**8-2 Journal Portfolio Reflection**

Matthew J. Rearick

Department of Computer Science

CS-405 Secure Coding

Prof. Farley, Toni

8/25/2024

**8-2 Journal Portfolio Reflection**

### **Adoption of a Secure Coding Standard and Not Leaving Security to the End**

Adopting a secure coding standard early in development is not just a good practice, it's a crucial step for mitigating potential vulnerabilities. Secure coding practices, such as those outlined in the SEI CERT C++ Coding Standard, stress the importance of integrating security measures from the onset of development rather than as an afterthought. This proactive approach, which aligns with the 'shift left' philosophy, can lead to more robust and secure software, reducing the time and resources spent on remediation later.

### **Evaluation and Assessment of Risk and Cost-Benefit of Mitigation**

Effective risk management in software development involves evaluating the potential risks and assessing the cost-benefit of implementing mitigation strategies. Risk assessment tools, such as static analysis, can help identify vulnerabilities early, allowing developers to weigh the costs of mitigation against the potential impact of a security breach. For instance, while implementing certain security features may increase development costs, the long-term benefits of preventing a security incident often outweigh these initial investments. Moreover, organizations must consider the reputational and financial consequences of a security breach, which can far exceed the cost of implementing robust security measures. The decision to invest in security should be based on a comprehensive analysis of the risks and the potential return on investment regarding reduced vulnerability and enhanced trust.

### **Zero Trust**

Zero trust is a security model that operates on the principle of "never trust, always verify," ensuring that access to resources is granted based on strict identity verification and continuous authentication. Unlike traditional security models that rely on perimeter-based defenses, zero trust assumes that threats can originate outside and inside the network. This approach requires organizations to implement multifactor authentication, encryption, and continuous monitoring to ensure access is tightly controlled and limited to authorized users. Adopting a zero-trust framework is especially important in today's interconnected and distributed environments, where data is accessed across multiple devices and networks. By focusing on identity and access management, zero trust minimizes the risk of unauthorized access and enhances the overall security posture of an organization.

### **Implementation and Recommendations of Security Policies**

The successful implementation of security policies requires a comprehensive approach encompassing clear guidelines, regular training, and continuous evaluation. This ongoing evaluation is crucial as it reassures you that your policies are effective and adaptable to new challenges. Security policies should be tailored to the organization's specific needs, addressing key areas such as data protection, access control, and incident response. Recommendations for improving security policies often include adopting best practices, such as implementing encryption protocols, regular security audits, and employee awareness programs. Additionally, policies should be regularly updated to address emerging threats and changes in the technological landscape. By fostering a security awareness and accountability culture, organizations can ensure that their security policies are effective and adaptable to new challenges.