PEARSON IT CERTIFICATION

Save 10% on Exam Voucher
See Inside

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

CompTIA® Advanced Security Practitioner (CASP+) CAS-004 Cert Guide

ISBN-13: 978-0-13-734895-4

ISBN-10: 0-13-734895-9

Library of Congress Control Number: 2022933627

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Indexer
Tim Wright

Proofreader
Barbara Mack

Technical Editor
Chris Crayton

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

About the Author

Troy McMillan, CASP, is a product developer and technical editor for CyberVista as well as a full-time trainer. He became a professional trainer more than 20 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. His recent work includes

- Author of *CompTIA CySA+ CS0-002 Cert Guide* (Pearson IT Certification)
- Author of *CompTIA A+ Complete Review Guide* (Sybex)
- Author of *CompTIA Server + Study Guide* (Sybex)
- Contributing subject matter expert for *CCNA Cisco Certified Network Associate Certification Exam Preparation Guide* (Kaplan)
- Prep test question writer for *Network+ Study Guide* (Sybex)
- Technical editor for *Windows 7 Study Guide* (Sybex)
- Contributing author for *CCNA-Wireless Study Guide* (Sybex)
- Technical editor for *CCNA Study Guide*, *Revision 7* (Sybex)
- Author of *VCP VMware Certified Professional on vSphere 4 Review Guide: Exam VCP-410* and associated instructional materials (Sybex)
- Author of *Cisco Essentials* (Sybex)
- Co-author of *CISSP Cert Guide* (Pearson IT Certification)
- Prep test question writer for *CCNA Wireless 640-722* (Cisco Press)

He also has appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND 1; ICND 2; and Cloud+.

He now creates certification practice tests and study guides and online courses for Cybervista. Troy lives in Asheville, North Carolina, with his wife, Heike.

Managing the Impact of Emerging Technologies on Enterprise Security and Privacy

- **Nano Technology:** This section discusses the use of matter on atomic, molecular, and supramolecular scales for industrial purposes.
- **Deep Learning:** This section covers the implementation of machine learning (ML), including natural language processing and deep fakes.
- **Biometric Impersonation:** This section covers measurement and mitigation of targeted biometric impersonation.

This chapter covers CAS-004 Objective 1.8: Explain the impact of emerging technologies on enterprise security and privacy.

Security professionals must stay abreast of all the latest trends and emerging technologies, especially as they relate to security. In this chapter you'll learn about some of these technologies and concepts and how to manage their effects in enterprise security and privacy.

Artificial Intelligence

Artificial intelligence (AI) and ***machine learning (ML)*** have fascinated humans for decades. Since the first time we conceived of the idea of talking to a computer and getting an answer like characters did in comic books years ago, we have waited for the day to come when smart robots would not just do the dirty work but learn just as humans do.

Today, robots are taking on increasingly more and more detailed work. One of the exciting areas where AI and ML are yielding dividends is in intelligent network security—or intelligent networks. Intelligent networks seek out their own vulnerabilities before attackers do, learn from past errors, and work on a predictive model to prevent attacks.

For example, automatic exploit generation (AEG) is the "first end-to-end system for fully automatic exploit generation," according to the Carnegie Mellon

Institute's own description of its AI named Mayhem. Developed for off-the-shelf as well as the enterprise software being increasingly used in smart devices and appliances, AEG can find a bug and determine whether it is exploitable.

Machine Learning

Machine learning is what makes AI possible. It is the use of generated training data to build a model that makes predictions and decisions without being explicitly programmed to do so. For example, in the case of using AI to adapt to network threats, algorithms can identify unusual activity and match it with similar activity that led to an attack. thereby leading to an action designed to head off or mitigate such an attack.

Quantum Computing

Quantum computing is the use of quantum states, such as superposition and entanglement, to perform computation. These states are properties founded in quantum science. Quantum computing uses these properties to perform encryption and to solve extremely difficult mathematical equations. It is anticipated that the use of quantum computing will enhance the machine learning process.

Blockchain

Another implementation of cryptography is cryptocurrency, such as bitcoin. Cryptocurrencies make use of a process called blockchain. A ***blockchain*** is a continuously growing list of records, called blocks, that are linked and secured using cryptography. Blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. The blockchain process is depicted in Figure 8-1.

Key Topic

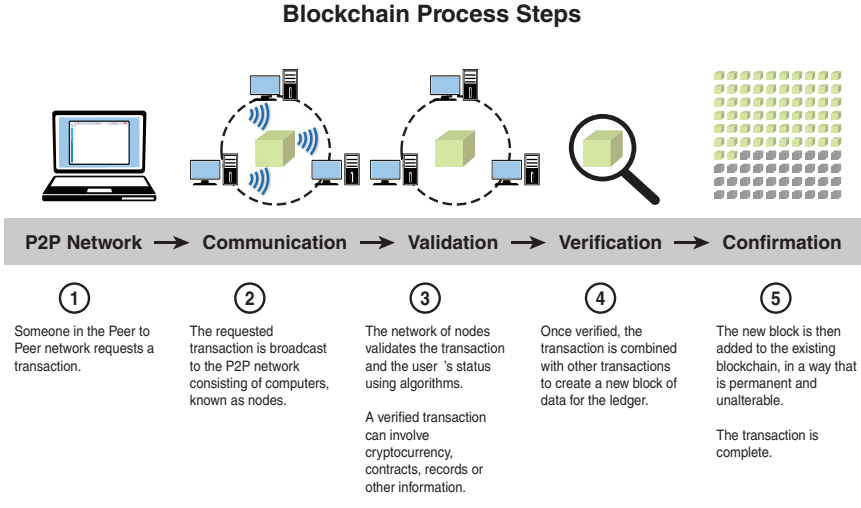

Figure 8-1 Blockchain

Homomorphic Encryption

Homomorphic encryption is a form of encryption that is unique in that it allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext. Its great value lies in the fact that privacy can be maintained because the data is never in a plaintext state, even though edits have been made. With other encryption processes, the data would be required to be decrypted to make the edits. In this section you'll learn about several operations that are possible using homomorphic encryption.

Secure Multiparty Computation

Private Information Retrieval

A ***private information retrieval (PIR)*** protocol can retrieve information from a server without revealing which item is retrieved. One of the ways to construct a protocol for private information retrieval is based on homomorphic encryption.

Secure Function Evaluation

Secure function evaluation (SFE) is a process in which multiple parties collectively compute a function and receive its output without learning the inputs from any other party. It allows for two parties to each contribute a value to a computation and generate the same answer without knowing the value the other party contributes. This can be done using fully homomorphic encryption.

Private Function Evaluation

Private function evaluation (PFE) is the process of evaluating one party's private data using a private function owned by another party. PFEs solutions seek to ensure that the privacy of the data and the function are both preserved. Existing solutions for PFE secure multiparty computations by hiding the circuit's topology and the gate's functionality through additive homomorphic encryption.

Distributed Consensus

Earlier in this chapter you learned about blockchain. One of the mechanisms of blockchain is distributed consensus. ***Distributed consensus*** is a process whereby distributed nodes reach agreement or consensus on the validity of transactions. Since blockchain lacks a central authority, distributed consensus provides a necessary function to the blockchain. Consensus algorithms ensure that the protocol rules are being followed and guarantee that all transactions occur in such a way that the coins

are only able to be spent once. Consider the diagram in Figure 8-2. When the failed node loses all data or transactions due to failure, the other nodes contribute what they know about what was contained in that node, and the information is used to restore the failed node.

Key Topic

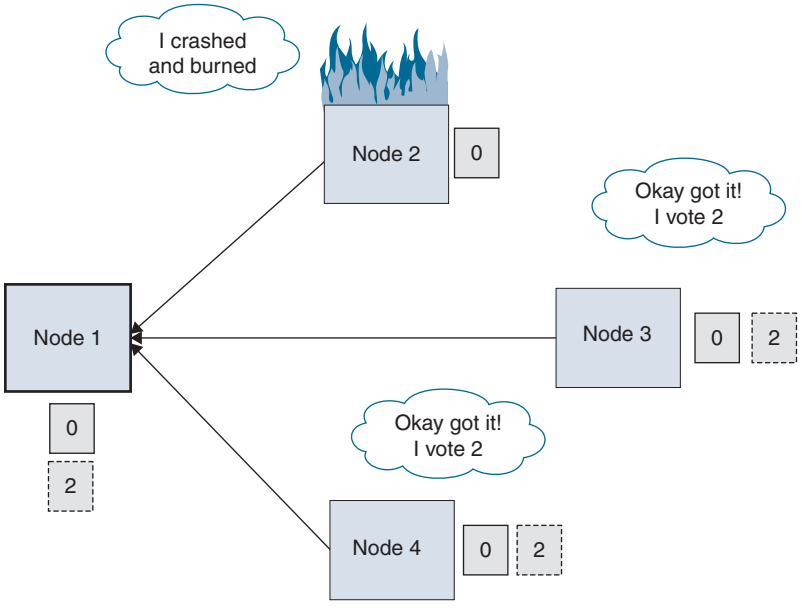

Figure 8-2 Distributed Consensus

Big Data

Big data is a term for sets of data so large or complex that they cannot be analyzed by using traditional data processing applications. Specialized applications have been designed to help organizations with their big data. The big data challenges that may be encountered include data analysis, data capture, data search, data sharing, data storage, and data privacy.

While big data is used to determine the causes of failures, generate coupons at checkout, recalculate risk portfolios, and find fraudulent activity before it ever has a chance to affect an organization, its existence creates security issues. The first issue is its unstructured nature. Traditional data warehouses process structured data and can store large amounts of it, but there is still a requirement for structure.

Big data typically uses Hadoop, which requires no structure. Hadoop is an open-source framework used for running applications and storing data. With the Hadoop Distributed File System (HDFS), individual servers that are working in a cluster can

fail without aborting the entire computation process. There are no restrictions on the data that this system can store.

While big data is enticing because of the advantages it offers, it presents a number of issues:

Key Topic

- Organizations still do not understand it very well, and unexpected vulnerabilities can easily be introduced.
- Open-source codes are typically found in big data, which can result in unrecognized backdoors. Big data can contain default credentials.
- Attack surfaces of the nodes may not have been reviewed, and servers may not have been hardened sufficiently.
- Authentication of users and data access from other locations may not be controlled.
- Log access and audit trails may be an issue.
- Opportunities for malicious activity, such as malicious data input and poor validation, are plentiful.
- The relative security of a big data solution rests primarily on the knowledge and skill sets of the individuals implementing and managing the solution and the partners involved rather than the hardware and software involved.

Virtual/Augmented Reality

Virtual/augmented reality (AR) provides a view of a physical, real-world environment whose elements are "augmented" by computer-generated or extracted real-world sensory input such as sound, video, graphics, or GPS data. Many mobile devices support AR when the proper apps are installed. An interesting AR device is the Twinkle in the Eye contact lens. This lens, which is implanted in an eye, is fabricated with an LED, a small radio chip, and an antenna. The unit is powered wirelessly by RF electrical signal and represents the start of research that could eventually lead to screens mounted onto contact lenses worn on human eyes. When this lens technology is perfected, we will no longer need mobile devices, as AR chips will eventually be able to be implanted into our eyes and ears, making humans the extension of their own reality.

So, what is the difference between virtual and augmented reality? Well, there is a bit of difference. ***Virtual reality (VR)*** immerses users in a fully artificial digital environment, while ***augmented reality (AR)*** overlays virtual objects on the real-world environment.

Security issues with AR and VR revolve around the following issues:

- Breaches that expose tremendous amounts of data
- Privacy issues as hackers may gain access to a user's augmented reality device and record the user's behavior
- Unreliable data and data manipulation when delivered by a third party

3-D Printing

3-D printers create objects or parts by joining or solidifying materials under computer control to create three-dimensional objects. Some versions use a data source such as an additive manufacturing file (AMF) file (usually in sequential layers). 3-D printers use rolls of special filament as the material source. This filament comes in various colors (see Figure 8-3).

Key Topic

Figure 8-3 Plastic Filament

Security issues with 3-D printing are related to the fact that thousands of 3-D printers are exposed online to remote cyber attacks. The SANS Internet Storm Center scanned the Internet for vulnerable 3-D printers and found more than 3,700 instances of interfaces exposed online.

Passwordless Authentication

Many enterprises are continuing to move toward passwordless authentication. ***Passwordless authentication*** is any authentication method that does not rely on the

use of passwords. You have already learned of one such method: biometrics. Other methods include the use of certificates and methods that rely on public key cryptography. Some definitions also include methods that combine passwords with other forms of authentication, such as a smart card or a password in addition to a biometric sample.

Moving toward passwordless authentication has increased the security of the authentication and authorization process because alternatives such as biometrics and certificate-based authentication are much harder to defeat than passwords.

Nano Technology

A nanometer is a unit of measurement that is incredibly small. In fact, it would take three atoms of gold lined up to make one nanometer. ***Nano technology*** is the use of matter on atomic, molecular, and supramolecular scales for industrial purposes. Examples of its implementation include

- Tennis balls to last longer
- Golf balls to fly straighter
- Bandages infused with silver nanoparticles to heal cuts faster
- Diesel engines with cleaner exhaust fumes

Nano technology can help increase security in that it may enable more complex cryptographic schemes. Advances in nanoscale technology and the use of quantum technology may make quantum chips available that will be far more secure than traditional cryptographic hardware.

Deep Learning

Deep learning is a form of machine learning that uses artificial neural networks and representational learning. It has been applied to many fields, including computer science. While neural networks are conceptually like biological networks, they have some differences—the biggest one being that a biological network is dynamic, and a neural network is static. Nevertheless, deep learning has been used to observe and learn in fields such as speech recognition, drug design, medical image analysis, material inspection, and board game programs.

Natural Language Processing

Natural language processing (NLP) is a form of machine learning that attempts to enable a computer system to read and understand a document, including the

nuances. One common application of this is an automated chat or help function. As a deep understating of what the user is typing in the chat box is essential to providing good service, the application of natural language processing makes this possible.

Deep Fakes

Deep fakes comprise synthetic media that impersonates a real person's appearance and speech. A deep fake is so named because it uses a form of deep learning to learn both the appearance and the speech patterns of the target individual.

Biometric Impersonation

While we have in the past considered biometric authentication to be the gold standard in security, it is not without weaknesses. ***Biometric impersonation***, once thought to be difficult or even impossible, is apparently possible in some cases. For example, it has been shown that by accessing data generated by someone's activity-monitoring software, like Fitbit, and using a generic algorithm, information can be derived that can be used to impersonate that person.

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-1 lists these key topics and the page number on which each is found.

Key Topic

Table 8-1 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Figure 8-1	Blockchain	220
Figure 8-2	Distributed Consensus	222
List	Issues with big data	223
Figure 8-3	Plastic Filament	224
List	Implementations of nano technology	225

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

artificial intelligence (AI), machine learning (ML), quantum computing, blockchain, homomorphic encryption, private information retrieval (PIR), secure function evaluation (SFE), private function evaluation (PFE), distributed consensus, big data, virtual reality (VR), augmented reality (AR), 3-D printer, passwordless authentication, nano technology, deep learning, deep fake, biometric impersonation

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following makes artificial intelligence possible?
   a. Machine learning
   b. Distributed consensus
   c. Secure function
   d. Quantum computing

2. Activity-monitoring software, like Fitbit, can make which attack possible?
   a. Data exfiltration
   b. Biometric impersonation
   c. Side channel attack
   d. SYN flood

3. Which of the following is expected to enhance the machine learning process?
   a. Multiparty computation
   b. Distributed consensus
   c. Secure function
   d. Quantum computing

4. Which of the following comprises synthetic media that impersonates a real person's appearance and speech?
   a. Digital certificate
   b. Machine learning
   c. Deep fake
   d. Distributed consensus

5. Cryptocurrencies make use of which of the following?
   a. Distributed consensus
   b. Deep fake
   c. Quantum computing
   d. Blockchain

6. Which of the following is used to make tennis balls last longer?
   a. Nano technology
   b. Blockchain
   c. Machine learning
   d. Deep learning

7. Which of the following allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext?
   a. Asymmetric encryption
   b. Homomorphic encryption
   c. Hashing
   d. Salting

8. Which of the following processes used an additive manufacturing file (AMF)?
   a. Deep learning
   b. Distributed consensus
   c. 3-D printing
   d. Virtual reality

9. Which of the following is a type of protocol that can retrieve information from a server without revealing which item is retrieved?
   a. Secure function evaluation
   b. Private function evaluation
   c. Private information retrieval
   d. Public function evaluation

10. Which of the following immerses users in a fully artificial digital environment?
    a. IR
    b. AR
    c. DR
    d. VR