The CIA Triad and Where Authentication and Authorization Fit Into It

The CIA triad acts as the fundamental guide for information security practices and stands for confidentiality, integrity, and availability. Confidentiality refers to who has access to the data, integrity involves the information's accuracy, and availability has to do with the accessibility to the data. Within the CIA triad, authentication and authorization come into play in order to help maintain the best possible privacy practices when it comes to keeping information secure. Though the two are often conflated, they do have entirely separate meanings, and they factor into the CIA triad in multiple different ways.

Confidentiality

The aspect of confidentiality, as it relates to the CIA triad, has to do with who can access what information. Within confidentiality there are different levels of privacy required for different types of information and this section of the triad has to do with making sure that the information can only be accessed by trustworthy people who need to have access to it to do their job. Only allowing certain people to have access to certain information helps to maintain confidentiality by lowering the number of accounts with access to the data and thus having fewer potential ways to break into said information. By only allowing people to see what they need to see, there would be less information at risk in the event of a data leak. Also, being selective with who has access and who doesn't mean that only the most trusted employees will have access to any private information.

Integrity

Integrity mostly focuses on the information or data itself and tangentially relates to the people who have access to it. This is because integrity concentrates on the data remaining accurate and consistent rather than the people who are maintaining the data's integrity, which is more of a confidentiality concern. Integrity prioritizes keeping data intact and correct for both the organization and customer/consumer. Incorrect data can lead to a multitude of problems within a system and some ways to prevent the loss of integrity involve encrypting and backing up sensitive information (Hashemi-Pour & Chai, 2023).

Availability

Availability is about making sure that data can be accessed by those who are qualified to access it whenever they need to access it while still making sure the system stays secure (Geek For Geeks, 2025). This means having a low downtime percentage while still being able maintain and update the system accurately and safely within both the downtime and the uptime. Not being able to access a system when needed can be annoying and frustrating to both customers and employees, and it can even cause serious problems depending on what the systems is for. For example, if an online banking service is down when a customer is trying to pay bills or rent, and it takes a while for It to come back up, it could possibly result in a pricy late fee.

Authentication VS Authorization

Often the terms authentication and authorization get mixed up or used interchangeably, however they in fact mean to two different things. Authentication is when a person has to prove that they are who they say they are, and there are many different ways to do this. Some examples of authentication are passwords, that theoretically only the owner of an account should know; biometric authentication, like a fingerprints and face id; and pin numbers (Codecademy Team, 2025). Systems that use two or more methods of authentication tend to be more secure than systems that only use one. A person must authenticate who they are before accessing private information which helps to uphold confidentiality.

Authorization on the other hand has to do with what information or data a user has access to. This relates to both confidentiality and integrity. Typically, if a person has a higher security clearance, they are authorized and trusted to maintain the integrity of more confidential information. Authorization tends to rely on many factors, but the main qualifications are usually experience, knowledge/expertise, and time/dedication to an organization.

Conclusion

The CIA triad is the base for information security systems. CIA represents confidentiality, integrity, and availability. Confidentiality is the information's privacy, integrity is the information's accuracy, and availability is the information's accessibility (Hashemi-Pour & Chai, 2023). Within the confidentiality and integrity sections of the triad, there is both authentication and authorization. Even though they are often mistaken for each other, authentication is verifying identification while authorization is verifying what a person can access (Codecademy Team, 2025). Together these concepts are essential in creating cybersecurity systems.

Works Cited

Codecademy Team. (2025). *Authentication vs Authorization vs Encryption*. Retrieved from Codecademy: https://www.codecademy.com/article/authentication-vs-authorization-vs-encryption

Geek For Geeks. (2025, August 28). *What is CIA Triad?* Retrieved from Geeks for geeks: https://www.geeksforgeeks.org/computer-networks/the-cia-triad-in-cryptography/

Hashemi-Pour, C., & Chai, W. (2023, December 21). *What is the CIA Triad (confidentiality, integrity, and availability)?* Retrieved from Tech Target: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on