Prescott Kowalski

CYSE 200T Feb 9th

The **CIA Triad** is a cornerstone in information security, encompassing three vital principles: Confidentiality, Integrity, and Availability (Chai, 2022).

1. **Confidentiality** ensures that information remains accessible only to authorized individuals. Utilizing techniques such as encryption, access controls, and user authentication helps maintain this confidentiality, preventing unauthorized access and protecting sensitive data from exposure.
2. **Integrity** ensures that data remains accurate, complete, and unaltered throughout its lifecycle. Techniques like checksums, digital signatures, and hashing algorithms are employed to detect and prevent unauthorized modifications, guaranteeing that the information can be trusted and remains unchanged from its original form.
3. **Availability** ensures that information and resources are accessible to authorized users whenever needed. Measures such as redundancy, failover systems, and regular maintenance contribute to maintaining availability, ensuring that users can access the necessary information and services without interruption.

Authentication and **Authorization** are two distinct yet interrelated processes in information security:

- **Authentication** is the process of verifying the identity of a user or system, ensuring that the entity attempting to access a system is who they claim to be. Common authentication methods include passwords, biometrics (e.g., fingerprints, facial recognition), and multi-factor authentication (MFA), which combines two or more verification methods (NIST, 2023).
- **Authorization** is the process of granting or denying access to resources based on the authenticated identity. It determines what an authenticated user is permitted to do within a system,

such as accessing specific files, applications, or services. Authorization is typically managed through access control policies and permissions.

Example: Consider a corporate intranet system.

When an employee logs into the intranet, the system first requires authentication. The employee might enter a username and password, and then provide a fingerprint scan. This multi-factor authentication process ensures the person accessing the system is who they claim to be. Once authenticated, the system then performs authorization to determine what resources the employee can access.

In summary, the CIA Triad underscores the importance of Confidentiality, Integrity, and Availability in information security. Authentication and authorization are essential processes to ensure that only authorized users can access and perform actions within a system.

References:

Chai, Y. (2022). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology (NIST). Retrieved from NIST website.

National Institute of Standards and Technology (NIST). (2023). Cybersecurity and Identity Management. Retrieved from NIST website.