

SSCP^{Q&As}

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/sscp.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Which of the following is NOT a common integrity goal?

- A. Prevent unauthorized users from making modifications.
- B. Maintain internal and external consistency.
- C. Prevent authorized users from making improper modifications.
- D. Prevent paths that could lead to inappropriate disclosure.

Correct Answer: D

Inappropriate disclosure is a confidentiality, not an integrity goal.

All of the other choices above are integrity goals addressed by the Clark-Wilson integrity model.

The Clark-Wilson model is an integrity model that addresses all three integrity goals:

1.
prevent unauthorized users from making modifications,
2.
prevent authorized users from making improper modifications, and
3.
maintain internal and external consistency through auditing. NOTE: Biba address only the first goal of integrity above

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One uide, 6th Edition (p. 1384). McGraw-Hill. Kindle Edition.

QUESTION 2

Which of the following can be defined as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client?

- A. IMAP4
- B. SMTP
- C. MIME
- D. PEM

Correct Answer: A

RFC 2828 (Internet Security Glossary) defines the Internet Message Access Protocol, version 4 (IMAP4) as an Internet

protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client. IMAP4 has mechanisms for optionally authenticating a client to a server and providing other security services. MIME is the MultiPurpose Internet Mail Extension. MIME extends the format of Internet mail to allow non-US-ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers. Simple Mail Transfer Protocol (SMTP) is a TCP-based, application-layer, Internet Standard protocol for moving electronic mail messages from one computer to another. Privacy Enhanced Mail (PEM) is an Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 3

Which of the following keys has the SHORTEST lifespan?

- A. Secret key
- B. Public key
- C. Session key
- D. Private key

Correct Answer: C

As session key is a symmetric key that is used to encrypt messages between two users. A session key is only good for one communication session between users.

For example , If Tanya has a symmetric key that she uses to encrypt messages between Lance and herself all the time , then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using encryption. However , using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If , on the other hand , a new symmetric key were generated each time Lance and Tanya wanted to communicate , it would be used only during their dialog and then destroyed. if they wanted to communicate

and hour later , a new session key would be created and shared.

The other answers are not correct because :

Public Key can be known to anyone.

Private Key must be known and used only by the owner.

Secret Keys are also called as Symmetric Keys, because this type of encryption relies on each user to keep the key a secret and properly protected.

REFERENCES:

SHON HARRIS , ALL IN ONE THIRD EDITION : Chapter 8 : Cryptography , Page : 619-620

QUESTION 4

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

Correct Answer: B

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. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Pages 5-6.

in process of correction

QUESTION 5

Which of the following is NOT a factor related to Access Control?

- A. integrity
- B. authenticity
- C. confidentiality
- D. availability

Correct Answer: B

These factors cover the integrity, confidentiality, and availability components of information system security.

Integrity is important in access control as it relates to ensuring only authorized subjects can make changes to objects.

Authenticity is different from authentication. Authenticity pertains to something being authentic, not

necessarily having a direct correlation to access control.

Confidentiality is pertinent to access control in that the access to sensitive information is controlled to protect confidentiality.

availability is protected by access controls in that if an attacker attempts to disrupt availability they would first need access.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 49.

[SSCP PDF Dumps](#)

[SSCP Study Guide](#)

[SSCP Exam Questions](#)