**CS 405 Secure Coding**

**Module Eight** **Journal: Reflection**

Michael Quilici

Southern New Hampshire University

April 19, 2021

*This is your final course reflection as well as your portfolio submission. Reflect on and include a discussion of the following topics, using readings from throughout the course to support your views.*

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

To create secure code, it is important to adopt a secure coding standard and not leave security to the end. Secure coding standards like SEI CERT are guidelines that enable developers to create secure and reliable software systems. When followed, secure coding standards reduce the chances that vulnerabilities will be introduced into the code that can later be exploited by attackers.

Security should be an integral part of the development process. Using secure development practices like unit testing, developers can ensure that security is addressed intrinsically and fix vulnerabilities early in the development process. Unit testing is the process of creating automated tests to check that specific sections of code behave as intended. These tests help to identify errors before they become security vulnerabilities. For example, a unit test might check that an index used to access an array is within bounds so that an attacker cannot exploit an out-of-bounds access vulnerability.

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

Mitigating errors prevents them from becoming exploitable vulnerabilities. When errors are identified early in the development process, the cost of fixing the errors is much less than would be if a software product were released with security vulnerabilities. If a security vulnerability makes it into a final product, hackers may be able to exploit the vulnerability, for example, to steal customer information. When this occurs, an organization can incur significant financial damages. According to IBM, the average cost of a data breach in the U.S. is $3.86 million. (IBM, 2020). In addition to remediation costs, an organization’s reputation can also be damaged. Customers may decide to take their business elsewhere, investors may sell stock, and business partners may cut ties with the organization.

* *Zero trust*

Zero-trust is a security principle in which an organization does not trust any activity inside or outside its network. The organization acts, in effect, as if a security breach has already occurred and implements appropriate security measures. Zero trust principles include verifying user identity, using least privileged access, and preventing breaches by segmenting networks. (Microsoft, 2020) Because attackers’ motivations are not known in advance, one should not trust that any user will behave in an orderly manner. For example, when creating a form to collect user input, a developer should expect that users will try to perform buffer overflow attacks or SQL injection attacks. To guard against this, the developer must adopt secure coding practices, like validating input and implement multiple layers of protection using defense-in-depth.

* *Implementation and recommendations of security policies*

Organizations that handle sensitive information, like customer records, should have a security policy in place to protect the data. The policy can include secure coding standards, Triple-A, and encryption among other topics. Coding standards, like SEI CERT, outline coding best practices that reduce the likelihood of vulnerabilities being introduced into the software. The standards address coding errors, like integer overflow, dangling pointers, and SQL injection, which can lead to the execution of arbitrary code by an attacker. SEI CERT provides example code that demonstrates how to correct a given vulnerability, rates the severity of the vulnerability, and recommends tools that can be used to discover and fix the vulnerability. (SEI CERT, 2021)

Another important component of an effective security policy is Triple-A, which stands for authentication, authorization, and accounting. Triple-A is a framework for controlling access to computer systems and auditing usage. Authentication verifies the identity of a user requiring information, like a password or fingerprint, that is unique to the user. When using passwords for authentication, one must ensure that passwords have sufficient complexity, are not repeated, and are changed regularly. Also, the number of user login attempts should be limited to a few tries before locking the account to prevent brute-force attacks. Authorization limits the locations and resources to which a given user has access. For example, a systems administrator can add new users to a network, but a typical user should not be able to add new users. Authorization should be used on all systems where user access should be limited to prevent them from accessing sensitive information or performing certain operations. Lastly, accounting refers to recording usage information like who is accessing a system, what commands are issued, session duration, and data being sent and received. Network security tools with accounting can be used to detect and flag suspicious activity and send alerts to IT.

Encryption should also be included in an organization's security policy. Encryption is the process of encoding information into a form that obscures the original content from would-be attackers. In cybersecurity, there are three categories of encryption: encryption in flight, encryption at rest, and encryption in use. Encryption in flight refers to the encryption of transmitted data. Examples of encryption in-flight include HTTPS for web traffic and VPNs for creating secure tunnels between endpoints and an organization’s network. Encryption at rest refers to the encryption of stored data. Storage devices like hard disks should utilize encryption at rest to prevent attackers from retrieving information, even if a device is stolen or compromised. Lastly, encryption in use refers to the encryption of data stored in memory. If an attacker has physical access to a device, they may be able to perform a memory dump to see the contents of memory and reveal sensitive information like passwords. Using encrypted memory can prevent hackers from deciphering this information.

# Works Cited

GAO. (2018, August). *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* Retrieved from Elizabeth Warren: https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf

IBM. (2020). *Security*. Retrieved April 19, 2021, from IBM: https://www.ibm.com/security/data-breach

Microsoft. (2020). *Microsoft*. Retrieved April 12, 2020, from Security: https://www.microsoft.com/en-us/security/business/zero-trust

SEI CERT. (2021). *SEI CERT*. Retrieved 4 20, 2021, from SEI CERT: https://wiki.sei.cmu.edu/confluence/display/seccode