U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Energy Sector Security Appliances in a System for Intelligent Learning Network Configuration Management and Monitoring (Essence)

Software defined network to assist small electric cooperatives with limited resources for securing utility operational networks

Background

Utilities of all sizes are faced with the challenge of configuring, managing, monitoring, and securing their information technology and operational technology (IT and OT) networks; but the challenge is more acute for small utilities and electric cooperatives with limited resources and personnel. As the electric industry increasingly migrates utility IT and OT systems to virtualization and cloud-managed services, these small electric cooperatives could benefit from shared solutions that keep up with these trends.

New solutions can further take advantage of emerging software defined networking (SDN) capabilities to automate the network response to a cyber compromise. SDN automates secure operational network management while reducing the effort and risk associated with manual processes. Small electric cooperatives could leverage this technology to provide stronger network security and to manage operational and back office networks.

Barriers

- Small utilities and electric cooperatives have limited resources for managing/securing networks.
- A "reactive" approach to detecting threats is new and unfamiliar.
- Quantifying return on cybersecurity investments is challenging.

Project Description

The Essence project is developing tools that facilitate more secure operational network management. SDN will provide a solution to assist cooperatives with mapping their networks, analyzing traffic, and learning expected traffic flow to better inform human operators.

Traditional approaches to cybersecurity have been largely prescriptive in the sense that a series of experts defines tests to detect malware and suspicious communications. The effectiveness of such systems depends on a long sequence of individuals all doing their jobs perfectly, ranging from experts in cybersecurity forensics to utility staff who maintain firewalls. The Essence project is focusing on systems that are reactive, detecting potential threats by learning normal operational patterns (using machine intelligence) and monitoring for anomalies.

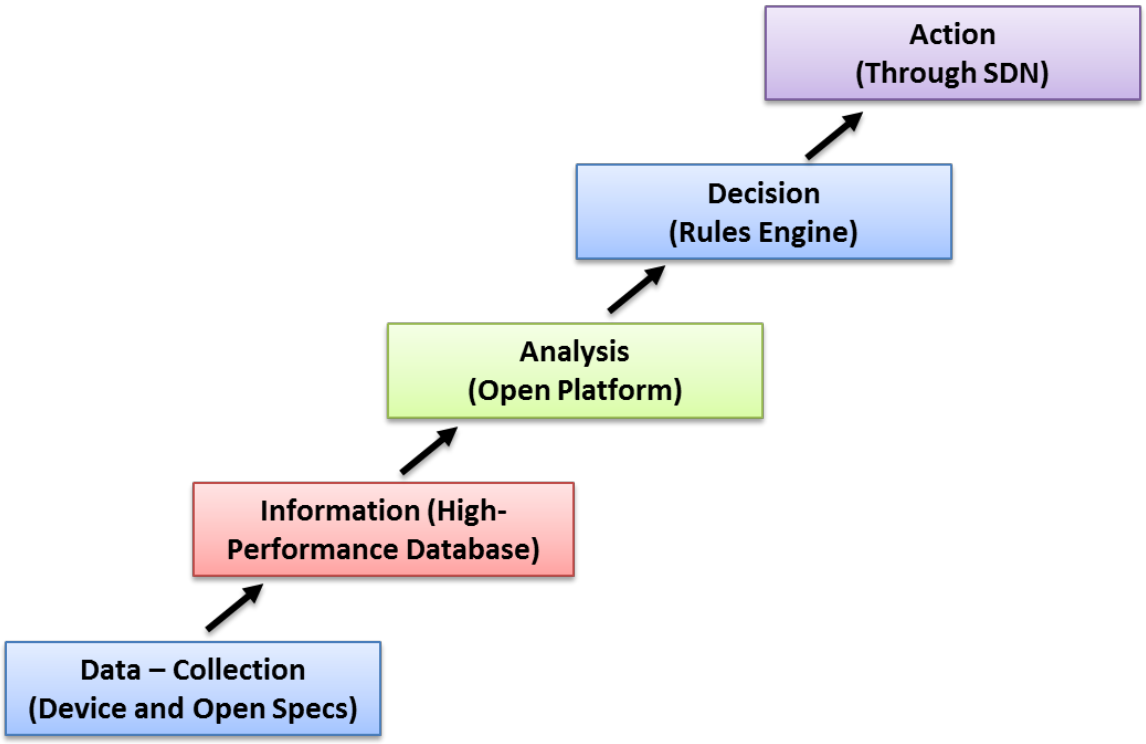
Essence is providing the ability to update a utility's security policy as business needs and cyber threats evolve, while ensuring that changes conform to a utility's security policy. By using utility protocols (e.g., MultiSpeak, DNP3), filtering rules are applied to detect and prevent malicious operational network traffic.

Benefits

- Provides electric cooperatives with cybersecurity tools that emphasize the "human factor": technology that helps smaller utilities and electric cooperatives, with limited resources, to more easily design and manage more secure operational networks
- Detects zero-day exploits
- Integrates detection with methods and tools for remediation
- Provides real-time cybersecurity that is aware of power grid operations
- Provides flexible and reliable development and enforcement of utility security policies
- Uses dynamic, role-based access control
- Prevents malicious network traffic
- Simplifies security reporting and compliance tasks for utility operational networks

Partners

- **National Rural Electric Cooperative Association**
- Honeywell
- Carnegie Mellon University
- Pacific Northwest National Laboratory
- Cigital, Inc.



Abstraction model of the Essence system

Technical Objectives

The project is developing tools that facilitate more secure operational network management in two phases.

Phase 1: Develop and Test System

- Develop a fully operational system
- Test the system's ability to capture data at realistic volumes, train a model of "normal" communications traffic, and detect anomalies with an acceptable level of false positive and false negative findings; conduct tests at a small number of utilities at lower traffic volumes

Phase 2: Refine System Performance

- Test the improved version of the Essence system, based on the Phase 1 results from several utilities with different technologies and modus operandi
- Refine system performance and traffic-handling capabilities as appropriate

End Results

Project results will include the following:

- Automated tools for learning what normal utility operations look like
- Automated tools for detecting potential breaches
- Automated software defined network management tools to isolate and perform graceful degradation of compromised communication channels

November 2014

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) research and development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks.

Contact Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Craig Miller
Chief Scientist, National Rural
Electric Cooperative Association
703-626-9683
craig.miller@nreca.coop

For More Information:

- http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity
- www.controlsystemsroadmap.net