JOHNS HOPKINS
WHITING SCHOOL *of* ENGINEERING

Spire: Intrusion-Tolerant SCADA for the Power Grid

Amy Babay, Tom Tantillo, Trevor Aron, Yair Amir
Department of Computer Science
Johns Hopkins University

Distributed Systems and Networks Lab
www.dsn.jhu.edu

Abstract

Motivation:

SCADA systems are used to monitor and control critical infrastructure such as the power grid. It is of paramount importance that these systems are operational at all times — without electricity there are potential huge losses of life and money. These systems are under threat by hackers. Spire is a system that runs correctly even if parts of it have been compromised.

Methods:

We built an event-based SCADA system from the ground up with all open source components. We then integrated it with the Prime intrusion-tolerant replication engine, running over the Spines intrusion-tolerant messaging system, replicating the SCADA master.

Results:

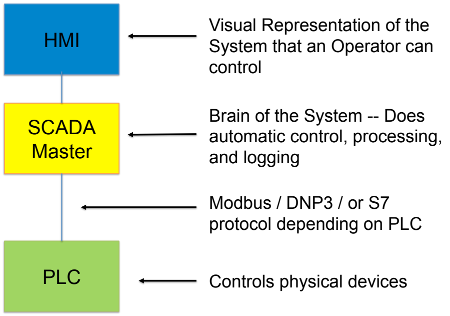
Spire was recently tested in the DoD ESTCP project titled “Critical Energy Infrastructure Cyber Defense-in-Depth”, led by Resurgo Inc, where it successfully controlled a small power grid in the presence of several days of cyberattacks from a Sandia National Laboratory red team.

Background

What is SCADA:

- Supervisory Control and Data Acquisition Systems form the backbone of critical infrastructure services such as power grids, water treatment facilities, and even running air craft carriers
- For power grids, there are timeliness requirements of 100-200 milliseconds for critical monitoring and control data

Traditional SCADA Architecture



HMI ← Visual Representation of the System that an Operator can control

SCADA Master ← Brain of the System -- Does automatic control, processing, and logging

← Modbus / DNP3 / or S7 protocol depending on PLC

PLC ← Controls physical devices

SCADA Security Concerns:

- SCADA systems are moving from specialized networks to IP networks
- STUXNET was a virus that targeted a Iranian SCADA system, showing that sophisticated attackers exist

Intrusion Tolerance:

- Byzantine fault tolerant replication is replication of a server such that for every 3*f* + 1 servers, *f* server intrusions or faults can occur and the system will operate correctly

Spire Components

Prime (www.dsn.jhu.edu/prime)

- Provides Byzantine Fault Tolerant semantics with timeliness guarantees even under attack

Spines (www.spines.org)

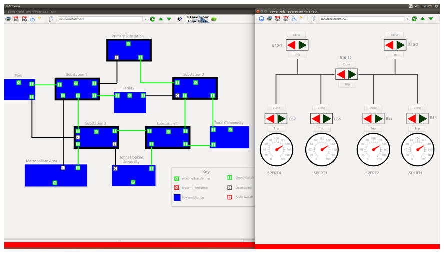
- Network that provides authentication, encryption, and the ability to work despite the presence of most network attacks. Daemon on each device

SCADA Master (www.dsn.jhu.edu/spire)

- Custom built SCADA Master designed to integrate with Prime

PvBrowser (https://pvbrowser.de/pvbrowser/index.php)

- Open Source HMI software that is used in Romanian power grid



PLC/RTU Proxy (www.dsn.jhu.edu/spire)

- Speaks DNP3 (using OpenDNP3) and Modbus (using PvBrowser add-ons)

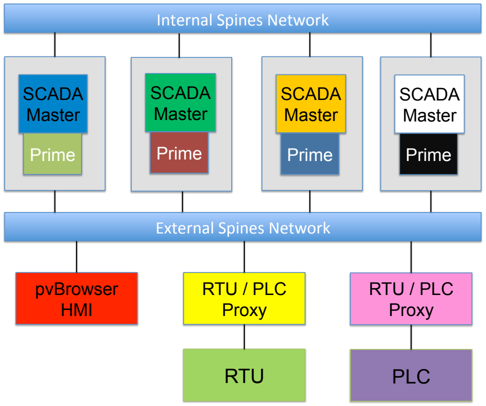
OpenPLC (http://www.openplcproject.com/)

- PLC development software that speaks Modbus and DNP3

Multicompiler (https://github.com/securesystemslab/multicompiler)

- Provides diversity to prevent the same attacks working twice

Spire Architecture: Single Control Center



Internal Spines Network

SCADA Master / Prime | SCADA Master / Prime | SCADA Master / Prime | SCADA Master / Prime

External Spines Network

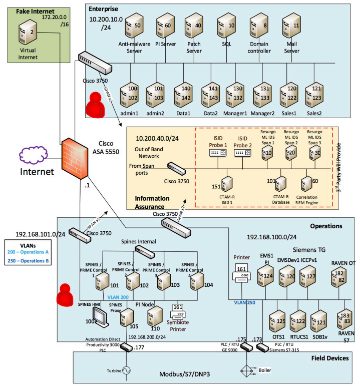
pvBrowser HMI | RTU / PLC Proxy | RTU / PLC Proxy

RTU | PLC

24 April 2017

ESTCP Red Team

- Spire was tested as a part of a DoD ESTCP project titled “Critical Energy Infrastructure Cyber Defense-in-Depth” at Pacific Northwest National Laboratories
- Conducted by Resurgo Inc March 27 – April 7, 2017
- A Sandia National Laboratories red team attacked both Spire, and a NIST-compliant SCADA system
- Both systems emulated the same scenario



Results

- The red team attacked the NIST-compliant SCADA system from the corporate network and completely took control of it by breaking into the operations network with the PLC
- They then spent several days trying to subvert our system from both the corporate network and from the operations network before they eventually gave up.
- The Proxy prevented the attacks from directly getting to the PLC
- Spines proved to be difficult for the red team to break
- During the last day, the red team was given root access on one of the SCADA Master replicas. Despite controlling one node, they could not affect Spire, showing the power of building intrusion tolerant systems

Conclusions

- Current SCADA systems are more vulnerable to attackers than we expected
- We made our system hard to attack by taking the PLC off the network and using Spire
- Intrusion tolerance is a powerful tool to keep SCADA systems working in the face of determined nation-state attackers

Additional Questions?

Contact us!

{babay, tantillo, taron1, yairamir}@cs.jhu.edu

http://www.dsn.jhu.edu

http://www.dsn.jhu.edu/spire