Charlie Vinson

CS-405

4/28/2024

Reflection

1. **Adopting a Secure Coding Standard**

Adopting a secure coding standard is critical to the success of secure systems. The earlier that security policies are implemented, the lower the likelihood of successful attack and the lower the cost will be to address any vulnerabilities that are discovered. It gives developers the ability to understand where the system is most vulnerable before attackers do, and therefore an advantage in preventing attacks before they occur.

1. **Risk and Cost Benefit**

While the initial cost of developing a secure system can be greater than the cost of rapidly developing a less secure system, as there are significant considerations to be made that will result in spending both time and money, the overall cost will likely be lower when security is considered from the earliest stages. This is because the likelihood of attack is decreased, which can be exponentially more expensive than the security costs associated with preventing them. Additionally, applications that consider security early are better planned, and therefore any vulnerability that is discovered can be addressed efficiently and at a generally lower cost.

1. **Zero Trust**

Zero trust assumes that nobody in the system is safe from attack. It encourages security at every level of the system and the security of every aspect of the application. It works to mitigate potential threats and the harm that they can cause when they are successful. From a user’s perspective this may imply a longer time spent authenticating themselves and gaining proper authorization to use the system, but comes with the benefit of greater security of their data and usage of the system.

1. **Implementation of Security Policies**

By following the standards outlined in the security policy, developers can be sure that they have taken great steps toward effectively securing the system against a broad range of attacks. Memory leaks, data security, data integrity, and bad input are just a few of the issues addressed by the policy. This promotes a system that behaves as expected at all times, including both when an attacker is actively attempting to gain unauthorized access to the system and when a regular user has simply made a mistake in their use of the system.