Michael Cannon

Secure Coding

Southern New Hampshire University

Sunday October 23, 2022

# Journal – Reflection

Leaving security to the end of development increases many avoidable risks that threaten the integrity of a company’s data, the trust of the company’s customers, and the timeliness of developing features when security has to be added. In order to provide secure software solutions that provide the best value for a company, can be delivered accurately and on-time, a company needs to set forth security policies and procedures that serve as guidelines for developers to ensure they are meeting the base requirements, and code refactoring is limited. In a practical sense, the security guidelines should be easily applicable to any code written, remove any ambiguity related to how data should be handled in given states, and provide a framework for testing to ensure that the developed code is secure before being implemented into production.

The most effective, straightforward, and expandable way to accomplish this is unit testing. Setting up the tests in parallel with developing features is an excellent way to effectively utilize time, as well as prove out the requirements for the code while producing the tests. Test-driven development is a powerful and proven development method, which allows quality assurance to work alongside of the development team to ensure that everything works as intended, and that uncaught errors are minimized.

There are risks associated with ignoring or lagging behind with security policies. Any company has to weigh them against what they stand to lose, such as customer trust, governmental sanctions or fines, and potential legal judgements. Companies that handle and store customer data, especially sensitive data, would be wise to plan for all mitigating strategies related to security, which includes the adoption of Zero Trust policies and secured control schema. Zero Trust’s benefit is the protection and access control of all business-related data through a central authorization hub. This allows a company’s IT department to audit and control access to documents and ensure no data losses occur in the event an asset leaves the company. Additionally, it prevents side-loading attacks such as SSH tunneling.

No policy is one-size fits all, but companies should take the time to understand how Defense-in-Depth strategies can assist them in ensuring their data is secure and inaccessible to attackers, as well as how to encrypt and protect data to prevent any leaks from containing sensitive data that can be reverse engineered.