Matthew Johnson

4/25/2023

CS-405-R4887

***Journal: Portfolio Reflection***

**Adoption of a secure coding standard, and not leaving security to the end**

By adopting the policy of setting security code standards, you essentially give yourself a finish line to aim for. Instead of making some security and saying, yeah that’s good enough. You instead create a visible measurement to tell if you are secure enough. If not, you go back and fix your mistakes. To that end, you should never leave security to the end. If you must go back and edit the code, you could have already implemented there are many risks involved. You might break it, or even worse have to redo it altogether.

**Evaluation and assessment of risk and cost benefit of mitigation**

When dealing with security it is a must that you figure out how much security you actually need. You could vie for the most amount of security, but you run the risk of slowing down or hampering your program to the point where users won’t want to use it. Or too little and you run the risk of crashes and data leaks. You need to way how much security you need by what threats you will most likely face. And then find cost effective, but not compromising, ways to ensure it.

**Zero trust**

The concept of Zero-trust helps us to limit which users have access to our data. A user could sign in with their username/password, but they need to send additional verification by way of two-factor authentication. This helps with the zero-trust policy because the user technically hasn't even touch data storage or sign in info. The system will only allow the sign in attempt if the second verification works. This prevents hackers from accessing data because even if a hacker finds your login info, they need access to the two-factor which they may not have. Also, two factor apps often have alerts to let you know of sign in attempts allowing you to catch faulty ones.

**Implementation and recommendations of security policies**

I would implement a security policy similar to how we did on this course. Both a presentation and an easily referenceable document that everyone has access to. This way everyone has access and can check themselves and each other.