Study on the CIA Triad

Antonio E. SantiagoFigueroa

Old Dominion University

CYSE 200T

Professor Haghnegahdar

September 15, 2024

The CIA Triad, also known as the AIC Triad, is a foundational model developed to guide policies in the world of cybersecurity. It comprises three principles: Confidentiality, Integrity, and Availability, each of which cannot exist in a vacuum without the others. Confidentiality is the idea of keeping access to information away from people who are not authorized to view it. Confidentiality can be categorized by the harm it would cause if accessed by an adversary. Ideally only those with authorization would be able to have access, this is often accomplished by using passwords, two factor authorization and biometric verification. In extreme cases, it is done by keeping the information in a hard copy and storing it to make it impossible to access through technology. Another way to accomplish this is by training personnel on maintaining confidentiality.

Integrity refers to maintaining data in its original form throughout its storage. It is essential to ensure it is not altered during exchange or by unauthorized users. A common way to accomplish this is by requiring permission to access files or utilizing version control programs that track changes over time. If data is altered, it is wise to keep backups to restore it. We can also use nonrepudiation measures to show us who has accessed files and what changes they have done to them.

Availability means that anyone who should have access to the information should be able to access it at any time they desire. This means the information will be held somewhere always available, so it also introduces more possibilities for confidentiality to be threatened. It is accomplished by maintaining system infrastructures and having plans in cases where the system

is compromised. In case of data loss, backups must be kept to restore information swiftly. Equipment and software such as firewalls or proxy servers can guard against downtime, DoS attacks, and network intrusions.

In conclusion, the CIA triad provides a fantastic starting point for protecting information and should be used by everyone. It should guide your decisions when building a system, constantly considering all three principles. While the CIA triad provides a fantastic start, it may not be enough to handle the current security landscape. It gives an excellent theoretical foundation but should be used with other models, such as the Parkerian hexad, the DIE model, O-IMS3, and NIST.

Authorization and authentication concepts can be easily misunderstood but differ in what they try to accomplish. Authentication is the process of confirming a user's identity, which can be done by using a username and password, two-factor authentication, providing a form of identification, or many other ways. Authorization is done after authentication, ensuring the user can access whatever they are trying to access. This is done by confirming the specific user should have access to the resource. Imagining yourself in your house is an excellent example for understanding these different concepts. You hold all rights to your home and can let anyone in or deny anyone from entering. When you invite someone over, you see them at your front door and confirm they are the person you invited; that is authentication. When you let them enter your house, that is authorization.

References

Auth0. (n.d.). What is authorization? - examples and definition. Auth0. https://auth0.com/intro-to-iam/what-is-authorization

Auth0. (n.d.-a). Authentication vs. authorization. Auth0 Docs. https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization

Chai, W. (2023, December 21). What is the CIA triad?: Definition from TechTarget. TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Weingberger, J. (2023, July 19). Updating the CIA triad for today's threat landscape. ShardSecure®. https://shardsecure.com/blog/updating-cia-triad