

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : **SSCP**

Title : System Security Certified
Practitioner (SSCP)

Version : DEMO

1.A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:

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

Answer: D

Explanation: Because the optical unit utilizes a camera and infrared light to create the images, sun light can impact the aperture so it must not be positioned in direct light of any type. Because the subject does not need to have direct contact with the optical reader, direct light can impact the reader. An Iris recognition is a form of biometrics that is based on the uniqueness of a subject's iris. A camera like device records the patterns of the iris creating what is known as Iriscode. It is the unique patterns of the iris that allow it to be one of the most accurate forms of biometric identification of an individual. Unlike other types of biometrics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resolution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject's identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.

Reference(s) used for this question: AIO, 3rd edition, Access Control, p 134. AIO, 4th edition, Access Control, p 182. Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition

The following answers are incorrect:

concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue. the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the question would have been about long term problems then it could have been the best choice.

Recent research has shown that Irises actually do change over time:

<http://www.nature.com/news/ageing-eyes-hinder-biometric-scans-1.10722>

there is a relatively high rate of false accepts. Since the advent of the Iriscode there is a very low rate of false accepts, in fact the algorithm used has never had a false match. This all depends on the quality of the equipment used but because of the uniqueness of the iris even when comparing identical twins, iris patterns are unique.

2.In Mandatory Access Control, sensitivity labels attached to object contain what information?

- A. The item's classification
- B. The item's classification and category set
- C. The item's category
- D. The items's need to know

Answer: B

Explanation: A Sensitivity label must contain at least one classification and one category set. Category set and Compartment set are synonyms, they mean the same thing. The sensitivity label must contain at

least one Classification and at least one Category. It is common in some environments for a single item to belong to multiple categories. The list of all the categories to which an item belongs is called a compartment set or category set.

The following answers are incorrect:

the item's classification. Is incorrect because you need a category set as well. the item's category. Is incorrect because category set and classification would be both be required. The item's need to know. Is incorrect because there is no such thing. The need to know is indicated by the categories the object belongs to. This is NOT the best answer.

Reference(s) used for this question: OIG CBK, Access Control (pages 186 - 188) AIO, 3rd Edition, Access Control (pages 162 - 163) AIO, 4th Edition, Access Control, pp 212-214.

Wikipedia - http://en.wikipedia.org/wiki/Mandatory_Access_Control

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

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

Answer: D

Explanation: Both are the components of a sensitivity label.

The following are incorrect:

A Classification Set and a single Compartment. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classification and it is not a "single compartment" but a Compartment Set.

A single classification and a single compartment. Is incorrect because while there only is one classification, it is not a "single compartment" but a Compartment Set.

A Classification Set and user credentials. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classification and it is not "user credential" but a Compartment Set. The user would have their own sensitivity label.

4.What does it mean to say that sensitivity labels are "incomparable"?

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

Answer: D

Explanation: If a category does not exist then you cannot compare it. Incomparable is when you have two disjointed sensitivity labels, that is a category in one of the labels is not in the other label. "Because neither label contains all the categories of the other, the labels can't be compared.

They're said to be incomparable"

COMPARABILITY: The label:

TOP SECRET [VENUS ALPHA]

is "higher" than either of the labels:

SECRET [VENUS ALPHA] TOP SECRET [VENUS] But you can't really say that the label:

TOP SECRET [VENUS] is higher than the label:

SECRET [ALPHA] Because neither label contains all the categories of the other, the labels can't be

compared. They're said to be incomparable. In a mandatory access control system, you won't be allowed access to a file whose label is incomparable to your clearance.

The Multilevel Security policy uses an ordering relationship between labels known as the dominance relationship. Intuitively, we think of a label that dominates another as being "higher" than the other. Similarly, we think of a label that is dominated by another as being "lower" than the other. The dominance relationship is used to determine permitted operations and information flows.

DOMINANCE The dominance relationship is determined by the ordering of the Sensitivity/Clearance component of the label and the intersection of the set of Compartments.

Sample Sensitivity/Clearance ordering are:

Top Secret > Secret > Confidential > Unclassified $s_3 > s_2 > s_1 > s_0$

Formally, for label one to dominate label 2 both of the following must be true:

The sensitivity/clearance of label one must be greater than or equal to the sensitivity/clearance of label two. The intersection of the compartments of label one and label two must equal the compartments of label two.

Additionally: Two labels are said to be equal if their sensitivity/clearance and set of compartments are exactly equal. Note that dominance includes equality. One label is said to strictly dominate the other if it dominates the other but is not equal to the other. Two labels are said to be incomparable if each label has at least one compartment that is not included in the other's set of compartments.

The dominance relationship will produce a partial ordering over all possible MLS labels, resulting in what is known as the MLS Security Lattice.

The following answers are incorrect:

The number of classification in the two labels is different. Is incorrect because the categories are what is being compared, not the classifications.

Neither label contains all the classifications of the other. Is incorrect because the categories are what is being compared, not the classifications.

the number of categories in the two labels is different. Is incorrect because it is possible a category exists more than once in one sensitivity label and does exist in the other so they would be comparable.

Reference(s) used for this question:

O'Reilly - Computer Systems and Access Control (Chapter 3)

<http://www.oreilly.com/catalog/csb/chapter/ch03.html> and http://rubix.com/cms/mls_dom

5. Which of the following is true about Kerberos?

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

Answer: C

Explanation: Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.

The following answers are incorrect: It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers).

It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because

the passwords are not exchanged but used for encryption and decryption of the keys.

It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.

References:

MIT <http://web.mit.edu/kerberos/> Wikipedi http://en.wikipedia.org/wiki/Kerberos_%28protocol%29

OIG CBK Access Control (pages 181 - 184) AIOv3 Access Control (pages 151 - 155)

6.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)

7.What is Kerberos?

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

Answer: B

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

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

8.The three classic ways of authenticating yourself to the computer security software are by something you know, by something you have, and by something:

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

Answer: C

Explanation: This is more commonly known as biometrics and is one of the most accurate ways to authenticate an individual.

The rest of the answers are incorrect because they not one of the three recognized forms for Authentication.

9.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.

10.A confidential number used as an authentication factor to verify a user's identity is called a:

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

Answer: A

Explanation: PIN Stands for Personal Identification Number, as the name states it is a combination of numbers.

The following answers are incorrect: User ID This is incorrect because a Userid is not required to be a number and a Userid is only used to establish identity not verify it.

Password. This is incorrect because a password is not required to be a number, it could be any combination of characters.

Challenge. This is incorrect because a challenge is not defined as a number, it could be anything.

11.Which of the following exemplifies proper separation of duties?

- A. Operators are not permitted modify the system time.
- B. Programmers are permitted to use the system console.
- C. Console operators are permitted to mount tapes and disks.
- D. Tape operators are permitted to use the system console.

Answer: A

Explanation: This is an example of Separation of Duties because operators are prevented from modifying the system time which could lead to fraud. Tasks of this nature should be performed by they

system administrators.

AIO defines Separation of Duties as a security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.

The following answers are incorrect: Programmers are permitted to use the system console. Is incorrect because programmers should not be permitted to use the system console, this task should be performed by operators. Allowing programmers access to the system console could allow fraud to occur so this is not an example of Separation of Duties..

Console operators are permitted to mount tapes and disks. Is incorrect because operators should be able to mount tapes and disks so this is not an example of Separation of Duties.

Tape operators are permitted to use the system console. Is incorrect because operators should be able to use the system console so this is not an example of Separation of Duties.

References: OIG CBK Access Control (page 98 - 101) AIOv3 Access Control (page 182)

12.Which of the following is not a logical control when implementing logical access security?

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

Answer: C

Explanation: Employee badges are considered Physical so would not be a logical control.

The following answers are incorrect:

userids. Is incorrect because userids are a type of logical control. access profiles. Is incorrect because access profiles are a type of logical control. passwords. Is incorrect because passwords are a type of logical control.

13.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.

14. 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.

15. Which of the following would assist the most in Host Based intrusion detection?

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

Answer: A

Explanation: To assist in Intrusion Detection you would review audit logs for access violations.

The following answers are incorrect:

access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.

security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.

host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not detect intrusions.

16. Controls to keep password sniffing attacks from compromising computer systems include which of the following?

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

Answer: C

Explanation: To minimize the chance of passwords being captured one-time passwords would prevent a password sniffing attack because once used it is no longer valid. Encryption will also minimize these types of attacks.

The following answers are correct:

static and recurring passwords. This is incorrect because if there is no encryption then someone password sniffing would be able to capture the password much easier if it never changed.

encryption and recurring passwords. This is incorrect because while encryption helps, recurring passwords do nothing to minimize the risk of passwords being captured.

static and one-time passwords. This is incorrect because while one-time passwords will prevent these types of attacks, static passwords do nothing to minimize the risk of passwords being captured.

17.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.

18.In discretionary access environments, which of the following entities is authorized to grant information access to other people?

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

Answer: D

Explanation: In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.

The following answers are incorrect:

manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

IMPORTANT NOTE: The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data.

The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

19. 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.

20. 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.