A Look Into the CIA Triad

Tay Lamell

Department of Cybersecurity, Old Dominion University

CYSE 200T: Cybersecurity, Technology and Society

Prof. Charlie Kirkpatrick

January 28, 2024

There are many concepts that are crucial to successful cybersecurity, but none as crucial as the CIA Triad. Sometimes also referred to as the AIC Triad (Chai, 2022), the CIA Triad is a fundamental set of policy guidelines for ensuring the cyber security of an organization. These guidelines consist of three components: confidentiality, the rules that limit access to the organization's information; integrity, the guarantee that information remains accurate; and availability, the guarantee that the information can be consistently accessed by the right people (Chai, 2022). Examples of the CIA Triad in action can be seen everyday via measures such as university two factor log-ins (Washington University in St Louis, 2024) (confidentiality), backing up data to the cloud (Washington University in St Louis, 2024) (integrity), and malware detection software (Washington University in St Louis, 2024) (availability). Throughout my readings, I saw time and again that it was important for organizations to view the triad as one system instead of a multi-stepped process. When done successfully, the CIA Triad is able to help organizations avoid ransomware attacks and unwanted data modifications (Washington University in St Louis, 2024), and reliably recover data amongst many other things (Irwin, 2023).

From cloud storage to gym key fobs to usernames and passwords, we see the CIA Triad in action everyday, and thus far I would argue that it's one of the most fundamental concepts in cybersecurity. I say this because whereas the NIST framework seeks to help organizations implement stronger cyber security practices, the CIA Triad, at least as I have come to understand it, are those practices at work. From top to bottom, from the producer to the consumer and back, the triad focuses solely on the flow of data and its reliability for all parties involved. This focus brings to the forefront two critical components: authentication and authorization.

While the two terms may seem similar on the surface, they play two very distinct roles. Authorization is the process of selecting who can access what, and authentication is the confirmation that the person trying to access something is indeed who they claim to be (Okta, 2023). Using my own experiences as examples of the two at work: when I have to answer security questions before accessing my bank account on a different device than usual, that's my bank authenticating that I am the owner of said account. When I log into the gradebook system for the school I work at and can't access a student's test scores from previous years, that's because I lack the authorization, or proper credentials, to look at them. If either of these things weren't in place, the information of the student could be left for anyone to see and do with it as they pleased, thus bringing me to the final thing that I would like to discuss.

The most important purpose served by the CIA Triad and the system of authentication and authorization is not merely the protection of an organization's data, but the privacy of the people behind the devices. Though phishing schemes and data leaks still occur today, I hear about them less frequently than I did in the days of AOL. The CIA Triad has helped organizations combat the flaws of the past and given the layman an extra layer of protection in an ever changing technological landscape. Through the use of methods such as two-factor authentication, biometric verifications, multiple security questions prior to changing a password, several layers of data backups, etc, the CIA Triad is the epitome of cybersecurity.

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?jr=on

Irwin, L. (2023, February 14). *Demystifying the CIA Triad: Why It's Crucial for Cyber Security.* IT Governance UK Blog. https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

Okta. (2023, February 14). *Authentication vs Authorization*. Okta. https://www.okta.com/identity-101/authentication-vs-authorization/#:~:text=Authentication%20confirms%20that%20users%20are,and%20access%20management%20(IAM).

Washington University in St. Louis. (2024). *Availability.* Office of Information Security. https://informationsecurity.wustl.edu/items/availability/

Washington University in St. Louis. (2024). *Confidentiality.* Office of Information Security. https://informationsecurity.wustl.edu/items/confidentiality/

Washington University in St. Louis. (2024). *Integrity*. Office of Information Security. https://informationsecurity.wustl.edu/items/integrity/