PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Advanced Security Practitioner (CASP+)

CAS-004

TROY McMILLAN

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. What does the "value" portion of a key-value pair specify?
    a. The creation date of the item
    b. The sensitivity of the item
    c. The value of the item
    d. The location of the item

2. Which of the following is not a characteristic of virtualization?
    a. Reduced overall use of power in the data center
    b. Dynamic allocation of memory and CPU resources to the servers
    c. High availability
    d. High capital expenditures

3. Which of the following is not a component of blob storage?
    a. Storage account
    b. Container
    c. Blob
    d. Object

4. Before you installed your hypervisor, you installed an operating system. What type of hypervisor are you installing?
    a. Type 1
    b. Type 2
    c. Type 3
    d. Type 4

5. In what type of storage system is the data typically stored in a server as ordered and unordered flat files, ISAM, heaps, hash buckets, or B+ trees?
    a. Blob
    b. Block
    c. File
    d. Database

6. Which virtualization type is sometimes called operating system–level virtualization?

   a. Container-based

   b. Emulation

   c. Simulation

   d. Virtuation

7. Which of the following is a connection created directly between two virtual private clouds?

   a. VPN

   b. VPC peering

   c. Overlay

   d. TOTP

8. Which of the following changes the CPU instructions required for the architecture and executes them on another architecture successfully?

   a. Interpreter

   b. Manifest

   c. Emulator

   d. Hypervisor

9. A cloud access security broker is an example of which of the following?

   a. Firmware

   b. Middleware

   c. Ransomware

   d. Spyware

10. Which of the following cloud service models provides a complete software solution?

    a. IaaS

    b. PaaS

    c. SaaS

    d. SeCaaS

This chapter covers the following topics:

- **Privacy and Confidentiality Requirements:** This section covers issues related to ensuring the privacy of personal and other proprietary data types.
- **Integrity Requirements:** This section describes best practices for ensuring that unauthorized changes are not made to data.
- **Non-repudiation:** This section covers the purpose of and benefits provided by the cryptographic technique non-repudiation.
- **Compliance and Policy Requirements:** This section stresses the importance of aligning corporate policy with regulatory compliance.
- **Common Cryptography Use Cases:** This section discusses data at rest, data in transit, data in process/data in use, protection of web services, embedded systems, key escrow/management, mobile security, secure authentication, and smart cards.
- **Common PKI Use Cases:** This section discusses web services, email, code signing, federation, trust models, VPNs, and enterprise and security automation/orchestration.

This chapter covers CAS-004 Objective 1.7: Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.

One of the tools security professionals have used to accomplish the goals of the CIA triad is cryptography. In this chapter you'll learn how these technologies can be used in conjunction with a public key infrastructure (PKI) to satisfy those goals.

CHAPTER 7

Supporting Security Objectives and Requirements with Cryptography and Public Key Infrastructure (PKI)

Privacy and Confidentiality Requirements

Cryptography is one of the most complicated domains of the security knowledge base. Cryptography is a crucial factor in protecting data at rest, in transit, and in process/use. It is a science that involves either hiding data or making data unreadable by transforming it. In addition, cryptography provides message author assurance, source authentication, and delivery proof.

Cryptography concerns ***confidentiality***, integrity, and authentication but not availability. The CIA triad is a main security tenet that covers confidentiality, integrity, and availability, so cryptography covers two of the main tenets of the CIA triad. It helps prevent or detect the fraudulent insertion, deletion, and modification of data. Cryptography also provides non-repudiation by providing proof of origin.

Most organizations use multiple hardware devices to protect confidential data. These devices protect data by keeping external threats out of the network. In the event that one of an attacker's methods works and an organization's first line of defense is penetrated, data encryption ensures that confidential or private data will not be viewed.

The key benefits of encryption include

Key Topic

- **Power:** Encryption relies on global standards. The solutions are so large that they ensure an organization is fully compliant with security policies. Data encryption solutions are affordable and may provide even military-level security for any organization.
- **Transparency:** Efficient encryption allows normal business flow while crucial data is secured in the background, and it does so without the user being aware of what is going on.

- **Flexibility:** Encryption saves and protects any important data, whether it is stored on a computer, a removable drive, an email server, or a storage network. Moreover, it allows you to securely access your files from anyplace.

Integrity Requirements

Integrity, the second part of the CIA triad, ensures that data is protected from unauthorized modification or data corruption. The goal of integrity is to preserve the consistency of data. The opposite of integrity is corruption. Many individuals do not consider data integrity to be as important as data confidentiality. However, data modification or corruption can often be just as detrimental to an enterprise because the original data is lost. Examples of controls that improve integrity include digital signatures, checksums, and hashes. Organizations should include integrity requirements when classifying data types, as discussed in Chapter 4, "Securing the Enterprise Architecture by Implementing Data Security Techniques."

Non-repudiation

Non-repudiation is the assurance that a sender cannot deny an action. For example, in electronic communications, one party may deny having sent a contract, a document, or an email. Non-repudiation means putting measures in place to prevent a party from denying that it sent a message.

A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). You will learn about digital signatures later in this chapter.

NOTE Remember that non-repudiation is the assurance that something can't be denied by someone.

Compliance and Policy Requirements

Legal compliance is a vital part of any organization's security initiative. To ensure legal compliance, organizations must understand the laws that apply to their industry. Examples of industries that often have many federal, state, and local laws to consider include financial, healthcare, and industrial production. A few of the laws and regulations that must be considered by organizations are covered in Chapter 20, "Security Considerations Impacting Specific Sectors and Operational Technologies." The use of cryptography is often the key to ensuring compliance.

Common Cryptography Use Cases

As you may have gathered by now, cryptography can solve many of the issues we face with privacy and data security. In this section you'll learn about specific applications of cryptography.

Data at Rest

Data at rest refers to data that is stored physically in any digital form that is not active. This data can be stored in databases, data warehouses, files, archives, tapes, offsite backups, mobile devices, or any other storage medium. Data at rest is most often protected using data encryption algorithms.

Algorithms that are used in computer systems implement complex mathematical formulas when converting plaintext to ciphertext. The two main components of any encryption system are the key and the algorithm. In some encryption systems, the two communicating parties use the same key. In other encryption systems, the two communicating parties use different keys, but the keys are related.

Data in Transit

Transport encryption ensures that data is protected when it is transmitted over the Internet or another network. Transport encryption can protect ***data in transit*** against network sniffing attacks.

Security professionals should ensure that their data is protected in transit in addition to protecting data at rest. As an example, think of an enterprise that implements token and biometric authentication for all users, protected administrator accounts, transaction logging, full-disk encryption, server virtualization, port security, firewalls with ACLs, a NIPS, and secured access points. None of these solutions provides any protection for data in transport. Transport encryption would be necessary in this environment to protect data.

Data in Process/Data in Use

Data in process/data in use is data that is being accessed or manipulated in some way. Data manipulation includes editing data and compiling the data into reports. The main issues with data in process/use are to ensure that only authorized individuals have access to or can read the data and that only authorized changes to the data are allowed. Confidentiality can be provided by using privacy or screen filters to prevent unauthorized individuals from reading the data on a screen. It can also be provided by implementing a document shredding policy for all reports that contain PII, PHI, proprietary data, or other confidential information. Data integrity can be provided by implementing appropriate controls on the data and verifying the data