Understanding the CIA Triad and Authentication vs. Authorization

Jaden Walker

CYSE-200T

Charles E. Kirkpatrick

2/2/2025

Understanding the CIA Triad and Authentication vs. Authorization

A well-structured security model is critical in protecting data, ensuring system integrity, and maintaining availability for authorized users. The CIA Triad, which is Confidentiality, Integrity, and Availability serves as the foundation for cybersecurity policies and risk management frameworks. In my work experience with Active Directory, AWS security, and Splunk, I have implemented security policies to strengthen authentication and access controls.

The CIA Triad ensures that data remains protected, unaltered, and accessible to the right users. Confidentiality means restricting access to sensitive information and preventing unauthorized exposure. A good example of confidentiality is AES-256 encryption because it is used to protect stored data, and only authorized users can access it. Confidentiality can also include multi-factor authentication, Access Control Lists, and Zero Trust Frameworks to prevent unauthorized access (Chai, 2022). In my job experience managing Active Directory permissions, I have implemented Role-Based Access Control which helps enforce user access restrictions and ensures that employees can only access data necessary for their roles.

Integrity is important because it makes sure that information stays accurate and unmodified unless it gets changed by authorized personnel. There are hashing algorithms like SHA-256, cryptographic checksums, and digital signatures that are commonly used to verify data integrity. A good example of this is when downloading software updates, a checksum is provided to ensure that the file has not been altered during transmission. I have seen firsthand that database transaction logs and system monitoring tools like Splunk can help maintain data integrity by tracking any changes made to sensitive information.

Availability is vital because users need to have consistent and reliable access to systems and data. For example, if an organization experiences a Distributed Denial-of-Service (DDoS) attack or hardware failure, and availability is compromised it halts business operations. So implementing High availability is a great way to avoid something like this happening. I have personally set this up at my current job using AWS. High availability is basically when you set up your infrastructure across Availability Zones, which is hosted by different physical data centers across the country. In this scenario, imagine your data center on the east coast becomes compromised, then the infrastructure you have hosted on the West Coast would pick up the slack until the data center is restored.

Authentication is the process of verifying a user's identity. This can be done using passwords, biometrics (fingerprints, facial recognition),and security tokens. A real world example of this would be logging into a computer using a CaC card. As I work in government contracting, everyone gets a CaC card for authentication and you cannot log into anything on government equipment without one.

Authorization, on the other hand, is where you determine which services a user can utilize. It ensures that users can only access data and resources they are permitted to use. This is often time referred to as Zero Trust. This means that users only get access to what is absolutely necessary for their job functions. A good example is an employee logging into a corporate network and they may have access to internal documents but not financial records or administrative settings. Organizations need to enforce authorization through Role-Based Access Control to ensure there is no human error. In AWS, Identity and Access Management policies dictate what permissions a user or service has, ensuring that access is restricted to only what is necessary (Cyble, 2024).

In conclusion, the CIA Triad and authentication/authorization principles are essential for securing modern information systems. Confidentiality, integrity, and availability ensure that data remains protected, unaltered, and accessible only to authorized users. Authentication verifies identity, while authorization enforces security policies by restricting user actions. Through my experience managing Active Directory security policies, AWS IAM configurations, and SIEM monitoring, I have seen how properly implementing these concepts enhances security and minimizes cyber risks. Organizations that enforce robust authentication protocols, strict authorization policies, and CIA-based security controls can significantly reduce threat exposure and operational disruptions.

References:

Chai, W. (2022). What is the CIA Triad? Definition, Explanation, Examples. TechTarget.

https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Cyble. (2024). Identity & Access Management in the Cloud: Best Practices for Authorization. https://cyble.com/knowledge-hub/identity-and-access-management/

NIST. (2023). Ensuring Data Integrity in Information Security Policies. National Institute of Standards and Technology.https://www.nist.gov/topics/cybersecurity/data-integrity

SANS Institute. (2023). Cybersecurity Frameworks for Availability & Disaster Recovery.https://www.sans.org/white-papers/cybersecurity-frameworks/