**Module 8 Reflection**

Thomas R. Hummel

Southern New Hampshire University

CS-405: Secure Coding

Prof. Mike Prasad

23 April 2023

# Adoption of a Secure Coding Standard

In the past software development often ignored security concerns until the end of the development process. As threats have increased and become more sophisticated and as software development practices have matured, more and more organizations are using a DevSecOps approach instead. This approach considers security at all steps of the software development process, from design through coding and into deployment and maintenance.

One important part of this approach is using a secure coding standard. If developers are each left to their own methods the secure coding may be haphazard. At the very least it will be inconsistent. With a secure coding standard, the team can consider which practices are the most important for their project and find consistent ways to address them. This consistency brings both greater security and an easier time when developers need to deal with each other’s code.

# Evaluation and Assessment of Risk

Another important part of a security-based approach to software development is assessing risk at the start. Different systems will have different risks and different threat surfaces. Because of this, they will require different approaches to security. It’s impossible to make a system completely secure. The resource and time requirements to make a system completely secure are too high. Instead, organizations must use their risk assessment to guide them towards the best practices relevant to their own system and their own needs.

There are also potentially tradeoffs between security and the user experience, so it’s important that these are considered as well. Again, a risk assessment can help to guide these decisions.

# Zero Trust

Another newer approach to security in software is the zero-trust model. Rather than looking at a system as if it were an isolated fortress that must be guarded on the perimeter only, the zero-trust model doesn’t assume that any source is safe – even if it’s inside the organization’s firewall – until it has been authenticated an authorized individually. In addition to providing a more secure system, this approach also provides more flexibility. Now resources that exist outside of the organization’s perimeter can still utilize the system’s authentication and authorization processes so that they can be secured as well.

# Implementation and Recommendations

In providing a secure system it’s important that everyone within the organization recognizes the importance of security. As a team, including security experts, a set of policies can be developed which align with what the organization agrees is important and which work to achieve the organization’s security principles. With buy-in from the members of the organization these policies can be achieved, providing for a much more secure system.

It is also important to maintain the security principles and policies over time as both the organization and potential threats change. The organization must remain vigilant.