**Motivation: Why did you do it?**

James Porter

Department of Computer Science, Southern New Hampshire University

CS 405 Secure Coding

Professor Wasim Alim

October 13, 2022

**Applying what we know about Motivation**

Figuring out the motivations behind attacks is an important step in mitigating the threats that hackers present. Knowing whether a hacker is interested in financial gain, looking to disrupt a company or their business, or even just for their own pleasure can give an incite as to what or why they are hacking in the first place.

If a hacker is interested in monetary gain, more than likely, they are looking for information that they can sell or hold for ransom. When you have data that could give a hacker leverage to demand this money, (e.g., addresses, social security numbers, credit card numbers, etc.) you can also assume that you will need more protection of this information.

Another motivation that a hacker might have for trying to gain access to a system is to disrupt a business or operation. When you run a business, or more likely, a nation or state, there are hackers out there who are looking to either get information for themselves or disrupt a process to try and get ahead of their competition. This would be another indicator that would lead a company to protect its assets and invest more in software security.

Lastly, the motivation that can be the most dangerous are those hackers that are just interested in the prestige of hacking into a system. Because a hacker with this type of motivation is just trying to hack the biggest/most secure system possible, they are not as likely to care about the monetary gains that they could make, but rather concerned with the prestige around hacking a system. (This is very similar to how a fisherman is not always interested in the money to be gained from fishing, but the prestige/bragging rights to say they caught a bigger fish than you.) Motivations surrounding this praise are especially frightening, because typically this type of hacker is not looking for a monetary gain and will be willing to trade secrets found for very little.

**Explaining Motivation**

If we were to be talking to a new developer about motivations, it would be important to identify to them the different types of hackers and the hats that they might wear. What are the advantages of some hackers and the threats that others may introduce. It would also be beneficial to have the new developer put themselves in the shoes of a potential hacker and why they might attack a system.

**One Example for Module 8 Reflection**

Throughout this term, we have identified multiple secure coding techniques that we can use to better secure the code that we write. These should not only be a recommendation, but a requirement that developers are required to follow. This is the reason that we wrote the secure coding policy and why it should be standard practice to follow protocol that has been agreed upon by the developers and employers involved.

Some of the secure coding practices that we have introduced include encryption, overflow protection, and other error handling techniques to make sure that our code is as secure as possible. Lastly, this process of securing the code allows us to mitigate now so our issues further down the road don’t make as big of a splash (financially or in time lost responding to an issue).