Modbus and cyber-attacks

1. Setup Modbus Client - Server architecture
2. Modbus TCP Server

The server code will be running at the Control Centre and will be responsible for listening and responding to requests as well interacting with the database to store data values. A screenshot of the server code is attached below, and the same source code can be found in the appendix

Graphical user interface, text, application

Description automatically generated

Figure 1 : Modbus TCP Server Code

1. Modbus TCP Client

The client code will be running in the PLCs and RTUs. The client code allows the devices to send data and requests to the server. A screenshot of the client code is attached below, and the same source code can be found in the appendix.

Graphical user interface, text, application

Description automatically generated

Figure 2 : Modbus TCP Client Code

1. Encode data to Modbus format

The raw data is converted to Modbus format and is sent to the server. When the payload is fetched it is then finally decoded back to raw data using PyModbus. A screenshot of the payload encoder - decoder code is attached below, and the same source code can be found in the appendix.

A screenshot of a computer

Description automatically generated with medium confidence

Figure3 : PyModbus Payload Code

Text

Description automatically generated

Figure 4 : The decoded payload data, as received back by the client device.

1. Setup cyber-attack architecture

For this thesis, we started with two Windows devices which served as the client and server for Modbus communication. This was accompanied by a third device running Kali Linux on it. It utilised Ettercap v0.8.2 for sniffing and launching ARP Poisoning attacks.

1. Perform Man-in-the-middle attacks

A MITM attack was performed with an Ettercap tool that maliciously modified the Modbus TCP commands between the Master and PLC workstations. An Ettercap filter within the Ettercap tool was then created to modify Modbus TCP communications.



Figure 5 : Loading a filter in Ettercap

1. Gather cyber-attack data

Generate and gather the data produced from conducting cyber-attacks on the network. Perform data wrangling, feature extraction, etc on the gathered data to prepare it for the machine learning model.