8-2 Journal

Ryan O’Connor

Southern New Hampshire University

# Author Note

* Adoption of a secure coding standard, and not leaving security to the end
* Evaluation and assessment of risk and cost-benefit of mitigation
* Zero trust
* Implementation and recommendations of security policies

# 8-2 Journal

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

## The early steps taken by a team of developers can make security much easier as the project grows and expands. Adopted security principles early in a project can help a team establish ground rules. The most obvious first step is to plan security features before the team begins coding. Another important step is to have the developers collaborate with the security team to ensure that new features don’t compromise the security of existing features. The team should set up weekly meetings and ensure that time is spent with different members of the development team collaborating with the security team.

One of the most important practices in secure coding is to include security from the time the concept is developed. When a team starts to brainstorm on a project they should include security as one of their concerns. If they are creating a new form or a way for the user to access data from storage they should consider how malicious actors might try to take advantage of the feature. Another consideration during the brainstorming phase should be the effect on existing features. The addition of a new feature may create an opportunity for exploitation of older features especially features written several years ago that may not have been updated or maintained.

**Evaluation and assessment of risk and cost-benefit of mitigation**

A company or entity can mitigate the risks of a security breach by implementing the Triple-A standard. By adding authentication, authorization, and accounting the company can add a low-cost and high yield solution. Otherwise, the company should perform a specific evaluation for their company and determine the motives a hacker might have for gaining access to their system. It is not possible to protect a system completely but by understanding the motives for an attack the company can develop a specific use case for the defense in depth model to protect their data or servers.

**Zero Trust**

Zero Trust is an axiom that has become the standard for security protocol. Previously, many developers used 'trust but verify.' This proved to be insufficient in stopping attacks. This starts with a principle that states that all users must be verified. The principle is also known as 'never trust, always verify.' This process involves verifying every request that attempts to connect to a system.

**Implementation and Recommendation**

Implementation does not need to happen overnight. The first step is to document the policies and procedures that a company wants to use for its security. Once the policies and procedures are established then the whole team will know the rules moving forward. Any time there is a protocol deviation the team can discuss why the deviation occurred and why the rule should be followed.