

344).

QUESTION 91

Which of the following access control techniques best gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure?

- A. Access control lists
- B. Discretionary access control
- C. Role-based access control
- D. Non-mandatory access control

Correct Answer: C

Explanation:

Role-based access control (RBAC) gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are given to users in that role. An access control list (ACL) is a table that tells a system which access rights each user has to a particular system object. With discretionary access control, administration is decentralized and owners of resources control other users' access. Non-mandatory access control is not a defined access control technique.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 9).

QUESTION 92

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 an aggregate basis without understanding what objects can be accessible.
- D. to specify in full detail what objects can be accessible.

Correct 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.

HARRIS, Shon, All-In-One CISSP Certification Exam Guide 5th Edition, McGraw-Hill/Osborne, 2010, Chapter 4: Access Control (page 210-211).

QUESTION 93

Controlling access to information systems and associated networks is necessary for the preservation of their:

- A. Authenticity, confidentiality and availability
- B. Confidentiality, integrity, and availability.
- C. integrity and availability.
- D. authenticity, confidentiality, integrity and availability.

Correct Answer: B

Explanation:

Controlling access to information systems and associated networks is necessary for the preservation of their confidentiality, integrity and availability.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

QUESTION 94

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

Correct Answer: A

Explanation:

The Correct 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.

QUESTION 95

Which of the following statements pertaining to RADIUS is incorrect:

- A. A RADIUS server can act as a proxy server, forwarding client requests to other authentication domains.
- B. Most of RADIUS clients have a capability to query secondary RADIUS servers for redundancy.
- C. Most RADIUS servers have built-in database connectivity for billing and reporting purposes.
- D. Most RADIUS servers can work with DIAMETER servers.

Correct Answer: D

Explanation:

This is the correct answer because it is FALSE.

Diameter is an AAA protocol, AAA stands for authentication, authorization and accounting protocol for computer networks, and it is a successor to RADIUS.

The name is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius).

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

The main differences are as follows:

Reliable transport protocols (TCP or SCTP, not UDP) The IETF is in the process of standardizing TCP Transport for RADIUS Network or transport layer security (IPsec or TLS)

The IETF is in the process of standardizing Transport Layer Security for RADIUS Transition support for RADIUS, although Diameter is not fully compatible with RADIUS Larger address space for attribute-value pairs (AVPs) and identifiers (32 bits instead of 8 bits)

Client-server protocol, with exception of supporting some server-initiated messages as well Both stateful and stateless models can be used

Dynamic discovery of peers (using DNS SRV and NAPTR) Capability negotiation

Supports application layer acknowledgements, defines failover methods and state machines (RFC 3539)

Error notification

Better roaming support

More easily extended; new commands and attributes can be defined Aligned on 32-bit boundaries

Basic support for user-sessions and accounting

A Diameter Application is not a software application, but a protocol based on the Diameter base protocol (defined in RFC 3588). Each application is defined by an application identifier and can add new command codes and/or new mandatory AVPs. Adding a new optional AVP does not require a new application.

Examples of Diameter applications:

Diameter Mobile IPv4 Application (MobileIP, RFC 4004) Diameter Network Access Server Application (NASREQ, RFC 4005) Diameter Extensible Authentication Protocol (EAP) Application (RFC 4072) Diameter Credit-Control Application (DCCA, RFC 4006) Diameter Session Initiation Protocol Application (RFC 4740) Various applications in the 3GPP IP Multimedia Subsystem

All of the other choices presented are true. So Diameter is backward compatible with Radius (to some extent) but the opposite is false.

Reference(s) used for this question:

TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 38.

https://secure.wikimedia.org/wikipedia/en/wiki/Diameter_%28protocol%29

QUESTION 96

The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:

- A. 100 subjects per minute.
- B. 25 subjects per minute.
- C. 10 subjects per minute.
- D. 50 subjects per minute.

Correct Answer: C

Explanation:

The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system.

Acceptable throughput rates are in the range of 10 subjects per minute.

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

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

Things that may impact the throughput rate for some types of biometric systems may include:

A concern with retina scanning systems may be the exchange of body fluids on the eyepiece.

Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

QUESTION 97

Who first described the DoD multilevel military security policy in abstract, formal terms?

- A. David Bell and Leonard LaPadula
- B. Rivest, Shamir and Adleman
- C. Whitfield Diffie and Martin Hellman
- D. David Clark and David Wilson

Correct Answer: A

Explanation:

It was David Bell and Leonard LaPadula who, in 1973, first described the DoD multilevel military security policy in abstract, formal terms. The Bell-LaPadula is a Mandatory Access Control (MAC) model concerned with confidentiality. Rivest, Shamir and Adleman (RSA) developed the RSA encryption algorithm. Whitfield Diffie and Martin Hellman published the Diffie-Hellman key agreement algorithm in 1976. David Clark and David Wilson developed the Clark-Wilson integrity model, more appropriate for security in commercial activities.

Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (pages 78,109).

QUESTION 98

Which of the following is not a preventive login control?

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

Correct 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).

QUESTION 99

What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

- A. A
- B. D
- C. E

D. F

Correct Answer: B

Explanation:

D or "minimal protection" is reserved for systems that were evaluated under the TCSEC but did not meet the requirements for a higher trust level.

A is incorrect. A or "Verified Protection" is the highest trust level under the TCSEC. E is incorrect. The trust levels are A - D so "E" is not a valid trust level. F is incorrect. The trust levels are A - D so "F" is not a valid trust level.

CBK, pp. 329 - 330

AIO3, pp. 302 - 306

QUESTION 100

Identification and authentication are the keystones of most access control systems. Identification establishes:

- A. User accountability for the actions on the system.
- B. Top management accountability for the actions on the system.
- C. EDP department accountability for the actions of users on the system.
- D. Authentication for actions on the system

Correct Answer: A

Explanation:

Identification and authentication are the keystones of most access control systems. Identification establishes user accountability for the actions on the system.

The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three general factors can be used for authentication: something a person knows, something a person has, and something a person is. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.

For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting. Once these steps are completed successfully, the user can access and use network resources; however, it is necessary to track the user's activities and enforce accountability for his actions.

Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token.

These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are