Chadwick Bennett
February 15, 2026
CYSE 200T
Professor Duvall

The CIA Triad and the Difference Between Authentication and Authorization

BLUF (Bottom Line Up Front)

The CIA Triad (Confidentiality, Integrity, and Availability) is the cybersecurity framework that protects information from unauthorized disclosure, alteration, or loss of access. Authentication verifies identity: usernames and passwords. Authorization determines permissions after the identity is confirmed, like what security clearance someone has or needs. (Chai, n.d.; Nieles et al., 2017).

The CIA Triad

According to the National Institute of Standards and Technology (NIST, 2017), the CIA Triad defines the core goals of information security.

It is a model used to guide information security practices and protect digital assets.

Confidentiality

Confidentiality ensures that information is only accessible to authorized users. It protects privacy by preventing unauthorized individuals from viewing sensitive data. Common protections include encryption, passwords, and access controls. For example, a medical record should only be accessible to the patient and approved healthcare staff. (Chai, n.d.).

Integrity

Integrity is an additional layer of defense that guarantees that information remains accurate, complete, and unaltered unless changed by authorized users. Security mechanisms such as hashing, checksums, and version control help detect unauthorized modifications. If integrity fails, data can no longer be trusted.

Availability

Availability ensures that systems and data are accessible when needed. This includes maintaining hardware, infrastructure, preventing outages, and defending against attacks. Availability is supported by backups, redundancy, and system monitoring. (Nieles et al., 2017)

The Triad is important because it forms the data security and safety foundation and building blocks for cybersecurity professionals.

Authentication vs. Authorization

Authentication and authorization serve different purposes.

Authentication

Authentication confirms “who you are.” It validates identity through credentials such as:

- Passwords
- PINs
- Fingerprints
- Face ID
- Multi-factor authentication

Example: Entering your username and password to log into a school portal.

Authorization

Authorization determines “what you are allowed to do” after authentication. It controls permissions and access levels.

Example: After logging in, a student may view grades but cannot modify them, while a professor can update them.

- Authentication = identity check (identifies the individual = username & password)
- Authorization = permission check (who is authorized to view and/or make changes)

Example Scenario

Consider a hospital system. A nurse logs into the system using a password and badge (authentication). Once logged in, the system allows the nurse to view patient charts but prevents editing prescriptions (authorization). This setup protects confidentiality, integrity, and availability.

Conclusion

The CIA Triad provides the core structure for protecting information systems. Confidentiality protects privacy, integrity protects accuracy, and availability ensures reliable access. Authentication and authorization work together to enforce these protections by confirming identity and limiting permissions. Understanding these concepts is essential for anyone pursuing cybersecurity.

References

Chai, W. (n.d.). *CIA Triad Overview. What is the CIA Triad? Cybersecurity framework overview.*

Nieles, M., Dempsey, K., & Pillitteri, V. (2017, June 22). *An introduction to information security*. CSRC. https://csrc.nist.gov/pubs/sp/800/12/r1/final