Scott Cain

October 26, 2025

**Reflection: Project Two Security Policy Presentation**

**Adoption of a Secure Coding Standard**  
Secure coding standards must be adopted early in the development lifecycle—not retrofitted at the end. Delaying security implementation increases the risk of embedded vulnerabilities and costly rework. In my presentation, I ranked CS01–CS10 based on exploitability and impact, showing how early adoption of standards like input validation and proper error handling directly prevent injection and logic flaws. Security must be treated as a design requirement, not a final checklist item.

**Evaluation and Assessment of Risk and Cost Benefit of Mitigation**  
Risk assessment must balance exploit likelihood against mitigation cost. In my presentation, I used a simple matrix to show how high-impact vulnerabilities justify immediate action, while lower-risk items may be deferred. The cost of mitigation—such as implementing multi-factor authentication or static analysis tools—is often outweighed by the cost of a breach, especially when reputational damage and compliance penalties are considered.

**Zero Trust**  
Zero Trust architecture assumes no implicit trust—every access request must be verified. In my presentation, I recommend enforcing Zero Trust through multi-factor authentication, role-based access control, and continuous logging. By applying Zero Trust to both internal and external systems, organizations reduce lateral movement and insider threats, which are often overlooked in perimeter-based models.

**Implementation and Recommendations of Security Policies**  
Security policies must be actionable, enforceable, and aligned with technical capabilities. I recommended policies for encryption in flight (TLS), at rest (AES), and in use (secure memory handling), supported by automated testing and static analysis. These policies reflect best practices and were validated through tools like Cppcheck and Visual Studio. I also emphasized the need for centralized logging and patch scheduling, which support accountability and rapid incident response.