Hunter

Bailey

02/22/2026

The CIA Triad and the Processes of Authentication and Authorization

BLUF:

Modern digital security rests upon the foundation provided by the CIA triad and is built in layers through separate yet interwoven channels of authentication and authorization.

The CIA Triad and Its Components:

Security professionals rely on the foundational model of the CIA triad to establish basic security protocols for data and information security and enables them to build effective protections for information systems. Wesley Chai (2022) describes the CIA Triad as "a model designed to guide policies for information security within an organization," with each letter "representing a foundational principle in cybersecurity." These three letters stand for Confidentiality, Integrity, and Availability and form the core of the model, defining the essential goals of information security.

Components of the CIA Triad:

Confidentiality is the principle of privacy and ensures that those not authorized access to it, do not receive it. In the sense of a home, the inside where you and your possessions reside are the sensitive data while the walls, windows, doors, and locks are the mechanisms that ensure no uninvited party gains access without your permission. If an intruder does circumvent those mechanisms, your personal property could be lost, stolen, or damaged. This is what confidentiality aims to prevent in the realm of digital information security

Integrity is the protection of data accuracy, ensuring it is reliable, unaltered, and not tampered with. Keeping in line with our home analogy, integrity is akin to planning dinner based

on the ingredients in your refrigerator. If someone changes the ingredients without your knowledge, the information you relied on is no longer accurate and your plan is unreliable. Integrity is the assurance that the data we utilize and rely on remains accurate and unaltered so that we can utilize it reliably.

Availability ensures that all of the data and systems we protect are readily accessible to authorized users when they need them. Keeping with the home analogy, having the proper key to unlock your front door to be able to access your personal belongings or the items in your refrigerator is the cornerstone of availability. If the key is lost, or you are given the wrong one, all of the resources within it are unchanged and protected but are inaccessible for you.

Defining Authentication and Authorization:

Authentication and authorization are two fundamental tenets of access control and determine who can access a system and what they are allowed to do within it. Authentication is the process of verifying a user's identity to ensure the system knows exactly who is attempting to gain access (Kosinski, 2024). This is done to make certain that a user is allowed entry into a data system and can be accomplished in a few different ways such as single factor, multi factor, or two factor authentication. In an organizational setting, authentication happens when an employee or student scans their ID badge at a secure door. The badge confirms their identity and allows the system to recognize them.

Authorization is the process of determining what an authenticated user is allowed to access or do within a system (Kosinski, 2024). Once a user has been properly authenticated, they can then be granted access to the system and permissions can be assigned based on roles, attributes, or clearance levels. These permissions determine which applications, files, or databases they can use which is done through role based access control or attribute based access control. With the badge example, after an employee or student scans their ID badge, the system may allow them through but still restrict access to administrative areas which ensures that

legitimate users only access what they are permitted to.

Key Differences Between Authentication and Authorization:

Authentication and authorization, while closely related, serve different functions in access control and are often confused with one another. The key difference between the two is the difference of identity versus permissions. Authentication verifies who the user is and then authorization determines what that user can do. There is also the matter of the order of operations for the sequence where a user is always verified prior to determining their level of access. Authentication supports confidentiality by ensuring only legitimate users enter the system and authorization enforces least privilege by limiting their access to what is necessary for them. In the badge example used previously, the authentication occurs when the user scans the badge and verifies their identity, while the system determining which rooms the user can enter is authorization. Distinction as well as understanding that both processes work together in tandem is essential for effective access control.

Conclusion:

The CIA Triad gives us the basic idea of what needs to be protected while authentication and authorization are the tools that help make that protection real. Confidentiality, integrity, and availability, the core principles of information security, cover the fundamentals of information security while identity verification and permissions focus on controlling access to resources. By understanding the difference between authentication and authorization, the principles of information security can be applied to both, resulting in strong access control.

References:

Chai, W. (2022). *What is the CIA Triad? Definition, Explanation, Examples*. techtarget.com https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on

Kosinski, M. (2024, June 28). *Authentication vs authorization*. Ibm.com. https://www.ibm.com/think/topics/authentication-vs-authorization