

## [Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

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).

### **QUESTION 78**

Which of the following is an example of a passive attack?

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

**Correct Answer: B**

#### **Explanation:**

Shoulder surfing is a form of a passive attack involving stealing passwords, personal identification numbers or other confidential information by looking over someone's shoulder. All other forms of attack are active attacks, where a threat makes a modification to the system in an attempt to take advantage of a vulnerability.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 3: Security Management Practices (page 63).

### **QUESTION 79**

What does the (star) integrity axiom mean in the Biba model?

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

**Correct Answer: D**

#### **Explanation:**

The (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up).

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

### **QUESTION 80**

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

**Correct Answer: B**

#### **Explanation:**

Almost all types of detection permit a system's sensitivity to be increased or decreased during an

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

## **[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)**

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

**[SSCP Exam Dumps](#)   **[SSCP PDF Dumps](#)   **[SSCP VCE Dumps](#)   **[SSCP Q&As](#)********

**<https://www.ensurepass.com/SSCP.html>**

## [Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

device or software.

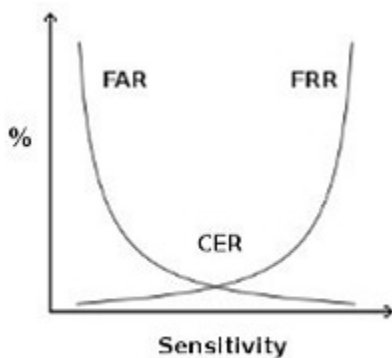
FAR and FRR are key metrics for biometric solutions, some biometric devices or software even allow to tune them so that the system more quickly matches or rejects. Both FRR and FAR are important, but for most applications one of them is considered most important.

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

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

## [Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

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.  
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.  
[http://www.biometric-solutions.com/index.php?story=performance\\_biometrics](http://www.biometric-solutions.com/index.php?story=performance_biometrics)

### **QUESTION 81**

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

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

**Correct Answer: D**

#### **Explanation:**

The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.

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

A UserId only provides for identification.

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

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

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

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

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

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

## **[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)**

unauthorized persons can (and do) obtain the cards and information.

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

NOTE FROM CLEMENT:

This question has been generating lots of interest. The keyword in the question is:

Individual (the person) and also the authenticated portion as well.

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

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

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

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

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

There are always THREE means of authentication, they are:

Something you know (Type 1)  
Something you have (Type 2)  
Something you are (Type 3)

Reference(s) used for this question:

TIPTON, Harold F.& KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) , 2000, CRC Press, Chapter 1, Biometric Identification (page 7).  
Search Security at <http://searchsecurity.techtarget.com/definition/masquerade>