Neesha Currier

CYSE 200
CIA Triad, Authentication, and Authorization
2/7/2026

Bottom Line Up Front (BLUF)

The CIA Triad provides the foundational principles of cybersecurity by emphasizing confidentiality, integrity, and availability, while authentication and authorization are access control mechanisms that ensure only verified users can access systems and perform permitted actions. Together, these concepts form the basis for protecting information systems from unauthorized access, data manipulation, and service disruption.

Introduction

Cybersecurity relies on well-established principles and controls to protect information systems from threats. Two fundamental concepts in this field are the CIA Triad and access control mechanisms such as authentication and authorization. The CIA Triad defines the primary goals of information security, while authentication and authorization govern how users interact with protected systems. This paper explains each component of the CIA Triad and clearly distinguishes between authentication and authorization using real-world examples.

The CIA Triad

The CIA Triad is a widely accepted model used to guide cybersecurity policies and system design. It consists of confidentiality, integrity, and availability.

Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized individuals or systems. This principle focuses on preventing unauthorized disclosure of data through controls such as encryption, passwords, and access restrictions (Chai, 2022).

For example, a company may encrypt employee payroll data so only human resources personnel can access it. Even if an unauthorized user gains access to the system, the encrypted data remains unreadable.

Integrity

Integrity ensures that information remains accurate, complete, and unaltered unless modified by authorized users. This principle protects data from unauthorized changes, whether accidental or malicious, through methods such as hashing, audit logs, and version control (Chai, 2022).

An example of integrity protection is a financial system that logs all changes to transaction records. If someone attempts to alter a transaction without authorization, the system can detect the change and identify who made it.

Availability

Availability ensures that systems and data are accessible to authorized users when needed. This principle is maintained through redundancy, regular maintenance, backups, and protection against denial-of-service attacks (Stallings & Brown, 2018).

For instance, an online banking service may use backup servers and failover systems to ensure customers can access their accounts even during system maintenance or hardware failures.

Authentication vs. Authorization

Authentication and authorization are closely related but serve different purposes within cybersecurity.

Authentication

Authentication is the process of verifying the identity of a user or system. It answers the question, “Who are you?” Authentication typically uses credentials such as usernames and passwords, biometric data, or multi-factor authentication methods (Chai, 2022).

A common example of authentication is logging into an email account using a password and a one-time verification code sent to a mobile device.

Authorization

Authorization determines what an authenticated user is allowed to access or do within a system. It answers the question, “What are you allowed to do?” Authorization is often based on roles, permissions, or access control policies.

For example, after logging into a company network, an employee may be authorized to access their own files but not confidential management or human resources records.

Key Differences

Authentication always occurs before authorization. A system must first confirm a user's identity before determining what resources they are permitted to access. While authentication confirms identity, authorization enforces access limitations and supports the principle of least privilege.

Conclusion

The CIA Triad and access control mechanisms are essential components of cybersecurity. Confidentiality, integrity, and availability define what needs to be protected, while authentication and authorization control who can access systems and what actions they can perform. Understanding these concepts helps organizations design secure systems that protect sensitive data, maintain trust, and ensure reliable access for authorized users.

References

Chai, W. (2022). *Confidentiality, integrity, and availability (CIA triad).* TechTarget.

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.