Benjamin Cleary

CS-405 Secure Coding

Prof. Joseph Kovacic

Journal 8-1: Reflection

To effectively address security concerns surrounding any software project, adoption of a security mindset should occur sooner rather than later in the process. Considering and adopting concepts like security design, policies for data encryption, ‘zero trust’, and a secure coding standard ensures that security is properly addressed. Things like a secure coding standard help reinforce key security concepts where the ‘rubber meets the road’. Additionally, a ‘zero trust’ environment ensures that systems or services are not accessed or used without explicit authentication and authorization. This protects those resources at every step but also enables proper accounting and maintaining a positive control over those resources no matter where in the process those resources get accessed.

These security policies must also address the balance of functionality, protection, and feasibility. The policies need to address and rank order the threats and their associated risks to prioritize the implementation and measures required to mitigate an incident. For example, if you were to secure your home, reinforcing the frame of your back door and adding a dead bolt might be warranted, given the ease at which someone could access it and attempt to break in despite the additional costs, where adding bars over a second story window might be excessive due to cost and probability that an intruder has a ladder.

Ultimately, the implementation and recommendations that come out of a security policy must be either adopted, modified, or rejected. This individual fate of any given piece of a policy must be weighed and judged but care must be taken to ensure that the balance struck between the functionality, protection, and feasibility supports robust security posture. Going beyond adoption, the policy must be enforced. Any policy that lacks the teeth to be enforced is just words on paper and functional meaningless. Buy in is required from the entire team not just security professionals or management. A security policy could be well crafted and a system well designed, but that would all be for no reason if the security practices laid out in policy are not actually practiced.