Report for the CPS Final Project

Andrea Auletta
andrea.auletta@studenti.unipd.it

Niccolò Zenaro
niccolo.zenaro@studenti.unipd.it

February 14, 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

2 System setup

3 Experiments

4 Results and Discussion