Isain Cortes, Jr.
CYSE200T
1/28/2024

# Understanding the CIA Triad and Differentiating Between Authentication & Authorization

## Introduction to the CIA Triad:

In the field of information security, the CIA Triad is a well-established model that forms the core of security policies. This model consists of three fundamental principles: Confidentiality, Integrity, and Availability. Each element plays a vital role in protecting information systems and sensitive data against a wide range of cyber threats.

## Confidentiality:

Confidentiality is about ensuring that sensitive information is not disclosed to unauthorized individuals or entities. This principle protects personal and proprietary information from external threats and internal vulnerabilities. Measures to maintain confidentiality include robust encryption methods, secure communication channels, and strict access controls. For example, you're asked for a password. If it's been a while since your last log-in, you may be asked to input a code that's been sent to you or some other form of two-factor authentication (Fasulo 2021).

## Integrity:

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data across its lifecycle. This principle ensures that information is not altered in an unauthorized or unexpected manner. Techniques to ensure integrity include checksums, hash functions, and version control mechanisms. For instance, data integrity is provided by making sure your purchases are reflected in your account and allowing you to contact a representative if there’s a discrepancy (Fasulo 2021).

**Availability:**

Availability is the assurance that information and resources are accessible to authorized users when needed. This aspect of the triad focuses on ensuring that systems, networks, and applications are up and running and can be accessed without unwarranted delays. Redundancy, failover systems, regular backups, and robust disaster recovery plans are measures to ensure high availability. A common example is that you can log into your account whenever you want, and you may even be able to contact customer support at any time of the day or night (Fasulo 2021).

**Authentication vs. Authorization:**

In the realm of information security, authentication and authorization are two critical concepts that are often confused but serve different purposes.

**Authentication:**

According to Moss (2022), “Authentication is the verification of a user or system’s identity.” It is a way to ensure that the individual or entity requesting access is who they claim to be. This verification can be achieved through various means, such as passwords, biometric scans, or security tokens. For example, when a user logs into a social media platform, they are asked to provide their username and password. The system then verifies these credentials against its database to confirm the user’s identity.

**Authorization:**

Once authentication is established, authorization comes into play. Authorization is the access privileges granted to an authenticated identity (Moss 2022, citing Stouffer et al. 2015). This process determines what an authenticated user is allowed to do within a system, such as what resources they can access and what actions they can perform. For instance, in a corporate setting, an employee may authenticate with their credentials, but their level of authorization determines whether they can access confidential company data or merely view public company resources.

**Combining CIA with Authentication and Authorization:**

Integrating the principles of the CIA Triad with authentication and authorization practices offers a comprehensive security strategy. Confidentiality is enhanced when access to sensitive information is limited to authenticated and authorized users. Integrity is maintained by ensuring that only authorized individuals can alter data. Availability is supported by allowing authenticated users timely access to the resources they are authorized to use.

**Conclusion:**

In summary, the CIA Triad provides a fundamental framework for information security, focusing on protecting data and resources from unauthorized access and breaches. Authentication and authorization, essential components of this framework, work in tandem to ensure secure and controlled access to systems and information. Understanding and effectively implementing these principles and processes are crucial for any organization to safeguard its digital assets and maintain the trust of its users and stakeholders.

## Works Cited

Hashemi-Pour, C., & Chai, W. (2023, December 21). *CIA triad (confidentiality, integrity and availability)*. WhatIs. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Moss, R. (2022, April 19). *The CIA triad, authentication, and Authorization – Ryan Moss*. https://sites.wp.odu.edu/ryanmoss/2022/04/19/the-cia-triad-authentication-and-authorization/#:~:text=The%20CIA%20triad%20also%20directly,authenticated%20identity%20(Stouffer%20et%20al.

SecurityScorecard, & Fasulo, P. (2021, September 1). *What is the CIA Triad? Definition, Importance, & Examples - SecurityScorecard*. SecurityScorecard. https://securityscorecard.com/blog/what-is-the-cia-triad/