Jeshiah Babumba
CYSE 200T
February 22, 2026
Professor Duvall

The CIA Triad and the Difference Between Authentication and Authorization

BLUF: The CIA Triad is the foundation of information security and focuses on confidentiality, integrity, and availability. Authentication confirms a user's identity, while authorization determines what that user is allowed to access. Both are essential to protecting organizational systems and data.

The CIA Triad

The CIA Triad is a model used to guide cybersecurity policies within organizations. It consists of three core principles: confidentiality, integrity, and availability.

Confidentiality means limiting access to sensitive information so that only authorized individuals can view it. Organizations protect confidentiality through tools such as encryption, strong passwords, multi-factor authentication, and access control lists. For example, requiring a verification code in addition to a password when logging into an online banking account helps prevent unauthorized access.

Integrity refers to maintaining the accuracy and trustworthiness of data. Information should not be altered in transit or modified by unauthorized users. Controls such as file permissions, version control, digital signatures, and checksums help ensure that data remains accurate. In a healthcare system, patient records must remain correct and unchanged to ensure proper treatment and compliance with regulations.

Availability ensures that systems and data are accessible to authorized users when needed. This includes maintaining hardware, performing system updates, using backups, and implementing disaster recovery plans. Redundancy and monitoring systems also help prevent downtime. If a company's network goes offline during business hours, productivity and revenue can be significantly impacted.

These three principles work together. If one fails, overall security is weakened.

Authentication vs. Authorization

Authentication and authorization are closely related but serve different purposes.

Authentication is the process of verifying identity. It answers the question: who are you? This is typically done through usernames and passwords, biometrics such as fingerprints, or multi-factor authentication.

Authorization occurs after authentication and determines what actions or resources a verified user can access. It answers the question: what are you allowed to do?

For example, at a university, a student logs into the online portal using their credentials. The login process verifies the student's identity, which is authentication. Once logged in, the system allows the student to view grades and register for classes but does not allow them to modify transcripts or payroll data. That level of access control is authorization. A professor, however, may be authorized to submit grades but not to access student financial accounts.

Authentication must happen before authorization. A system cannot grant permissions until it knows who the user is.

Conclusion

The CIA Triad remains the core framework for protecting information systems by ensuring confidentiality, integrity, and availability. Authentication verifies identity, and authorization defines access rights. Together, these concepts help organizations secure data, reduce risk, and maintain operational stability.

Reference

Chai, W. (2022). *What Is the CIA Triad? Definition, Explanation, Examples.* TechTarget.