The CIA Triad

Describe the CIA Triad and the Differences between Authentication & Authorization

Brandon Braxton

CYSE 200T: Cybersecurity, Technology, And Society

Professor Chris Bowman

JUNE 28, 2026

What is the CIA Triad? The CIA Triad is the foundational “model designed to guide policies for information security within an organization” which is broken down into three principles – Confidentiality, Integrity, and Availability (Hashemi-Pour & Chai, 2023). The three principles form an interconnected framework for policy creation as they are all codependent of each other.

Confidentiality ensures sensitive information is only accessible to authorized individuals. This can be enforced through multi-factor authentication, encryption and/or role-based access controls. Integrity ensures “the consistency, accuracy and trustworthiness of data over its entire lifecycle (Hashemi-Pour & Chai, 2023). This can be achieved through “hashing, encryption, digital certificates, or digital signatures” (What Is the CIA Triad and Why Is It Important? | Fortinet, n.d.). Finally, availability ensures that systems and data are consistently and readily accessible to authorized individuals at all times. Availability involves maintaining technical infrastructure (hardware and software), data backups, power backups, redundant systems, disaster recovery plans and systems monitoring. Each principle within the triad frameworks needs to be implemented with consideration for one another and without omitting one for another.

Within the CIA triad, particularly confidentiality, are the concepts of authentication and authorization. Authentication is the process of verifying a user’s identity which is done through things such as login credentials, employee ID or biometrics. Authorization is the process of checking and granting user privileges to access the network or certain systems. “Authorization is different from authentication in that authentication only checks a user’s identity, whereas authorization dictates what the user is allowed to do” (What Is AAA Security? | Fortinet, n.d.).

For example, when an employee wants to log into the company network, they must provide login credentials, complete a multi-factor authentication request, then, only after the first two steps are completed successfully, will the AAA server provide the employee access to the network or to the particular system they are trying to access based on the employee's role and permissions. In the example, authentication is shown by the employee verifying their identity through login credentials and MFA, and authorization is represented by the AAA server granting the user access only after they were authenticated and only to the resources, they are allowed based on the employee's role and permissions. Together, these two concepts strengthen the principles of the CIA Triad and help to form the solid foundation of an organization's cyber strategy.

References

Hashemi-Pour, C., & 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?jr=on

What is AAA Security? | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/aaa-security

What is the CIA Triad and Why is it important? | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/cia-triad