Walter Augustine

Professor O. Mill

SNHU CS-405

April 22, 2021

Adoption of a secure coding standard is something every software development company should do, both for themselves and for their customers. A secure coding standard will prepare the development team for many types of threats, and allow them to improve on their security in a maintainable way. When security is a first-class citizen of a software system, better outcomes can usually be achieved. Whereas if security standards are left to the end, they can end up being weakly implemented or poorly understood by the development team, which increases the vulnerability to attacks.

When time and resources are limited, software teams sometimes must weigh the costs and benefits of avoiding a vulnerability or mitigating it after it has been exposed or exploited. To do this, they must analyze the likelihood and cost of remediation of each potential vulnerability, determine if they have the time and resources to prevent each vulnerability, then implement the necessary prevention. In doing this, the potential vulnerabilities left are often extremely unlikely to be exploited, often because they require an unrealistic amount of computing power to be successful. For example, many web login forms don’t limit the number of incorrect password attempts, which allows an attacker to brute force a password by trying every possibility. Strong passwords can take supercomputers upwards of a million years to crack by trying every possible string, so having unlimited password attempts isn’t all that much of a risk.

Zero trust means that threats are assumed from any external source. This can greatly enhance the security of a system, but it can also be an inconvenience for users, since more security means more layers of checks and validations that a user must successfully fulfill in order to accomplish their goal. For example, many websites automatically log out their users after some time, to prevent unauthorized access to their account if someone else uses their computer while they’re away, or if they’re using a public computer. Other websites keep their users logged in indefinitely, such as Google, Amazon, and Facebook.

The first step in a company establishing and adopting a security policy is to understand what the threats to the system are. Then secure coding standards can be established and agreed upon by the development team. Finally, the team can set up automated procedures that integrate with their existing software development processes, such as unit testing and static analysis that run every time new code is pushed and compiled. Creating and implementing a security policy takes a significant amount of time and effort, but the benefits often outweigh the costs not only monetarily, but also in terms of the reputation of a company that has excellent security practices and has never had a security incident or data breach.