Reflection: Stephen Buchinskiy

In this project, I implemented the replay attack module and added command-line argument optionality when executing the main program. Although the command-line arguments are limited, they do feature three commands: one to turn debug mode on, one to turn the replay attack on, and the last one to control the time for the replay attack.

In this project, I was able to implement my own attack and develop skills on how to penetrate communication protocols by intercepting message transmissions and use them to disrupt an actively running process. Although I didn't work too much on the plc and scada systems, I was able to look at the implementations that my teammates made and see how a basic model is implemented in python. I also improved my python scripting skills and documentation skills.

A challenge I encountered in this project was getting the replay attack to correctly connect to the client to retrieve messages by subscribing to topics. On top of this, once I was able to get the message retrieval working, I slightly struggled to get the replay timing correct to disrupt the client.

This project deepened my understanding of ICS architecture and cybersecurity principles. I learned how simple attacks like the replay attack can bypass basic defenses and how multiple defenses help reduce their impact. This also taught me how important it is to secure control systems from attacks as the attacks can leave devastating impacts to the system.

The skills I learned from this project will help me implement more complex attacks against more secure systems in the future. This project will also help me build my own test environments that simulate real-world processes.