Blaine Gernandizo

Professor Bowman

CYSE 200T

28 September 2025

The CIA Triad, Authentication, and Authorization

The CIA Triad is a foundational model for information security, comprising three core principles: Confidentiality, Integrity, and Availability. It serves as a guide for developing security policies and evaluating an organization's security posture. Confidentiality guarantees that sensitive information is accessed only by authorized users. It aims to prevent unauthorized data access through measures such as encryption and access controls. For example, before a high-profile criminal trial, a grand jury issues an indictment. This document is highly sensitive and must remain secret to ensure a fair trial and protect the individuals involved. Confidentiality is maintained by sealing the document in a secure court records system with strict, court-ordered access controls. Integrity maintains the accuracy and trustworthiness of data throughout its lifecycle. It protects information from unauthorized alteration, ensuring it remains reliable and authentic. For example, when a university issues a digital transcript with a cryptographic signature, any attempt to alter the grades would break this signature, immediately revealing the document has been tampered with and is no longer trustworthy. Availability guarantees that systems and data are accessible to authorized users when needed. This principle focuses on preventing downtime through redundancy and maintenance. For example, when a patient arrives in the emergency room, doctors must be able to immediately access their medical history, allergies, and current medications. By balancing Confidentiality, Integrity, and Availability, organizations can build a comprehensive security framework that protects data while supporting business operations.

Authentication and authorization are foundational to access management. Authentication is the process of verifying a user's identity, using factors like passwords (what you know), security tokens (what you have), or biometrics (what you are) (Andrioaie, 2025). Once identity is confirmed, authorization determines the user's permissions, specifying what resources they can access and what actions they can perform. These concepts work together to enforce security. For example, multi-factor authentication verifies an employee's identity, while a Role-Based Access Control (RBAC) system then authorizes them to access only the data necessary for their job. This layered approach ensures that even if credentials are compromised, authorization limits limit the potential damage, forming a crucial defense against data breaches.

References

Chai, W. (2023, December 21). *What is the CIA triad (confidentiality, integrity and availability)?* WhatIs. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Andrioaie, A. (2025, September 26). *Authentication vs. Authorization: Key Differences and Types*. Heimdal Security Blog. https://heimdalsecurity.com/blog/authentication-vs-authorization/