Elizabeth Howard

CYSE 200T

Write -Up: The CIA Triad

February 2, 2025

How the CIA Triad Uses Authentication and Authorization to Keep Data Safe

The CIA Triad is an information security model made up of Confidentiality, Integrity and Availability measures to protect data. Confidentiality only provides data to authorized users, Integrity means this data will stay accurate and unchanged, and Availability keeps the data accessible when it is needed. Under the Confidentiality pillar Authentication confirms the identity of the users requesting access to the data, while Authorization signifies what permissions the user has with the data. The CIA Triad principal measures of authentication and authorization guarantee that only the correct people have access to and power over sensitive data.

Components of the CIA Triad

The CIA Triad is a cybersecurity model. CIA is an acronym for Confidentially, Integrity and Availability (Chai, 2022). According to Chai, “Confidentiality, integrity and availability together are considered the three most important concepts within information security.” (2022). The confidentiality component of the triad supports the best practices of making sure that access is limited to sensitive data. It is equivalent to privacy. The integrity portion of this model is focused on keeping data from unwanted change as it is used within a system. Finally, the availability pillar secures the hardware assuring that this data is accessible to the authorized parties that need it. All three measures have been brought together over time as more is learned about information systems and what is takes to protect them.

Authentication for Confidentiality

There are many available ways to practice data protection using the CIA Triad. When it comes to confidentiality and assuring that only the correct users have access, one key helper is Authentication. This means making sure of the identity of the user accessing the data. This can be conducted by administering data encryption, creating strong passwords, and most effectively using Two-factor authentication. Authentication determines who is accessing the data, while Authorization determines what the user can do with the data.

Authorization Protocols

According to Permify, “Authorization is a process of granting or denying a user or device access to specific resources, such as files, databases, or network segments.” (Permify.com, 2024) This can be accomplished through protocols such as Mandatory Access Control (MAC), Role-Based Access Control (RBAC), or Attribute Based Access Control (ABAC) to name a few. MAC is a centralized database control that is highly secure and inflexible. RBAC is a protocol which gives permissions based on a user’s role. ABAC is a more flexible system that considers the different attributes of the user like their location or the time to grant permissions. (Bass, and Manor, 2024.)

Conclusion

Cybersecurity Models like the CIA Triad are an excellent way to protect sensitive data. The Confidentiality, Integrity and Availability principals will allow for security, privacy and safety to be at the forefront of your information technology practices. Authorization and Authentication protcols are just a few of the many measures under the CIA Triad that will prove effective in securing data for every user.

References:

1. Chai, W. What is the CIA Triad? Definition, Explanation, Examples. TechTarget.com. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA Updated December, 2023

2. Permify.com, Authentication vs Authorization: How are They Different? https://permify.co/post/authentication-vs-authorization/ Published August 16, 2024.

3. Bass, D. Manor, G. MAC, DAC, RBAC, and FGA: A Journey Through Access Control. https://www.permit.io/blog/mac-dac-rbac-and-fga-and-access-control Published August 12, 2024