Robert Kratzke

CS-405-T5550

06/25/2023

Final Reflection

Throughout this course, we have discussed various topics and concepts related to security in software development.

One of the main aspects of security we discussed was the concept of not leaving security to the end. This concept refers to the idea that security is a core aspect of software development and that addressing security concerns should be a continuous effort throughout the software development lifecycle.

Another concept we discussed is the evaluation and assessment of risk as well as the costs and benefits associated with the mitigation of those risks. When analyzing risks and performing a cost-benefit analysis it is important to prioritize vulnerabilities and determine the most cost-effective strategies to mitigate them. There will always be vulnerabilities as the landscape of software development changes continuously. However, risk can be minimized to an acceptable level.

Another concept we discussed is zero trust. Zero trust refers to the prevention of access to the system by default. Before anything connects to a system the entity must be verified. This minimizes the risk that an unauthorized entity gains access to the system.

The last concept we discussed was the implementation and recommendations of security policies. Security policies are only as good as their implementation and thus if a security policy isn’t implemented properly security concerns and vulnerabilities can go unchecked. This is why it is essential to address security throughout the entire software development process. In terms of security recommendations, there are a few security policies that are simple and low-cost that can be implemented across the board. Taking on the policy of “default deny” and the principle of least privilege can significantly improve security while causing little friction in implementation and cost.