# MODELLING CYBER-ATTACKS ON MODBUS TCP PROTOCOL IN INDUSTRIAL CONTROL SYSTEMS

AUTHOR : KALVIN WILLIS C1914891

SUPERVISOR : NEETESH SAXENA  MODERATOR : YUHUA LI

School of Computer Science and Informatics 2022

One Semester Individual Project

40 Credits

# Contents

Project Description ..... 2
Aims and Objectives ..... 3
Ethical Considerations ..... 4
Use of Intellectual Property ..... 4
Data Privacy and Anonymity ..... 4
Work Plan and Deliverables ..... 5
References ..... 6
Abbreviations ..... 7

## Project Description

The Modbus protocol was developed by Modicon for use with Programmable Logic Controllers (PLCs), and is one of hundreds of Supervisory Controls and Data Acquisition (SCADA) protocols developed in the past three decades[1]. It allows for communication between a Modbus Master, usually a PC, and Modbus Slaves, which are PLCs[2]. The protocol operates at level 7 of the OSI model[3], mainly transmitting data and information through physical serial lines.

Because of how simple it is to use, and how efficient it is when used on an industrial scale, the Modbus protocol has quickly become the most popular protocol in manufacturing environments that use Industrial Control Systems (ICS).

The simplicity of the Modbus protocol is also a double-edged sword – the simplicity makes it vulnerable to cyber-attacks. An example of this is that devices using the Modbus protocol for communication communicate in plain text, and there is a lack of authentication on every message sent[4]. Along with this, there is also a distinct lack of integrity, meaning it is fully dependant on integrity being preserved by lower OSI layer protocols[3]. Attackers could quite easily control an ICS that uses Modbus if they have a direct connection to either the Modbus Master HMI, or any of the Modbus Slaves.

This project will design, develop and implement a new cyber-attack on a simulated environment demonstrating how the Modbus protocol is used in ICS based on a gap in the current research into it. The code used throughout will be done in python, due to the flexibility of the coding language and the nature of existing libraries. I will be modifying a provided base of code to mount cyber-attacks on a simulation to allow me to demonstrate just how big of an impact a cyber-attack on the Modbus protocol would have.

I have chosen this project as I have a deep-rooted interest in cyber security, specifically penetration testing. This project will improve my skills in this area, along with taking advantage of my understanding of python. I also want to demonstrate the importance of security around the Modbus protocol. It is a de-facto standard protocol for communication between PLCs, and is used everywhere. Cyber attacks targeting it would be unstoppable without some form of security on top of it, and I hope to present that through this project.

## Aims and Objectives

The overall aim of this project is to explore the vulnerabilities of the Modbus protocol, analysing different existing methods and finding a gap in current research that I can then create a tool to fill.

From this aim, I have chosen three objectives that this project should fulfil by its completion:

1 – Find a gap in the current research on the Modbus protocol that I could develop an attack to take advantage of.

2 – Implement an attack on the Modbus protocol to achieve control over a simulated ICS. This should be within the research gap identified in objective one.

3 – Develop a tool that can automate the attack developed previously and evaluate how effective it is compared to existing methods. This tool could include the functionality to produce attack performance statistics such as time to gain control.

# Ethical Considerations

From the below two points, I do not need to go through an ethical approval procedure, as although I know the skills that I will be demonstrating would be unethical in the real world, I am applying them on a network that is under my control and therefore will have no impact on the real world. Along with this, the final tool that I will create would be used for research purposes only, meaning that I would not need to do any consumer research, further justifying why I do not need to get any ethical approval.

## Use of Intellectual Property

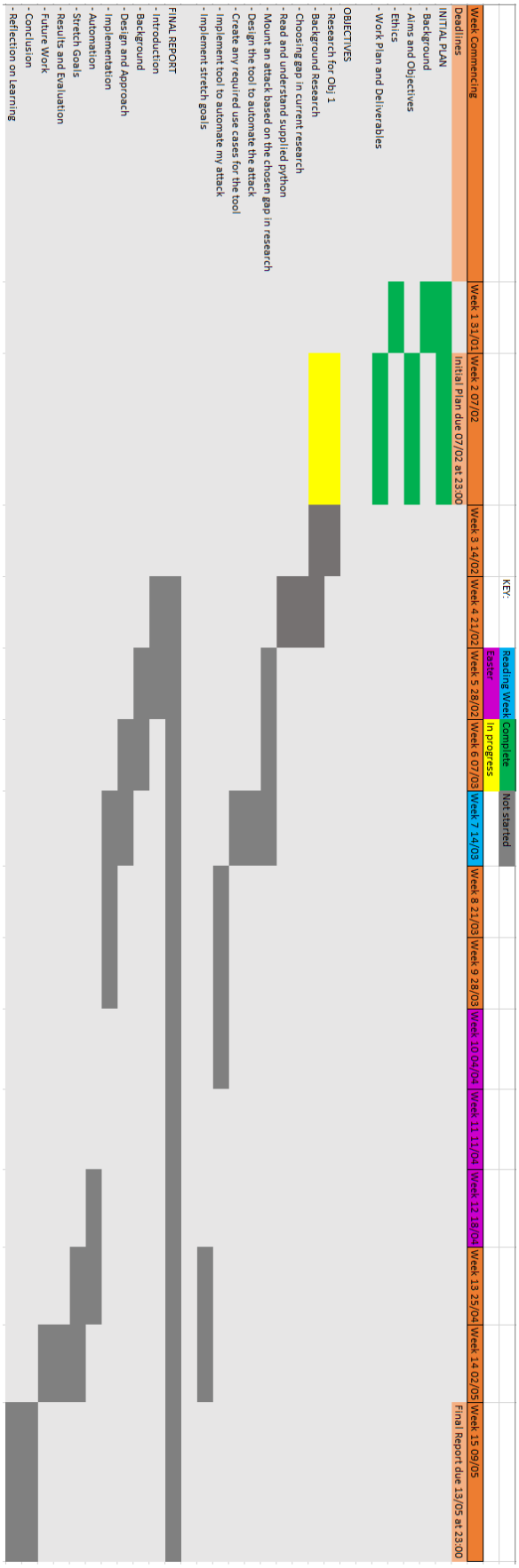
Throughout this project, I will be using resources to help inform and guide my decisions, along with helping build a solid background for the project that I can refer to right through to the end. I will be using Harvard Referencing for any resources used, crediting the author where available, or the domain I found any relevant information on, and the date I accessed it (where applicable).

## Data Privacy and Anonymity

This project does not require any personal data or human participation, so I do not need to consider this throughout.

## Work Plan and Deliverables

To show my work plan, I have created a Gantt Chart:



## References

[1] Modicon Inc, 1996. *Modicon Modbus Protocol Reference Guide*. [online] Available at: <https://www.modbus.org/docs/PI_MBUS_300.pdf> [Accessed 6 February 2022].

[2] Radiflow Security Team, 2021. *Hack the Modbus - Radiflow*. [online] Radiflow. Available at: <https://www.radiflow.com/blog/hack-the-modbus/> [Accessed 4 February 2022].

[3] Benbenishti, L., 2017. *SCADA MODBUS Protocol Vulnerabilities - Cyberbit*. [online] Cyberbit. Available at: <https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/> [Accessed 6 February 2022].

[4] Zou, C., n.d. *Online Digital Forensics Courses and Labs*. [online] Cyberforensic.net. Available at: <http://cyberforensic.net/labs/modbus-attack.html> [Accessed 4 February 2022].

# Abbreviations

ICS – Industrial Control System(s)

PLCs – Programmable Logic Controllers

SCADA - Supervisory Controls and Data Acquisition