Ashley Kimrey

CS 405

Doctor Tam

08/20/2025

Module Eight

One of the biggest takeaways for me has been the importance of adopting a secure coding standard and not waiting until the end to think about security. The readings on secure coding practices made it clear that if security is pushed off until the last step, the cost of fixing problems is much higher and often results in rushed patches rather than real solutions, like McGraw pointed out in Software Security. Building security into the process early makes it feel like second nature and it sets the expectation that secure practices are just as important as the functionality of the code.

I have also come to see how important it is to evaluate and assess risk in a realistic way. The NIST Risk Management Framework really helped me see that not every risk is equal, so it is necessary to look at the likelihood of something happening and the impact it could have. Sometimes the cost of fixing or preventing an issue might outweigh the actual risk and other times the opposite is true. Understanding this balance helps prioritize what really needs attention and keeps security decisions grounded in both protection and practicality.

The idea of zero trust also changed the way I think about security. The course readings on zero trust, including Forrester’s work on the model, drove home the mindset that no one is safe. That sounded intense at first, but it makes sense in today’s world where threats can come from inside or outside a network. Zero trust means that no one is automatically trusted and every request has to be verified. At first it feels strict, but it actually creates a safer environment where access is limited to exactly what is needed and nothing more.

Finally, I have realized how important it is to have strong security policies in place. Our readings on encryption and the Triple A framework which includes authentication, authorization, and accountability showed how policies turn these ideas into real steps. They set clear expectations for how things like encryption should be applied, how users should be verified, and how actions should be logged and audited. They also make sure that everyone is on the same page from developers to management and that security is not just an afterthought but a core part of the system.

Overall, I see how all of these pieces connect. Secure coding standards, risk assessments, zero trust, and strong policies all work together to build a solid foundation where security is not just added in at the end but is built in from the start.