The CIA Triad & the AAA Framework

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

February 18, 2025

Assignment:

Using the Chai Article, along with additional research you will conduct on your own, describe the CIA Triad, and the differences between Authentication & Authorization, including an example.

Summary

The CIA Triad is the "Gold standard" for organizations to use when securing their networks and technology. Confidentiality, Integrity, and Availability principles help build a theoretical baseline for any organization to safeguard its information. Using the AAA Framework—Identification, Authentication, Authorization, and Accounting—an organization can improve its relationship with information. The organization also protects and strengthens its relationship with its employees, third-party vendors, business partners, and customers.

What is the CIA Triad?

The CIA Triad is the 'Holy Trinity' of cybersecurity. The acronym is 'Confidentiality, Integrity, and Availability' (Hashemi-Pour, 2025). Confidentiality ensures that information is accessible only to authorized personnel (e.g., encryption, access controls, two-factor authentication). Integrity ensures data remains accurate and unaltered (e.g., checksums, hashing,

digital signatures, certificates, non-repudiation, air-gaped systems). Integrity ensures that information and resources are consistently and readily accessible when needed, preventing users from modifying data without detection. Availability includes properly maintaining software and hardware technical infrastructure systems that store and display the information (e.g., redundancy sources like RAID, fault tolerance, and patching). Most organizations aim to ensure 24/7 network availability year-round— the gold standard of high availability is 99.999% uptime or a maximum operational downtime of 5.26 minutes per year (Barta, 2019). Confidentiality, Integrity, and Availability are baseline principles for security frameworks: organizations will formulate, manage, and improve upon them using the AAA Framework (Messer, 2023c). The AAA Framework has four key components: Identification, Authentication, Authorization, and Accounting.

Identification

Identification is when a user claims an identity utilizing one or more unique attribute(s) or qualifier(s) (e.g., username, email address). The goal is to ensure the information is legitimate and accurate on the front end for later use. For example, an organization may implement identity proofing before creating a user's account and conduct annual reviews or attestation events during the life of the account. The organization will require the user to submit personal details or formal identification documents like a driver's license, passport, or monthly household bills showing one's full name and address. From my experience, organizations required that I provide many different forms of personal identification when taking on new or changing employee roles, including using specific systems and applications with internal departments and third-party business partners (e.g., ID.me account creation to gain access to VA mortgage records). Also, I have had regulatory agencies request upfront information when conducting background checks while becoming an

executor of estates for various family members. Thus, Identification is showing who a user claims to be to third parties, not someone or something else.

Authentication

Authentication is verifying the identity of the user, device, workstation, or system against a stored user database using passwords, biometrics, and Multi-Factor Authentication. In other words, authentication ensures individuals or entities are who they claim to be during a communication or transaction. There are five standard authentication methods: something you know, like a password or PIN (Knowledge Factor); something you have, like hardware/software tokens or one's phone (Possession Factor); something you are like biometric fingerprints or facial recognition (Inherence Factor), something you do (Action Factor), and somewhere you are like an IP address or mobile device location services (Location Factor) (Nieles, Dempsey, & Yan Pilli, 2017; Messer, 2023a). Mult-Factor Authentication (MFA) is the core of modern-day security processes and uses the abovementioned standard authentication methods (Messer, 2023b). Thus, MFA security requires a user to provide independent categories of layered identification credentials to gain access to their accounts or confidential information at an organization.

Authorization

Authorization determines the permissions or access levels of authenticated users. The goal is for users to access what is appropriate to their role in the organization. To achieve these security goals and reduce the risk of insider/external threats gaining unauthorized access to certain information, an organization will implement different access control models/lists (ACLs) with segmentation. Role-Based Access Control (RBAC) assigns users to roles and assigns permissions to those roles, mimicking the organization's hierarchy and following the principle of least

privileges. For example, an IT Department may segment the Accounting and HR Departments from one another, creating separate group policies and accounts for those users to access different resources based on their unique needs and responsibilities to the organization. The IT department can also create a higher-level group called 'Employees' to allow each department to gain access to essential employee resources like Payroll, Intranet Wikis, and Department Contact Lists. In coding terms, the Employee group will act like the parental group, and the Account and HR departments will be housed within the Employee group, 'inheriting' the parent's traits like biological children. Lastly, the IT Department itself has ACLs and RBACs for their different employees: a lower-level system administrator may have limited access—to read, write, and modify—applications or documents to fulfill their daily job tasks. However, a higher-level system administrator may have complete access control to handle daily job functions AND networkwide emergencies, outages, and threat actors. Thus, Authorization uses identification and authentication, determining what access a person can have and use that is relevant to their own role within an organization.

Accounting

Lastly, Accounting or 'auditing' is when an organization keeps tracks and records every user activity, including logins, actions, and changes. Accounting helps detect security incidents, identify vulnerabilities, and provide evidence in case of breaches. IT Departments will use SIEM (Security Information and Event Management) tools like Splunk, Azure Sentinel, or ELK Stack for real-time monitoring. Log capture details may include user identity, timestamps, accessed resources, actions performed, and sourced IP addresses. These recordings may seem reactive rather than proactive when trying to prevent human errors or threats; however, tracking and recording events from all network activity can help organizations understand the root causes and behaviors of those errors and threats and then modify existing security policies to reduce the likelihood of

them repeating or prevent them altogether in the future. Thus, Accounting tracks and records all user behavior and actions on a given network to help safely monitor and ensure network performance.

Conclusion

The CIA Triad is the 'Hallmark' and 'Gold standard' for developing secure networks. When combined with the AAA Framework, organizations have more power and flexibility to identify, protect, detect, respond, and recover information. Authentication and authorization look very similar to the untrained eye, but they are vastly different. For example, an authentication scenario is an employee logging into their company's network using their username and password (proving their identity). An authorization scenario is that after logging in, the employee's access level determines whether the person can view confidential reports, install software, or access specific network devices. Both authentication and authorization work together to ensure that only trusted individuals access the network and can only perform the authorized actions.

References

Barta, K. (2019, January 28). *99.999% vs. 99.9% Uptime: Difference Explained*. Retrieved from Intermedia: Cloud Communications: https://blog.intermedia.com/99-999-uptime-vs-99-9-uptime-the-difference-two-extra-nines-makes/

Hashemi-Pour, C. (2025, January 26). *What is the CIA Triad? Definition, Explanation, Examples*. (W. Chai, Editor) Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Messer, P. (2023, November 1). *Authentication, Authorization, and Accounting - CompTIA Security+ SY0-701 - 1.2*. Retrieved from YouTube: https://www.youtube.com/watch?v=AhaZtj5P2a8

Messer, P. (2023, December 6). *Multifactor Authentication - CompTIA Security+ SY0-701 - 4.6*. Retrieved from YouTube: https://www.youtube.com/watch?v=MpIzA4fNWew

Messer, P. (2023, November 1). *The CIA Triad - CompTIA Security+ SY0-701 - 1.2*. Retrieved from YouTube: https://www.youtube.com/watch?v=SBcDGb9l6yo

Nieles, M., Dempsey, K., & Yan Pilli, V. (2017). An Introduction to Information Security. *Computer Security, NIST Special Publication 800-12 Revision 1*, 101.

Ommeren, E. v., Borrett, M., Kuivenhoven, M., IBM, & Sogeti. (2014, April). *Staying Ahead in the Cyber Security Game: What Matters Now.* Creative Commons.