

Nathan Jimenez

CYSE 200T

September 14, 2025

Professor Duvall

The CIA Triad

BLUF

The CIA Triad means, Confidentiality, Integrity, and Availability. These 3 forms the foundation for IT or Information Security. With those 3 combined they cover everything between authentication and authorization, with these they ensure that data remains protected, accurate, and only accessible to the people with authorization.

The CIA Triad

The CIA Triad is a model for IT that focuses on the three principles confidentiality, integrity, and availability. Confidentiality makes sure that sensitive information is kept private and only authorized users can access this information. Integrity ensures that the data is accurate, consistent, and trustworthy throughout its existence. Availability is the final one which ensures that authorized users can access this information whenever it is needed (Chai, Confidentiality, Integrity, Availability).

Chai also explained that modern challenges including big data and the internet of things complicate the Triad. Since large amounts of diverse data require a lot more oversight and protection (Chai, Special challenges for the CIA triad). Think of the CIA Triad as a system that is interconnected which helps the organization make stronger policies and prevent risks.

Authentication

Authentication answered the question “Who are you?” when you are trying to access the information. It goes through a process which checks if you have certain access by inserting the password, a biometric scan, or 2FA (Two-factor authentication) [NIST]. This is a critical step because it prevents unauthorized people from entering the system. A good example of this is if a random person tries to login to ODU Portal without a student/faculty account it won't allow them.

Authorization

Authorization answered the question “What can you do?”. So once you go through authentication the system will determine what access you have. An example of this, which was similar to the Authentication one, is if a student wants to edit the class but can't because they don't have the type of Authorization as a professor would. Another thing about Authorization is that it enforces the principle of privilege only allowing the people with that role to perform actions with that type of Authorization (OWASP).

Example

A good example for these two would be when you do your banking online. You need to login using the user and password you created . After logging in, some banking apps have it, they send a code to either your number or email depending on which you choose with an authentication code to verify it's you on your device (Confidentiality). Once you are inside you can only see your account and only yours nobody else's as to protect everyone and keep it hidden

(Integrity). In the end they always have backup servers so anyone can access their own money at any given moment (availability).

Conclusion

In conclusion The CIA Triad and the separate two authentication and authorization is essential to cybersecurity. Chai emphasized that confidentiality, integrity, and availability should be treated as one. When they are combined they have strong identity verification (authentication) and permission management (authorization, this framework makes sure that information remains private, accurate, and available to people who need it. If you understand these principles it helps the organization and the individuals so that stronger protection is applied everyday in the digital world.

References

Chai, W. (2022, June 28). *What is the CIA Triad? Definition, explanation, examples*. TechTarget.

<https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>

National Institute of Standards and Technology. (2017). *Digital identity guidelines* (NIST Special Publication 800-63-3). U.S. Department of Commerce.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

OWASP Foundation. (2021). *Authentication and authorization*. OWASP Cheat Sheet Series.

<https://cheatsheetseries.owasp.org/>