U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Autonomous Tools for Attack Surface Reduction

IOWA STATE UNIVERSITY

Attack surface analysis and reduction metrics, algorithms, and tools to protect energy delivery systems

Advanced persistent threats present highly sophisticated, stealthy, and evolving attacks of control system environments to target physical system processes. While attacks on distribution systems may not have the same cascading impact found on transmissions systems, they can still cause widespread outages. Securing the grid against cyberattacks is challenging due to the legacy nature of the infrastructure, a dynamic threat landscape, and the ever-growing sophistication of the adversaries. Additionally, the grid's attack surface continues to grow with the increased dependence on digital communication and control that now extends to each consumer through smart meters and distributed energy resources. More systematic approaches are required to identify and reduce attack surfaces. The project team is developing an end-to-end framework and robust algorithms for continuous analysis and automated reduction of the attack surface across control center, substations, and the wide-area Supervisory Control and Data Acquisition (SCADA) communication networks. The team is establishing security metrics to support autonomous attack prevention, anomaly detection, and attack mitigation algorithms. This significantly reduces the exposure of energy transmission and distribution grid environments to cyber threats in a continuous and autonomous nature.

KEY TAKEAWAYS

- Delivers a validated methodology, metrics, and benchmarks for attack surface analysis
- Reduces energy delivery system attack surface via robust defense techniques and data-driven algorithms without interfering in critical system functions
- Automates the implementation of cybersecurity measures to protect critical control systems against attacks ranging from phishing to distributed denial-of-service

OUTCOME

This project establishes a security baseline to implement autonomous techniques for attack surface analysis and reduction across multiple system layers, minimizing phishing, denial-of-service, and data integrity attacks in various system components. This simplifies the application of security monitoring and attack surface reduction capabilities as part of future standard compliance programs.

PARTICIPANTS	ROLE
Iowa State University	Develops methodology, metrics, and algorithms for attack surface reduction, intrusion detection system for SCADA and substations, and anomaly detection and mitigation algorithms for Energy Management System (EMS) applications. Conducts testbed-based evaluation, tool integration into industry-grade SCADA and EMS platforms, and field demonstration of technologies and tools working in collaboration with partners.
Pacific Northwest National Laboratory	Contributes to the design, testing, and evaluation of attack surface analysis and reduction algorithms with realistic use-case scenarios.
Argonne National Laboratory	Develops and evaluates attack-resilient algorithms for microgrid applications in smart grid environments.
Washington State University	Develops, tests, and evaluates algorithms, metrics and a software tool for attack surface analysis. Field demonstration and technology transfer (via an open source repository) of the attack surface analysis tool for industry adoption.
GE Global Research	Develops and evaluates anomaly detection algorithms for synchrophasor-based EMS applications; tool integration with industry-grade synchrophasor analytics platform.
cfu Cedar Falls Utilities THE POWER OF SERVICE	Field deployment, demonstration, and testing of intrusion detection system in a real distribution grid involving multiple substations, SCADA communication, and a control center.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Manimaran Govindarasu
Principal Investigator
Iowa State University
515-294-9175
gmani@iastate.edu

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: October 2016 – December 2020

Total Award Value: $4,132,007
DOE Share: $2,981,103
Cost Share: $1,150,904

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021