Michael Everett

Date: February 16th, 2025

Course: CYSE 200T

Professor Duvall

Understanding the CIA Triad and the Differences Between Authentication and Authorization

BLUF: CIA Triad is an essential principle of cybersecurity that addresses the maintenance of confidentiality, integrity, and availability of data, while authentication and authorization are distinct but complementary security processes that support one another in controlling access to systems.

Information security ranks high on the cyber security priority list. CIA Triad and authentication and authorization form the basis for securing systems and data. CIA Triad provides us with a model to comprehend the most important security concepts, and authentication and authorization describe how resources are controlled and accessed.

The CIA Triad:

The CIA Triad refers to Confidentiality, Integrity, and Availability, Authentication, and Authorization.

Confidentiality ensures that sensitive data are only available to the individuals who are supposed to view them. It is more concerned with keeping data from being viewed by unauthorized persons. Encryption algorithms, secure communication protocols, and access control mechanisms are usually in place to provide confidentiality. Example: Patient medical records in a health care system need to be confidential, and only access needs to be granted to authorized health personnel.

Integrity is maintaining the data unchanged and correct during its entire life. This renders the data unchanged and trustworthy. Data integrity is protected by checksums and hashing that validate that the data is not altered. Example: A financial transaction system uses hash functions to validate that transaction records are not altered during transmission or storage.

Availability provides data and systems as and when needed by designated users with the purpose of avoiding cyber-attacks, for instance, Denial-of-Service attacks.

Example: An online business where the website is available 24/7 for people to purchase items.

Authentication is the process of determining whether a user, device, or system is authentic. The process typically asks for a password or something like a card. For instance: When a user logs in into a website based on username and password, the system verifies identity by matching the credentials in a database.

Types of Authentications:

-Single-factor authentication: With one method, password.

-Multi-factor authentication: With two or more methods, password and a one-time code by text message.

Authentication, on the other hand, is the authorization or denial of access to the resources once an identity has been identified and grants individuals what they can access. This is usually managed by access control lists (ACLs) where the individual is given some role or permission. Example: A user logs into a banking application and is permitted to view his or her account balance but not the account information of another user.

Types of Authorization:

-Role-based access control: Privileges are granted to users according to their organizational role.

-Discretionary access control: Owners of resources control access to their data.

-Mandatory access control: Access is controlled by a central authority and is typically used in high-security systems.

Authentication vs Authorization:

Example, a company employee is logging into an internal portal:

Authentication: The employee logs in using a username and password. This verifies that they are who they claim to be.

Authorization: Once opened, the employee's is then verified to see what they can access. The employee can access his or her own information but not the company's financial information, which would be accessed by managerial staff only.

Furthermore, authentication establishes identity, but authorization dictates what the authenticated user can do or access. Both are critical roles in providing secure and managed access to sensitive systems.

Conclusion:

Understanding the CIA Triad and how authentication and authorization differ in making an information system secure is crucial. The CIA Triad deals with the core components of cybersecurity in terms of confidentiality, integrity, and availability and authentication and authorization are processes which deal with who should have access to the resources and what should they be allowed to do. These being executed in the proper way ensures that systems are secure, and confidential information is not opened by the incorrect individuals.

Reference

"What Is the CIA Triad and Why Is It Important? | Fortinet." Fortinet, www.fortinet.com/resources/cyberglossary/cia-triad.

Hashemi-Pour, Cameron, and Wesley Chai. "What Is the CIA Triad (Confidentiality, Integrity and Availability)?" WhatIs, 21 Dec. 2023, www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.

https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/