Michael Palatta

CS 405 – Secure Coding

Prof. Joseph Conlan

26 June 2021

**Journal 8-2: Portfolio Reflection**

This course taught me how to effectively plan for a DevSecOps project through many different strategies. There are industry standards that should be used in order to secure your code covering topics like referencing standards documents, implementing triple-encryption and triple-A policies, structuring an IT infrastructure in accordance with defense-in-depth blueprint, and exercising the principle of least privilege. You can adopt a solid foundation by using documentation such as Carnegie Mellon University’s SEI CERT Coding Standards guide, which provides thorough information about potential code vulnerabilities in Android, C, C++, Java, and Perl. It is important to incorporate security from the beginning of a coding project, throughout each iteration, and tie everything together by the final publication of the code.

The goal of a comprehensive IT security plan is not to eliminate all vulnerabilities possible, because that will always be nearly impossible. There will always be malicious programs launched by hackers that continue to progress further than the state your code is in now. The goal is to mitigate risk and exposure as best as possible. This emphasizes a defense-in-depth layout from physical security to software security. Also, triple-encryption and triple-A practices must be implemented for the highest level of mitigation. The triple practices also emphasize the rule of zero trust, where attack vectors are anticipated to be everywhere and from everyone all at once. The encryption at rest, at flight, and at access essentially trusts no one with, or without, proper access to the data to be able to read without the correct keys. The authorization and authentication rules in particular are key in zero trust policy, ensuring that any prospective user on the system needs to undergo a rigorous verification protocol. Accounting, or auditing, is to be used after the fact for reflection and evaluation of how successful the other rules are. Having a comprehensive security plan is effective, only if your team respects it and abides by the rules. Furthermore, they need to support it and reflect those principles in their own work while coding securely.