CS 405 8-2 Journal: Portfolio Reflection

Larry E Williams Jr

Southern New Hampshire University

Prof. Mills

06/22/2023

When I think back on the most important things I learned from the class, one of the things that sticks out the most is the requirement of including security considerations from the earliest stages of any project by adopting a secure coding standard. This is one of the most important things I learned. My view of how to approach secure code has been profoundly altered as a result of this strategy of integrating security into the very fabric of the development process, as opposed to tacking it on at the very end. Not only does it make the process easier to complete, but it also makes the system inherently more safe when security concepts are built in right from the beginning.

The importance of doing risk assessments and cost-benefit analyses of potential mitigation strategies has been drilled into students' heads throughout the course. Every system, regardless of how secure it is, has flaws or weaknesses that could be exploited. A crucial component of the security strategy is the understanding of these risks, the estimation of their potential impact, and the weighing of these factors against the expense of mitigating them. It is also quite important to have an understanding that it is not only impossible but also not even required to protect against all of the potential threats. A more realistic strategy would be to concentrate on the factors that have the potential to inflict the most damage while also taking into account the expense of mitigating such factors.

My understanding of cybersecurity as a whole has been revolutionized by the 'Zero Trust' concept. This concept is based on the maxim "never trust, always verify," which entails that each and every transaction, user, and data packet must be authorized and confirmed, despite the fact that their origin could be anything. Adopting this concept provides a higher level of security since it eliminates any potential for danger coming from within the purportedly trusted circle of people. However, the implementation of zero trust must be carried out with careful consideration. It is vital to design comprehensive security policies that describe the procedures, duties, and rights associated with each user and system. This should be done in order to ensure that the increased security measures do not impede usability or workflows. A notion that I intend to adhere to in all of my next professional endeavors is that of striking a balance between functionality and security.