**Portfolio Reflection**

Eric Breznen

Southern New Hampshire University

CS-405-13379-M01 Secure Coding 2024 C-5 (Sep - Oct)

Professor Mimi Tam

10/24/2024

The adoption of a secure coding standard is only the beginning of secure programming. It sets guidelines for the developer or group of developers to follow so that they can, using best practices, code individual pieces of a program securely. But, adopting the standard also encourages other good practices, and it encourages designers and developers to keep security in mind and centric to their practices from the first diagram to implementation and beyond.

Technology is always evolving, and that goes for pure development and for methods of exploiting it. Carefully evaluating your work for known risks with existing algorithms and libraries and defining a method of determining the vulnerabilities within invented code is well worth the cost, and knowing the potential cost of repairing code after a breach, both technical (the easy part) and reputational (the hard part) is important in determining where to prioritize the main focus. It is important to think like someone who is trying to breach your defenses and patch any vulnerabilities that can become very expensive liabilities *when* your program gets breached. It can be something as simple as using std::string instead of a character array to prevent someone from overloading the assigned buffer for an input field or making sure that that exception you threw in the event someone tried to divide by zero actually handles the error rather than letting the code continue to something as complex as multiple layers of validation to make sure there isn’t any unauthorized access to the program or splitting up programs into multiple modules on multiple servers to make it more of a maze to access.

Another foundational concept in creating a secure system is not trusting any client device, assume anyone trying to access your servers are there to attack it and make them go through layers of protection, direction, and limitation in order to make sure that they stay within the system where they are supposed to stay. This has become increasingly important as working remotely is becoming more and more prevalent and more and more people are enjoying the freedom of working on the go as this means your trust can no longer be limited to the walls of your office building. The idea of anyone being able to access servers from anywhere means that it is all the more important to use methods such as single-sign-ons, LDAPs, proxies, VPNs, and many other methods to make sure that your sensitive data and proprietary information stays secure and safe.

Having a policy is great, but useless if it is not being used. Implementation and enforcement are vital practices to protecting a system, making sure that everyone has the resources necessary to be able to read and understand the policies and implementing defined consequences for violating the policies based on severity and potential risks that they create is just as important as building and nurturing an environment that encourages loyalty.