



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.passapply.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

What is the primary role of smartcards in a PKI?

- A. Transparent renewal of user keys
- B. Easy distribution of the certificates between the users
- C. Fast hardware encryption of the raw data
- D. Tamper resistant, mobile storage and application of private keys of the users

Correct Answer: D

Reference: HARRIS, Shon, All-In-One CISSP Certification uide, 2001, McGraw- Hill/Osborne, page 139;

SNYDER, J., What is a SMART CARD?.

Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance

Security

Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures. Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.

It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:

physical attack of various forms (microprobing, drills, files, solvents, etc.)

freezing the device

applying out-of-spec voltages or power surges

applying unusual clock signals

inducing software errors using radiation

measuring the precise time and power requirements of certain operations (see power analysis)

Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of-specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.

Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.



QUESTION 2

Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at which layer of the OSI model?

- A. Application Layer.
- B. Transport Layer.
- C. Session Layer.
- D. Network Layer.

Correct Answer: A

The Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at the Application Layer of the Open Systems Interconnect (OSI) model.

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 89.

QUESTION 3

Which of the following rules is least likely to support the concept of least privilege?

- A. The number of administrative accounts should be kept to a minimum.
- B. Administrators should use regular accounts when performing routine operations like reading mail.
- C. Permissions on tools that are likely to be used by hackers should be as restrictive as possible.
- D. Only data to and from critical systems and applications should be allowed through the firewall.

Correct Answer: D

Only data to and from critical systems and applications should be allowed through the firewall is a detractor. Critical systems or applications do not necessarily need to have traffic go through a firewall. Even if they did, only the minimum required services should be allowed. Systems that are not deemed critical may also need to have traffic go through the firewall.

Least privilege is a basic tenet of computer security that means users should be given only those rights required to do their jobs or tasks. Least privilege is ensuring that you have the minimum privileges necessary to do a task. An admin NOT using his admin account to check email is a clear example of this.

Reference(s) used for this question:

National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 9.

QUESTION 4



In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

- A. Both client and server
- B. The client's browser
- C. The web server
- D. The merchant's Certificate Server

Correct Answer: B

Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client.

Source: ANDRESS, Mandy, ram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112).

Also: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2001, page 569.

QUESTION 5

Which of the following statements regarding an off-site information processing facility is TRUE?

- A. It should have the same amount of physical access restrictions as the primary processing site.
- B. It should be located in proximity to the originating site so that it can quickly be made operational.
- C. It should be easily identified from the outside so in the event of an emergency it can be easily found.
- D. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Correct Answer: A

It is very important that the offsite has the same restrictions in order to avoid misuse.

The following answers are incorrect because:

It should be located in proximity to the originating site so that it can quickly be made operational is incorrect as the offsite is also subject to the same disaster as of the primary site.

It should be easily identified from the outside so in the event of an emergency it can be easily found is also incorrect as it should not be easily identified to prevent intentional sabotage.

Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive is also incorrect as it should be like its primary site.

Reference : Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 265).



VCE & PDF

PassApply.com

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

2024 Latest passapply SSCP PDF and VCE dumps Download

[SSCP PDF Dumps](#)

[SSCP VCE Dumps](#)

[SSCP Study Guide](#)