Hector Phan

Professor Duvall

2/15/2025

CYSE 200T

The CIA Triad and the Differences Between Authentication and Authorization

BLUF: A key concept in information security, the CIA Triad (Confidentiality, Integrity, and Availability) strives to protect data. Although they are sometimes used together, authorization and authentication have different functions. authorization dictates what actions an authenticated user is permitted to utilize, while authentication verifies the user's identity.

Introduction

Safeguarding sensitive data is crucial to an organization's functionality and reputation in the digital world. A popular design for information security, the CIA Triad ensures certain that data is secure against attacks. In addition, the concepts of authorization and authentication are vital to system safety. To create effective safety protocols, it is important to understand how these components interact. The CIA triad consists of three core principles that protects data and systems. Such as:

1. Confidentiality: Only those who are permitted to look over information may do so thanks to confidentiality. Unauthorized data access poses serious security issues and may result in breaches. Confidentiality is preserved through secure communication protocols, encryption, and access controls.

   Example: A company encrypts its customer database to prevent unauthorized individuals from accessing sensitive personal information, even if they gain access to the system.

2. Integrity: During the time it exists, integrity ensures that the data is accurate, consistent, and reliable. While even small modifications to data can have major implications, protection against unauthorized modifications is important.

   Example: A financial institution uses checksums to verify that transactions have not been tampered with during transmission between systems.

3. Availability: Availability ensures that when needed, authorized users can access information and systems. In situations where data and services must always be accessible, this idea is important.

   Example: A healthcare provider implements backup systems and disaster recovery protocols to ensure patient data is available, even in the event of hardware failures.

Authentication vs. Authorization: Key Differences

Although while authorization and authentication are crucial for information security, both serve different functions:

1. Authentication: The process of verifying a user, device, or system's identity can be referred to as authentication. It offers an answer to the question, "Who are you?" Multi-factor authentication (MFA), biometric scans, and passwords are examples of methods used for authentication.

   Example: When logging into an online banking app, you enter your username and password. The system authenticates your identity by checking the entered credentials against its database.

2. Authorization: What an authenticated user is allowed to do is determined by authorization. It offers an answer to the question, "What are you allowed to do?" Authorization systems based on roles, policies, or permissions offer or restrict access to resources once a user's identity has been verified.

   Example: After authenticating into a corporate email system, you may be authorized to read and send emails but not change account settings, depending on your user role.

Key Differences Between Authentication and Authorization

The main difference between authentication and authorization lies in their respective functions:

The purpose of authentication is to verify a user's identity to be certain the system or individual trying to access information is who they say they are. After authentication, authorization determines the extent of the authenticated user's access, ensuring that their identities can only access resources which they are authorized to use.

To illustrate:

1. Authentication: Utilizing your username and password, you enter a secure platform where the system authenticates you.
2. Authorization: The platform looks at your role (for example, as an administrator or user) when you log in to determine what you can conduct.

Conclusion

The basic principle for modern information security being the CIA Triad, which means Confidentiality, Integrity, and Availability. It assists in ensuring that data can be accessed when needed and remains protected from unauthorized access and modification. While their occasional overlap, authorization and authentication have unique yet complimentary functions in safety protocols. While authorization determines what actions users are permitted to act, authentication ensures users are who they claim to be. These concepts work together to offer a thorough strategy for maintaining the integrity and security of digital systems.

References:

https://www.fortinet.com/resources/cyberglossary/cia-triad?utm_source=chatgpt.com

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html