Brittany Ritsick

CIS 145 – SP24

Summary Chapter 6

20 February 2024

 In chapter 6, there were a lot of new things that I was able to learn. First, I learned the difference between an integrity threat and a necessity threat. While I have heard of terms such as encryption and decryption through my job, I had not previously known of the term cryptography. I was also interested to learn the difference between cipher text and plain text. I did have knowledge that some things are encrypted, while others are not; but I did not know the terminology for these prior to this chapter.

 Another topic I was interested to learn about were the types of encryptions. While private key encryption practically is what its name says, I found it fun to think about what in my life I might use that is private key encrypted. The first thing that came to mind is our weekly in class quizzes. As those quizzes become available, we log in and use the password that is provided by our instructor (you) to gain access to the quiz. It is truly amazing to think of all the things that we use daily, that we don’t necessarily know the names to.

 The closest thing I could relate public key encryption to in my life would be the daily VPN that I use for my job. I launch the VPN application and then enter my user information, followed by a key that is provided through a separate cellphone application. Once I enter the key, the system can verify I am who I say I am, allowing me to gain access to our works Intranet. I also have experienced spoofing within my workspace as well as in my personal email. There was a time that I received an email from Showtime, which was typical, advising me of a gift card I had won. However, when looking closer you could see that the email was not actually from the Showtime team, it was a spoofer. Thankfully in that scenario, I caught it before causing any serious issues.

 The first time I remember seeing a digital watermark, was when I was younger and searching on google images for a class project. I was lucky enough to have my sixth-grade computer science teacher explain to me what it was for. This chapter was the first time I had heard about a DoS attack. However, even though I haven’t heard of the term, I do know that the company I work for went through a scenario that sounds very similar to this. There was a period before I was hired that all the companies’ files were compromised, and agents could not access any tools they needed.

 Before my current occupation in the internet industry, I worked at a bank, so I was previously aware of identity theft. There were times where I would have to inform customers of how best to protect their identity. I personally found that identity theft was happening most when a customer would click on a phishing link and fill out personal information including bank accounts and passwords. Although I was able to help guide customers in how to protect their identity and their information, I was also aware of the growing amount of information that the Internet holds.

 I also have extensive previous knowledge on viruses, malware, adware, worms, trojan horses and web bugs. Due to my occupation, I also have knowledge on ports and a general idea of how they operate and what they do. Again, going back to my job, I have also used single and multi-factor authentication methods to assist me with working remotely. Some new things I learned about at the end of this chapter were digital certificates, digital IDs and trust seals, I had not previously known of them. The last new thing I learned about was SSL and TLS. While I had previously seen these acronyms, I did not know what they stood for or what they did. I now know that they are encryption protocols.