# ISC2

## Exam Questions SSCP

System Security Certified Practitioner (SSCP)

# About Exambible

*Your Partner of IT Exam*

## Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

## Our Advances

* 99.9% Uptime

  All examinations will be up to date.

* 24/7 Quality Support

  We will provide service round the clock.

* 100% Pass Rate

  Our guarantee that you will pass the exam.

* Unique Gurantee

  If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**NEW QUESTION 1**
- (Topic 1)
Crime Prevention Through Environmental Design (CPTED) is a discipline that:

A. Outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.
B. Outlines how the proper design of the logical environment can reduce crime by directly affecting human behavior.
C. Outlines how the proper design of the detective control environment can reduce crime by directly affecting human behavior.
D. Outlines how the proper design of the administrative control environment can reduce crime by directly affecting human behavior.

**Answer:** A

**Explanation:**
Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance about lost and crime prevention through proper facility contruction and environmental components and procedures.
CPTED concepts were developed in the 1960s. They have been expanded upon and have matured as our environments and crime types have evolved. CPTED has been used not just to develop corporate physical security programs, but also for large-scale activities such as development of neighborhoods, towns, and cities. It addresses landscaping, entrances, facility and neighborhood layouts, lighting, road placement, and traffic circulation patterns. It looks at microenvironments, such as offices and rest-rooms, and macroenvironments, like campuses and cities.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 435). McGraw- Hill. Kindle Edition.
and
CPTED Guide Book

**NEW QUESTION 2**
- (Topic 1)
To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:

A. Access Rules
B. Access Matrix
C. Identification controls
D. Access terminal

**Answer:** A

**Explanation:**
Controlling access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up access rules.
These rules can be classified into three access control models: Mandatory, Discretionary, and Non-Discretionary.
An access matrix is one of the means used to implement access control.
Source: 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 3**
- (Topic 1)
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

**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).

**NEW QUESTION 4**
- (Topic 1)
In the Bell-LaPadula model, the Star-property is also called:

A. The simple security property
B. The confidentiality property
C. The confinement property
D. The tranquility property

**Answer:** B

**Explanation:**
The Bell-LaPadula model focuses on data confidentiality and 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 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 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 an access control matrix to specify the discretionary access control.
The transfer of information from a high-sensitivity document to a lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the property. Untrusted subjects are.
Trusted Subjects must be shown to be trustworthy with regard to the security policy. This security model is directed toward access control and is characterized by the phrase: "no read up, no write down." Compare the Biba model, the Clark-Wilson model and the Chinese Wall.
With Bell-LaPadula, users can create content only at or above their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down). Conversely, users can view content only at or below their own security level
(i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).
Strong Property
The Strong Property is an alternative to the Property in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual Property is not present, only a write-to-same level operation. The Strong Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns.
Tranquility principle
The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle: the "principle of strong tranquility" states that security levels do not change during the normal operation of the system and the "principle of weak tranquility" states that security levels do not change in a way that violates the rules of a given security policy.
Another interpretation of the tranquility principles is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/label will not change during an operation (such as read or write); the weak tranquility principle means that an object's security level/label may change in a way that does not violate the security policy during an operation.
Reference(s) used for this question: http://en.wikipedia.org/wiki/Biba_Model
http://en.wikipedia.org/wiki/Mandatory_access_control http://en.wikipedia.org/wiki/Discretionary_access_control http://en.wikipedia.org/wiki/Clark-Wilson_model
http://en.wikipedia.org/wiki/Brewer_and_Nash_model

**NEW QUESTION 5**
- (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 6**
- (Topic 1)
What is the most critical characteristic of a biometric identifying system?

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

**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).

**NEW QUESTION 7**
- (Topic 1)
Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

A. The Take-Grant model
B. The Biba integrity model
C. The Clark Wilson integrity model
D. The Bell-LaPadula integrity model

**Answer:** C

**Explanation:**
The Clark Wilson integrity model addresses the three following integrity goals: 1) data is protected from modification by unauthorized users; 2) data is protected from unauthorized modification by authorized users; and 3) data is internally and externally consistent. It also defines a Constrained Data Item (CDI), an Integrity Verification Procedure (IVP), a Transformation Procedure (TP) and an Unconstrained Data item. The Bell-LaPadula and Take-Grant models are not integrity models.
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 205).

**NEW QUESTION 8**
- (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 9**
- (Topic 1)
Which of the following biometric devices has the lowest user acceptance level?

A. Retina Scan
B. Fingerprint scan
C. Hand geometry
D. Signature recognition

**Answer:** A

**Explanation:**
According to the cited reference, of the given options, the Retina scan has the lowest user acceptance level as it is needed for the user to get his eye close to a device and it is not user friendly and very intrusive.
However, retina scan is the most precise with about one error per 10 millions usage. Look at the 2 tables below. If necessary right click on the image and save it on your
desktop for a larger view or visit the web site directly at
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy . Biometric Comparison Chart

**BIOMETRICS COMPARISON CHART**

| Biometric | Verify | ID | Accuracy | Reliability | Error Rate | Errors | False Pos | False Neg |
|---|---|---|---|---|---|---|---|---|
| Fingerprint | Yes | Yes | Very High | High | 1 in 500+ | dryness, dirt, age | Ext. Diff | Ext. Diff |
| Facial Recognition | Yes | No | High | Medium | no data | lighting, age, glasses, hair | Difficult | Easy |
| Hand Geometry | Yes | No | High | Medium | 1 in 500 | hand injury, age | Very Diff | Medium |
| Speaker Recognition | Yes | No | Medium | Low | 1 in 50 | noise, weather, colds | Medium | Easy |
| Iris Scan | Yes | Yes | Very High | High | 1 in 131,000 | poor lighting | Very Diff | Very Diff |
| Retinal Scan | Yes | Yes | Very High | High | 1 in 10,000,000 | glasses | Ext. Diff | Ext. Diff |
| Signature Recognition | Yes | No | Medium | Low | 1 in 50 | changing signatures | Medium | Easy |
| Keystroke Recognition | Yes | No | Low | Low | no data | hand injury, tiredness | Difficult | Easy |
| DNA | Yes | Yes | Very High | High | no data | none | Ext. Diff | Ext. Diff |

| Biometric | Security Level | Long-term Stability | User Acceptance | Intrusive | Ease of Use | Low Cost | Hardware | Standards |
|---|---|---|---|---|---|---|---|---|
| Fingerprint | High | High | Medium | Somewhat | High | Yes | Special, cheap | Yes |
| Facial Recognition | Medium | Medium | Medium | Non | Medium | Yes | Common, cheap | ? |
| Hand Geometry | Medium | Medium | Medium | Non | High | No | Special, mid-price | ? |
| Speaker Recognition | Medium | Medium | High | Non | High | Yes | Common, cheap | ? |
| Iris Scan | High | High | Medium | Non | Medium | No | Special, expensive | ? |
| Retinal Scan | High | High | Medium | Very | Low | No | Special, expensive | ? |
| Signature Recognition | Medium | Medium | Medium | Non | High | Yes | Special, mid-price | ? |
| Keystroke Recognition | Medium | Low | High | Non | High | Yes | Common, cheap | ? |
| DNA | High | High | Low | Extremely | Low | No | Special, expensive | Yes |

C:\Users\MCS\Desktop\1.jpg

Aspect descriptions

| | |
|---|---|
| Verify | Whether or not the Biometric is capable of verification. Verification is the process where an input is compared to specific data previously recorded from the user to see if the person is who they claim to be |
| ID | Whether or not the Biometric is capable of identification. Identification is the process where an input is compared to a large data set previously recorded from many peoplete see which person the user is. |
| Accuracy | How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results |
| Reliability | How dependable the Biometric is for recognition purposes. |
| Error Rate | This is calculated as the crossing point when graphed of false positives and false negtives created using this Biometric |
| Errors | Typical causes of errors for this Biometric |
| False Pos. | How easy it is to create a false positive reading with this biometric (someone is able to impersonate someone else) |
| False Neg. | How easy it is to create a false negative reading with this biometric (someone is able to avoid identification as oneself) |
| Security Level | The highest level of security that this Biometric is capable of working at |
| Long-term Stability | How well this Biometric continues to work without data updates over long periods of time |
| User Acceptance | How willing the public is to use this Biometric |
| Intrusiveness | How much the Biometric is considered to invade one's privacy or require interaction by the user |
| Ease of Use | How easy this Biometric is for both the user and the personnel involved |
| Low Cost | Whether or not there is a low cost option for this Biometric to be used |
| Hardware | Type and cost of hardware required to use this Biometric |
| Standards | Whether or not standards exist for this Biometric |

C:\Users\MCS\Desktop\1.jpg
Biometric Aspect Descriptions Reference(s) used for this question:
RHODES, Keith A., Chief Technologist, United States General Accounting Office, National Preparedness, Technologies to Secure Federal Buildings, April 2002 (page 10).
and
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy

**NEW QUESTION 10**
- (Topic 1)
Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

A. TCP
B. SSL
C. UDP
D. SSH

**Answer:** C

**Explanation:**
The original TACACS, developed in the early ARPANet days, had very limited functionality and used the UDP transport. In the early 1990s, the protocol was extended to include additional functionality and the transport changed to TCP.
TACACS is defined in RFC 1492, and uses (either TCP or UDP) port 49 by default. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. TACACSD uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back.
TACACS+
TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Since TCP is connection oriented
protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet loss, timeout etc. since it rides on UDP which is connectionless.
RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore it is vulnerable to different types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.
RADIUS and TACACS + are client/ server protocols, which means the server portion cannot send unsolicited commands to the client portion. The server portion can only speak when spoken to. Diameter is a peer-based protocol that allows either end to initiate communication. This functionality allows the Diameter server to send a message to the access server to request the user to provide another authentication credential if she is attempting to access a secure resource.
Reference(s) used for this question: http://en.wikipedia.org/wiki/TACACS
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 239). McGraw- Hill. Kindle Edition.

**NEW QUESTION 10**
- (Topic 1)
Which of the following was developed by the National Computer Security Center (NCSC) for the US Department of Defense ?

A. TCSEC
B. ITSEC
C. DIACAP
D. NIACAP

**Answer:** A

**Explanation:**
The Answer TCSEC; The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications.
Initially issued by the National Computer Security Center (NCSC) an arm of the National Security Agency in 1983 and then updated in 1985, TCSEC was replaced with the development of the Common Criteria international standard originally published in 2005.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 197-199.
Wikepedia http://en.wikipedia.org/wiki/TCSEC

**NEW QUESTION 13**
- (Topic 1)
Which of the following statements pertaining to biometrics is false?

A. Increased system sensitivity can cause a higher false rejection rate

B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
C. False acceptance rate is also known as Type II error.
D. Biometrics are based on the Type 2 authentication mechanism.

**Answer:** D

**Explanation:**
Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based on the Type 3 authentication mechanism.
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 37).

**NEW QUESTION 18**
- (Topic 1)
In the CIA triad, what does the letter A stand for?

A. Auditability
B. Accountability
C. Availability
D. Authentication

**Answer:** C

**Explanation:**
The CIA triad stands for Confidentiality, Integrity and Availability.

**NEW QUESTION 23**
- (Topic 1)
Which of the following attacks could capture network user passwords?

A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing

**Answer:** B

**Explanation:**
A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.
Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.
A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.
Another method for sniffing is to use a network tap??a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.
The packets captured by sniffer are decoded and then displayed by the sniffer. Therfore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).
Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.
The following answers are incorrect:
Data diddling involves changing data before, as it is enterred into a computer, or after it is extracted.
Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.
Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.
The following reference(s) were/was used to create this question: CISA Review manual 2014 Page number 321
Official ISC2 Guide to the CISSP 3rd edition Page Number 153

**NEW QUESTION 27**
- (Topic 1)
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:

A. These factors include the enrollment time and the throughput rate, but not acceptability.
B. These factors do not include the enrollment time, the throughput rate, and acceptability.
C. These factors include the enrollment time, the throughput rate, and acceptability.
D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.

**Answer:** C

**Explanation:**
In addition to the accuracy of the biometric systems, there are other factors that must also be considered.
These factors include the enrollment time, the throughput rate, and acceptability. Enrollment time is the time it takes to initially "register" with a system by providing samples
of the biometric characteristic to be evaluated. An acceptable enrollment time is around two
minutes.
For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.
In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.

Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

**NEW QUESTION 30**
- (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

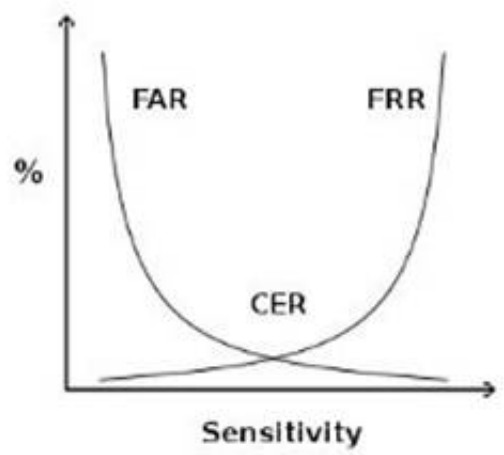
**Explanation:**
In 1973 Bell and LaPadula created the first mathematical model of a multi- level security system.
The following answers are incorrect:
Diffie and Hellman. This is incorrect because Diffie and Hellman was involved with cryptography.
Clark and Wilson. This is incorrect because Bell and 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 33**
- (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 (FRR) 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 conistency. 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 37**
- (Topic 1)
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)

**NEW QUESTION 38**
- (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 authorzied individuals from running processes.

**NEW QUESTION 41**

- (Topic 1)
Which division of the Orange Book deals with discretionary protection (need-to-know)?

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

**Answer:** B

**Explanation:**
C deals with discretionary protection. See matric below:

**TNI/TCSEC MATRIX**

| | A1 | B3 | B2 | B1 | C2 | C1 |
|---|---|---|---|---|---|---|
| **DISCRETIONARY ACCESS** | | | | | | |
| Discretionary Access Control | | | | | | |
| Identification and Authentication | | | | | | |
| System Integrity | | | | | | |
| System Architecture | | | | | | |
| Security Testing | | | | | | |
| Security Features User's Guide Trusted Facility Manual Design Documentation Test Documentation | | | | | | |
| **CONTROLLED ACCESS** | | | | | | |
| Protect Audit Trails | | | | | | |
| Object Reuse | | | | | | |
| **MANDATORY ACCESS CONTROL** | | | | | | |
| Labels | | | | | | |
| Mandatory Access Control | | | | | | |
| Process isolation in system architecture | | | | | | |
| Design Specification & Verification | | | | | | |
| Device labels | | | | | | |
| Subject Sensitivity Labels | | | | | | |
| Trusted Path | | | | | | |
| Separation of Administrator and User functions | | | | | | |
| Covert Channel Analysis (Only Covert Storage Channel at B2) | | | | | | |
| Trusted Facility Management | | | | | | |
| Configuration Management | | | | | | |
| Trusted Recovery | | | | | | |
| Covert Channel Analysis (Both Timing and Covert Channel analysis at B3) | | | | | | |
| Security Administrator Role Defined | | | | | | |
| Monitor events and notify security personnel | | | | | | |
| Trusted Distribution | | | | | | |
| Formal Methods | | | | | | |
| | A1 | B3 | B2 | B1 | C2 | C1 |

C:\Users\MCS\Desktop\1.jpg
TCSEC Matric
The following are incorrect answers:
D is incorrect. D deals with minimal security.
B is incorrect. B deals with mandatory protection. A is incorrect. A deals with verified protection. Reference(s) used for this question:
CBK, p. 329 ?C 330
and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

**NEW QUESTION 42**
- (Topic 1)
What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

A. Biometrics
B. Micrometrics
C. Macrometrics
D. MicroBiometrics

**Answer:** A

**Explanation:**
The Answer Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

**NEW QUESTION 46**
- (Topic 1)
Which of the following statements pertaining to Kerberos is TRUE?

A. Kerberos does not address availability
B. Kerberos does not address integrity
C. Kerberos does not make use of Symmetric Keys
D. Kerberos cannot address confidentiality of information

**Answer:** A

**Explanation:**
The question was asking for a TRUE statement and the only correct statement is "Kerberos does not address availability".
Kerberos addresses the confidentiality and integrity of information. It does not directly address availability.

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 42).

**NEW QUESTION 51**
- (Topic 1)
What is one disadvantage of content-dependent protection of information?

A. It increases processing overhead.
B. It requires additional password entry.
C. It exposes the system to data locking.
D. It limits the user's individual address space.

**Answer:** A

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

**NEW QUESTION 53**
- (Topic 1)
The following is NOT a security characteristic we need to consider while choosing a biometric identification systems:

A. data acquisition process
B. cost
C. enrollment process
D. speed and user interface

**Answer:** B

**Explanation:**
Cost is a factor when considering Biometrics but it is not a security characteristic.
All the other answers are incorrect because they are security characteristics related to Biometrics.
data acquisition process can cause a security concern because if the process is not fast and efficient it can discourage individuals from using the process.
enrollment process can cause a security concern because the enrollment process has to be quick and efficient. This process captures data for authentication.
speed and user interface can cause a security concern because this also impacts the users acceptance rate of biometrics. If they are not comfortable with the interface and speed they might sabotage the devices or otherwise attempt to circumvent them.
References:
OIG Access Control (Biometrics) (pgs 165-167)
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Pages 5-6.
in process of correction

**NEW QUESTION 55**
- (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?CLaPadula 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?CLaPadula 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?CLaPadula 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 59**
- (Topic 1)
Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

A. Wave pattern motion detectors
B. Capacitance detectors
C. Field-powered devices
D. Audio detectors

**Answer:** B

**Explanation:**
Capacitance detectors monitor an electrical field surrounding the object being monitored. They are used for spot protection within a few inches of the object, rather than for overall room security monitoring used by wave detectors. Penetration of this field changes the electrical capacitance of the field enough to generate and alarm. Wave pattern motion detectors generate a frequency wave pattern and send an alarm if the pattern is disturbed as it is reflected back to its receiver. Field-powered devices are a type of personnel access control devices. Audio detectors simply monitor a room for any abnormal sound wave generation and trigger an alarm.
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 344).

**NEW QUESTION 64**
- (Topic 1)
Access Control techniques do not include which of the following?

A. Rule-Based Access Controls
B. Role-Based Access Control
C. Mandatory Access Control
D. Random Number Based Access Control

**Answer:** D

**Explanation:**
Access Control Techniques Discretionary Access Control
Mandatory Access Control Lattice Based Access Control Rule-Based Access Control Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

**NEW QUESTION 67**
- (Topic 1)
Which of the following biometric devices offers the LOWEST CER?

A. Keystroke dynamics
B. Voice verification
C. Iris scan
D. Fingerprint

**Answer:** C

**Explanation:**
From most effective (lowest CER) to least effective (highest CER) are: Iris scan, fingerprint, voice verification, keystroke dynamics.
Reference : Shon Harris Aio v3 , Chapter-4 : Access Control , Page : 131
Also see: http://www.sans.org/reading_room/whitepapers/authentication/biometric-selection-body-parts-online_139

**NEW QUESTION 72**
- (Topic 1)
Which of the following is not a preventive login control?

A. Last login message
B. Password aging
C. Minimum password length
D. Account expiration

**Answer:** A

**Explanation:**
The last login message displays the last login date and time, allowing a user to discover if their account was used by someone else. Hence, this is rather a detective control.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 63).

**NEW QUESTION 76**
- (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 77**
- (Topic 1)
How can an individual/person best be identified or authenticated to prevent local masquarading attacks?

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

**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 Masquarade. 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 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).
and
Search Security at http://searchsecurity.techtarget.com/definition/masquerade

**NEW QUESTION 78**
- (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:

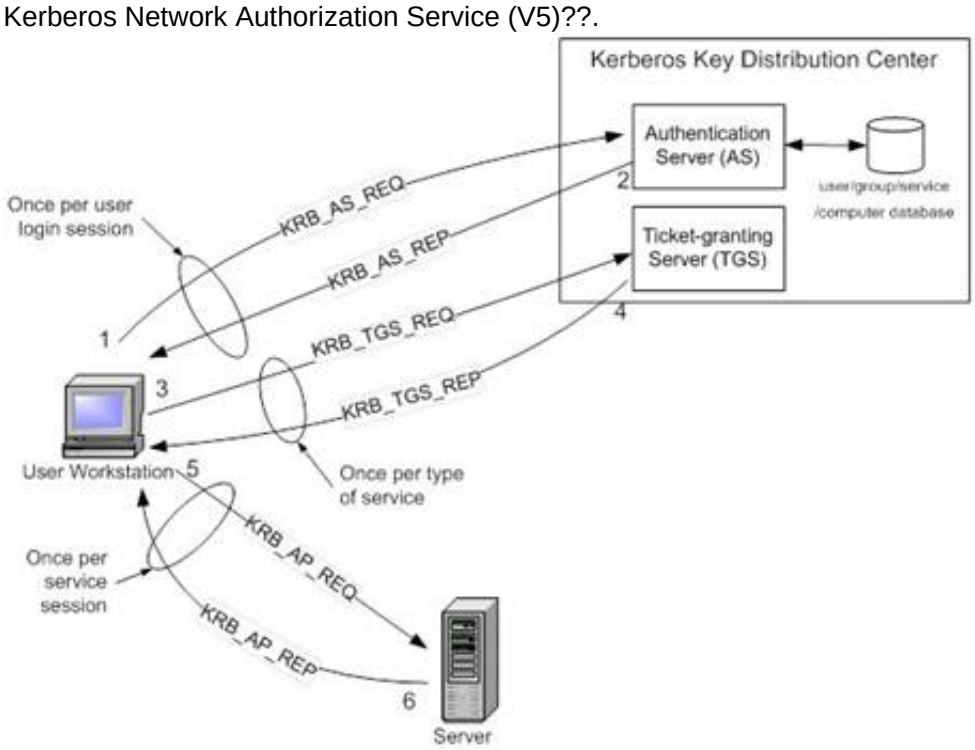
badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.
locks Locks are a Preventative Physical control and has no Technical 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 81**
- (Topic 1)
Which of the following is NOT true of the Kerberos protocol?

A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication

**Answer:** B

**Explanation:**
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:
It is secure: it never sends a password unless it is encrypted.
Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.
The concept depends on a trusted third party ?C a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.
It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.
Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS ?C a ticket is a time-limited
cryptographic message ?C giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.
Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication. Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 ??The Kerberos Network Authorization Service (V5)??.




C:\Users\MCS\Desktop\1.jpg Kerberos Authentication Step by Step
Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).
Step 2: The Authorization Server verifies the user??s access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user??s password and sends a message back to the user workstation.
The workstation prompts the user for a password and uses the password to decrypt the incoming message. When decryption succeeds, the user will be able to use the TGT to request a service ticket.
Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.
Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key
?C one encrypted with the client password, and one encrypted by the service password.
Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.
Step 6: If mutual authentication is required, then the server will reply with a server authentication message.
The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above.
To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.
Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.
For more information about Kerberos, see http://web.mit.edu/kerberos/www/.
References:

Introduction to Kerberos Authentication from Intel
and
http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3 and
http://www.ietf.org/rfc/rfc4120.txt

**NEW QUESTION 84**
- (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 85**
- (Topic 1)
Access Control techniques do not include which of the following choices?

A. Relevant Access Controls
B. Discretionary Access Control
C. Mandatory Access Control
D. Lattice Based Access Control

**Answer:** A

**Explanation:**
Access Control Techniques Discretionary Access Control
Mandatory Access Control Lattice Based Access Control Rule-Based Access Control Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

**NEW QUESTION 89**
- (Topic 1)
Which of the following statements pertaining to the Bell-LaPadula is TRUE if you are NOT making use of the strong star property?

A. It allows "read up."
B. It addresses covert channels.
C. It addresses management of access controls.
D. It allows "write up."

**Answer:** D

**Explanation:**
Bell?CLaPadula Confidentiality Model10 The Bell?CLaPadula model is perhaps the most well-known and significant security model, in addition to being one of the oldest models used in the creation of modern secure computing systems. Like the Trusted Computer System Evaluation Criteria (or TCSEC), it was inspired by early U.S. Department of Defense security policies and the need to prove that confidentiality could be maintained. In other words, its primary goal is to prevent disclosure as the model system moves from one state (one point in time) to another.
When the strong star property is not being used it means that both the property and the
Simple Security Property rules would be applied.
The Star (*) property rule of the Bell-LaPadula model says that subjects cannot write down, this would compromise the confidentiality of the information if someone at the secret layer would write the object down to a confidential container for example.
The Simple Security Property rule states that the subject cannot read up which means that a subject at the secret layer would not be able to access objects at Top Secret for example.
You must remember: The model tells you about are NOT allowed to do. Anything else would be allowed. For example within the Bell LaPadula model you would be allowed to write up as it does not compromise the security of the information. In fact it would upgrade it to the point that you could lock yourself out of your own information if you have only a secret security clearance.
The following are incorrect answers because they are all FALSE:
"It allows read up" is incorrect. The "simple security" property forbids read up.
"It addresses covert channels" is incorrect. Covert channels are not addressed by the Bell- LaPadula model.
"It addresses management of access controls" is incorrect. Management of access controls are beyond the scope of the Bell-LaPadula model.
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 17595-17600). Auerbach Publications. Kindle Edition.

**NEW QUESTION 90**
- (Topic 1)
Which access control model is also called Non Discretionary Access Control (NDAC)?

A. Lattice based access control
B. Mandatory access control
C. Role-based access control

D. Label-based access control

**Answer:** C

**Explanation:**
RBAC is sometimes also called non-discretionary access control (NDAC) (as Ferraiolo says "to distinguish it from the policy-based specifics of MAC"). Another model that fits within the NDAC category is Rule-Based Access Control (RuBAC or RBAC). Most of the CISSP books use the same acronym for both models but NIST tend to use a lowercase "u" in between R and B to differentiate the two models.
You can certainly mimic MAC using RBAC but true MAC makes use of Labels which contains the sensitivity of the objects and the categories they belong to. No labels means MAC is not being used.
One of the most fundamental data access control decisions an organization must make is the amount of control it will give system and data owners to specify the level of access users of that data will have. In every organization there is a balancing point between the access controls enforced by organization and system policy and the ability for information owners to determine who can have access based on specific business requirements. The process of translating that balance into a workable access control model can be defined by three general access frameworks:
Discretionary access control Mandatory access control Nondiscretionary access control
A role-based access control (RBAC) model bases the access control authorizations on the roles (or functions) that the user is assigned within an organization. The determination of what roles have access to a resource can be governed by the owner of the data, as with DACs, or applied based on policy, as with MACs. Access control decisions are based on job function, previously defined and governed by policy, and each role (job function) will have its own access capabilities. Objects associated with a role will inherit privileges assigned to that role. This is also true for groups of users, allowing administrators to simplify access control strategies by assigning users to groups and groups to roles.
There are several approaches to RBAC. As with many system controls, there are variations on how they can be applied within a computer system.
There are four basic RBAC architectures:
1. Non-RBAC: Non-RBAC is simply a user-granted access to data or an application by traditional mapping, such as with ACLs. There are no formal ??roles?? associated with the mappings, other than any identified by the particular user.
2. Limited RBAC: Limited RBAC is achieved when users are mapped to roles within a single application rather than through an organization-wide role structure. Users in a limited RBAC system are also able to access non-RBAC-based applications or data. For example, a user may be assigned to multiple roles within several applications and, in addition, have direct access to another application or system independent of his or her assigned role. The key attribute of limited RBAC is that the role for that user is defined within an application and not necessarily based on the user??s organizational job function.
3. Hybrid RBAC: Hybrid RBAC introduces the use of a role that is applied to multiple
applications or systems based on a user??s specific role within the organization. That role is then applied to applications or systems that subscribe to the organization??s role-based model. However, as the term ??hybrid?? suggests, there are instances where the subject may also be assigned to roles defined solely within specific applications, complimenting (or, perhaps, contradicting) the larger, more encompassing organizational role used by other systems.
4. Full RBAC: Full RBAC systems are controlled by roles defined by the organization??s policy and access control infrastructure and then applied to applications and systems across the enterprise. The applications, systems, and associated data apply permissions based on that enterprise definition, and not one defined by a specific application or system. Be careful not to try to make MAC and DAC opposites of each other -- they are two different access control strategies with RBAC being a third strategy that was defined later to address some of the limitations of MAC and DAC.
The other answers are not correct because:
Mandatory access control is incorrect because though it is by definition not discretionary, it is not called "non-discretionary access control." MAC makes use of label to indicate the sensitivity of the object and it also makes use of categories to implement the need to know.
Label-based access control is incorrect because this is not a name for a type of access control but simply a bogus detractor.
Lattice based access control is not adequate either. A lattice is a series of levels and a subject will be granted an upper and lower bound within the series of levels. These levels could be sensitivity levels or they could be confidentiality levels or they could be integrity levels.
Reference(s) used for this question: All in One, third edition, page 165.
Ferraiolo, D., Kuhn, D. & Chandramouli, R. (2003). Role-Based Access Control, p. 18.
Ferraiolo, D., Kuhn, D. (1992). Role-Based Access Controls. http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 1557-1584). Auerbach Publications. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 1474-1477). Auerbach Publications. Kindle Edition.

**NEW QUESTION 95**
- (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 97**
- (Topic 1)
Which of the following logical access exposures INVOLVES CHANGING data before, or as it is entered into the computer?

A. Data diddling
B. Salami techniques
C. Trojan horses
D. Viruses

**Answer:** A

**Explanation:**
It involves changing data before , or as it is entered into the computer or in
other words , it refers to the alteration of the existing data. The other answers are incorrect because :
Salami techniques : A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed.

Trojan horses: A Trojan Horse is a program that is disguised as another program. Viruses:A Virus is a small application , or a string of code , that infects applications.
Reference: Shon Harris , AIO v3
Chapter - 11: Application and System Development, Page : 875-880 Chapter - 10: Law, Investigation and Ethics , Page : 758-759

**NEW QUESTION 101**
- (Topic 1)
Which access control model would a lattice-based access control model be an example of?

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

**Answer:** A

**Explanation:**
In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access
files.
TIPS FROM CLEMENT
Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.
Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:
FIRST: The Lattice
A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.
SECOND: DAC (Discretionary Access Control)
Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.
THIRD: MAC (Mandatory Access Control)
All of the following are forms of Mandatory Access Control: Mandatory Access control (MAC) (Implemented using the lattice)
You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity leval and the categories the object belongs to. The categories are used to implement the Need to Know.
All of the following are forms of Non Discretionary Access Control:
Role Based Access Control (RBAC)
Rule Based Access Control (Think Firewall in this case)
The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.
I hope this clarifies the whole drama related to what is what in the world of access control. In the same line of taught, you should be familiar with the difference between Explicit
permission (the user has his own profile) versus Implicit (the user inherit permissions by
being a member of a role for example).
The following answers are incorrect:
Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the users. It is identity based access control only. It does not make use of a lattice.
Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC.
Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.
References:
AIOv3 Access Control (pages 161 - 168)
AIOv3 Security Models and Architecture (pages 291 - 293)

**NEW QUESTION 102**
- (Topic 1)
Which access model is most appropriate for companies with a high employee turnover?

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

**Answer:** A

**Explanation:**
The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company.
Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitely inherit the permissions of the role or roles they have been assigned to. When they leave the company or change jobs, their role assignment is revoked/changed appropriately.
Mandatory access control is incorrect. While controlling access based on the clearence level of employees and the sensitivity of obects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees

constantly leaving or joining the company.
Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324- 325.
Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.
References
Alll in One, third edition page 165
RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

**NEW QUESTION 104**
- (Topic 1)
Which security model introduces access to objects only through programs?

A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model

**Answer:** C

**Explanation:**
In the Clark-Wilson model, the subject no longer has direct access to objects but instead must access them through programs (well -formed transactions).
The Clark?CWilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.
The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.
Clark?CWilson is more clearly applicable to business and industry processes in which the integrity of the information content is paramount at any level of classification.
Integrity goals of Clark?CWilson model:
Prevent unauthorized users from making modification (Only this one is addressed by the Biba model).
Separation of duties prevents authorized users from making improper modifications. Well formed transactions: maintain internal and external consistency i.e. it is a series of operations that are carried out to transfer the data from one consistent state to the other.
The following are incorrect answers:
The Biba model is incorrect. The Biba model is concerned with integrity and controls access to objects based on a comparison of the security level of the subject to that of the object.
The Bell-LaPdaula model is incorrect. The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearence level of the subject to the classification level of the object.
The information flow model is incorrect. The information flow model uses a lattice where objects are labelled with security classes and information can flow either upward or at the
same level. It is similar in framework to the Bell-LaPadula model. References:
ISC2 Official Study Guide, Pages 325 - 327 AIO3, pp. 284 - 287
AIOv4 Security Architecture and Design (pages 338 - 342) AIOv5 Security Architecture and Design (pages 341 - 344) Wikipedia at:
https://en.wikipedia.org/wiki/Clark-Wilson_model

**NEW QUESTION 105**
- (Topic 1)
What is a common problem when using vibration detection devices for perimeter control?

A. They are vulnerable to non-adversarial disturbances.
B. They can be defeated by electronic means.
C. Signal amplitude is affected by weather conditions.
D. They must be buried below the frost line.

**Answer:** A

**Explanation:**
Vibration sensors are similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.
Such sensors are proned to false positive. If there is a large truck with heavy equipment driving by it may trigger the sensor. The same with a storm with thunder and lighting, it may trigger the alarm even thou there are no adversarial threat or disturbance.
The following are incorrect answers: All of the other choices are incorrect. Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (pp. 495-496).
McGraw-Hill . Kindle Edition.

**NEW QUESTION 109**
- (Topic 1)
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes

**Answer:** A

**Explanation:**
The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.

Management monitoring of audit logs is a detective control and it would not prevent collusion.
Changing passwords regularly would not prevent such attack.
This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

**NEW QUESTION 111**
- (Topic 1)
Which of the following are not Remote Access concerns?

A. Justification for remote access
B. Auditing of activities
C. Regular review of access privileges
D. Access badges

**Answer:** D

**Explanation:**
Access badges are more relevant to physical security rather than remote access.
"Justification for remote access" is incorrect. Justification for remote access is a relevant concern.
"Auditing of activities" is incorrect. Auditing of activites is an imporant aspect to assure that malicious or unauthorized activities are not occuring.
"Regular review of access privileges" is incorrect. Regular review of remote accept privileges is an important management responsibility.
References:
AIO3, pp. 547 - 548

**NEW QUESTION 113**
- (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 118**
- (Topic 1)
In Discretionary Access Control the subject has authority, within certain limitations,

A. but he is not permitted to specify what objects can be accessible and so we need to get an independent third party to specify what objects can be accessible.
B. to specify what objects can be accessible.
C. to specify on a aggregate basis without understanding what objects can be accessible.
D. to specify in full detail what objects can be accessible.

**Answer:** B

**Explanation:**
With Discretionary Access Control, the subject has authority, within certain limitations, to specify what objects can be accessible.
For example, access control lists can be used. This type of access control is used in local, dynamic situations where the subjects must have the discretion to specify what resources certain users are permitted to access.
When a user, within certain limitations, has the right to alter the access control to certain objects, this is termed as user-directed discretionary access control. In some instances, a hybrid approach is used, which combines the features of user-based and identity-based discretionary access control.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.
and
HARRIS, Shon, All-In-One CISSP Certification Exam Guide 5th Edition, McGraw- Hill/Osborne, 2010, Chapter 4: Access Control (page 210-211).

**NEW QUESTION 123**
- (Topic 1)
Passwords can be required to change monthly, quarterly, or at other intervals:

A. depending on the criticality of the information needing protection
B. depending on the criticality of the information needing protection and the password's frequency of use
C. depending on the password's frequency of use
D. not depending on the criticality of the information needing protection but depending on the password's frequency of use

**Answer:** B

**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.
Source: 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 126**
- (Topic 2)
Which of the following is BEST defined as a physical control?

A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms

**Answer:** B

**Explanation:**
Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
The following answers are incorrect answers:
Monitoring of system activity is considered to be administrative control.
Identification and authentication methods are considered to be a technical control. Logical access control mechanisms is also considered to be a technical control.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 1280-1282). McGraw-Hill. Kindle Edition.

**NEW QUESTION 128**
- (Topic 2)
Which of the following should NOT be performed by an operator?

A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow

**Answer:** C

**Explanation:**
Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.
System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system??s security policy. As such, use of these
privileges should be monitored through audit logs.
Some of the privileges and responsibilities assigned to operators include:
Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.
Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.
Volume mounting: This allows the desired application access to the system and its data. Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow
an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation
of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.
Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.
Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.
Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.
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 19367-19395). Auerbach Publications. Kindle Edition.

**NEW QUESTION 132**
- (Topic 2)
Which software development model is actually a meta-model that incorporates a number of the software development models?

A. The Waterfall model
B. The modified Waterfall model
C. The Spiral model
D. The Critical Path Model (CPM)

**Answer:** C

**Explanation:**
The spiral model is actually a meta-model that incorporates a number of the software development models. This model depicts a spiral that incorporates the various phases of software development. The model states that each cycle of the spiral involves the same series of steps for each part of the project. CPM refers to the Critical Path Methodology.
Source: 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 246).

**NEW QUESTION 134**

- (Topic 2)
During which phase of an IT system life cycle are security requirements developed?

A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation

**Answer:** C

**Explanation:**
The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.
The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:
This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:
• Conduct the risk assessment and use the results to supplement the baseline security controls;
• Analyze security requirements;
• Perform functional and security testing;
• Prepare initial documents for system certification and accreditation; and
• Design security architecture.
Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.
Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:
Project initiation
Functional design analysis and planning System design specifications
Software development Installation Maintenance support
Revision and replacement
According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.
SDLC POSITIONING FROM NIST 800-64

C:\Users\MCS\Desktop\1.jpg
SDLC Positioning in the enterprise
Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency??s vital business operations, their supporting assets, and existing interdependencies and relationships.
With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program??s cost-effective performance as well as articulate its business impact and value to the agency.
SDLC OVERVIEW FROM NIST 800-64
SDLC Overview from NIST 800-64 Revision 2

C:\Users\MCS\Desktop\1.jpg
NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at:
http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned.
People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development

Life Cycle has slightly different names, the activities mostly remains the same.
NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.
Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:
The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.
At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.
By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.
NIST says:
NIST`s Information Technology Laboratory recently issued Special Publication (SP) 800- 64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.
I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956
and
NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf and
http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc- system-development

**NEW QUESTION 139**
- (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 140**
- (Topic 2)
Which of the following are NOT a countermeasure to traffic analysis?

A. Padding messages.
B. Eavesdropping.
C. Sending noise.
D. Faraday Cage

**Answer:** B

**Explanation:**
Eavesdropping is not a countermeasure, it is a type of attack where you are collecting traffic and attempting to see what is being send between entities communicating with each other.
The following answers are incorrect:
Padding Messages. Is incorrect because it is considered a countermeasure you make messages uniform size, padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover patterns.
Sending Noise. Is incorrect because it is considered a countermeasure, tansmitting non- informational data elements to disguise real data.
Faraday Cage Is incorrect because it is a tool used to prevent emanation of electromagnetic waves. It is a very effective tool to prevent traffic analysis.

**NEW QUESTION 143**
- (Topic 2)
What can best be described as an abstract machine which must mediate all access to subjects to objects?

A. A security domain
B. The reference monitor
C. The security kernel
D. The security perimeter

**Answer:** B

**Explanation:**
The reference monitor is an abstract machine which must mediate all access to subjects to objects, be protected from modification, be verifiable as correct, and is always invoked. The security kernel is the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. The security perimeter includes the security kernel as well as other security-related system functions that are within the boundary of the trusted computing base. System elements that are outside of the security perimeter need not be trusted. A security domain is a domain of trust that shares a single security policy and single management.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

**NEW QUESTION 145**
- (Topic 2)
In what way could Java applets pose a security threat?

A. Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP
B. Java interpreters do not provide the ability to limit system access that an applet could have on a client system.
C. Executables from the Internet may attempt an intentional attack when they are downloaded on a client system.
D. Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.

**Answer:** C

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

**NEW QUESTION 150**
- (Topic 2)
Making sure that the data is accessible when and where it is needed is which of the following?

A. confidentiality
B. integrity
C. acceptability
D. availability

**Answer:** D

**Explanation:**
Availability is making sure that the data is accessible when and where it is needed.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

**NEW QUESTION 153**
- (Topic 2)
Within the context of the CBK, which of the following provides a MINIMUM level of security ACCEPTABLE for an environment ?

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

**Answer:** A

**Explanation:**
Baselines provide the minimum level of security necessary throughout the organization.
Standards specify how hardware and software products should be used throughout the organization.
Procedures are detailed step-by-step instruction on how to achieve certain tasks. Guidelines are recommendation actions and operational guides to personnel when a
specific standard does not apply.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 3: Security Management Practices (page 94).

**NEW QUESTION 155**
- (Topic 2)
Which of the following is responsible for MOST of the security issues?

A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure

**Answer:** C

**Explanation:**
Personnel cause more security issues than hacker attacks, outside espionage, or equipment failure.
The following answers are incorrect because:
Outside espionage is incorrect as it is not the best answer. Hackers is also incorrect as it is not the best answer. Equipment failure is also incorrect as it is not the best answer.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 56

**NEW QUESTION 159**
- (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 160**
- (Topic 2)
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)

**NEW QUESTION 162**
- (Topic 2)
A 'Pseudo flaw' is which of the following?

A. An apparent loophole deliberately implanted in an operating system program as a trap for intruders.
B. An omission when generating Psuedo-code.
C. Used for testing for bounds violations in application programming.
D. A normally generated page fault causing the system to halt.

**Answer:** A

**Explanation:**
A Pseudo flaw is something that looks like it is vulnerable to attack, but really acts as an alarm or triggers automatic actions when an intruder attempts to exploit the flaw.
The following answers are incorrect:
An omission when generating Psuedo-code. Is incorrect because it is a distractor. Used for testing for bounds violations in application programming. Is incorrect, this is a testing methodology.
A normally generated page fault causing the system to halt. This is incorrect because it is distractor.

**NEW QUESTION 164**
- (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 165**
- (Topic 2)
It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?

A. security administrator
B. security analyst
C. systems auditor
D. systems programmer

**Answer:** D

**Explanation:**
Reason: The security administrator, security analysis, and the system auditor need access to portions of the security systems to accomplish their jobs. The system programmer does not need access to the working (AKA: Production) security systems.
Programmers should not be allowed to have ongoing direct access to computers running production systems (systems used by the organization to operate its business). To maintain system integrity, any changes they make to production systems should be tracked by the organization??s change management control system.
Because the security administrator??s job is to perform security functions, the performance of non-security tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users abusing their authority by taking actions outside of their assigned functional responsibilities.

References:
OFFICIAL (ISC)2® GUIDE TO THE CISSP® EXAM (2003), Hansche, S., Berti, J., Hare,
H., Auerbach Publication, FL, Chapter 5 - Operations Security, section 5.3,??Security Technology and Tools,?? Personnel section (page 32).
KRUTZ, R. & VINES, R. The CISSP Prep Guide: Gold Edition (2003), Wiley Publishing Inc., Chapter 6: Operations Security, Separations of Duties (page 303).

**NEW QUESTION 167**
- (Topic 2)
A Security Kernel is defined as a strict implementation of a reference monitor mechanism responsible for enforcing a security policy. To be secure, the kernel must meet three basic conditions, what are they?

A. Confidentiality, Integrity, and Availability
B. Policy, mechanism, and assurance
C. Isolation, layering, and abstraction
D. Completeness, Isolation, and Verifiability

**Answer:** D

**Explanation:**
A security kernel is responsible for enforcing a security policy. It is a strict implementation of a reference monitor mechanism. The architecture of a kernel operating system is typically layered, and the kernel should be at the lowest and most primitive level.
It is a small portion of the operating system through which all references to information and all changes to authorizations must pass. In theory, the kernel implements access control and information flow control between implemented objects according to the security policy.
To be secure, the kernel must meet three basic conditions: completeness (all accesses to information must go through the kernel),
isolation (the kernel itself must be protected from any type of unauthorized access),
and verifiability (the kernel must be proven to meet design specifications).
The reference monitor, as noted previously, is an abstraction, but there may be a reference validator, which usually runs inside the security kernel and is responsible for performing security access checks on objects, manipulating privileges, and generating any resulting security audit messages.
A term associated with security kernels and the reference monitor is the trusted computing base (TCB). The TCB is the portion of a computer system that contains all elements of the system responsible for supporting the security policy and the isolation of objects. The security capabilities of products for use in the TCB can be verified through various evaluation criteria, such as the earlier Trusted Computer System Evaluation Criteria (TCSEC) and the current Common Criteria standard.
Many of these security terms??reference monitor, security kernel, TCB??are defined loosely by vendors for purposes of marketing literature. Thus, it is necessary for security professionals to read the small print and between the lines to fully understand what the vendor is offering in regard to security features.
TIP FOR THE EXAM:
The terms Security Kernel and Reference monitor are synonymous but at different levels. As it was explained by Diego:
While the Reference monitor is the concept, the Security kernel is the implementation of such concept (via hardware, software and firmware means).
The two terms are the same thing, but on different levels: one is conceptual, one is "technical"
The following are incorrect answers: Confidentiality, Integrity, and Availability Policy, mechanism, and assurance Isolation, layering, and abstraction
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 13858-13875). Auerbach Publications. Kindle Edition.

**NEW QUESTION 170**
- (Topic 2)
What can best be described as a domain of trust that shares a single security policy and single management?

A. The reference monitor
B. A security domain
C. The security kernel
D. The security perimeter

**Answer:** B

**Explanation:**
A security domain is a domain of trust that shares a single security policy and single management.
The term security domain just builds upon the definition of domain by adding the fact that resources within this logical structure (domain) are working under the same security policy and managed by the same group.
So, a network administrator may put all of the accounting personnel, computers, and network resources in Domain 1 and all of the management personnel, computers, and network resources in Domain 2. These items fall into these individual containers because they not only carry out similar types of business functions, but also, and more importantly, have the same type of trust level. It is this common trust level that allows entities to be managed by one single security policy.
The different domains are separated by logical boundaries, such as firewalls with ACLs, directory services making access decisions, and objects that have their own ACLs indicating which individuals and groups can carry out operations on them.
All of these security mechanisms are examples of components that enforce the security policy for each domain. Domains can be architected in a hierarchical manner that dictates the relationship between the different domains and the ways in which subjects within the different domains can communicate. Subjects can access resources in domains of equal or
lower trust levels.
The following are incorrect answers:
The reference monitor is an abstract machine which must mediate all access to subjects to objects, be protected from modification, be verifiable as correct, and is always invoked. Concept that defines a set of design requirements of a reference validation mechanism (security kernel), which enforces an access control policy over subjects?? (processes, users) ability to perform operations (read, write, execute) on objects (files, resources) on a system. The reference monitor components must be small enough to test properly and be tamperproof.
The security kernel is the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept.
The security perimeter includes the security kernel as well as other security-related system functions that are within the boundary of the trusted computing base. System elements that are outside of the security perimeter need not be trusted. not every process and resource falls within the TCB, so some of these components fall outside of an imaginary boundary referred to as the security perimeter. A security perimeter is a boundary that divides the trusted from the untrusted. For the system to stay in a secure and trusted state, precise communication standards must be developed to ensure that when a component within the TCB needs to communicate with a component outside the TCB, the communication cannot expose the system to unexpected security compromises. This type of communication is handled and controlled through interfaces.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 28548-28550). McGraw-Hill. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 7873-7877). McGraw-Hill. Kindle Edition.

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition , Access Control, Page 214-217
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1280-1283). . Kindle Edition.
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
AIO 6th edition chapter 3 access control page 214-217 defines Security domains. Reference monitor, Security Kernel, and Security Parameter are defined in Chapter 4, Security Architecture and Design.

**NEW QUESTION 172**
- (Topic 2)
Which of the following best describes the purpose of debugging programs?

A. To generate random data that can be used to test programs before implementing them.
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.
D. To compare source code versions before transferring to the test environment

**Answer:** B

**Explanation:**
Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production.
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 298).

**NEW QUESTION 175**
- (Topic 2)
A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?

A. Covert channel
B. Overt channel
C. Opened channel
D. Closed channel

**Answer:** B

**Explanation:**
An overt channel is a path within a computer system or network that is designed for the authorized transfer of data. The opposite would be a covert channel which is an unauthorized path.
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.
All of the other choices are bogus detractors. 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 219. and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 380 and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 378). McGraw- Hill. Kindle Edition.

**NEW QUESTION 179**
- (Topic 2)
One of these statements about the key elements of a good configuration process is NOT true

A. Accommodate the reuse of proven standards and best practices
B. Ensure that all requirements remain clear, concise, and valid
C. Control modifications to system hardware in order to prevent resource changes
D. Ensure changes, standards, and requirements are communicated promptly and precisely

**Answer:** C

**Explanation:**
Configuration management isn't about preventing change but ensuring the integrity of IT resources by preventing unauthorised or improper changes.
According to the Official ISC2 guide to the CISSP exam, a good CM process is one that can:
(1) accommodate change;
(2) accommodate the reuse of proven standards and best practices;
(3) ensure that all requirements remain clear, concise, and valid;
(4) ensure changes, standards, and requirements are communicated promptly and precisely; and
(5) ensure that the results conform to each instance of the product.
Configuration management
Configuration management (CM) is the detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Special configuration management software is available. When a system needs a hardware or software upgrade, a computer technician can accesses the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.
An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems
Configuration management is also used in software development, where it is called Unified Configuration Management (UCM). Using UCM, developers can keep track of the source code, documentation, problems, changes requested, and changes made.
Change management
In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operating system release is running on each computer and which fixes have been applied).

**NEW QUESTION 183**

.....

# Relate Links

**100% Pass Your SSCP Exam with Exambible Prep Materials**

https://www.exambible.com/SSCP-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/