Chess Master

Operational networks that deny-by-default unexpected cyber activity to help prevent an intrusion and have pre-engineered response to adapt and survive should an intrusion occur

Background

To sustain critical energy delivery functions during a cyber intrusion, control system operators need a method that ensures only approved and expected cyber-activity takes place, called "whitelisting", and that unexpected cyber-activity is automatically denied by default. Because layers of cyber-defense technologies reduce risk, in addition to proactive whitelisting of communications and processes, the control system must automatically adapt to survive a cyber-intrusion, for instance, by automatic identification and containment of the affected network areas, and re-routing of critical information and control flows around the isolated area of the network. Energy delivery system operational networks that automatically adapt to survive a cyber-incident must provide the operator a global view of all the control system operational network communication flows and the ability to rapidly set-up and implement operational network policies.

Objectives

The Chess Master team will build on the successful commercial release of utility rated software defined network (SDN) technology under the previous CEDS project, Watchdog, and produce a solution operators can use to quickly establish and apply network policies. Operators will be able to proactively engineer incident response profiles that can be selected based on the cybersecurity state of their operational networks. Communication in the control system network is whitelisted, that is, only approved cyber-activity is allowed. Should unapproved traffic appear, the operational network will alarm and record the traffic as well as potentially transition to a more secure state. This whitelisting approach allows the system owners to protect against both known cyber-attacks, and attacks that have not yet become widely known, that is zero-day, attacks.

Project Description

This project will provide system operators, with a global view of their operational network, enabling them to set and view field network security policy and validate operational adherence to those policies. Operators will be able to engineer and gain visibility into every communication flow and preconfigure response actions to events, including automated responses to undesired behavior. The technology will provide the operators a quick visual representation of what happened, which communications are impacted, and how they were affected. Security control options that will be integrated include:

- Configure field network access control and verify that configurations satisfy security and compliance policies
- Define specific actions to take on any new communication flow attempts
- Establish central management capabilities for whitelisting protocols, applications, and devices on field networks

Benefits

- Strengthen cybersecurity with central visibility of operational networks that deny-by-default to help prevent unexpected, and therefore undesired, cyber-activity
- Automate cyber-incident response using pre-engineered response actions

Partners

- Schweitzer Engineering Laboratories, Inc. (lead)
- Ameren Energy Resources
- Sempra
- Veracity Security Intelligence

Period of Performance

October 2016 – October 2020

Total Project Cost Total:

$5,097,162

Federal: $3,952,679

Cost Share: $1,144,483

Content last updated: May 2017

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) 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 emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

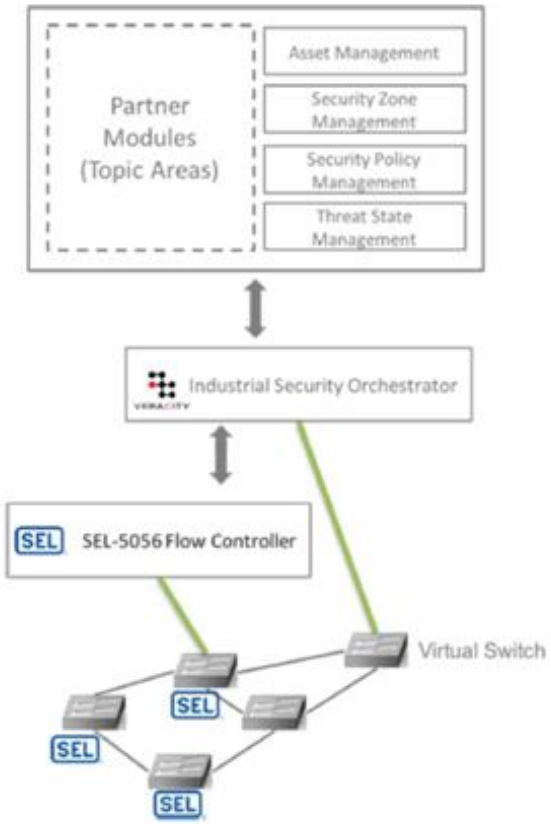
Initial Leads

Carol Hawk
Program Manager

Rhett Smith
Principal Investigator
Schweitzer Engineering Laboratories
509-336-7939
rhett_smith@selinc.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov



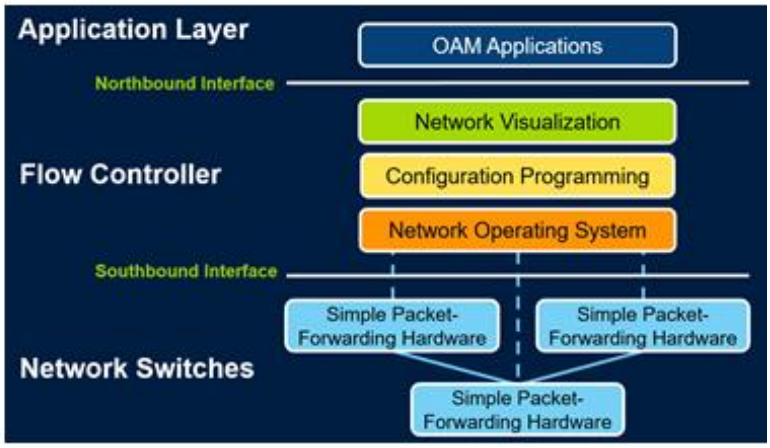


Figure 1. Chess Master Architecture

Technical Approach

This project will build on the success of the Watchdog and SDN projects that produced a software-defined switch and flow controller, respectively. The Chess Master project will develop a security northbound application and standardize the application programming interface (API) between the flow controller and the application. The Chess Master project will research, develop, test, and release the following:

- Security policy enforcer application that receives data from and orchestrates the OpenFlow flow controller. This may be released commercially for the SEL-5056 flow controller.
- Visualization tools for situational awareness to help the operator know quickly what threat level and operational profile is active in all field networks.
- Technology and tools to automatically enforce pre-configured security profiles and change between levels of ever increasing defensive controls.
- Technology and methods to secure field networks with pre-defined recommended security controls to apply based on the applications and services running and behavioral characteristics of the devices.

Anticipated Results

Project results will include the following:

- Research, develop, test, and commercialize a security validation and policy enforcement application that connects into a flow controller managing all field networks centrally.
- Field test, and demonstrate the technology in real world control system installations and prepare best practice guides for testing, deployment, and long term management of the technology.