**CYBR 3520 Introduction to Cyber-Physical Systems Security**

**Homework #2**

***This homework is due: September 9, 2022, 11:00 PM***

***Total points: 12 Andrew Koenig***

1. [3 pts] Pick one of the publicly reported cyber-physical security incidents in Chapter 2. Identify the types of cyber impact (breach of confidentiality, breach of integrity, and breach of availability) and the types of physical impact caused by the incident. Stuxnet was a major breach of integrity. It breached their offline systems and caused a lot of physical damage to the centrifuges in the plant. You could also consider it a breach of availability as the goal was to slow down the Iranian nuclear development by destroying their equipment.

2. [3 pts] For the above incident, discuss the likely motivation behind it, whether it was a targeted attack or not. The most likely motivation behind the attack was slowing down or stopping the Iranian nuclear development. It was definitely a targeted attack as the actual virus was very specific, designed for certain machines, and designed to be discrete.

3. [3 pts] Assuming that Stuxnet’s sole objective was to delay the Iranian nuclear program by damaging centrifuges, why would it be allowed to infect thousands of other computers worldwide? Suggest three likely reasons. One reason would be to have the best chance of affecting the systems in that specific plant. Like more of a shotgun type of attack, just spread it in the area instead of targeting the specific workers there. Another could be that it was designed to spread quickly and they didn’t care who it spread to. Another reason could be that they knew it would only target a very specific system and that others wouldn’t be affected.

4. [3 pts]Consider the simplified scenario of two cities that are connected by a railway line and two busy highways. The one highway includes a long tunnel through the mountains. Can you think of two different approaches with which a hacker could create traffic jam on either highway? Discuss the difficulty and likelihood of occurrence of each approach. One approach could be for an attacker to gain access to the railway and cause it to close, this would generate a lot more traffic as the people riding the train would then have to drive as well. This would be harder as the systems for the trains are more than likely heavily guarded. Another way would be to cause an accident on one of the highways, whether it be by messing with traffic lights or disabling a vehicle that has some sort of wifi connection. This scenario would also be difficult as the vehicle would have to be in the right place at the right time.