SSCP$^{Q\&As}$

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

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

QUESTION 1

Which of the following does NOT concern itself with key management?

A. Internet Security Association Key Management Protocol (ISAKMP)

B. Diffie-Hellman (DH)

C. Cryptology (CRYPTO)

D. Key Exchange Algorithm (KEA)

Correct Answer: C

Cryptology is the science that includes both cryptography and cryptanalysis and is not directly concerned with key management. Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.

The following are all concerned with Key Management which makes them the wrong choices:

Internet Security Association Key Management Protocol (ISAKMP) is a key management protocol used by IPSec. ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange. The actual key exchange is done by the Oakley Key Determination Protocol which is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.

Diffie-Hellman and one variation of the Diffie-Hellman algorithm called the Key Exchange Algorithm (KEA) are also key exchange protocols. Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. DiffieHellman key exchange (DH) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Reference(s) used for this question:

Mike Meyers CISSP Certification Passport, by Shon Harris and Mike Meyers, page 228.

It is highlighted as an EXAM TIP. Which tells you that it is a must know for the purpose of the exam.

HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, Fifth Edition, Chapter

8: Cryptography (page 713-715).

and

https://en.wikipedia.org/wiki/ISAKMP

and

http://searchsecurity.techtarget.com/definition/cryptology

QUESTION 2

The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit is called:

A. alteration

B. investigation

C. entrapment

D. enticement.

Correct Answer: D

Enticement deals with someone that is breaking the law. Entrapment encourages someone to commit a crime that the individual may or many have had no intention of committing. Enticement is not necessarily illegal but does raise ethical arguments and may not be admissible in court. Enticement lures someone toward some evidence (a honeypot would be a great example) after that individual has already committed a crime.

Entrapment is when you persuade someone to commit a crime when the person otherwise had no intention to commit a crime. Entrapment is committed by a law enforcement player where you get tricked into committing a crime for which you woud later on get arrested without knowing you rare committing such a scrime. It is illegal and unethical as well.

All other choices were not applicable and only detractors.

References:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

and

CISSP Study Guide (Conrad, Misenar, Feldman). Elsevier. 2010. p. 428

and http://www.dummies.com/how-to/content/security-certification-computer-forensics-and- inci.html

QUESTION 3

Which of the following statements is true about data encryption as a method of protecting data?

A. It should sometimes be used for password files

B. It is usually easily administered

C. It makes few demands on system resources

D. It requires careful key management

Correct Answer: D

In cryptography, you always assume the "bad guy" has the encryption algorithm (indeed, many algorithms such as DES, Triple DES, AES, etc. are public domain). What the bad guy lacks is the key used to complete that algorithm and encrypt/decrypt information. Therefore, protection of the key, controlled distribution, scheduled key change, timely destruction, and several other factors require careful consideration. All of these factors are covered under the umbrella term of "key management".

Another significant consideration is the case of "data encryption as a method of protecting data" as the question states. If that data is to be stored over a long period of time (such as on backup), you must ensure that your key management scheme stores old keys for as long as they will be needed to decrypt the information they encrypted.

The other answers are not correct because:

"It should sometimes be used for password files." - Encryption is often used to encrypt passwords stored within password files, but it is not typically effective for the password file itself. On most systems, if a user cannot access the contents of a password file, they cannot authenticate. Encrypting the entire file prevents that access.

"It is usually easily administered." - Developments over the last several years have made cryptography significantly easier to manage and administer. But it remains a significant challenge. This is not a good answer.

"It makes few demands on system resources." - Cryptography is, essentially, a large complex mathematical algorithm. In order to encrypt and decrypt information, the system must perform this algorithm hundreds, thousands, or even millions/billions/trillions of times. This becomes system resource intensive, making this a very bad answer.

Reference:

Official ISC2 Guide page: 266 (poor explanation)

All in One Third Edition page: 657 (excellent explanation)

Key Management - Page 732, All in One Fourth Edition

QUESTION 4

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)

Correct Answer: C

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. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 7: Applications and Systems Development (page 246).

QUESTION 5

Which of the following is true about link encryption?

A. Each entity has a common key with the destination node.

B. Encrypted messages are only decrypted by the final node.

C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.

D. Only secure nodes are used in this type of transmission.

Correct Answer: C

In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.

Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re- encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised.

Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers.

In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (pp. 845-846). McGraw- Hill.

And:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 132).