Anthony Quijano

22 August 2021

CS 405

Course Reflection

**Secure Coding: Reflection**

Throughout this course, I have come to better understand the significance of a secure coding standard and the importance of tight IT security policies like the “zero trust” policy. The SEI CERT C++ Coding standards were an excellent starting point in the implementation of a secure coding standard. Understanding the challenges of upholding a secure coding standard was also an important aspect of this course. Often, software engineers will struggle to understand the severity of code vulnerabilities and the importance of coding standards implemented to avoid them. An exceptional engineer will be able to identify these developers and help them understand why the standards exist. Along with this comes the ability to communicate to team developers the importance of not saving security to the end. Often, a developer will fail to implement a fully secure feature because they may feel the responsibility of security lies with someone else. Other members of a team or organization may share this sentiment and may unintentionally keep passing on this responsibility. While it may be true that there is a security team within an organization, it should not be entirely that team’s burden to bear. Implementing security at multiple steps in the SDLC is the most effective way for secure application development.

Adopting a “zero trust” IT security policy is another highly effective method for improving organization security along with the user experience. To ensure user authorization remains consistent across multiple company applications, a method like SAML can be used for single sign on (SSO). SSO is one of the key principles of implementing a “zero trust” security policy. This allows users to have a central server to which they authenticate and creates a smoother login process. Using SAML for SSO also improves organization security because user access can be shared across all applications within the organization. This means a user must be explicitly granted the ability to perform an action and cannot use a successful sign in to grant themselves permissions to other applications within the organization.