Module Eight Journal

Jordan Whitney

CS-405 Secure Coding

Professor: Alan Spencer

8/22/2025

Adopting a coding standard and how security should be engineered into programs, rather than inspecting for problems to occur making security measurable and automatable. I think you should follow established standards like SEI CERT C/C++ guidelines, and others provide measurable and enforceable criteria for having secure code. You will be using things like automation through static analysis tools, compiler hardening, dependency scanning, and unit tests. This allows teams to prevent vulnerabilities systematically, rather than reacting to them after deployment.

Realistically you can’t fix everything at once, so structured evaluations and assessing risks require balancing security investments with business priorities. Structured risk models help to determine where to focus resources, since not every vulnerability can or should be addressed immediately. By making risk-based decisions, teams and companies can prioritize mitigations that address entire classes of vulnerabilities, reduce operational overhead, and provide more structured improvements in security posture.

Zero trust involves strong coding discipline, since applications must enforce authorizations and validation constantly across multiple requests. It shifts the mindset away from perimeter-based defense toward continuous verification of identity, device health, and context. When implemented effectively, zero trust not only minimizes the impact of breaches but also strengthens resilience by ensuring security decisions are enforced at every layer of the architecture.

Finally, the implementation and recommendation of security policies provides the organizational structure that makes these practices sustainable. Security policies translate high-level principles into enforceable expectations for secure development, data protection, identity management, and vulnerability response. These elements together the secure coding standards, structured risk evaluation, zero trust, form a holistic security strategy. Each reinforcing the other, by combining these approached, companies can build software that is both resilient and cost-effective, while enforcing security into every stage of the development process.