CS 405 Secure Coding C C++

Hai Nguyen

Southern New Hampshire University

# CS 405 Module Eight

**Name:** Hai Nguyen

**Date:** 20 April 2023.

Journal: Portfolio Reflection.

1. The approach of adopting a secure coding standard ensures that security is integrated into every step of the development process, rather than being added as an afterthought. By doing so, the software is less likely to have vulnerabilities that could be exploited by attackers, as security is a fundamental part of its design and development. One example of adopting a secure coding standard from SEI CERT C++ is to follow the guideline on “DCL30-C. Do not declare an identifier with conflicting linkage classifications” which states that “identifiers declared with external linkage shall have unique names within a program.” This guideline aims to prevent errors related to the usage of variables and functions with the same name in different parts of the program. This ensures that the code is robust and secure from the very beginning of the development process, rather than trying to fix security issues at the end of the development cycle. On the other hand, not leaving security to the end means considering security as a fundamental aspect of software development from the beginning of the development lifecycle. By doing so, the developers can identify potential security vulnerabilities and threats early on and combine secure coding practices into the development process, including adoption of secure coding standards like SEI CERT C++. Therefore, the concept of not leaving security to the end assists the adoption of secure coding standard by ensuring that secure coding practices are integrated throughout the entire software development lifecycle, from requirements gathering to deployment, resulting in more secure and reliable software system.
2. Evaluation and assessment of risk and cost benefit of mitigation are essential activities in the field of cybersecurity, including identifying potential risks and threats to a system, evaluating the likelihood and impact of those risks, and then determining the most cost-effective mitigation strategies. These activities help organizations to make informed decisions about which security measures to implement, based on the value of assets that need protection and the likelihood of a security breach. Overall, by performing evaluation and assessment of risk and cost-benefit of mitigation, organizations can identify and prioritize potential security risks, and develop a plan for implementing the most effective security measures. This approach helps organizations to proactively manage security risks and minimize the potential impact of a security breach on their operations.
3. Zero trust emphasizes the “No one is safe” concept in which all devices, users, and applications are potential threats and should be default trusted. Therefore, developers must adopt a proactive and full approach to security that is based on continuous monitoring and risk assessment. In addition, developers should assume that no device or user is intrinsically trustworthy and that security controls must be in place to verify and monitor access continuously.
4. There are several implementation and recommendations of security policies that developers should practice, such as adopting a secure coding standard from SEI CERT C++, performing regular code review as soon as possible, using static code analysis tools, implementing access controls, encrypting sensitive data, using secure communication protocols, keeping software and libraries up-to-date, training and educating developers, and conducting security testing to identify any security weaknesses in their applications.

References:

* CERT. (2021). Secure Coding Standards. Retrieved from <https://www.cert.org/secure-coding/standards/>.
* Carnegie Mellon University Software Engineering Institute. (n.d.). CERT C Coding Standard. SEI Digital Library. Retrieved April 6, 2023, from <https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682>