Derrick Amissah

2/1/25

Understanding the CIA Triad and the Differences Between Authentication & Authorization

This paper gives an overview of the CIA Triad foundational model in cybersecurity and explains, with examples, the difference between authentication and authorization.

Introduction

It all begins with setting rules based on three key goals in cybersecurity: keeping information confidential, ensuring its integrity, and making sure it's available, also known as the CIA triad. To protect systems from unauthorized access, it's important to know the difference between authentication (proving who you are) and authorization (deciding what you're allowed to do). This helps in creating strong access controls to keep data safe.

CIA TRIAD

This triad presents three basic requirements for information to be secured using the following triad:

Confidentiality: This principle focuses on ensuring that sensitive information is accessible only to those with proper authorization. Techniques like data encryption, strong password protocols, two-factor authentication, and biometric verification help maintain confidentiality. For example, online banking systems require account numbers and passwords to restrict unauthorized access (Chai, 2022).

Integrity: The Integrity property assures accuracy and dependability of the data during its whole life cycle. It should be made that the data is protected against unauthorized alternations; protective measures can involve checksum, signature, even version control. Example: Something like downloading a software application where authenticity is checked by applying cryptographic hashes.

Availability: Through availability, information and resources are accessible to authorized users when required. It is achieved through regular system maintenance, redundancy, failover mechanisms, and sound disaster recovery plans. Cloud service providers, for

example, deploy multiple redundant servers to ensure that minimal time is wasted in case of hardware failure (Chai, 2022).

Differences Between Authentication and Authorization

Authentication is the process of identifying a person. It might be through password, security token, biometric, or other multi-factor methods. For example, accessing an e-mail account using username and password authenticates the identity of a user.

Authorization: Authorization is the process of determining what actions an authenticated user can perform. It is a process after authentication that allows different types of actions based on user roles. For example, an employee logging onto the corporate network would have permission to access only certain files relevant to his department while others are not accessible.

Example: Consider a secure office building:

Authentication: The security guard checks your ID badge to verify you are an employee.

Authorization**:** Once inside, your access card only allows entry to floors and rooms of your department.

Conclusion: The CIA Triad consists of confidentiality, integrity, and availability as the backbone of cybersecurity practices. Similarly important is the knowledge of the difference between authentication and authorization to implement secure yet efficient access control in systems.

References

Chai, W. (2022, June 28). *What is the CIA Triad?* Definition, Explanation, Examples.file:///Users/derrickamissah/Downloads/What%20is%20the%20CIA%20Triad_%20Definition,%20Explanation,%20Examples%20-%20TechTarget.pdf