Name: Demontae Watson

Date: 9/11/2024

The CIA Triad: Role of Authentication and Authorization

The fundamental principles for protecting sensitive data are known as the CIA Triad, which include availability, integrity, and confidentiality. In accordance with authentication and authorization, the CIA Triad offers an excellent strategy for protecting data security by ensuring that only verified users can interact with sensitive data.

What is CIA Triad?

Confidentiality, integrity, and availability, or CIA Triad, is an acronym that offers a careful framework for comprehending and resolving the complex issues related to protecting confidential information. It serves as the foundation of data security. It is a theoretical concept that, on the other hand, stands in for the underlying principles that guide the development and implementation variety of contexts. Each member of the triad contributes to the protection of information assets in a unique but connected way.

Confidentiality

Information protection from unauthorized access and disclosure is referred to as confidentiality. Sensitive information, whether it be personal or financial must only be accessed by persons or organizations who are authorized to do so. According to Chai, “It is common for data to be categorized according to the amount and type of damage . . . More or less stringent measures can then be implemented according to those categories” (2022). For example, encryption converts plaintext to ciphertext, making it unreadable by unauthorized individuals. Furthermore, role-based, or optional access controls ensure that specific data can only be accessed by those who

have the required authorization.

Integrity

When information is accurate and complete, it ensures that it does not change during processing, transmission, or storage. This is known as data integrity. This part of the CIA Triad is particularly important because any unapproved data change or modification can have significant consequences, such as loss of money, harm to a company's reputation, or legal troubles. For instance, according to Zarour et. al, “incorrect data might become significant health threats for patients and a big responsibility for clinicians, resulting in problems such as scam, misconduct, inadequate treatment and data theft” (2021).

Availability

Availability guarantees that resources and information are available to authorized users when they are needed. This element is especially important in settings where downtime can cause significant disruptions to operations. According to Osazuwa (2023), it is critical to protect information systems against disruptions that might make it more difficult for users to access information. Increased availability can be achieved by regular system maintenance or failover techniques. It is important to note that, in addition to cyberattacks, events like hardware failures or natural disasters can also affect availability.

Authentication & Authorization

A key step in information security is authentication, which is the process of confirming a user's, device's, or system's identity (e.g., through passwords or biometrics) before allowing access to resources. For instance, you enter your username and password when you log in to a website. The system verifies that you are who you say you are by determining whether these credentials

match a legitimate account. According to Kim & Lee, authentication is a prerequisite for authorization (2017). “Access control, or authorization, is the process of determining whether an entity (a device or a user) can access resources” (Kim & Lee, 2017, p. 28). In other words, access control mechanisms make sure that only devices or people with the proper authorization are allowed to interact with particular systems or data. For instance, if you work for a company, depending on your credentials, you might only be able to view particular files after successfully logging in because you are an employee and not an administrator.

Conclusion

Confidentiality guarantees that only those with permission can view or access data. Integrity ensures that data is accurate, protecting against manipulation. Availability ensures that resources and data are kept accessible to authorized users when required. Significant in holding together these three principles and making sure that the access to the information is appropriately controlled and monitored, authentication and authorization are crucial. Knowing the distinction between authorization and authentication is essential because, after a user has been verified or authenticated, authorization controls the access and permissions that can be granted to them. This distinction ensures that only verified users are granted the appropriate rights, maintaining security across sensitive systems and data.

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

Kim, H., & Lee, E. A. (2017). Authentication and Authorization for the Internet of Things. IT Professional, 19(5), 27-33.

Mohammad Zarour, Mamdouh Alenezi, Md Tarique Jamal Ansari, Abhishek Kumar Pandey, Masood Ahmad, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan (2021). Dementia and cognitive impairment: A review of the evidence. American Journal of Alzheimer's Disease & Other Dementias, 36, 1–12.

Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., ... & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, *8*(3), 66-77.