Michael Oelschlager

Prof. Kraya

CS-405

29 June 2025

8-2 Journal: Portfolio Reflection

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

This topic is all about developing software while keeping security in mind as a primary concern. When security is added at a later stage in the development process, it can leave gaps and vulnerabilities in the program’s security that would have been found and resolved during development if security was one of the programmers’ main priorities while the program was being made. For this reason, while planning out a software program’s security beforehand and building it in tandem with the program itself may make the initial coding process longer and more difficult, it reduces the number of errors and problems that will be encountered later, making the development process more efficient and effective in the long run.

* Evaluation and assessment of risk and cost benefit of mitigation

Risk assessment and mitigation is a process of identifying the risks and possible hazards a software program is likely to encounter, then finding ways to reduce or eliminate the impacts of those risks, either by reducing the chances of that risk being able to affect the program in the first place, or by reducing the amount of damage the hazards you have identified could inflict if they did affect the program or otherwise come into effect.

* Zero trust

Zero trust is the concept that a program’s security should never assume that nothing is wrong. If a layer of security fails to trigger because another layer of security should have caught the problem, it may technically be efficient, but it also becomes a minor security vulnerability each time it happens. Ideally, a hacker who manages to make their way past the first security layer should not be able to pass through further layers uncontested just because the first layer didn’t trigger. Instead, the program’s security should always check the user’s credentials when they do anything requiring authentication, even if they shouldn’t have been able to even approach that part of the code without the necessary authorization.

* Implementation and recommendations of security policies

Security policies define rules and procedures for protecting information assets, ensuring confidentiality, integrity, and availability, and helping block opportunities for cyberattacks from arising in a system. Rather than being part of the code like a secure coding standard, a security policy is a set of guidelines for employees and users to follow to maintain the program’s security, so implementing it is less a matter of adding it to the code or building the code around those guidelines and more communicating with the users about what they need to do and ensuring that they actually do it. To aid in this, the security policies that are developed and recommended should be clearly stated, sensible, and comprehensive, allowing the users to both know and understand what they should do in any given situation to maintain the system’s security.