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

HELOT: Hunting Evil Life in Operational Technology

SEEDS CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Provides live forensics in combined information technology/ operational technology environments

After a cyberattack in the energy sector, post-event inspection and forensics tasks usually require the shutdown of the operational technology (OT) systems under investigation. However, the nature of OT systems does not allow these procedures. This project develops a system that provides live forensics analysis in combined information technology (IT)/OT environments, where minimal security logs and storage are available on OT devices that are geographically dispersed and require no-service-downtime policies for capturing forensics artifacts. In developing this capability, the project team uses a live forensics pipeline of configuration data and network traces, in addition to OT device artifacts, gathered by light-weight clients and/or clientless connections in wide-area networks using Google Rapid Response (GRR)-based plugins. The collected information is classified and stored into Elasticsearch-based information storage for continuous analysis.

KEY TAKEAWAYS

- Enables live forensic analysis in combined information technology/operational technology environments without the need to shut down operations
- Leverages Google Rapid Response to offer a plugin-based, infrastructure agnostic, live forensics solution to IT/OT operators

OUTCOME

This project delivers a suite of effective and scalable tools for conducting live incident response on a wide variety of devices and systems used in OT in the energy sector. It is based on the GRR framework adding plugin capabilities for OT devices on top of support for all major operating system platforms. This enhances the capabilities and effectiveness in industrial control systems.

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.
UA LITTLE ROCK George W. Donaghey EMERGING ANALYTICS CENTER	Leads system prototype development, testing, and deployment preparation
EPRI ELECTRIC POWER RESEARCH INSTITUTE	Enables testing on a wide range of OT devices
Electric Cooperatives of Arkansas *Your Local Energy Partners*	Collaborates on discussion of operational requirements; supports additional field testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Jan P Springer
Director, Emerging Analytics Center
UA Little Rock
501-916-3140
jpspringer@ualr.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