Jovana Helms (LLNL)
Matthias Engels (PNNL)
Craig Rieger (INL)
Peter Scheibel (LLNL)

Safe Active Scanning for Energy Delivery Systems

Cybersecurity for Energy Delivery Systems Peer Review

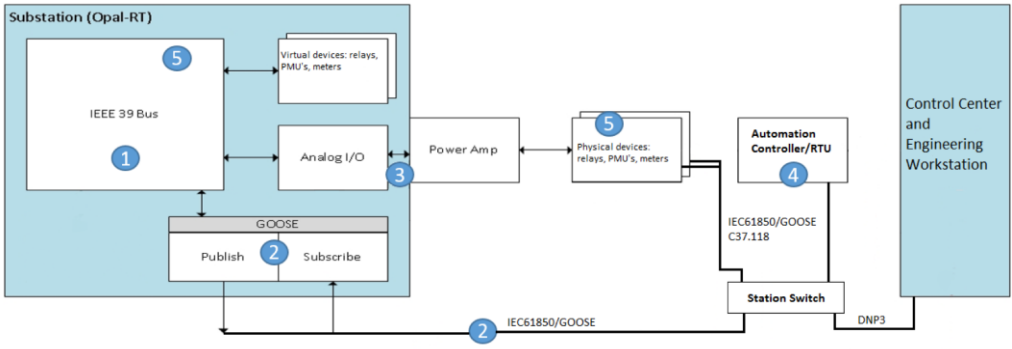
December 7-9, 2016

LLNL-PRES-713261
This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

Summary: Safe Active Scanning for Energy Delivery Systems

Objective

- Identify whether active network scanning techniques may be safely applied to EDS
- Identify negative impacts to the EDS that can result from active scanning



Schedule

- 09/2015 – 06/2017
- Deliverables:
  - Literature survey and industry partners interviews – **complete**
  - Experimentation plan – **complete**
  - Conduct experiments in two testbed environments – **complete**
  - Analysis of experiment results and path forward for further evaluating safety and value of active scanning for EDS – **in progress**

Performer:	**Lawrence Livermore National Laboratory**
Partners:	**PNNL, INL**
Federal Cost:	**$600k**
Cost Share:	**N/A**
Total Value of Award:	**$ 600k**
Funds Expended to Date:	**50%**

Advancing the State of the Art (SOA)

Problem Statement and State of the Art:

- Active scanning is a valuable tool in securing our networks, but due to a bad reputation it is not used on EDS networks as a standard practice
- While some concerns about active scanning are valid, literature points to very few high impact documented incidents
- The incidents reported in literature are over a decade old and occurred on legacy devices (devices manufactured before 2005)

Approach:

- Use NeMS scanning tool to conduct a series of active scans ranging from non-invasive to invasive and identify, document and analyze failures and issues that occur
- Understand which scans are “safe” and under which circumstances

Benefits:

- Create a baseline for safe active network scanning in EDS
- Understand the negative impact of active network scanning in EDS

Challenges to Success

Challenge 1: Difficult to draw general conclusions about active scanning

- Increase the number of devices that are being scanned and create a production like environment

Challenge 2: Legacy devices are more likely to have issues, but were not included in the initial set of experiments

- Additional scans will be performed on legacy devices

Challenge 3: Characterizing the value of active scanning and moving past “active scanning is dangerous” is difficult

- Propose looking into characterizing the benefits of active scanning and characterizing the system level impact if failures result from active scanning

Progress to Date

Major Accomplishments

- Completed literature survey and industry partner interviews
- Developed an experimentation plan that includes scans ranging from minimally invasive to invasive
- Completed experiments in two testbed environments representative of EDS
- Industry partners interested in the results of the experiments

Collaboration/Technology Transfer

- State of the Art assessment in Phase 1 of the project and Experimentation Plan were developed in collaboration with industry partners
- Future deliverable includes developing a testing plan with industry partners specific to their environments
- Industry partners can execute the plan in their non-production environment

Next Steps for this Project

Approach for the next year or to the end of project

- Additional testing on industry specific substation testbed
- Analyze results from the experiments
- Develop a roadmap for testing with industry partners

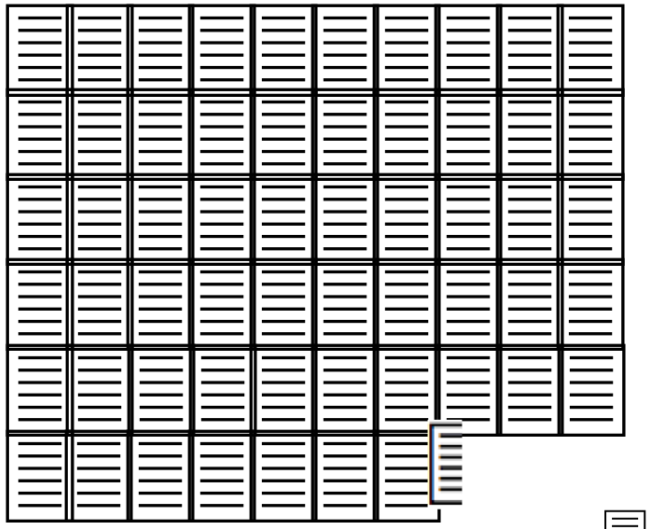
Literature Survey

Duggan, D., Berg, M., Dillinger, J., & Stamp, J. (2005). Penetration testing of industrial control systems. *Sandia National Laboratories*.

37 citations

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16.

574 citations



= 10 citations

*"While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. Luckily, the person in the room was outside the reach of the arm."**

*"On a PCS network, a ping sweep was being performed to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. The outcome was the destruction of $50K worth of wafers. "**

*"A gas utility hired an IT security consulting company to conduct penetration testing on their corporate IT network and carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours."**

*Duggan, D., Berg, M., Dllinger, J., & Stamp, J., (2005) Penetration Testing of Industrial Control Systems, Sandia National Laboratories

Experiments: Description and Results

Experiment description:

- ✓ Primary scanning tool NeMS
- ✓ nmap used for a small subset of per-target scans
- ✓ Two independent testbeds (at INL and PNNL) were used
- ✓ All scans were uncredentialed

Scans performed:

- ✓ TCP SYN scan
- ✓ Host detection
- ✓ Service detection
- ✓ OS Type detection
- ✓ High intensity scans

- ✓ The testbeds included over 19 devices representative of an EDS environment
- ✓ All scans were performed on individual devices in a standalone and in an integrated mode
- ✓ Two devices experienced issues with the more invasive scans
  - A relay became unresponsive from an UDP/TCP service detection scan (medium impact)
  - An SQL Server did not update the batch number and a timestamp (low impact)
- ✓ No other scans resulted in issues or failures
- ✓ Additional experiments are needed that will investigate the device behavior in a production like environment.