Cyber Security and Privacy, IIT Madras
Prof. Saji K Mathew

Week 2 Quiz
(All questions carry 1 point each)

1. CIA triad refers to:
   a. Confidentiality, Integrity and Availability
   b. Confidentiality, Integrity and Authentication
   c. Confidentiality, Integrity and Authorization
   d. Cybersecurity, Investigation and Authentication

   Ans: a. Confidentiality, Integrity and Availability

   Explanation: The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.

2. What aspect emerges from the intersection of 3 components of Information Security?
   a. Technology
   b. Policy
   c. Human Security
   d. None of the above

   Ans: b. Policy

   Explanation: The intersection of all 3 forms the central region from which “policy”, primarily emerging from the management perspective, guides the security related decisions and practice.

3. -------------, authentication and authorization are means to ensure CIA.
   a. Investigation
   b. Identification
   c. Classification
   d. Verification

   Ans: b.Identification

   Explanation: Identification refers to the process of proving one's identity to a system or service by providing credentials that claim the individual's identity.

4. Should all 27 cells of McCumber’s Cube be addressed with the same priority?
   a. True
   b. False

Ans: b.False

Explanation: Although addressing each cell can provide a more comprehensive approach to security, The Security Model does not mandate that all 27 cells must be individually addressed. Organizations can prioritize their security efforts based on their specific requirements, resources and risks.

5. Which of the following is/ are the design principles of high availability systems?
   a. Eliminate single points of failure
   b. Ensure reliable crossover
   c. Identify failures in real time
   d. All the above

   Ans: d. All the above

   Explanation: The mentioned design principles help to maintain the availability of systems and services at all times.

6. In ensuring confidentiality, what is the crucial process that involves classifying information and individuals, and mapping them based on the level of access?
   a. Identification
   b. Authentication
   c. Authorization
   d. Encryption

   Ans: c. Authorization

   Explanation: In ensuring confidentiality, the crucial process involves classifying both information and individuals, and then mapping them based on the level of access they require.

7. In addition to cryptography, a number of measures may be used for confidentiality, including:
   a. Information classification
   b. Secure document storage
   c. Application of general security policies
   d. All the above

   Ans: d. All the above

   Explanation: Measures such as information classification, secure document storage, application of general security policies, and education of information custodians and end users may be used for confidentiality

8. When a control provides assurance that every activity undertaken can be attributed to a named person or automated process, it is known as:
    a. Integrity
    b. Accountability
    c. Accessibility
    d. Authenticity

    Ans: b. Accountability

    Explanation: Accountability in cybersecurity refers to the principle of holding individuals, organizations, or entities responsible for their actions. It involves assigning clear roles and responsibilities to ensure compliance.

9. Identify the components of Information Security
    a. Network Security
    b. Computer & Data Security
    c. Management of Information Security
    d. All of the above

    Ans: d. All the above

    Explanation: Information Security entails all the 3 components such as Network Security, Computer & Data Security, Management of Information Security from whose intersection Policy emerges.

10. Which are the three types of power McCumber's Cube identifies?
    e. Technologies
    f. Policies and Practices
    g. People
    h. All the above

    Ans: d. All the above

    Explanation: "Technologies" encompass devices and products for protecting information systems and thwarting cybercriminals. "Policies and practices" entail procedures and guidelines to ensure cyber safety and adherence to best practices. "People" refers to the users who are aware and knowledgeable about their cyber environment and the associated threats.