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

Watching Grid Infrastructure Stealthily Through Proxies (WISP)

Raytheon Technologies

Using publicly available, real-time pricing mechanisms against cyberattacks

Locational marginal pricing (LMP) mechanisms provide critical insights into power grid operations. They assess various operating characteristics and constraints on transmission capabilities to dynamically determine regional pricing information. LMP inputs may also serve as indicators of anomalous events and cyberattacks. This project is researching and developing an open-source, non-intrusive, energy market monitoring tool that uses publicly available information to detect and distinguish cyberattacks from normal power system events. WISP uses real-time LMP and other publicly available information, such as bids, weather, and power outage data, to analyze power pricing behaviors and then correlates those observations to localized regions of interest, identifying potential cyber events. The tool will use a library of LMP-based signatures to feed a machine learning algorithm and inform its monitoring processes and optimal detection thresholds to minimize system losses.

KEY TAKEAWAYS

- Detects, mitigates, and alerts operators of malicious information injection into energy management systems
- Develops machine learning algorithms that use electricity market data streams and system conditions to detect the effects of malicious manipulation
- Uses publicly available real-time prices to detect and distinguish cyberattacks from normal power system events

OUTCOME

WISP is an open-source, advanced attack detection and energy market monitoring platform deployable for utilities and regional transmission organizations and independent system operators. This technology builds and informs models by harnessing advanced analytics from various data streams from the electricity market, social media, and weather agents, to detect cyber events localized to regions of interest. WISP transparently augments cybersecurity and resiliency to the market, control, and the grid layers without impeding critical energy delivery functions.

PARTICIPANTS	ROLE
Raytheon Technologies	Conducts technical design, development, validation, and commercialization activities; studies spatial and temporal signatures and sensitivities of locational marginal prices; designs and develops anomaly detection module
The University of Tennessee Knoxville	Performs system vulnerability analysis, identifies high cyber risk time periods and locations, and assists in technology demonstration
Southern California Edison — Energy for What's Ahead	Serves as an energy sector advisor for research, demonstration, and commercialization activities
Pacific Northwest National Laboratory	Provides subject matter expertise and assists in anomaly root cause analysis for identifying regions of interest

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Lingyu Ren
Principal Investigator
Raytheon Technologies Research Center
860-610-7705
lingyu.ren@rtx.com

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 2018 – November 2021

Total Award Value: $2,813,666
DOE Share: $2,011,098
Cost Share: $802,568

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