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

Detecting Compromised Devices

SEEDS
CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Intelligently identifying malicious behaviors within smart grid architectures

Smart grid devices across energy delivery systems (EDS) are attractive targets for cyberattacks that can cause significant damage to complex systems. Smart grid devices that have been infected by malware often demonstrate extra functionality that healthy devices do not, making them identifiable within a well-monitored EDS infrastructure. This project develops a configurable framework that can detect compromised devices performing unauthorized operations inside the critical parts of the smart grid architecture. Such operations include leaking information, poisoning measurements, or storing and sending valuable power status information to unauthorized entities. The software developed by the team combines system call tracing with statistical and machine learning techniques to detect and prevent compromised device behavior through a distributed network of monitoring software. The tool can be rapidly deployed into devices in the smart grid through firmware update.

KEY TAKEAWAYS

- Develops a software solution to monitor and identify unauthorized activities across smart grid devices
- Combines machine learning and statistical modeling to efficiently detect malicious device behavior
- Deploys a distributed architecture for efficient event detection and prevention

OUTCOME

This project demonstrates and delivers an intelligent framework for identifying malicious behavior on smart grid devices across EDS networks. EDS operators will be able to deploy an activity analyzer component to more easily track energy consumption, CPU utilization, and the memory activities of the events associated with various field devices.

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	Leads research and engages industry collaborators

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

A. Selcuk Uluagac
Associate Professor
Florida International University
305-348-3710
suluagac@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