Report for the CPS Final Project

Andrea Auletta
andrea.auletta@studenti.unipd.it

Niccolò Zenaro
niccolo.zenaro@studenti.unipd.it

February 15, 2025

Contents

Abstract

Modbus is a commonly used protocol in Supervisory Control And Data Acquisition (*SCADA*) environments for monitoring, control and data acquisition. Despite its wide popularity, Modbus is not secure because when it was developed and adopted (1979) security was not considered to be a concern in isolated Industrial Control Systems (*ICS*), thus is not designed to be secure like modern IT networks. Among the various attacks, 4 different taxonomies can be identified to facilitate formal risk analysis efforts for clarifying the nature and the scope of the security threats on Modbus systems and networks.

1 Introduction and objectives

The Modicon Commuication Bus (*Modbus*) protocol operates in a master-slave or client-server based model. The master devices initiates the queries while the slave devices respond to all such queries. Masters can either send a broadcast message to all the slaves or indivdually poll a specific device. All the experiments run in this work, like in the original paper [1] are focused on TCP/IP implementation, while Modbus protocol can be implemented also on top of several communication networks like serial or UDP.

2 System setup

3 Experiments

4 Results and Discussion

References

[1] Peter Huitsing et al. "Attack taxonomies for the Modbus protocols". In: *International Journal of Critical Infrastructure Protection* 1 (2008), pp. 37–44.