Brian Engel

Module 7 Journal

There are quite a few different motivations for attacking vulnerabilities in a system, such as financial gain, disruption, espionage, and just simple recognition. Attackers seeking financial gain might try to take over a system and hold it hostage for money (ransomware) or extract personal information to sell or use for fraudulent purposes. Attackers aiming for disruption would likely try to take out a sensitive system, making it inoperable, such as an electric grid, water plant, or air traffic control system. An attacker seeking recognition might target any system, looking for information that proves they were able to hack it and then share it publicly. In the case of espionage, attackers would be after sensitive information on systems or personnel and would probably be the hardest to detect since there wouldn’t necessarily be any demands or clear signs of their presence in the system.

By understanding the different motivations for attacking vulnerabilities, it becomes easier to defend against them. Reviewing the list of motivations, we see that information on a system can be valuable to various actors. However, financial information, medical records, credit card numbers, passport numbers, and other highly sensitive data are universally sought after and thus require extra attention to ensure their security.

To impress the importance of security to a new developer, there are some essential strategies and principles from this course that I would share. First, Defense in Depth is a powerful concept involving multiple layers of protection so that any weaknesses in one layer are mitigated by another. Triple A (Authentication, Authorization, and Accounting) is another critical framework. Many major attacks start with phishing scams, leading to hijacked credentials. Multifactor authentication (MFA) can help prevent these takeovers by adding an extra layer of security. The principle of least privilege deals primarily with authorization, ensuring no user has access to areas they don’t need to perform their job. As for accounting, if a security breach does occur, proper logging and monitoring are crucial for identifying and addressing the issue. Additionally, sensitive and personal information should be encrypted to ensure that even in the event of a breach, the gathered data remains useless. Encryption should be applied in transit, at rest, and, if possible, while in use. Understanding the motives behind potential threats helps create more robust and targeted security measures. By implementing these best practices and principles, we can better protect our systems and data from various attacks, ensuring a secure development environment.