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

Tri-Modular Framework for an Intelligent Visualization of Smart Grid Cyberattacks

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Increases situational awareness by optimizing data analysis and visualization for system operators

This project boosts situational awareness at the command and control center, especially during a cyberattack. Protection modes, like defense-in-depth and defense-in-breadth, do not address human performance and human-machine interaction. This results in a gap between what is visualized and what system operators need to understand to make time-critical, well-informed decisions that must be supported by quality data. Automated tools rely on humans to analyze and address the issue at the same time, which stresses the operators and increases the chances of erroneous decisions. Critical gaps also remain between new events generation rates and the rate at which the operators can capture these events. The Tri-Modular Framework reduces these gaps with its 3-layer architecture. The architecture is comprised of a data module that manages the different varieties of stream data from various sources, such as sensors and generation meters. This data stream is processed and fed into a classification module that categorizes the data as normal, error, natural, and malicious. The action module provides operators with optimized options on a visual dashboard.

KEY TAKEAWAYS

- Optimizes visualizations to ensure operators make well-informed decisions when responding to cyberattacks
- Expedites human-machine interactions during time-critical events

OUTCOME

This framework provides computer-generated visualizations that provide the information necessary for human operators to make well-informed, time-sensitive decisions. Machine-assisted data processing, classification, and presentation enables operators to quickly identify the ideal response to active cyberattacks with the highest possible degree of confidence in the likely outcome.

PARTICIPANTS	ROLE
SEEDS CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS	This project is part of the Secure Evolvable Energy Delivery Systems (SEEDS) academic consortium. SEEDS researches and develops innovative cybersecurity technologies, tools, and methodologies to advance the energy sector's ability to survive cyber incidents while sustaining critical functions.
FIU FLORIDA INTERNATIONAL UNIVERSITY	Research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Dr. Arif Sarwat
Professor
Florida International University
305-348-4941
asarwart@fiu.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

This is a subproject sponsored by the SEEDS academic consortium, led by the University of Arkansas.

SEEDS Period of Performance: October 2015 – March 2022

SEEDS Total Award Value: $15,309,114
DOE Share: $12,226,504
Cost Share: $3,082,610

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