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

Ambassador Project

SCHWEITZER ENGINEERING LABORATORIES

Advanced application orchestration for delivering joint capability and secure data sharing between converged information and operational technology systems for utilities

Software-defined networking (SDN) technology enables the rapid deployment and scaling of network management and orchestration software. Many software companies are leveraging the benefits of SDN capabilities, but it also introduces interoperability challenges into SD infrastructures. This project researches, develops, and demonstrates a trust, data, and resource management technology that enables multiple software applications from different suppliers to cooperate simultaneously. The project builds upon the successful completion of the Watchdog and SDN projects with an engineered solution to manage the trust, data, and resources that are passed between software applications operating in the SDN environment. Ambassador enables security orchestration for the controller, providing complete network visibility, situational awareness, automated flows creation, and active defense measures for detected threats.

KEY TAKEAWAYS

- Advances trust management and authentication mechanisms between multiple manufacturers' applications including network management and network monitoring for both the enterprise and energy delivery systems
- Adds intrusion detection capability with software defined networks, with the ability to prescribe remediation against threats and vulnerabilities
- Provides continuous monitoring, prioritization of application functions, visualization of the overall software-defined networking security posture and improves active defense response

OUTCOME

This project supports the commercialization of a software ecosystem that maintains interoperability, cybersecurity, and reliability where the end-user can safely scale their software to leverage the benefits of SDN. It enables operators to utilize and advance SDN-supported services, such as rapid cyber event detection and visualization, without facing compatibility issues.

PARTICIPANTS	ROLE
SEL SCHWEITZER ENGINEERING LABORATORIES	Self-configuration of substation networks based on the end devices configuration; develops the interface application, scheduler, priority queue system, trust management engine, and the SDN telemetry data for improved security awareness
JUNIPER NETWORKS	Provides circuit provisioning and telemetry monitoring software
DRAGOS	Delivers an intrusion detection and incident response software application with the capability to integrate active defense measures
Bonneville POWER ADMINISTRATION	Conducts testing and validation

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Dennis Gammel
Principal Investigator
Schweitzer Engineering Laboratories
509-336-7981
dennis_gammel@selinc.com

Current Contact as of October 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 – September 2021

Total Award Value: $5,114,520
DOE Share: $3,999,416
Cost Share: $1,115,104

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: October 2020