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

Correct Answer: B Explanation:

The Clark-Wilson model addresses integrity. It incorporates mechanisms to enforce internal and external consistency, a separation of duty, and a mandatory integrity policy. Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten

Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

QUESTION 161

In the context of Biometric authentication, what is a quick way to compare the accuracy of devices. In general, the device that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

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

Correct Answer: A

Explanation:

equal error rate or crossover error rate (EER or CER): the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

In the context of Biometric Authentication almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher False Reject Rate (FRR).

Conversely, if the sensitivity is decreased, the False Acceptance Rate (FAR) will increase. Thus, to have a valid measure of the system performance, the CrossOver Error Rate (CER) is used.

The following are used as performance metrics for biometric systems:

false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value.

false reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

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

Download Full Version SSCP Exam Dumps(Updated in Feb/2023)

failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

template capacity: the maximum number of sets of data which can be stored in the system.

Reference(s) used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37. Wikipedia at: https://en.wikipedia.org/wiki/Biometrics

QUESTION 162

An alternative to using passwords for authentication in logical or technical access control is:

- A. manage without passwords
- B. biometrics
- C. not there
- D. use of them for physical access control

Correct Answer: B

Explanation:

An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism-something you are. Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

QUESTION 163

What is the most critical characteristic of a biometric identifying system?

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

Correct Answer: C

Explanation:

Accuracy is the most critical characteristic of a biometric identifying verification system.

Accuracy is measured in terms of false rejection rate (FRR, or type I errors) and false acceptance rate (FAR or type II errors).

The Crossover Error Rate (CER) is the point at which the FRR equals the FAR and has become the most important measure of biometric system accuracy.

Source: TIPTON, Harold F.& KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 9).

QUESTION 164

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

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

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html D. Public Key

Correct 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.

QUESTION 165

Which of the following would be used to implement Mandatory Access Control (MAC)?

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

Correct Answer: C **Explanation:**

The lattice is a mechanism use to implement Mandatory Access Control (MAC)

Under Mandatory Access Control (MAC) you have: Mandatory Access Control

Under Non Discretionary Access Control (NDAC) you have: Rule-Based Access Control Role-Based Access Control

Under Discretionary Access Control (DAC) you have: Discretionary Access Control

The Lattice Based Access Control is a type of access control used to implement other access control method. A lattice is an ordered list of elements that has a least upper bound and a most lower bound. The lattice can be used for MAC, DAC, Integrity level, File Permission, and more

For example in the case of MAC, if we look at common government classifications, we have the following:

TOP SECRET SECRET ------I am the user at secret CONFIDENTIAL SENSITIVE BUT UNCLASSIFIED UNCLASSIFIED

If you look at the diagram above where I am a user at SECRET it means that I can access document at lower classification but not document at TOP SECRET. The lattice is a list of ORDERED ELEMENT, in this case the ordered elements are classification levels. My least upper

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html

Download Full Version SSCP Exam Dumps(Updated in Feb/2023)

bound is SECRET and my most lower bound is UNCLASSIFIED.

However the lattice could also be used for Integrity Levels such as:

VERY HIGH HIGH MEDIUM -----I am a user, process, application at the medium level LOW VERY LOW In the case of of Integrity levels you have to think about TRUST. Of course if I take for example

the the VISTA operating system which is based on Biba then Integrity Levels would be used. As a user having access to the system I cannot tell a process running with administrative privilege what to do. Else any users on the system could take control of the system by getting highly privilege process to do things on their behalf. So no read down would be allowed in this case and this is an example of the Biba model.

Last but not least the lattice could be use for file permissions:

RWX RW -----User at this level R

If I am a user with READ and WRITE (RW) access privilege then I cannot execute the file because I do not have execute permission which is the X under linux and UNIX.

Many people confuse the Lattice Model and many books says MAC = LATTICE, however the lattice can be use for other purposes.

There is also Role Based Access Control (RBAC) that exists out there. It COULD be used to simulate MAC but it is not MAC as it does not make use of Label on objects indicating sensitivity and categories. MAC also require a clearance that dominates the object.

You can get more info about RBAC at:http://csrc.nist.gov/groups/SNS/rbac/faq.html#03

Also note that many book uses the same acronym for Role Based Access Control and Rule Based Access Control which is RBAC, this can be confusing.

The proper way of writing the acronym for Rule Based Access Control is RuBAC, unfortunately it is not commonly used.

References:

There is a great article on technet that talks about the lattice in VISTA: http://blogs.technet.com/b/steriley/archive/2006/07/21/442870.aspx

also see:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33). http://www.microsoft-watch.com/content/vista/gaging_vistas_integrity.html

QUESTION 166

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.

Download Full Version SSCP Exam Dumps(Updated in Feb/2023)

- C. the number of categories in the two labels are different.
- D. Neither label contains all the categories of the other.

Correct 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 s3 > s2 > s1 > s0

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

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html