Stephen Mathew

10/23/24

CS405 – Module 8 Journal

Adopting a security code standard makes sure the development process and the security features of a project are consistent. This is true no matter who is involved in creating/adding code to the main branch. A strong and consistent security standard helps protect the project from near and far threats. The idea of "don't leave security to the end" means that security measures should be built into the development process from the start. If security is only added at the end, it can cause compatibility issues or even mess with the project due to unreliable code. Depending on the project, the security features and the overall system might not match up, which could force a team to restart the project to integrate security measures correctly.

Threats are typically divided into different levels. By grouping threats, teams can manage their time effectively. This allows them to focus on addressing and defending against the most serious risks first. This helps ensure the project is protected without going over budget or missing a deadline.

Currently, security systems must continually update/improve to keep up with the growing number of attacks. Zero trust policies, which are in many government systems, are now becoming more common in day-to-day companies. These policies require advanced authentication like 2FA and encryption. This goes even for employees when they need to access data. Over time, security systems have changed from acting as a stronghold that blocks outside threats. Now, they’re more complex like a maze and it only allows access to people with the proper credentials.

Security policies need to be flexible. They need to be regularly updated to stay ahead of attacks that are different and more complex every day. Both security systems and hackers learn based on their attempts. Since more data is being stored digitally, cyberattacks will happen more. Developers must be certain their security features are good enough to defend against current and future threats.