Southern New Hampshire University

CS 405 Secure Coding

Journal 7-1

George Harrison Jr

When it is said to “consider the motive”, we need to consider why an attacker is exploiting vulnerabilities. This could be for numerous reasons; some good while others aren’t good. For example, an attacker could have malicious intentions when exploiting a weakness in a network like stealing financial information and or sensitive personal data. These attacks may happen to make a social point, espionage or just a plain old challenge just to see if it can be done. These are the “outsiders”.

There are also attackers who want to be helpful to companies to help them to find vulnerabilities in their system. These attack “act” as intruders to a given companies network. If there is a vulnerability found. These hackers will alert the company of what they have found and even help them find ways to fix these bugs. These are the “insiders” or “white hats”.

In the future, I will apply these concepts to find vulnerabilities in my own code. The best way to avoid potential exploit points in my code I would follow know best practices. Learning from the mistakes of other teaches some of the best lessons. I will use the experiences published by companies who have been attacked. There solutions will be valuable to preventing the same attack on my projects.

Ways to avoid attack vary depending on the type of information and its destination. Encryption is the process of ciphering data to prevent it from being accessed by unauthorized user. Even if the information is misappropriated the attacker would not be able to read the encrypted file without the encryption key. Encryption can also be done on several different bit depths like 16, 32, 64 and 128. The larger the bit depth, the more difficult it is to be accessed by attackers.