

Name: Timothy Taylor

Date: September 16th, 2023

The CIA Triad

The CIA Triad is a valid and reliable framework that has existed for decades. It emphasizes the fundamentals of security by restricting data access to those with the credentials and permissions to view it. Although it may remain imperfect, it is still effective and widely used in government and commercial organizations.

What is “CIA”?

CIA is an acronym that stands for Confidentiality, Integrity, and Availability. This ‘triad’ is used to gauge the effectiveness of an information security system. The goal of the CIA framework is to ensure the consistency in the reliability and accessibility of information while maintaining data privacy from unauthorized users.

Origins of CIA Framework

It is believed that the concept of the CIA framework originated from the United States Navy in the mid-to-late 1970's. The government funded two studies between 1970 to 1972 focused on confidentiality of information and organizational security to minimize internal threats. These studies laid the foundation for future research conducted by Academic researchers Saltzer and Schroeder. They first introduced the concept of protecting digital information rather than firewall security of hardware and software in a fundamental paper published in 1975.

Authentication - What is it?

Authentication is the process of validating whether a login attempt was from a specific user. If a user has the valid credentials but cannot authenticate that they are the recipient of the account, then they will be unable to gain entry. For example, some sites use robot verification to deny entry to spam accounts, therefore minimizing malicious software from gaining entry to a particular webpage.

Authorization - What's The Difference?

While authentication is used to verify a person's identity, authorization determines what resources a user is authorized to access. Authorization typically occurs in sequence to authentication. If a user is verified to be who they claim but does not meet the requirements to access certain levels of information, they will be denied access. For example, Google Docs uses authorization to grant a user access to a particular shared document. If the user has not received access to the document, then it will remain hidden and inaccessible until the permission is granted.

Conclusion

In summary, The CIA Triad has actively maintained its role in security as a framework for future organizational practices including authentication and authorization. It has laid the groundwork for future technologies such as biometric locks, two-factor authentication, and much more. I firmly support the use and upholding of this framework in the field of cybersecurity.

References

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity, and availability in security. <https://www.proso.com/dl/Samonas.pdf>

What is the difference between authentication and authorization?. SailPoint. (2023, March 7).

<https://www.sailpoint.com/identity-library/difference-between-authentication-and-authorization/#:~:text=So%2C%20what%20is%20the%20difference,a%20user%20has%20access%20to>

Fenrich, K. (2008). Securing your control system: The "CIA triad" is a widely used benchmark for evaluating information system security effectiveness. *Power Engineering*, 112(2), 44.

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

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

H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," in *IT Professional*, vol. 19, no. 5, pp. 27-33, 2017, doi: 10.1109/MITP.2017.3680960.