Luke Peters

Professor Mike Prasad

CS – 405

20 June 2023

8-2 Journal: Portfolio Reflection

Throughout this course, I have gained valuable insights into software security and its integration throughout the development lifecycle. I have learned about the importance of secure coding standards, risk assessment, Zero Trust architecture, and security policy implementation.

Adoption of a secure coding standard, and not leaving security to the end:

One key lesson from this course is the significance of adopting secure coding standards early in the software development process and prioritizing security throughout the entire lifecycle. These standards provide guidelines and best practices for developers to write secure and robust code, mitigating vulnerabilities like injection attacks and cross-site scripting. Integrating security from the beginning is crucial, as leaving it until the end can lead to costly patches or system compromise. Proactive measures such as security reviews, code audits, and penetration testing help identify and address vulnerabilities more efficiently.

Evaluation and assessment of risk and cost-benefit of mitigation:

The course also covered risk evaluation and cost-benefit analysis of mitigation strategies. Assessing software vulnerabilities allows organizations to prioritize security efforts and allocate resources effectively. Techniques like threat modeling and vulnerability scanning help identify potential threats and evaluate their impact. The cost-benefit analysis aids in selecting the most effective mitigation strategies, considering the costs of security measures versus potential losses from incidents.

Zero Trust:

Zero Trust architecture was another significant topic discussed. This security framework challenges implicit trust in users and devices, emphasizing strict access controls, continuous authentication, and constant monitoring. Implementing Zero Trust requires a comprehensive approach including identity and access management, network segmentation, multifactor authentication, and encryption. Its benefits include protection against insider threats, lateral movement, and unauthorized access.

Implementation and recommendations of security policies:

Furthermore, the course explored the implementation and recommendations of security policies. These policies define rules and guidelines for an organization's security practices, covering areas such as access control, password management, data handling, and incident response. Well-defined policies aligned with industry standards and regulations are crucial. Regular reviews, employee awareness programs, and enforcement mechanisms ensure compliance, with senior management playing a vital role in driving policy adoption and enforcement.