Virtualizing Industrial Control Systems
Testbeds for Cybersecurity Research

ACSAC ICSS 2016

Rishabh Das
Thiago Alves
Dr. Tommy Morris
Overview

Problems:
- Industrial Control Systems are too big to fit in a lab
- ICS Cybersecurity researchers rely on small testbeds to collect data
- Small testbeds may not have all the data required for cybersecurity research

Accomplishments:
- Create a high fidelity virtual copy of a physical SCADA system
- Compare results between the physical and virtual testbeds during normal and attack conditions
- Scale up the virtual testbed to model a full-size ICS
SCADA Components

Physical System (sensors and actuators)  Wire bridge Analog and digital I/O  Programmable Logic Controller (PLC)  Network / SCADA Protocol  Human-Machine Interface
First Example
Gas Pipeline Testbed
Physical System

Characteristics:

One inch diameter pipeline network
Four 90° pipe bends
Two T-joints.
Positive displacement pump connected to a 0.5 Hp 1Φ 120 Volts induction motor

Sensors:

Analog pressure sensor

Actuators:

Relay - Turn pump on and off
Wire Bridge - Analog and Digital I/O

- Sends sensor signals to the controller
- Sends controller commands to the actuators
- Electrical communication between the controller and its physical interfaces
PLC - Programmable Logic Controller

- Digital computer used on automation
- Input modules read data from sensors
- User program decides what to do based on the input data
- Output modules control actuators on the industrial plant
OpenPLC - An Open Source Industrial Controller

http://www.openplcproject.com

Valuable research tool since entire source code is available online
OpenPLC - An Open Source Industrial Controller
OpenPLC - An Open Source Industrial Controller

Supports all five IEC 61131-3 programming languages
OpenPLC - An Open Source Industrial Controller

Compatible with Modbus/TCP SCADA
OpenPLC - An Open Source Industrial Controller

Supported platforms

- Raspberry Pi
- UniPi
- PiXtend
- ESP8266

- Arduino
- Windows (soft-PLC)
- Linux (soft-PLC)
OpenPLC - Multiple platform support

Very easy to port to another platform
HMI - Human Machine Interface

- Built in C# using the EasyModbusTCP library
- Uses Modbus/TCP to communicate with the PLC
- Queries PLC for data every 100ms
- Display status on the screen
Virtualizing the Gas Pipeline Testbed
SCADA Components Virtualized

- Physical System (sensors and actuators)
- Wire bridge
- Analog and digital I/O
- Programmable Logic Controller (PLC)
- Network / SCADA Protocol
- Human-Machine Interface
SCADA Components Virtualized

- Physical System (sensors and actuators)
- Wire bridge
- Analog and digital I/O
- Programmable Logic Controller (PLC)
- Network / SCADA Protocol
- Human-Machine Interface

Model with virtual sensors and actuators

OpenPLC (on a Virtual Machine)

UDP Packets

Network / SCADA Protocol

Human-Machine Interface

MATLAB® SIMULINK®

OpenPLC

Network / SCADA Protocol

Human-Machine Interface
SCADA Components Virtualized

Physical System (sensors and actuators)

Model with virtual sensors and actuators

Wire bridge
Analog and digital I/O

Programmable Logic Controller (PLC)

Network / SCADA Protocol

OpenPLC (on a Virtual Machine)

Network / SCADA Protocol

Human-Machine Interface

Human-Machine Interface
Matlab Model
Other Examples Using the Same Approach
Water Storage Tank Testbed

- Tower: 40cm height x 20cm diameter
- Total volume: 0.0126 m³
- Constant flow rate pump to fill the tower
- One outlet valve for water distribution
Power System

- 9 Bus Standard IEEE Power System
- 18 Simulated Relays with auto reclose
- Each relay can be controlled over Modbus
- 1 PMU Unit with C37-118 protocol support
Virtual Gas Pipeline Testbed Fidelity Evaluation
Performed Tests

• Real-time response

• Pressure rising curve

• Pressure discharge curve

• Man-in-the-middle attack
Real-Time response of the OpenPLC
Comparison Results - Pressure Characteristics

**Rising curve**
- Pressure (in psi) vs. Time (in Sec)
- 2 lines: Physical and Virtual

**Falling curve**
- Pressure (in psi) vs. Time (in Sec)
- 2 lines: Physical and Virtual
Comparison Results - Attacks (MiTM Injection)
Expansion of the Virtual Gas Pipeline
Virtual 15km Pipeline Testbed
Questions