



ISC2

Exam Questions SSCP

System Security Certified Practitioner (SSCP)

NEW QUESTION 1

- (Topic 1)

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

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

Answer: A

Explanation:

An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.

DAC is good for low level security environment. The owner of the file decides who has access to the file.

If a user creates a file, he is the owner of that file. An identifier for this user is placed in the file header and/or in an access control matrix within the operating system.

Ownership might also be granted to a specific individual. For example, a manager for a certain department might be made the owner of the files and resources within her department. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources.

This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers, are the owners of the data within their specific department. Being the owner, they can specify who should have access and who should not.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 220). McGraw- Hill . Kindle Edition.

NEW QUESTION 2

- (Topic 1)

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

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

Answer: B

Explanation:

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

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

also see:

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

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

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

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

Answer: D

Explanation:

Unauthorized access of restricted network services by the circumvention of security access controls is known as logon abuse. This type of abuse refers to users who may be internal to the network but access resources they would not normally be allowed. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep

Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3:
Telecommunications and Network Security (page 74).

NEW QUESTION 5

- (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 6

- (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 7

- (Topic 1)

Which of the following is NOT a type of motion detector?

- A. Photoelectric sensor
- B. Passive infrared sensors
- C. Microwave Sensor.
- D. Ultrasonic Sensor.

Answer: A

Explanation:

A photoelectric sensor does not "directly" sense motion there is a narrow beam that won't set off the sensor unless the beam is broken. Photoelectric sensors, along with dry contact switches, are a type of perimeter intrusion detector.

All of the other answers are valid types of motion detectors types.

The content below on the different types of sensors is from Wikipedia: Indoor Sensors

These types of sensors are designed for indoor use. Outdoor use would not be advised due to false alarm vulnerability and weather durability. Passive infrared detectors



C:\Users\MCS\Desktop\1.jpg Passive Infrared Sensor

The passive infrared detector (PIR) is one of the most common detectors found in household and small business environments because it offers affordable and reliable functionality. The term passive means the detector is able to function without the need to generate and radiate its own energy (unlike ultrasonic and microwave volumetric intrusion detectors that are "active" in operation). PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or nonpresence, PIRs verify if an intruder or object is actually there. Creating individual zones of detection where each zone comprises one or more layers can achieve differentiation. Between the zones there are areas of no sensitivity (dead zones) that are used by the sensor for comparison.

Ultrasonic detectors

Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event:

There must be motion of an object either towards or away from the receiver.

The motion of the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency.

The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard-surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy.

When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

Microwave detectors

This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monostatic) for indoor applications, and separate housings (bistatic) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dualtec" alarm.

Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder.

Photo-electric beams

Photoelectric beam systems detect the presence of an intruder by transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, it can be avoided. The technology can be an effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a 'sealed' condition whilst an intruder passes through, most systems use and detect a modulated light source.

Glass break detectors

The glass break detector may be used for internal perimeter building protection. When glass breaks it generates sound in a wide band of frequencies. These can range from infrasonic, which is below 20 hertz (Hz) and can not be heard by the human ear, through the audio band from 20 Hz to 20 kHz which humans can hear, right up to ultrasonic, which is above 20 kHz and again cannot be heard. Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass break detectors are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors "feel" these shock frequencies and in turn generate an alarm condition.

The more primitive detection method involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it.

Breaking the glass is practically guaranteed to tear the foil and break the circuit.

Smoke, heat, and carbon monoxide detectors



C:\Users\MCS\Desktop\1.jpg Heat Detection System

Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon monoxide detectors protect from the risk of carbon monoxide. Although an intruder

alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarm system.

Other types of volumetric sensors could be:

Active Infrared

Passive Infrared/Microwave combined Radar

Accoustical Sensor/Audio Vibration Sensor (seismic) Air Turbulence

NEW QUESTION 8

- (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 9

- (Topic 1)

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

A. Mechanisms based on IP addresses

B. Mechanism with reusable passwords

C. one-time password mechanism.

D. challenge response mechanism.

Answer: A

Explanation:

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

NOTE FROM CLEMENT:

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

The following answers are incorrect:

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

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

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

NEW QUESTION 10

- (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 10

- (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 11

- (Topic 1)

Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?

- A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
- B. The initial logon process is cumbersome to discourage potential intruders.
- C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
- D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems

Answer: A

Explanation:

Single Sign-On is a distributed Access Control methodology where an individual only has to authenticate once and would have access to all primary and secondary network domains. The individual would not be required to re-authenticate when they needed additional resources. The security issue that this creates is if a fraudster is able to compromise those credentials they too would have access to all the resources that account has access to. All the other answers are incorrect as they are distractors.

NEW QUESTION 15

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 17

- (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 21

- (Topic 1)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 26

- (Topic 1)

Which TCSEC class specifies discretionary protection?

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

Answer: D

Explanation:

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

NEW QUESTION 30

- (Topic 1)

Guards are appropriate whenever the function required by the security program involves which of the following?

- A. The use of discriminating judgment
- B. The use of physical force
- C. The operation of access control devices
- D. The need to detect unauthorized access

Answer: A

Explanation:

The Answer The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.

The following answers are incorrect:

The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force.

The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc. The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.

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 10: Physical security (page 339).

Source: ISC2 Official Guide to the CBK page 288-289.

NEW QUESTION 34

- (Topic 1)

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

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

Answer: A

Explanation:

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

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

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

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

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

and

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

NEW QUESTION 37

- (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 40

- (Topic 1)

In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on :

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

Answer: B

Explanation:

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

NEW QUESTION 44

- (Topic 1)

The Orange Book is founded upon which security policy model?

- A. The Biba Model
- B. The Bell LaPadula Model
- C. Clark-Wilson Model
- D. TEMPEST

Answer: B

Explanation:

From the glossary of Computer Security Basics:

The Bell-LaPadula model is the security policy model on which the Orange Book requirements are based. From the Orange Book definition, "A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving the system is secure. A system state is defined to be 'secure' if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object and a determination is made as to whether the subject is authorized for the specific access mode."

The Biba Model is an integrity model of computer security policy that describes a set of rules. In this model, a subject may not depend on any object or other subject that is less trusted than itself.

The Clark Wilson Model is an integrity model for computer security policy designed for a commercial environment. It addresses such concepts as nondiscretionary access control, privilege separation, and least privilege. TEMPEST is a government program that prevents the compromising electrical and electromagnetic signals that emanate from computers and related equipment from being intercepted and deciphered.

Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, 1991.

Also: U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

NEW QUESTION 48

- (Topic 1)

This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

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

Answer: C

Explanation:

Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.

The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).

If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred.

Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.

The following answers are incorrect:

All of the other choices presented were simply detractors. The following reference(s) were used for this question:

Handbook of Information Security Management

NEW QUESTION 51

- (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 55

- (Topic 1)

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

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

Answer: B

Explanation:

Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in a biometric authentication system, the system becomes increasingly selective and has a higher False Rejection Rate (FRR).

Conversely, if the sensitivity is decreased, the False Acceptance Rate (FAR) will increase. Thus, to have a valid measure of the system performance, the Cross Over Error (CER) rate is used. The Crossover Error Rate (CER) is the point at which the false rejection rates and the false acceptance rates are equal. The lower the value of the CER, the more accurate the system.

There are three categories of biometric accuracy measurement (all represented as percentages):

False Reject Rate (a Type I Error): When authorized users are falsely rejected as unidentified or unverified.

False Accept Rate (a Type II Error): When unauthorized persons or imposters are falsely accepted as authentic.

Crossover Error Rate (CER): The point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.

NOTE:

Within the ISC2 book they make use of the term Accept or Acceptance and also Reject or Rejection when referring to the type of errors within biometrics. Below we make use of Acceptance and Rejection throughout the text for consistency. However, on the real exam you could see either of the terms.

Performance of biometrics

Different metrics can be used to rate the performance of a biometric factor, solution or application. The most common performance metrics are the False Acceptance Rate FAR and the False Rejection Rate FRR.

When using a biometric application for the first time the user needs to enroll to the system. The system requests fingerprints, a voice recording or another biometric factor from the

operator, this input is registered in the database as a template which is linked internally to a user ID. The next time when the user wants to authenticate or identify himself, the biometric input provided by the user is compared to the template(s) in the database by a matching algorithm which responds with acceptance (match) or rejection (no match).

FAR and FRR

The FAR or False Acceptance rate is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a valid template. The FAR is normally expressed as a percentage, following the FAR definition this is the percentage of invalid inputs which are incorrectly accepted.

The FRR or False Rejection Rate is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input provided by the user with a stored template. The FRR is normally expressed as a percentage, following the FRR definition this is the percentage of valid inputs which are incorrectly rejected.

FAR and FRR are very much dependent on the biometric factor that is used and on the technical implementation of the biometric solution. Furthermore the FRR is strongly person dependent, a personal FRR can be determined for each individual.

Take this into account when determining the FRR of a biometric solution, one person is insufficient to establish an overall FRR for a solution. Also FRR might increase due to environmental conditions or incorrect use, for example when using dirty fingers on a fingerprint reader. Mostly the FRR lowers when a user gains more experience in how to use the biometric device or software.

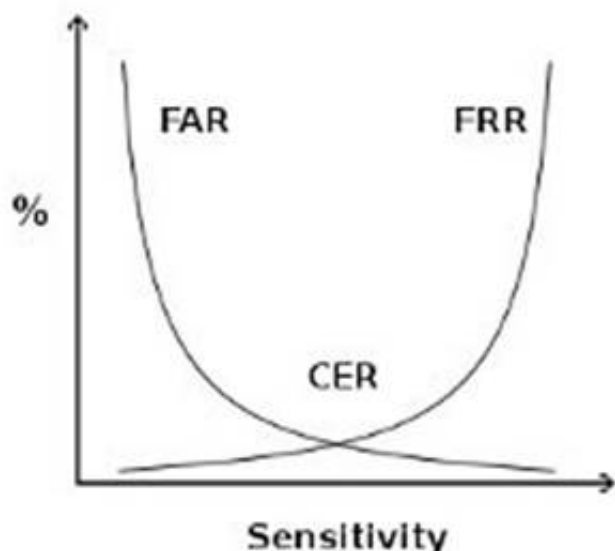
FAR and FRR are key metrics for biometric solutions, some biometric devices or software even allow to tune them so that the system more quickly matches or rejects. Both FRR and FAR are important, but for most applications one of them is considered most important. Two examples to illustrate this:

When biometrics are used for logical or physical access control, the objective of the application is to disallow access to unauthorized individuals under all circumstances. It is clear that a very low FAR is needed for such an application, even if it comes at the price of a higher FRR.

When surveillance cameras are used to screen a crowd of people for missing children, the objective of the application is to identify any missing children that come up on the screen. When the identification of those children is automated using a face recognition software, this software has to be set up with a low FRR. As such a higher number of matches will be false positives, but these can be reviewed quickly by surveillance personnel.

False Acceptance Rate is also called False Match Rate, and False Rejection Rate is sometimes referred to as False Non-Match Rate.

crossover error rate



crossover error rate

Above see a graphical representation of FAR and FRR errors on a graph, indicating the CER

CER

The Crossover Error Rate or CER is illustrated on the graph above. It is the rate where both FAR and FRR are equal.

The matching algorithm in a biometric software or device uses a (configurable) threshold which determines how close to a template the input must be for it to be considered a match. This threshold value is in some cases referred to as sensitivity, it is marked on the X axis of the plot. When you reduce this threshold there will be more false acceptance errors (higher FAR) and less false rejection errors (lower FRR), a higher threshold will lead to lower FAR and higher FRR.

Speed

Most manufacturers of biometric devices and softwares can give clear numbers on the time it takes to enroll as well on the time for an individual to be authenticated or identified using their application. If speed is important then take your time to consider this, 5 seconds might seem a short time on paper or when testing a device but if hundreds of people will use the device multiple times a day the cumulative loss of time might be significant.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 2723-2731). Auerbach Publications. Kindle Edition.

and

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

and

http://www.biometric-solutions.com/index.php?story=performance_biometrics

NEW QUESTION 58

- (Topic 1)

Who first described the DoD multilevel military security policy in abstract, formal terms?

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

Answer: A

Explanation:

It was David Bell and Leonard LaPadula who, in 1973, first described the DoD multilevel military security policy in abstract, formal terms. The Bell-LaPadula is a Mandatory Access Control (MAC) model concerned with confidentiality. Rivest, Shamir and Adleman (RSA) developed the RSA encryption algorithm. Whitfield Diffie and Martin Hellman published the Diffie-Hellman key agreement algorithm in 1976. David Clark and David Wilson developed the Clark-Wilson integrity model, more appropriate for security in commercial activities.

Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (pages 78,109).

NEW QUESTION 63

- (Topic 1)

Which of the following is the WEAKEST authentication mechanism?

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

Answer: B

Explanation:

Most of the time users usually choose passwords which can be guessed , hence passwords is the BEST answer out of the choices listed above.

The following answers are incorrect because :

Passphrases is incorrect as it is more secure than a password because it is longer.

One-time passwords is incorrect as the name states , it is good for only once and cannot be reused.

Token devices is incorrect as this is also a password generator and is an one time password mechanism.

Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 139 , 142.

NEW QUESTION 68

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 73

- (Topic 1)

Which of the following remote access authentication systems is the most robust?

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

Answer: A

Explanation:

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

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 122).

NEW QUESTION 77

- (Topic 1)

Why should batch files and scripts be stored in a protected area?

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

Answer: C

Explanation:

Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.

Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION 82

- (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 87

- (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 91

- (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 94

- (Topic 1)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 96

- (Topic 1)

Which of the following is NOT part of the Kerberos authentication protocol?

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

Answer: D

Explanation:

There is no such component within kerberos environment. Kerberos uses only symmetric encryption and does not make use of any public key component.

The other answers are incorrect because :

Symmetric key cryptography is a part of Kerberos as the KDC holds all the users' and services' secret keys.

Authentication service (AS) : KDC (Key Distribution Center) provides an authentication service

Principals : Key Distribution Center provides services to principals , which can be users , applications or network services.

References: Shon Harris , AIO v3 , Chapter - 4: Access Control , Pages : 152-155.

NEW QUESTION 97

- (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 98

- (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 99

- (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 104

- (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 106

- (Topic 1)

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

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

Answer: B

Explanation:

In Non-Discretionary Access Control, when Role Based Access Control is being used, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization.

Reference(S) used for this question:

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

NEW QUESTION 110

- (Topic 1)

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

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

Answer: C

Explanation:

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

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

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

Also check:

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

NEW QUESTION 115

- (Topic 1)

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

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

Answer: D

Explanation:

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

Reference(s) used for this question:

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

NEW QUESTION 116

- (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 118

- (Topic 1)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 122

- (Topic 1)

Which of the following are additional access control objectives?

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

Answer: B

Explanation:

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

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

NEW QUESTION 127

- (Topic 1)

Which of the following is related to physical security and is not considered a technical control?

- A. Access control Mechanisms
- B. Intrusion Detection Systems
- C. Firewalls
- D. Locks

Answer: D

Explanation:

All of the above are considered technical controls except for locks, which are physical controls.

Administrative, Technical, and Physical Security Controls

Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance,

security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.

Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information. Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.

Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.

From the GIAC.ORG website

NEW QUESTION 132

- (Topic 1)

Which of the following is NOT a factor related to Access Control?

- A. integrity
- B. authenticity
- C. confidentiality
- D. availability

Answer: B

Explanation:

These factors cover the integrity, confidentiality, and availability components of information system security.

Integrity is important in access control as it relates to ensuring only authorized subjects can make changes to objects.

Authenticity is different from authentication. Authenticity pertains to something being authentic, not necessarily having a direct correlation to access control.

Confidentiality is pertinent to access control in that the access to sensitive information is controlled to protect confidentiality.

Availability is protected by access controls in that if an attacker attempts to disrupt availability they would first need access.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION 136

- (Topic 1)

Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

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

Answer: A

Explanation:

B level is the first Mandatory Access Control Level.

First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for

the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.

Reference used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition.

and

THE source for all TCSEC "level" questions: <http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt> (paragraph 3 for this one)

NEW QUESTION 138

- (Topic 1)

What security model is dependent on security labels?

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

Answer: C

Explanation:

With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and the classification or sensitivity of the object. Label-based access control is not defined. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION 143

- (Topic 1)

What is the difference between Access Control Lists (ACLs) and Capability Tables?

- A. Access control lists are related/attached to a subject whereas capability tables are related/attached to an object.
- B. Access control lists are related/attached to an object whereas capability tables are related/attached to a subject.
- C. Capability tables are used for objects whereas access control lists are used for users.
- D. They are basically the same.

Answer: B

Explanation:

Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's possession of a capability (or ticket) for the object. It is a row within the matrix.

To put it another way, 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.

CLEMENT NOTE:

If we wish to express this very simply:

Capabilities are attached to a subject and it describe what access the subject has to each of the objects on the row that matches with the subject within the matrix. It is a row within the matrix.

ACL's are attached to objects, it describe who has access to the object and what type of access they have. It is a column within the matrix.

The following are incorrect answers:

"Access control lists are subject-based whereas capability tables are object-based" is incorrect.

"Capability tables are used for objects whereas access control lists are used for users" is incorrect.

"They are basically the same" is incorrect. References used for this question:

CBK, pp. 191 - 192

AIO3 p. 169

NEW QUESTION 145

- (Topic 1)

Which type of password provides maximum security because a new password is required for each new log-on?

- A. One-time or dynamic password
- B. Cognitive password
- C. Static password
- D. Passphrase

Answer: A

Explanation:

"one-time password" provides maximum security because a new password is required for each new log-on.

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

NEW QUESTION 147

- (Topic 1)

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

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

Answer: D

Explanation:

By reviewing system logs you can detect events that have occurred.

The following answers are incorrect:

avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.

deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.

prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

NEW QUESTION 149

- (Topic 1)

Which of the following is needed for System Accountability?

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

Answer: A

Explanation:

Is a means of being able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.

Accountability is the ability to identify users and to be able to track user actions. The following answers are incorrect:

Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.

Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.

Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.

References:

OIG CBK Glossary (page 778)

NEW QUESTION 154

- (Topic 1)

Which of the following is addressed by Kerberos?

- A. Confidentiality and Integrity
- B. Authentication and Availability
- C. Validation and Integrity
- D. Auditability and Integrity

Answer: A

Explanation:

Kerberos addresses the confidentiality and integrity of information. It also addresses primarily authentication but does not directly address availability.

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 42.

and <https://www.ietf.org/rfc/rfc4120.txt> and

<http://learn-networking.com/network-security/how-kerberos-authentication-works>

NEW QUESTION 157

- (Topic 1)

Which of the following statements pertaining to RADIUS is incorrect:

- A. A RADIUS server can act as a proxy server, forwarding client requests to other authentication domains.
- B. Most of RADIUS clients have a capability to query secondary RADIUS servers for redundancy.
- C. Most RADIUS servers have built-in database connectivity for billing and reporting purposes.
- D. Most RADIUS servers can work with DIAMETER servers.

Answer: D

Explanation:

This is the correct answer because it is FALSE.

Diameter is an AAA protocol, AAA stands for authentication, authorization and accounting protocol for computer networks, and it is a successor to RADIUS.

The name is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius).

The main differences are as follows:

Reliable transport protocols (TCP or SCTP, not UDP)

The IETF is in the process of standardizing TCP Transport for RADIUS Network or transport layer security (IPsec or TLS)

The IETF is in the process of standardizing Transport Layer Security for RADIUS Transition support for RADIUS, although Diameter is not fully compatible with RADIUS Larger address space for attribute-value pairs (AVPs) and identifiers (32 bits instead of 8 bits)

Client-server protocol, with exception of supporting some server-initiated messages as well Both stateful and stateless models can be used

Dynamic discovery of peers (using DNS SRV and NAPTR) Capability negotiation

Supports application layer acknowledgements, defines failover methods and state machines (RFC 3539)

Error notification Better roaming support

More easily extended; new commands and attributes can be defined Aligned on 32-bit boundaries

Basic support for user-sessions and accounting

A Diameter Application is not a software application, but a protocol based on the Diameter base protocol (defined in RFC 3588). Each application is defined by an application identifier and can add new command codes and/or new mandatory AVPs. Adding a new optional AVP does not require a new application.

Examples of Diameter applications:

Diameter Mobile IPv4 Application (MobileIP, RFC 4004)

Diameter Network Access Server Application (NASREQ, RFC 4005) Diameter Extensible Authentication Protocol (EAP) Application (RFC 4072) Diameter Credit-Control Application (DCCA, RFC 4006)

Diameter Session Initiation Protocol Application (RFC 4740) Various applications in the 3GPP IP Multimedia Subsystem

All of the other choices presented are true. So Diameter is backward compatible with Radius (to some extent) but the opposite is false.

Reference(s) used for this question:

TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 38.

and https://secure.wikimedia.org/wikipedia/en/wiki/Diameter_%28protocol%29

NEW QUESTION 161

- (Topic 2)

Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?

- A. Interface errors are detected earlier.
- B. Errors in critical modules are detected earlier.
- C. Confidence in the system is achieved earlier.
- D. Major functions and processing are tested earlier.

Answer: B

Explanation:

The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and work upwards until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices refer to advantages of a top down approach which follows the opposite path.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

NEW QUESTION 162

- (Topic 2)

Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

- A. IS security specialists
- B. Senior Management
- C. Senior security analysts
- D. systems Auditors

Answer: B

Explanation:

If there is no support by senior management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assets. The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program. It is senior management that could face legal repercussions if they do not have sufficient controls in place.

The following answers are incorrect:

IS security specialists. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.

Senior security analysts. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.

systems auditors. Is incorrect because it is not the best answer, system auditors are responsible that the controls in place are effective. Senior management bears the primary responsibility for determining the level of protection needed.

NEW QUESTION 165

- (Topic 2)

Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in a system?

- A. Fail proof
- B. Fail soft
- C. Fail safe
- D. Fail Over

Answer: C

Explanation:

NOTE: This question is referring to a system which is Logical/Technical, so it is in the context of a system that you must choose the right answer. This is very important to read the question carefully and to identify the context whether it is in the Physical world or in the Technical/Logical world.

RFC 2828 (Internet Security Glossary) defines fail safe as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.

A secure state means in the Logical/Technical world that no access would be granted or no packets would be allowed to flow through the system inspecting the packets such as a firewall for example.

If the question would have made reference to a building or something specific to the Physical world then the answer would have been different. In the Physical World everything becomes open and full access would be granted. See the valid choices below for the Physical context.

Fail-safe in the physical security world is when doors are unlocked automatically in case of emergency. Used in environment where humans work around. As human safety is prime concern during Fire or other hazards.

The following were all wrong choices:

Fail-secure in the physical security world is when doors are locked automatically in case of emergency. Can be in an area like Cash Locker Room provided there should be alternative manually operated exit door in case of emergency.

Fail soft is selective termination of affected non-essential system functions and processes when a failure occurs or is detected in the system.

Fail Over is a redundancy mechanism and does not apply to this question.

There is a great post within the CCCure Forums on this specific QUESTION NO: :

saintrockz who is a long term contributor to the forums did outstanding research and you have the results below. The CCCure forum is a gold mine where thousands of QUESTION NO: s related to the CBK have been discussed.

According to the Official ISC2 Study Guide (OIG):

Fault Tolerance is defined as built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults. It means a system can operate in the presence of hardware component failures. A single component failure in a fault-tolerant system will not cause a system interruption because the alternate component will take over the task transparently. As the cost of components continues to drop, and the demand for system availability increases, many non-fault-tolerant systems have redundancy built-in at the subsystem level. As a result, many non-fault-tolerant systems can tolerate hardware faults - consequently, the line between a fault-tolerant system and a non-fault-tolerant system becomes increasingly blurred.

According to Common Criteria:

Fail Secure - Failure with preservation of secure state, which requires that the TSF (TOE security functions) preserve a secure state in the face of the identified failures.

Acc. to The CISSP Prep Guide, Gold Ed.:

Fail over - When one system/application fails, operations will automatically switch to the backup system.

Fail safe - Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system.

Fail secure - The system preserves a secure state during and after identified failures occur. Fail soft - Pertaining to the selective termination of affected non-essential processing when a hardware or software failure is detected in a system.

Acc. to CISSP for Dummies:

Fail closed - A control failure that results all accesses blocked. Fail open - A control failure that results in all accesses permitted.

Failover - A failure mode where, if a hardware or software failure is detected, the system automatically transfers processing to a hot backup component, such as a clustered server. Fail-safe - A failure mode where, if a hardware or software failure is detected, program execution is terminated, and the system is protected from compromise.

Fail-soft (or resilient) - A failure mode where, if a hardware or software failure is detected, certain, noncritical processing is terminated, and the computer or network continues to function in a degraded mode.

Fault-tolerant - A system that continues to operate following failure of a computer or network component.

It's good to differentiate this concept in Physical Security as well: Fail-safe

- Door defaults to being unlocked
- Dictated by fire codes

Fail-secure

- Door defaults to being locked

Reference(s) used for this question:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 170

- (Topic 2)

Ensuring least privilege does not require:

- A. Identifying what the user's job is.
- B. Ensuring that the user alone does not have sufficient rights to subvert an important process.
- C. Determining the minimum set of privileges required for a user to perform their duties.
- D. Restricting the user to required privileges and nothing more.

Answer: B

Explanation:

Ensuring that the user alone does not have sufficient rights to subvert an important process is a concern of the separation of duties principle and it does not concern the least privilege principle.

Source: DUPUIS, Clément, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 33).

NEW QUESTION 175

- (Topic 2)

Which of the following is NOT a proper component of Media Viability Controls?

- A. Storage
- B. Writing

C. Handling
D. Marking

Answer: B

Explanation:

Media Viability Controls include marking, handling and storage.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 231.

NEW QUESTION 178

- (Topic 2)

Step-by-step instructions used to satisfy control requirements is called a:

A. policy
B. standard
C. guideline
D. procedure

Answer: D

Explanation:

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

NEW QUESTION 182

- (Topic 2)

Which of the following is an advantage of prototyping?

A. Prototype systems can provide significant time and cost savings.
B. Change control is often less complicated with prototype systems.
C. It ensures that functions or extras are not added to the intended system.
D. Strong internal controls are easier to implement.

Answer: A

Explanation:

Prototype systems can provide significant time and cost savings, however they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added to the system that were not originally intended.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 306).

NEW QUESTION 186

- (Topic 2)

Which of the following security mode of operation does NOT require all users to have the clearance for all information processed on the system?

A. Compartmented security mode
B. Multilevel security mode
C. System-high security mode
D. Dedicated security mode

Answer: B

Explanation:

The multilevel security mode permits two or more classification levels of information to be processed at the same time when all the users do not have the clearance of formal approval to access all the information being processed by the system.

In dedicated security mode, all users have the clearance or authorization and need-to-know to all data processed within the system.

In system-high security mode, all users have a security clearance or authorization to access the information but not necessarily a need-to-know for all the information processed on the system (only some of the data).

In compartmented security mode, all users have the clearance to access all the information processed by the system, but might not have the need-to-know and formal access approval.

Generally, Security modes refer to information systems security modes of operations used in mandatory access control (MAC) systems. Often, these systems contain information at various levels of security classification.

The mode of operation is determined by:

The type of users who will be directly or indirectly accessing the system.

The type of data, including classification levels, compartments, and categories, that are processed on the system.

The type of levels of users, their need to know, and formal access approvals that the users will have.

Dedicated security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system. Proper clearance for ALL information on the system.

Formal access approval for ALL information on the system. A valid need to know for ALL information on the system.

All users can access ALL data. System high security mode

In this mode of operation, all users must have: Signed NDA for ALL information on the system.

Proper clearance for ALL information on the system.

Formal access approval for ALL information on the system. A valid need to know for SOME information on the system.

All users can access SOME data, based on their need to know. Compartmented security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system. Proper clearance for ALL information on the system.

Formal access approval for SOME information they will access on the system. A valid need to know for SOME information on the system.

All users can access SOME data, based on their need to know and formal access approval.

Multilevel security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system. Proper clearance for SOME information on the system.
Formal access approval for SOME information on the system. A valid need to know for SOME information on the system.
All users can access SOME data, based on their need to know, clearance and formal access approval. REFERENCES:
WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 6).
and http://en.wikipedia.org/wiki/Security_Modes

NEW QUESTION 187

- (Topic 2)

What can be defined as: It confirms that users' needs have been met by the supplied solution ?

- A. Accreditation
- B. Certification
- C. Assurance
- D. Acceptance

Answer: D

Explanation:

Acceptance confirms that users' needs have been met by the supplied solution. Verification and Validation informs Acceptance by establishing the evidence – set against acceptance criteria - to determine if the solution meets the users' needs. Acceptance should also explicitly address any integration or interoperability requirements involving other equipment or systems. To enable acceptance every user and system requirement must have a 'testable' characteristic. Accreditation is the formal acceptance of security, adequacy, authorization for operation and acceptance of existing risk. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Certification is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended. The certification is a Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Assurance is the descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Targets (ST) and Protection Profiles (PP), respectively.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 4, August 1999.

and

Official ISC2 Guide to the CISSP CBK, Second Edition, on page 211. and

<http://www.aof.mod.uk/aofcontent/tactical/randa/content/randaintroduction.htm>

NEW QUESTION 189

- (Topic 2)

What prevents a process from accessing another process' data?

- A. Memory segmentation
- B. Process isolation
- C. The reference monitor
- D. Data hiding

Answer: B

Explanation:

Process isolation is where each process has its own distinct address space for its application code and data. In this way, it is possible to prevent each process from accessing another process' data. This prevents data leakage, or modification to the data while it is in memory. Memory segmentation is a virtual memory management mechanism. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. Data hiding, also known as information hiding, is a mechanism that makes information available at one processing level is not available at another level.

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

NEW QUESTION 191

- (Topic 2)

One of the following assertions is NOT a characteristic of Internet Protocol Security (IPsec)

- A. Data cannot be read by unauthorized parties
- B. The identity of all IPsec endpoints are confirmed by other endpoints
- C. Data is delivered in the exact order in which it is sent
- D. The number of packets being exchanged can be counted.

Answer: C

Explanation:

IPSec provide replay protection that ensures data is not delivered multiple times, however IPsec does not ensure that data is delivered in the exact order in which it is sent. IPSEC uses TCP and packets may be delivered out of order to the receiving side depending which route was taken by the packet.

Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:

Confidentiality. IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.

Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

Peer Authentication. Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

Replay Protection. The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is

delivered in the exact order in which it is sent.

Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.

Access Control. IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.

The following are incorrect answers because they are all features provided by IPSEC:

"Data cannot be read by unauthorized parties" is wrong because IPsec provides confidentiality through the usage of the Encapsulating Security Protocol (ESP), once encrypted the data cannot be read by unauthorized parties because they have access only to the ciphertext. This is accomplished by encrypting data using a cryptographic algorithm and a session key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has a copy of the session key.

"The identity of all IPsec endpoints are confirmed by other endpoints" is wrong because IPsec provides peer authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

"The number of packets being exchanged can be counted" is wrong because although IPsec provides traffic protection where a person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged, the number of packets being exchanged still can be counted.

Reference(s) used for this question:

NIST 800-77 Guide to IPsec VPNs . Pages 2-3 to 2-4

NEW QUESTION 195

- (Topic 2)

What would BEST define a covert channel?

- A. An undocumented backdoor that has been left by a programmer in an operating system
- B. An open system port that should be closed.
- C. A communication channel that allows transfer of information in a manner that violates the system's security policy.
- D. A trojan horse.

Answer: C

Explanation:

The Answer A communication channel that allows transfer of information in a manner that violates the system's security policy.

A covert channel is a way for an entity to receive information in an unauthorized manner. It

is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way.

Receiving information in this manner clearly violates the system's security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:

- Oversight in the development of the product
- Improper implementation of access controls
- Existence of a shared resource between the two entities
- Installation of a Trojan horse

The following answers are incorrect:

An undocumented backdoor that has been left by a programmer in an operating system is incorrect because it is not a means by which unauthorized transfer of information takes place. Such backdoor is usually referred to as a Maintenance Hook.

An open system port that should be closed is incorrect as it does not define a covert channel.

A trojan horse is incorrect because it is a program that looks like a useful program but when you install it it would include a bonus such as a Worm, Backdoor, or some other malware without the installer knowing about it.

Reference(s) used for this question:

Shon Harris AIO v3 , Chapter-5 : Security Models & Architecture AIOv4 Security Architecture and Design (pages 343 - 344) AIOv5 Security Architecture and Design (pages 345 - 346)

NEW QUESTION 199

- (Topic 2)

What is the main issue with media reuse?

- A. Degaussing
- B. Data remanence
- C. Media destruction
- D. Purging

Answer: B

Explanation:

The main issue with media reuse is data remanence, where residual information still resides on a media that has been erased. Degaussing, purging and destruction are ways to handle media that contains data that is no longer needed or used. Source: WALLHOFF, John, CBK#10 Physical Security (CISSP Study Guide), April 2002 (page 5).

NEW QUESTION 201

- (Topic 2)

What can best be defined as the sum of protection mechanisms inside the computer, including hardware, firmware and software?

- A. Trusted system
- B. Security kernel
- C. Trusted computing base
- D. Security perimeter

Answer: C

Explanation:

The Trusted Computing Base (TCB) is defined as the total combination of protection mechanisms within a computer system. The TCB includes hardware, software, and firmware. These are part of the TCB because the system is sure that these components will enforce the security policy and not violate it.

The security kernel is made up of hardware, software, and firmware components at fall within the TCB and implements and enforces the reference monitor

concept.
Reference:
AIOv4 Security Models and Architecture pgs 268, 273

NEW QUESTION 203

- (Topic 2)

When backing up an applications system's data, which of the following is a key question to be answered first?

- A. When to make backups
- B. Where to keep backups
- C. What records to backup
- D. How to store backups

Answer: C

Explanation:

It is critical that a determination be made of WHAT data is important and should be retained and protected. Without determining the data to be backed up, the potential for error increases. A record or file could be vital and yet not included in a backup routine. Alternatively, temporary or insignificant files could be included in a backup routine unnecessarily.

The following answers were incorrect:

When to make backups Although it is important to consider schedules for backups, this is done after the decisions are made of what should be included in the backup routine.

Where to keep backups The location of storing backup copies of data (Such as tapes, on- line backups, etc) should be made after determining what should be included in the backup routine and the method to store the backup.

How to store backups The backup methodology should be considered after determining what data should be included in the backup routine.

NEW QUESTION 204

- (Topic 2)

A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?

- A. project initiation and planning phase
- B. system design specification phase
- C. development & documentation phase
- D. acceptance phase

Answer: D

Explanation:

The Answer: "acceptance phase". Note the question asks about an

"evaluation report" - which details how the system evaluated, and an "accreditation statement" which describes the level the system is allowed to operate at.

Because those two activities are a part of testing and testing is a part of the acceptance phase, the only answer above that can be correct is "acceptance phase".

The other answers are not correct because:

The "project initiation and planning phase" is just the idea phase. Nothing has been developed yet to be evaluated, tested, accredited, etc.

The "system design specification phase" is essentially where the initiation and planning phase is fleshed out. For example, in the initiation and planning phase, we might decide we want the system to have authentication. In the design specification phase, we decide that that authentication will be accomplished via username/password. But there is still nothing actually developed at this point to evaluate or accredit.

The "development & documentation phase" is where the system is created and documented. Part of the documentation includes specific evaluation and accreditation criteria. That is the criteria that will be used to evaluate and accredit the system during the "acceptance phase".

In other words - you cannot evaluate or accredit a system that has not been created yet. Of the four answers listed, only the acceptance phase is dealing with an existing system. The others deal with planning and creating the system, but the actual system isn't there yet.

Reference:

Official ISC2 Guide Page: 558 - 559

All in One Third Edition page: 832 - 833 (recommended reading)

NEW QUESTION 208

- (Topic 2)

Which of the following addresses a portion of the primary memory by specifying the actual address of the memory location?

- A. direct addressing
- B. Indirect addressing
- C. implied addressing
- D. indexed addressing

Answer: A

Explanation:

Absolute/Direct

```
+-----+-----+-----+-----+
| load | reg | address |
+-----+-----+-----+-----+
```

(Effective address = address as given in instruction)

This requires space in an instruction for quite a large address. It is often available on CISC machines which have variable-length instructions, such as x86.

Some RISC machines have a special Load Upper Literal instruction which places a 16-bit constant in the top half of a register. An OR literal instruction can be used to insert a 16-bit constant in the lower half of that register, so that a full 32-bit address can then be used via the register-indirect addressing mode, which itself is provided as "base-plus-offset" with an offset of 0.

http://en.wikipedia.org/wiki/Addressing_mode (Very good coverage of the subject)

also see:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 186.

also see: <http://www.comsci.us/ic/notes/am.html>

NEW QUESTION 212

- (Topic 2)

What mechanism does a system use to compare the security labels of a subject and an object?

- A. Validation Module.
- B. Reference Monitor.
- C. Clearance Check.
- D. Security Module.

Answer: B

Explanation:

Because the Reference Monitor is responsible for access control to the objects by the subjects it compares the security labels of a subject and an object. According to the OIG: The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects based on information in an access control database. The reference monitor must mediate all access, be protected from modification, be verifiable as correct, and must always be invoked. The reference monitor, in accordance with the security policy, controls the checks that are made in the access control database.

The following are incorrect:

Validation Module. A Validation Module is typically found in application source code and is used to validate data being inputted.

Clearance Check. Is a distractor, there is no such thing other than what someone would do when checking if someone is authorized to access a secure facility.

Security Module. Is typically a general purpose module that performs a variety of security related functions.

References:

OIG CBK, Security Architecture and Design (page 324)

AIO, 4th Edition, Security Architecture and Design, pp 328-328. Wikipedia - http://en.wikipedia.org/wiki/Reference_monitor

NEW QUESTION 214

- (Topic 2)

Which of the following statements pertaining to software testing approaches is correct?

- A. A bottom-up approach allows interface errors to be detected earlier.
- B. A top-down approach allows errors in critical modules to be detected earlier.
- C. The test plan and results should be retained as part of the system's permanent documentation.
- D. Black box testing is predicated on a close examination of procedural detail.

Answer: C

Explanation:

A bottom-up approach to testing begins testing of atomic units, such as programs or modules, and works upwards until a complete system testing has taken place. It allows errors in critical modules to be found early. A top-down approach allows for early detection of interface errors and raises confidence in the system, as programmers and users actually see a working system. White box testing is predicated on a close examination of procedural detail. Black box testing examines some aspect of the system with little regard for the internal logical structure of the software.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

Top Down Testing: An approach to integration testing where the component at the top of the component hierarchy is tested first, with lower level components being simulated by stubs. Tested components are then used to test lower level components. The process is repeated until the lowest level components have been tested.

Bottom Up Testing: An approach to integration testing where the lowest level components are tested first, then used to facilitate the testing of higher level components. The process is repeated until the component at the top of the hierarchy is tested.

Black Box Testing: Testing based on an analysis of the specification of a piece of software without reference to its internal workings. The goal is to test how well the component conforms to the published requirements for the component.

NEW QUESTION 217

- (Topic 2)

What is called a system that is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it?

- A. A fail safe system
- B. A fail soft system
- C. A fault-tolerant system
- D. A failover system

Answer: C

Explanation:

A fault-tolerant system is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it. In a fail-safe system, program execution is terminated, and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a fail-soft system, when a hardware or software failure occurs and is detected, selected, non-critical processing is terminated. The term failover refers to switching to a duplicate "hot" backup component in real-time when a hardware or software failure occurs, enabling processing to continue.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 196).

NEW QUESTION 218

- (Topic 2)

Which of the following would MOST likely ensure that a system development project meets business objectives?

- A. Development and tests are run by different individuals
- B. User involvement in system specification and acceptance
- C. Development of a project plan identifying all development activities
- D. Strict deadlines and budgets

Answer: B

Explanation:

Effective user involvement is the most critical factor in ensuring that the application meets business objectives.

A great way of getting early input from the user community is by using Prototyping. The prototyping method was formally introduced in the early 1980s to combat the perceived weaknesses of the waterfall model with regard to the speed of development. The objective is to build a simplified version (prototype) of the application, release it for review, and use the feedback from the users' review to build a second, better version.

This is repeated until the users are satisfied with the product. It is a four-step process: initial concept,

design and implement initial prototype,

refine prototype until acceptable, and complete and release final version.

There is also the Modified Prototype Model (MPM). This is a form of prototyping that is ideal for Web application development. It allows for the basic functionality of a desired system or component to be formally deployed in a quick time frame. The maintenance phase is set to begin after the deployment. The goal is to have the process be flexible enough so the application is not based on the state of the organization at any given time. As the organization grows and the environment changes, the application evolves with it, rather than being frozen in time.

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 12101-12108 and 12099-12101). Auerbach Publications. Kindle Edition.

and

Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 296).

NEW QUESTION 221

- (Topic 2)

What is the difference between Advisory and Regulatory security policies?

- A. there is no difference between them
- B. regulatory policies are high level policy, while advisory policies are very detailed
- C. Advisory policies are not mandate
- D. Regulatory policies must be implemented.
- E. Advisory policies are mandated while Regulatory policies are not

Answer: C

Explanation:

Advisory policies are security policies that are not mandated to be followed but are strongly suggested, perhaps with serious consequences defined for failure to follow them (such as termination, a job action warning, and so forth). A company with such policies wants most employees to consider these policies mandatory. Most policies fall under this broad category.

Advisory policies can have many exclusions or application levels. Thus, these policies can control some employees more than others, according to their roles and responsibilities within that organization. For example, a policy that

requires a certain procedure for transaction processing might allow for an alternative procedure under certain, specified conditions.

Regulatory

Regulatory policies are security policies that an organization must implement due to compliance, regulation, or other legal requirements. These companies might be financial institutions, public utilities, or some other type of organization that operates in the public interest. These policies are usually very detailed and are specific to the industry in which the organization operates.

Regulatory policies commonly have two main purposes:

- * 1. To ensure that an organization is following the standard procedures or base practices of operation in its specific industry
- * 2. To give an organization the confidence that it is following the standard and accepted industry policy

Informative

Informative policies are policies that exist simply to inform the reader. There are no implied or specified requirements, and the audience for this information could be certain internal (within the organization) or external parties. This does not mean that the policies are authorized for public consumption but that they are general enough to be distributed to external parties (vendors accessing an extranet, for example) without a loss of confidentiality.

References:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 12, Chapter 1: Security Management Practices.

also see:

The CISSP Prep Guide: Mastering the Ten Domains of Computer Security by Ronald L.

Krutz, Russell Dean Vines, Edward M. Stroz

also see:

<http://i-data-recovery.com/information-security/information-security-policies-standards-guidelines-and-procedures>

NEW QUESTION 223

- (Topic 2)

What is RAD?

- A. A development methodology
- B. A project management technique
- C. A measure of system complexity
- D. Risk-assessment diagramming

Answer: A

Explanation:

RAD stands for Rapid Application Development.

RAD is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.

RAD is a programming system that enables programmers to quickly build working programs.

In general, RAD systems provide a number of tools to help build graphical user interfaces that would normally take a large development effort.

Two of the most popular RAD systems for Windows are Visual Basic and Delphi. Historically, RAD systems have tended to emphasize reducing development time, sometimes at the expense of generating in-efficient executable code. Nowadays, though, many RAD systems produce extremely faster code that is optimized.

Conversely, many traditional programming environments now come with a number of visual tools to aid development. Therefore, the line between RAD systems and other development environments has become blurred.

Reference:

Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 307)

<http://www.webopedia.com>

NEW QUESTION 224

- (Topic 2)

Which expert system operating mode allows determining if a given hypothesis is valid?

- A. Blackboard
- B. Lateral chaining
- C. Forward chaining
- D. Backward chaining

Answer: D

Explanation:

Backward-chaining mode - the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs.

Incorrect answers are:

In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs.

Blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual blackboard, wherein information or potential solutions are placed on the blackboard by a plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated.

Lateral-chaining mode - No such expert system mode. Sources:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 259).

KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Expert Systems (page 354).

NEW QUESTION 225

- (Topic 2)

Which of the following choices describe a condition when RAM and Secondary storage are used together?

- A. Primary storage
- B. Secondary storage
- C. Virtual storage
- D. Real storage

Answer: C

Explanation:

Virtual storage a service provided by the operating system where it uses a combination of RAM and disk storage to simulate a much larger address space than is actually present. Infrequently used portions of memory are paged out by being written to secondary storage and paged back in when required by a running program.

Most OS's have the ability to simulate having more main memory than is physically available in the system. This is done by storing part of the data on secondary storage, such as a disk. This can be considered a virtual page. If the data requested by the system is not currently in main memory, a page fault is taken. This condition triggers the OS handler. If the virtual address is a valid one, the OS will locate the physical page, put the right information in that page, update the translation table, and then try the request again. Some other page might be swapped out to make room. Each process may have its own separate virtual address space along with its own mappings and protections.

The following are incorrect answers:

Primary storage is incorrect. Primary storage refers to the combination of RAM, cache and the processor registers. Primary Storage The data waits for processing by the processors, it sits in a staging area called primary storage. Whether implemented as memory, cache, or registers (part of the CPU), and regardless of its location, primary storage stores data that has a high probability of being requested by the CPU, so it is usually faster than long-term, secondary storage. The location where data is stored is denoted by its physical memory address. This memory register identifier remains constant and is independent of the value stored there. Some examples of primary storage devices include random-access memory (RAM), synchronous dynamic random-access memory (SDRAM), and read-only memory (ROM). RAM is volatile, that is, when the system shuts down, it flushes the data in RAM although recent research has shown that data may still be retrievable. Contrast this

Secondary storage is incorrect. Secondary storage holds data not currently being used by the CPU and is used when data must be stored for an extended period of time using high- capacity, nonvolatile storage. Secondary storage includes disk, floppies, CD's, tape, etc. While secondary storage includes basically anything different from primary storage, virtual memory's use of secondary storage is usually confined to high-speed disk storage.

Real storage is incorrect. Real storage is another word for primary storage and distinguishes physical memory from virtual memory.

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 17164-17171). Auerbach Publications. Kindle Edition.

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17196-17201). Auerbach Publications. Kindle Edition.

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17186-17187). Auerbach Publications. Kindle Edition.

NEW QUESTION 226

- (Topic 2)

Who is responsible for initiating corrective measures and capabilities used when there are security violations?

- A. Information systems auditor
- B. Security administrator
- C. Management
- D. Data owners

Answer: C

Explanation:

Management is responsible for protecting all assets that are directly or indirectly under their control. They must ensure that employees understand their obligations to protect the company's assets, and implement security in accordance with the company policy. Finally, management is responsible for initiating corrective actions when there are security violations.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

NEW QUESTION 229

- (Topic 2)

What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?

- A. The reference monitor
- B. Protection rings
- C. A security kernel
- D. A protection domain

Answer: C

Explanation:

A security kernel is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. A reference monitor is a system component that enforces access controls on an object. A protection domain consists of the execution and memory space assigned to each process. The use of protection rings is a scheme that supports multiple protection domains.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 194).

NEW QUESTION 234

- (Topic 2)

Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?

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

Answer: A

Explanation:

Confidentiality is the prevention of the intentional or unintentional unauthorized disclosure of contents.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

NEW QUESTION 239

.....

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](#)