Chris Gollnick

CS405-T4538

Journal 8-2

20 April 2022

Throughout this course, multiple topics related to security have been discussed. Many of these offered different insights or views on the topics and brought to mind questions of how I could use this information in the future in my career and how to implement it.

Adoption of a secure coding standard and not leaving security to the end brought to light a lot of views of how and when to address security. It brings up the idea that if you leave security to the end of the process, it can cost a lot more in time, money, and resources than if you incorporated it from the beginning. This concept seems like one you don’t really think about until you’re in a paid environment and on a team. As such, I found through this topic that incorporating security early and while going through the process can eliminate a lot of issues such as needing to redo entire sections of code later on or running into issues when merging with other developers’ parts by adapting to standards early.

Risk and cost benefit of mitigation offered further insight into considering what happens when you don’t integrate a security policy or don’t deal with security. I think this concept highlights the idea of how mitigating security risks may be a large upfront cost, but thinking about how you sell that to a project lead or a supervisor that is not tech knowledgeable and how to convince them that the cost is worth the risk. While on the other hand trying to make them understand that what happens when you do nothing could potentially lead to damages to the company in the form of image, reputation, and finances.

Zero Trust offers a view on how to view security and having a proactive method to prevent attacks. While Defense in Depth works well, it is really a reactive method. Zero trust gives a more offensive strategy to keep malicious actors out of internal data. The idea of having higher levels and requirements to authenticate into a website or application and then require constant verification each time they try to change something or go somewhere else provides a tedious but possibly effective manner in which to deter a malicious actor from accessing things you don’t want them to.

Implementation and recommendation of security policies gave a strong look at how you craft, detail, and present a security policy. This part seemed critical in understanding exactly what goes into crafting a security policy but also how the implementation and how you should persuade and present your argument for implementing it should work.

All of these concepts gave a lot of good information, critical thoughts, and views to consider with security. I think not leaving security to the end and implementing a security policy may be the more beneficial ones for me in my career. When in the development process all of them will be useful, but as a tech director, these two can transfer more to other areas beyond development a little easier. Not leaving security to the end will certainly be something I can translate into non-tech areas when we discuss building projects and how new practices will be implemented. Implementing a security policy I feel will be beneficial as my department grows and evolves I will be implementing strong security measures and the need to convince administration that they need to adhere to these will be critical. The skills learned from that aspect will definitely be aiding me in that part of my job.