RIT | Golisano College of Computing and Information Sciences
Department of Computing Security

ASSESSING SECURITY OF CONTEMPORARY INDUSTRIAL CONTROL SYSTEMS: INVESTIGATED THROUGH MODBUS HIJACKING

Christopher Tremblay, Graduate Capstone Advisors: Daryl Johnson, Dr. Sumita Mishra

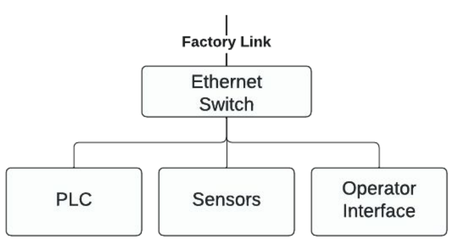
Introduction

Industrial Control Systems (ICS) are a critical security concern where increased connectivity and data-driven practices are becoming commonplace in factories. Many industrial communication protocols, like Modbus, were designed in a time where security was not a concern. These security flaws within industrial protocols are still relevant despite advances in cyber security.

Background

- A Programmable Logic Controller (PLC) is specialized microcontroller designed to automate factories
- A typical production line has a PLC that communicates with an interface where an operator can control the machine
- Industrial equipment is networked and supports basic TCP/IP stacks

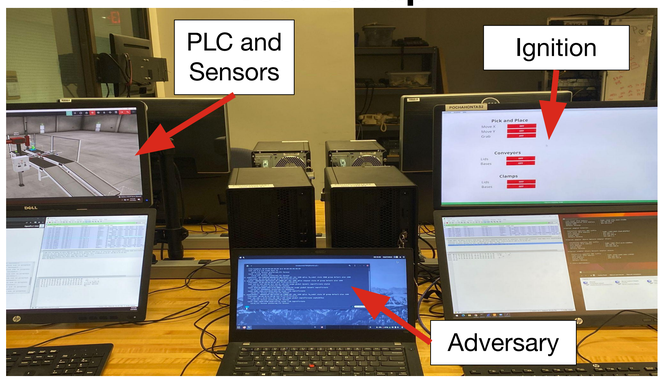
Github



Objectives

- Exploit a simple network composed of a PLC and sensors through a *Gratuitous Modbus Request*
- Exploit a more complex network composed of a PLC, sensors, and **Ignition** software with an *MITM attack*

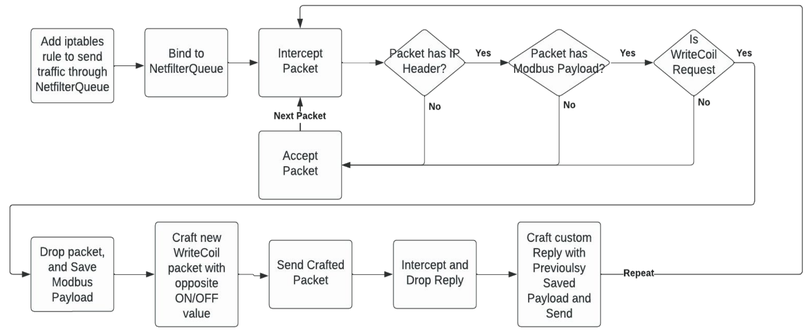
Test Setup



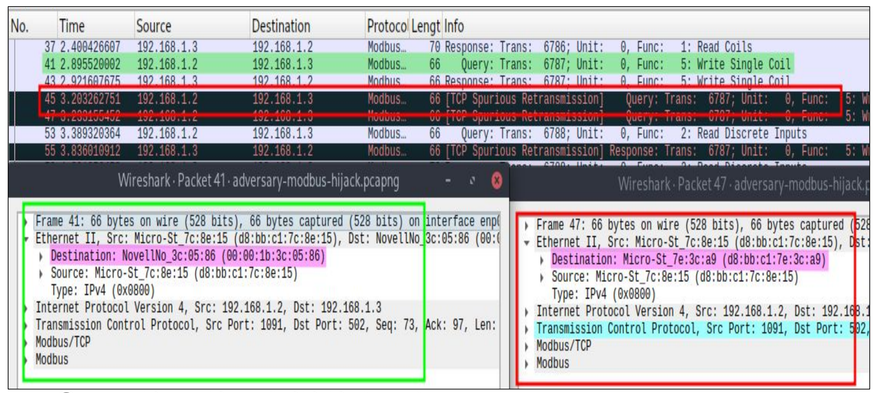
Attack Pipeline Architecture

- *CAM Overflow*
  - Turn switch into a hub, and see all traffic flowing through the switch
- *ARP Poisoning*
  - Craft specialized ARP requests to coerce traffic through adversary
- *Modbus Hijacking*
  - Selectively drop Modbus WriteCoil requests, and craft packets to fool **Ignition** and **OpenPLC** that everything completed successfully

Modbus Hijacking Attack



Results



Green Box: Pre-ARP Poisoning
Red Box: Post-ARP Poisoning

Conclusions and Future Work

- The exploit was successful in a lab environment
- The exploit demonstrated that industrial protocols need to balance security and latency
- Expand this to actual PLC and industrial hardware in the future