Rejection Rate (FRR) or False Reject Rate (FRR)).

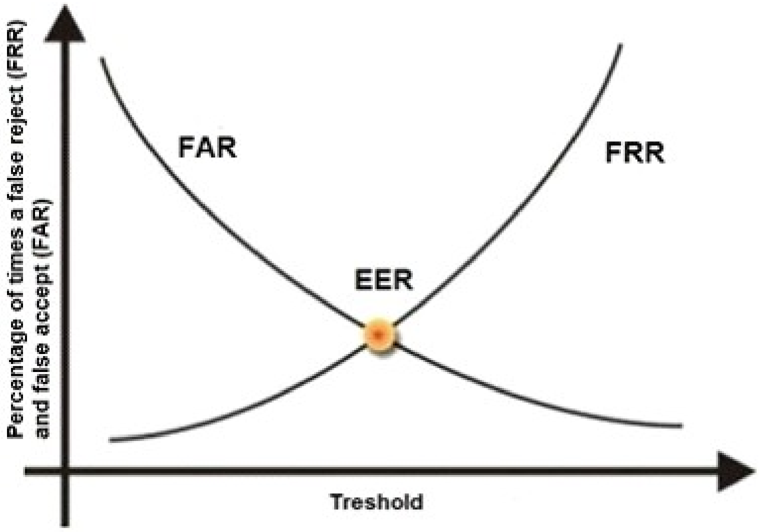
When the system accepts impostors who should be rejected, it is called a Type II error (False Acceptance Rate (FAR) or False Accept Rate (FAR)). Type II errors are the most dangerous and thus the most important to avoid.

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

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

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

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



Cross Over Error Rate

The other answers are incorrect:

Type I error is also called as False Rejection Rate where a valid user is rejected by the system.
Type III error : there is no such error type in biometric system.

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

Reference(s) used for this question:

http://www.biometria.sk/en/principles-of-biometrics.html
Shon Harris, CISSP All In One (AIO), 6th Edition , Chapter 3, Access Control, Page 188-
Tech Republic, Reduce Multi_Factor Authentication Cost

QUESTION 196
How should a doorway of a manned facility with automatic locks be configured?

A. It should be configured to be fail-secure.
B. It should be configured to be fail-safe.
C. It should have a door delay cipher lock.
D. It should not allow piggybacking.

Correct Answer: B
Explanation:
Access controls are meant to protect facilities and computers as well as people.

In some situations, the objectives of physical access controls and the protection of people's lives may come into conflict. In theses situations, a person's life always takes precedence.

Many physical security controls make entry into and out of a facility hard, if not impossible. However, special consideration needs to be taken when this could affect lives. In an information processing facility, different types of locks can be used and piggybacking should be prevented, but the issue here with automatic locks is that they can either be configured as fail-safe or fail-secure.

Since there should only be one access door to an information processing facility, the automatic lock to the only door to a man-operated room must be configured to allow people out in case of emergency, hence to be fail-safe (sometimes called fail-open), meaning that upon fire alarm activation or electric power failure, the locking device unlocks. This is because the solenoid that maintains power to the lock to keep it in a locked state fails and thus opens or unlocks the electronic lock.

Fail Secure works just the other way. The lock device is in a locked or secure state with no power applied. Upon authorized entry, a solinoid unlocks the lock temporarily. Thus in a Fail Secure lock, loss of power of fire alarm activation causes the lock to remain in a secure mode.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 451). McGraw- Hill. Kindle Edition.
And Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20249-20251). Auerbach Publications. Kindle Edition.

QUESTION 197
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

Correct Answer: B
Explanation:
In the lattice model, users are assigned security clearences and the data is classified. Access decisions are made based on the clearence 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 clearence 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 disqualiifes 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 aprticularly Figure 5-19 on p. 293 for an illustration of bounds in action.

QUESTION 198
Which of the following access control models is based on sensitivity labels?

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

Correct Answer: B
Explanation:
Access decisions are made based on the clearance of the subject and the sensitivity label of the object.

Example: Eve has a "Secret" security clearance and is able to access the "Mugwump Missile Design Profile" because its sensitivity label is "Secret." She is denied access to the "Presidential Toilet Tissue Formula" because its sensitivity label is "Top Secret."

The other answers are not correct because:

Discretionary Access Control is incorrect because in DAC access to data is determined by the data owner. For example, Joe owns the "Secret Chili Recipe" and grants read access to Charles.

Role Based Access Control is incorrect because in RBAC access decsions are made based on the role held by the user. For example, Jane has the role "Auditor" and that role includes read permission on the "System Audit Log."

Rule Based Access Control is incorrect because it is a form of MAC. A good example would be a Firewall where rules are defined and apply to anyone connecting through the firewall.

References:
All in One third edition, page 164.
Official ISC2 Guide page 187.

QUESTION 199
Which authentication technique best protects against hijacking?

A. Static authentication
B. Continuous authentication
C. Robust authentication
D. Strong authentication

Correct Answer: B
Explanation:
A continuous authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. This is the best protection against hijacking. Static authentication is the type of authentication provided by traditional password schemes and the strength of the authentication is highly dependent on the difficulty of guessing passwords. The robust authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, and it does not protect against hijacking. Strong authentication refers to a two-factor authentication (like something a user knows and something a user is).
Source: TIPTON, Harold F.& KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3: Secured Connections to External Networks (page 51).

QUESTION 200
For maximum security design, what type of fence is most effective and cost-effective method (Foot are being used as measurement unit below)?

A. 3' to 4' high
B. 6' to 7' high
C. 8' high and above with strands of barbed wire
D. Double fencing

Correct Answer: D
Explanation:
The most commonly used fence is the chain linked fence and it is the most affordable. The standard is a six-foot high fence with two-inch mesh square openings. The material should consist of nine-gauge vinyl or galvanized metal. Nine-gauge is a typical fence material installed in residential areas.

Additionally, it is recommended to place barbed wire strands angled out from the top of the fence at a 45?angle and away from the protected area with three strands running across the top. This will provide for a seven-foot fence. There are several variations of the use of "top guards" using V-shaped barbed wire or the use of concertina wire as an enhancement, which has been a replacement for more traditional three strand barbed wire "top guards."

The fence should be fastened to ridged metal posts set in concrete every six feet with additional bracing at the corners and gate openings. The bottom of the fence should be stabilized against intruders crawling under by attaching posts along the bottom to keep the fence from being pushed or pulled up from the bottom. If the soil is sandy, the bottom edge of the fence should be installed below ground level.

For maximum security design, the use of double fencing with rolls of concertina wire positioned between the two fences is the most effective deterrent and cost-efficient method. In this design, an intruder is required to use an extensive array of ladders and equipment to breach the fences.

Most fencing is largely a psychological deterrent and a boundary marker rather than a barrier, because in most cases such fences can be rather easily penetrated unless added security measures are taken to enhance the security of the fence. Sensors attached to the fence to provide electronic monitoring of cutting or scaling the fence can be used.

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 24416-24431). Auerbach Publications. Kindle Edition.

QUESTION 201
What are called user interfaces that limit the functions that can be selected by a user?

A. Constrained user interfaces
B. Limited user interfaces
C. Mini user interfaces
D. Unlimited user interfaces

Correct Answer: A
Explanation:
Constrained user interfaces limit the functions that can be selected by a user.

Another method for controlling access is by restricting users to specific functions based on their role in the system. This is typically implemented by limiting available menus, data views, encryption, or by physically constraining the user interfaces.

This is common on devices such as an automated teller machine (ATM). The advantage of a constrained user interface is that it limits potential avenues of attack and system failure by restricting the processing options that are available to the user.

On an ATM machine, if a user does not have a checking account with the bank he or she will not be shown the "Withdraw money from checking" option. Likewise, an information system might have an "Add/Remove Users" menu option for administrators, but if a normal, non-administrative user logs in he or she will not even see that menu option. By not even identifying potential options for non-qualifying users, the system limits the potentially harmful execution of unauthorized system or application commands.

Many database management systems have the concept of "views." A database view is an extract of the data stored in the database that is filtered based on predefined user or system criteria. This permits multiple users to access the same database while only having the ability to access data they need (or are allowed to have) and not data for another user. The use of database views is another example of a constrained user interface.

The following were incorrect answers:
All of the other choices presented were bogus answers.

The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition