8-2 Journal

Steven Anderson

There are many things I learned throughout this course and all of them are things that moving forward in my life and career will be important to know and employ in my own work. From the secure coding standards to mitigation assessment of both risks and costs and the concept and practice of zero trust security. Things that moving forward I will be able to implement and use as recommendations in the field to help increase the overall security of the projects I am working on.

Secure coding standards is a vitally important part of this course that I will take with me. Learning what resources I can tap into to do secure code testing and to review the best practices until they become second nature to me will be something I will always remember. I will also be looking for similar secure coding standards for other languages I find myself working with like Java and Python. Creating new guides to reinforce what are important secure coding practices for those languages that may differ or be language specific. The testing tools are a huge part of this as well since I will be able to take knowledge of what kind of tools are available and how to best use them into working on future projects.

Mitigation assessment is another key part of this course I hope to adopt into my regular style of working. Being able to evaluate what may become a problem within code can help to prevent major risks from forming but also knowing what threats or risks are in comparison to the costs to mitigate them is very important knowledge to have. The three forms of encryption being a good example in that encryption at rest is the most cost-effective way of keeping data safe and but that encryption in flight is very important for any data being sent over network to ensure that data makes it safe and isn’t stolen in the process. But that encryption in use for data is one of the most cost ineffective methods in that the cost of implementing it can be huge in terms of processing power and energy compared to the two other but has more specific use cases where this kind of encryption can be a very helpful tool. I already plan on seeing how I can use encryption methods to enhance previous projects for my CS-499 class coming up.

Zero trust is something from this course that while I was aware of the concept didn’t know the name of it and how deeply it can be implemented. I knew that on networks and systems the less you give inherent trust to users the safer the network is and coupled with segmentation of the network can help prevent cascading attacks throughout the system. What I didn’t know was the name of the concept and how it can be implemented using least trust and how determining least trusts is done. I now know that it can be a concept that you can implement into almost every layer of a defense in depth security layout and will increase the security of the program and network massively. Perfect for mitigating the damage done during an attack and keeping risks down during operation of the network.

I plan on implementing a lot of what I learned during this course in my future along with implementing a lot of it in my CS-499 course coming up since the security practices and secure coding techniques I learned in this course will definitely improve previous assignments from another course that I will be working on improving. While I won’t be using C++ for most of the work, I will be able to take what I learned and build similar secure coding playbooks for other languages I will be using. I will also take what I learned and be recommending these kind of security practices in future jobs and projects to ensure what I am working on is secure and the best possible product that I can produce. The concepts of security I learned in this course also will help me to explain to others why certain security practices are so important. Like strong passwords with multilayer security for things like personal Wi-Fi networks and online accounts can be the difference between data safety and possible data theft or identity theft.