBAC)

Rule Based Access Control (Think Firewall in this case)

The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.

I hope this clarifies the whole drama related to what is what in the world of access control. In the same line of taught, you should be familiar with the difference between Explicit

permission (the user has his own profile) versus Implicit (the user inherit permissions by being a member of a role for example).

The following answers are incorrect:

Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the users. It is identity based access control only. It does not make use of a lattice.

Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC.

Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.

References:

AI0v3 Access Control (pages 161 - 168)

AI0v3 Security Models and Architecture (pages 291 - 293)

NEW QUESTION 191

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

SSCP Practice Exam Features:

- * SSCP Questions and Answers Updated Frequently
- * SSCP Practice Questions Verified by Expert Senior Certified Staff
- * SSCP Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SSCP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SSCP Practice Test Here](#)