Supervisory Control and Data Acquisition Test Bed

RowanUniversity COLLEGE OF SCIENCE & MATHEMATICS

STEM ROWAN UNIVERSITY STEM SYMPOSIUM April 20th, 2018

Tapan Soni, John Stranahan, and Vahid Heydari Ph.D
Department of Computer Science, Rowan University

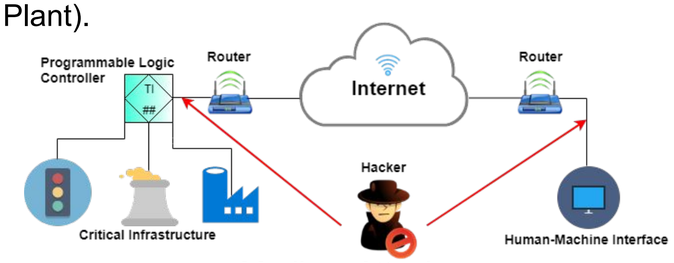
The Threat

Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say

By NICOLE PERLROTH JULY 6, 2017 The New York Times

Industrial Control Systems (ICS) such as **bridges, power plants, water treatment plants, and gas pipelines** are controlled by SCADA control systems. The software used to monitor, diagnose, and communicate with the SCADA system is **unencrypted and prone to cyberattacks**. This is a major flaw in the critical infrastructure of the United States and other countries.

For years, security professionals have warned that hackers can gain **remote access to these systems to cause physical destruction.** These types of attacks happened in Australia (Waste Management Plant), Iran (Stuxnet), Ukraine (Electric Grid), and parts of the US (Texas Water Plant).



Modbus Attacks

- **Unauthorized Command Execution**
- **Denial-of-Service Attacks**
- **Man-in-the-Middle Attacks**
- **Replay Attacks**

SCADA Process Control Test Bed

Abstract

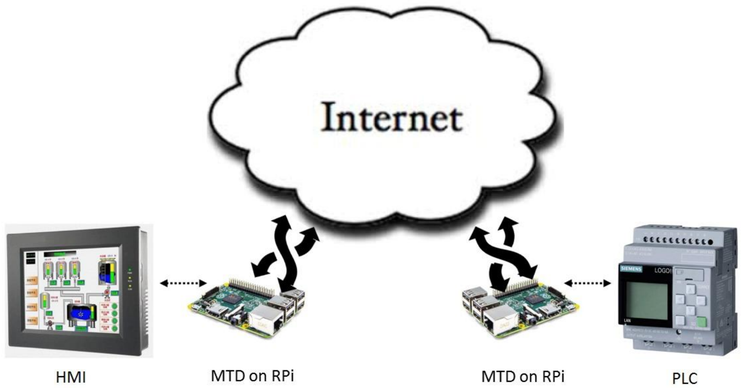
The proposed project involves us building a Supervisory Control and Data Acquisition (SCADA) Test Bed. The test bed consists of a real world model of an Industrial Control System (ICS) that is implemented on a small scale. It emulates a physical SCADA system using industrial equipment such as sensors, motors, and a Programmable Logic Controller (PLC) which are deployed to a physical system for local control and monitoring. The PLC is also connected to a computer running a human-machine interface (HMI) software for monitoring the status of the physical processes remotely. The test bed is a useful resource for cybersecurity education and research including PLC programming, SCADA protocol analysis, the demonstration, analysis, and prevention of cyberattacks, and forensics.

Main Points of Vulnerability

- **Unpatched published vulnerabilities**
- **Network connected Human Machine Interface**
- **Protocols with lack of support for authentication**

Secure Modbus via Moving Target Defense Integration

Securing the unencrypted communication protocol, Modbus, is imperative because it is used in many Industrial Control Systems (ICS) worldwide. Our research is aimed at integrating the Modbus protocol with the IPv6 Moving Target Defense (MTD) system, and implementing it into the Scada Test Bed. This concept works by changing the IP address of the connected devices every quantum which makes the system secured against cyberattacks. MTD hosts are much more difficult to locate on a subnet than a static host because the address is constantly changing. The less addresses on a subnet, the more likely a hacker is certain of a targets host identity.



We propose combining the moving target defense system with our SCADA test bed, as well as integrating and discovering new methods to protect ICS and other critical infrastructure.