

The CIA Triad

Nicholas Duggins

06/06/2026

The CIA Triad and the Difference Between Authentication and Authorization

Introduction

The CIA Triad is the foundation of information security and consists of confidentiality, integrity, and availability. These three principles guide organizations in protecting information and ensuring that systems remain secure and accessible. Authentication and authorization are essential security processes that support the CIA Triad by verifying user identities and controlling access to resources.

Cybersecurity professionals rely on established security models to protect information systems and sensitive data. One of the most widely recognized models is the CIA Triad, which consists of confidentiality, integrity, and availability. These principles provide a framework for developing security policies and implementing safeguards that protect organizational data. In addition, authentication and authorization are critical access control mechanisms that help maintain the security objectives defined by the CIA Triad.

The C.I.A Triad

Confidentiality refers to protecting sensitive information from unauthorized access. According to Chai (2022), confidentiality is achieved through measures such as encryption, passwords, access

controls, and multi-factor authentication. These safeguards ensure that only authorized individuals can view or access protected information. For example, online banking systems require users to provide credentials before accessing account information.

Integrity refers to maintaining the accuracy, consistency, and trustworthiness of data throughout its lifecycle. Data must remain accurate and free from unauthorized modification. Organizations use methods such as checksums, version control, backups, and digital signatures to ensure data integrity. These controls help detect unauthorized changes and restore data when necessary.

Availability ensures that authorized users can access information and systems when needed. Maintaining availability requires reliable hardware, software updates, network monitoring, backup systems, and disaster recovery plans. Redundancy measures such as failover systems and RAID storage can help organizations continue operations even when hardware failures occur.

Authentication vs. Authorization

Although authentication and authorization are often discussed together, they serve different purposes within information security. Authentication is the process of verifying the identity of a user. "Authenticity is the property that an entity is what it claims to be." (Witcher, 2026) It answers the question, "Who are you?" Common authentication methods include usernames and passwords, biometric scans, security tokens, and multi-factor authentication. Before a user can access a system, the system must confirm that the user is who they claim to be. Authorization occurs after authentication and determines what resources or actions a user is allowed to access. It answers the question, "What are you allowed to do?" Authorization policies help ensure that users only access information necessary for their job responsibilities.

Example

A company employee logs into a secure network using a username, password, and a one-time verification code sent to a mobile device. This process is authentication because the system is verifying

the employee's identity. After logging in, the employee can view departmental reports but cannot access payroll records or executive files. This restriction is authorization because the system is determining which resources the employee is permitted to access.

Conclusion

The CIA Triad provides the foundation for modern cybersecurity by focusing on confidentiality, integrity, and availability. These principles help organizations protect sensitive information, maintain accurate data, and ensure reliable access to systems. Authentication and authorization further support these goals by verifying user identities and controlling access to resources. Together, these concepts form essential components of an effective information security program.

References

Chai, W. (2022, June 28). *What is the CIA triad_ definition, explanation, examples - techtarget.pdf*.

Google Drive. <https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view>

Witcher, R. (2026, February 4). *The Five Pillars of Information Security: CIA Triad and more*. Destination

Certification. <https://destcert.com/resources/five-pillars-information-security/>