Research Spotlight Forum

SAND2019-9182PE

8.6.19 Cybersecurity

Cybersecurity for Energy Delivery Systems Project Overviews

PRESENTED BY:

Adrian Chavez
adrchav@sandia.gov
505-284-6664
Autonomous Cyber Systems
Sandia National Laboratories

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2019-xxxx

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories

Georgia Institute of Technology

ILLINOIS

PURDUE UNIVERSITY

THE UNIVERSITY OF TEXAS AT AUSTIN

THE UNIVERSITY OF NEW MEXICO

NM STATE UNIVERSITY

NEW MEXICO TECH SCIENCE • ENGINEERING • RESEARCH UNIVERSITY

ABOUT YOURSELF

Education

- 2000-2004, B.S. in Computer Science, University of New Mexico
- 2004-2005, M.S. in Computer Science, University of Colorado, Boulder
- 2012-2017, Ph.D. in Computer Science, University of California, Davis

Research Areas

- Cyber security red team assessments
- Code obfuscation
- Moving Target Defense
- Real-time software upgrades
- Cybersecurity for critical infrastructure systems
- Autonomy

Research group interests, size and demographics

- Work focused on cybersecurity for IT/OT systems
- Industry, academic, and government partnerships critical
- > 100 staff in 0582x, and 0588x
- > 10,0000 employees at SNL in NM and CA

Keywords:

Critical Infrastructure, SCADA, Moving Target Defense, Cybersecurity, Autonomy, Machine Learning, Secure Computing, Live-upgrades, Live-migration, Containerization, Virtualization.

CURRENT WORK IN CYBERSECURITY

Containerized Application Security for Industrial Control Systems (CAPSec)

- Docker containers to support live-updates and live-migration of software
- Minimize or eliminate any downtime
- Apply towards a microgrid at a partner site
- Partners: Georgia Tech, Fort Belvoir NVESD, Schweitzer Engineering Laboratories, Pacific Northwest National Laboratories, Grimm, Chevron

Survivable Industrial Control Systems

- Automated cyber-physical detection and response within critical infrastructure systems
- Correlate physical events with mod/sim environment and alarm/respond on discrepancies
- Apply towards a microgrid at a partner site
- Partners: Georgia Tech, Fort Belvoir NVESD, Schweitzer Engineering Laboratories, Pacific Northwest National Laboratories, Grimm, Chevron

Alliance

- Combine cyber/physical access control system for Industrial Control Systems (ICS) into a single device
- Red team assessment of prototype
- Partner: Schweitzer Engineering Laboratories

CURRENT WORK IN CYBERSECURITY (cont.)

SDN4EDS

- Document a best-practices guide for deploying Software Defined Networking within ICS environments
- Red team assessment of reference implementation
- Partners: PNNL, Schweitzer Engineering Laboratory, Juniper, SCE, CAISO, Dispersive, USPACOM, and Cisco

Ekhi

- Develop a low-power, low-cost bump-in-the-wire solution for Distributed Energy Resources that can detect/respond to threats
- Apply machine learning algorithms and signature-based intrusion detection systems
- Apply towards emulytics environment
- Partners: OPAL-RT, EPRI

2030 HECO Assessment

- Red team assessment of high-penetration PV system
- Partners: HECO, NREL

Threat Detection & Response

- Distinguish cyber events from physical events in ICS environments
- Machine learning and natural language processing
- Partners: Electric Power Board of Chattanooga, Idaho National Laboratory, Lawrence Berkley National Laboratory, Lawrence Livermore National Laboratory (prime), National Rural Electric Cooperative Association, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, Sandia National Laboratories Schweitzer Engineering Laboratory

FUNDING SOURCES

Department of Energy – Cybersecurity, Energy Security, and Emergency Response (CESER) office - Cybersecurity for Energy Delivery Systems (CEDS)

- Survivable ICS Academic Alliance partnership with Georgia Tech
- CyberForce competition

Department of Energy – Grid Modernization Laboratory Consortium (GMLC)

- Survivable ICS Academic Alliance partnership with Georgia Tech

Department of Energy – Solar Energy Technology Office (SETO)

Department of Homeland Security – Science and Technology

Laboratory Directed Research and Development

RESEARCH NEEDS

Representative IT/OT data to train machine learning algorithms

- Labeled or unlabeled data

Autonomous cyber security for IT/OT systems

- Identify
- Protect
- Detect
- Respond
- Recover

Automated blue team/red team systems to guide secure configuration/deployments of hardware/firmware/software

- Caldera automated adversary emulation

Partnerships for DOE CEDS and GMLC required

- Academic partnerships critical
- Research ideas that have a commercialization path

Questions?

Contact Information:

Adrian Chavez
adrchav@sandia.gov
505-284-6664
Autonomous Cyber Systems
Sandia National Laboratories