Anthony Miranda Aponte

June 27, 2025

Journal - Portfolio Reflection

Never leave security until the end. This message stood out the most for me throughout this course. This message is so critical to prevent catastrophe from happening in the future. If we start security early the whole system structure will rely on it rather than it being just a tarp over a roof. Looking back at one of the articles from a previous module, there are steps we can take to be able to start with security such as threat modeling, utilizing and adopting coding standards, implementing monitoring tools. (Ryther, 2022) Having this mindset could lead to lower costs on repairs which companies would appreciate avoiding lawsuits for missed flaws in the development.

We learned on this course how important risk assessments can be. A risk assessment main goal is to point out threats that are within the system as a whole and find ways to mitigate by creating a plan to tackle them with specific tools such as how we did in our project utilizing Google test to flag any errors in the system. This is a crucial thing to do in the developing world because without assessing minor or major threats could lead to a significant financial burden. (Finn & Downie, 2024)

We recently went over zero trust, and it is one of the mentalities I try to keep everyday not only on programming but also in my career with aircraft maintenance. While we would love to trust anyone and everyone is doing the right thing for the right reasons that are not always the case. Which means we need to consistently verify what others do to monitor things that are being done safely and correctly. In a software developing job there are steps to take for the zero-trust concept, which in the blog posted by Data Loss Prevention explains it further. Prioritize authentication such as user trust, data trust, or even application trust. Implement the least privilege user and device access to have prevent unnecessary users in the system. Introduce micro-segmentation to reduce lateral risks. (Brook, 2024)

There are multiple ways to establish and implement security policies into a system as this course has thought us previously. One of the ways to do this is by the Triple-A framework. Triple-A framework stands for authentication, authorization, and accounting, which is the foundation for managing access to data in a system. Authentication creates a protection to account for unauthorized access with a two-factor authentication or username & password. Authorization permits access to data given that the user or system has the proper authentication. Accounting logs and monitors who are accessing what data and keeps a record for auditing. Implementing these major components can create a good level of security for appropriate access and monitorization. (Mylonas, 2018)

Reference

Ryther, J. (2022, February 6). *Don’t Leave Security to the End.* Medium. <https://medium.com/%40jryther91/dont-leave-security-to-the-end-ca13b107d4>

Finn, T. & Downie, A. (2024, May 7). *What is risk mitigation.* IBM. <https://www.ibm.com/think/topics/risk-mitigation#:~:text=Risk%20mitigation%20is%20one%20of,strategic%20management%20errors%20and%20accidents>.

Brook, C. (2024, October 23). Understanding the zero trust security model to safeguard digital infrastructure | Digital Guardian. *Data Loss Prevention*. <https://www.digitalguardian.com/blog/understanding-zero-trust-security-model-safeguard-digital-infrastructure>

Mylonas, L. (2018, November 27). *What is AAA security? An introduction to authentication, authorization, and accounting.* Codebots. <https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting>