Ben Easterday

CYSE 200T

15 September 2024

Understanding the CIA Triad and the Difference Between Authentication and Authorization

Data security is the practice of keeping computer systems and related data free from intrusion, modification, and disturbance. Confidentiality, Integrity, and Availability (the CIA Triad) provide the groundwork for this to happen. Organizations can safeguard themselves against various cyber dangers by adhering to this triangle, which governs data protection within an information system. When it comes to managing who can access these secure systems, two critical processes are authentication and authorization. Despite the common misunderstanding, these procedures serve different purposes and have different applications.

The CIA Triad stands for three important concepts:

Making sure that information can only be seen by people who are allowed to see it is what confidentiality means. When it comes to protecting sensitive data like personal identification information (PII), financial records, or intellectual property, this concept is especially important. Encryption, strong passwords, two-factor authentication, and biometric scans are some of the ways that privacy is protected. An organization might secure customer data so that hackers can't read it even if they get a hold of it without the right decryption key.

Integrity is essentially about keeping data's accuracy and dependability across its lifetime. It guarantees that, whether by system faults, human mistakes, or deliberate interference, data is kept free from illegal alterations. Data backups, version control, and checksums help to sustain integrity. In a banking system, for example, the integrity concept guarantees that, following a transaction, the balance is precisely updated free from data corruption or illegal change.

Availability guarantees that, should necessary access to the information and resources required be sought by authorized users. Many services depend on this idea since inaccessibility or downtime may cause major losses for companies or other organizations. Usually, failover mechanisms, redundancy, and frequent backups help to reach high availability. One real-world example is how banks guarantee that strong network architecture and backup systems enable access to their ATMs and online services around the clock.

Every component of the CIA Triad is linked, hence the absence of one part could endanger the whole security of a system. An attack using a Denial of Service (DoS), for example, compromises availability if an assailant disrupts a service. In a same vein, data changed without permission compromises its integrity.

Authorization and Authentication: Different but complimentary

Apart from the CIA Triad, management of system and data access depends on the ideas of authentication and authorization. Though they have different purposes, these two procedures are sometimes employed in concert

Verifying the identify of a user or system is known as authentication. It replies, "Who are you?" Verification guarantees that someone or system claiming access is exactly who they say they are. Common techniques include passwords, biometric data—such as fingerprints or facial recognition—and two-factor authentication, therefore offering an additional degree of protection. When you enter into your bank's mobile app, for instance, the system first authenticates you by requesting your username, password, and maybe a one-time code texted to your phone

Conversely, authorization controls the actions permitted of an authenticated user. It responds to the inquiry, "What can you do?" Following successful user authentication, the system verifies their rights to access particular resources or actions. For example, an ordinary client might be allowed to view their account balance and transfer money once they log into a bank's system, but not access the administrative settings or back-end database.

Everyday office life is a perfect illustration of these ideas in action. One way for a worker to verify their identity is by entering their credentials while accessing their work computer. But, their job function inside the organization could dictate which files, databases, or systems they have access to (authorization). For example, according to SentinelOne, customer service representatives may have access to client records but may not have the authority to change financial data. Those responsibilities would typically fall on managers or IT administrators.

In summary

To summarize, the CIA Triad—Confidentiality, Integrity, and Availability—offers a basic foundation for comprehending and executing successful cybersecurity protocols. When it comes

to protecting data against disturbance, alteration, or unauthorized access, each principle is crucial. For safe access control, it's also important to remember the difference between authentication and authorization. Users' permissions to do certain tasks within the system are defined by authorization, while authentication checks their identities. Taken as a whole, these ideas are foundational to cybersecurity strategies that try to keep private data safe in our increasingly digital society.

Sources:

https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view

https://ieeexplore.ieee.org/abstract/document/6508262?casa_token=I-sNAM5SHoMAAAAA:ervEA7a2G8pyXMsPUFXX9jdWYjagOlCc2pZ50xdyXyS7T5xVO8TT4ZO8vtrTSjpb0_Zlk9bd_g