# 

# CS 405 8-2 Journal: Portfolio Reflection

Raymond Aponte

raymond.aponte@snhu.edu

Southern New Hampshire University

**Adopting a Secure Coding Standard**

I am incredibly in favor of adopting a secure coding standard in any project that I am working on. Not only should a secure coding standard be adopted, but it should be adopted early to ensure vulnerabilities do not make their way into source code. There are many secure coding best practices to reference including those in the OWASP and SEI CERT secure coding standards to help mitigate potential vulnerabilities (Morrow, 2022). Some essential best practices that I encourage and will implement myself include input validation, keeping it simple to avoid vulnerabilities caused by complex code, error handling and logging, threat modeling to pinpoint threats and determine how to counter them, authentication and password management, and more (Morrow, 2022). Ultimately, which practices to follow depends on the organization and the project but adopting a secure coding model is the best way to start with a secure mindset shared by you and your team.

**Don’t Leave Security to the End**

“Don’t leave security to the end” is an important best practice in secure coding. This practice means to be proactive to security threats rather than reactive which can have incredibly detrimental effects. For example, it is important to make conscious decisions about the kinds of sensitive information collected such as how long it should be kept and who is authorized to access that data (Federal Trade Commission, 2015). Another approach is ensuring that developers are the first line of defense to prevent vulnerabilities that hackers/attackers can take advantage of. It is not enough and is far more costly to detect and react to vulnerabilities in written code than ensuring that code is not insecure from the start (Henriquez, 2019). Developers should start with a secure code mindset and organizations should partake in training their teams and developers to do so (Henriquez, 2019).

**Evaluation and Assessment of Risk and Cost Benefit of Mitigation**

Risk assessment and evaluation is important for developers to understand the severity of consequences that may occur if vulnerabilities are not addressed/mitigated. Using risk assessment, these vulnerabilities can be valued based on severity, level, priority, likelihood, and remediation cost to fully flesh out each vulnerability (Ballman & Svoboda, 2021). The cost benefit of mitigation can be determined by analyzing the expense of complying with a security rule. Rules that can result in high remediation costs should be identified and the type of work and detection required to uphold these rules should also be pointed out (Ballman & Svoboda, 2021). This way, an optimal tradeoff between mitigation strategy and cost can be well thought-out and priorities can be established for various rules pertaining to a project.

**Zero Trust**

Zero trust refers to a security approach where there is continuous verification of trust across users, applications, and devices to ensure that only required access is granted to trusted sources (Kueh, 2020). I believe zero trust is a security model that should be implemented, and I can use the motivations for hackers to attack to enforce the point as to why zero trust is the right model to adopt. For instance, even if a hacker were to breach the system in a motivation for cash, that hacker would need to constantly verify their trust to reach the data that they seek. Also, there is no guarantee that they can even reach that data if device trust and session trust are implemented which includes only allowing trusted devices to access resources and enforcing the principle of least privilege so that the user can only access resources that are required for them to do their job (Kueh, 2020). Lastly, technologies like data loss prevention can be used to make sure data such as passwords and credit card info cannot be stolen (Kueh, 2020), totally negating the hacker’s motivation in the first place.

**Implementation and Recommendations of Security Policies**

Implementing security policies is highly recommended as they can be used to guide how an employee thinks about and acts upon secure coding standards and the data that is being protected (Dunham, 2020). These policies map out what is expected of employees from a security standpoint including the who, what, and why. They also support the company’s ethical and legal responsibilities and priorities. If compliance is ever an issue, the individual is held responsible because these policies have been established and (more importantly) enforced (Dunham, 2020). Based on the organization, there are many policies that can be established revolving around secure coding practices including the implementation of Triple-A, encryption in its three stages, access control, physical security, remote access, acceptable use, and more. With security policies in place and enforced fairly, a great security foundation is established and potential risks can be better mitigated (Dunham, 2020).

**References**

Ballman, A., & Svoboda, D. (2021, April 14). *How this coding standard is organized*. Confluence. Retrieved December 17, 2022, from https://wiki.sei.cmu.edu/confluence/display/cplusplus/How+this+Coding+Standard+Is+Organized#HowthisCodingStandardIsOrganized-RiskAssessment

Dunham, R. (2020, May 5). *The importance of a company information security policy*. Linford & Company LLP. Retrieved December 17, 2022, from https://linfordco.com/blog/information-security-policies/

Federal Trade Commission. (2015, June). *Start with security: A Guide for Business*. Federal Trade Commission. Retrieved December 10, 2022, from https://www.ftc.gov/business-guidance/resources/start-security-guide-business

Henriquez, M. (2019, October 29). *Don't shift left, start left: Why developers should be the first line of Defense*. Security. Retrieved December 10, 2022, from https://www.securitymagazine.com/articles/91181-dont-shift-left-start-left--why-developers-should-be-the-first-line-of-defense-in-enterprises

Kueh, T. (2020, January 15). *A practical guide to zero-trust security*. Threatpost. Retrieved December 16, 2022, from https://threatpost.com/practical-guide-zero-trust-security/151912/

Morrow, S. (2022, September 20). *What is secure coding and why is it important?* vpnoverview. Retrieved December 17, 2022, from https://vpnoverview.com/internet-safety/business/what-is-secure-coding/#:~:text=Secure%20code%20will%20help%20to,Software%20vulnerabilities%20are%20rampant.