U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Artificial Diversity and Defense Security (ADDSec)

Introducing unpredictability and enhanced situational awareness to energy delivery systems through software defined networks

Background

Energy Delivery control systems traditionally have predictable communication paths and static configurations. These wide area networks (WAN) use Time Division Multiplexing (TDM) as the current best methodology for deterministic, reliable, wide area communications for critical control systems.

Methods currently available for software defined networks (SDN) should be extended to WANs. Then it is possible for these devices to change IP addresses and routing information to dynamically reconfigure in order to defeat reconnaissance and ethernet based attacks.

Objectives

- Bring moving-target capability to wide-area networks in the energy sector
- Ensure integrated technology continues to meet high availability and real-time constraints
- Scaling this solution to large networks while avoiding implementation/design error

Project Description

The ADDSec project will develop solutions to introduce unpredictability and enhance situational awareness to energy delivery control systems, protecting them against cyber attack. The project will leverage software defined networking (SDN) to introduce randomness to control system networks and extend solutions from the local network area to the WAN.

ADDSec will develop three main components for this solution: 1) Automatic Reconfigurable Network Settings (ARN), 2) Randomizing Application Instructions Sets (RAIS), and 3) Machine-based Dynamic Defense (MDD). The ARN component will manage network configurations, securely communicate reconfiguration specifications, and ensure uninterrupted connectivity between nodes. The RAIS component will randomize the instruction sets that execute programs on the end devices, protect against code injection attacks, buffer overruns, and reverse engineering of software. The MDD component will be designed to dynamically defend against active attacks by recognizing patterns, providing situational awareness, and taking appropriate actions when necessary.

Benefits

- Increase the difficulty and complexity required for adversarial attacks on energy delivery control systems
- Increase the likelihood that an adversary will be detected while attempting to attack a system
- Proactively classify and mitigate threats at both the host and network levels of a control system as they are detected.
- Scalable to large networks and interoperable with other SDN capable vendor units.
- Significantly increase the security of both legacy and modern systems by improving overall situational awareness and converting static systems into moving targets.

Partners

- **Sandia National Laboratories** (lead)
- Lawrence Livermore National Laboratory
- Washington Gas Energy Systems
- Ft. Belvoir
- Chevron
- Grimm
- Schweitzer Engineering Laboratories

Period of Performance

October 2014 – December 2021

Total Project Cost

$2,998,364

Content last updated: May 2016

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

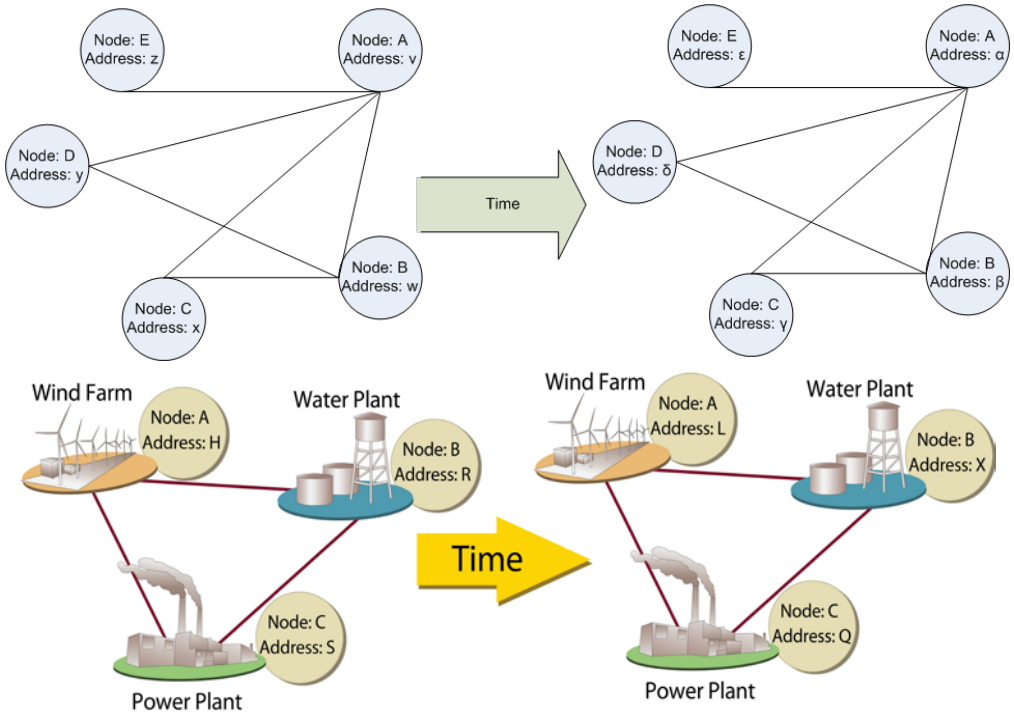
Initial Leads

Carol Hawk
Program Manager

Adrian Chavez
Principal Investigator
Sandia National Laboratory
505-284-6664
adrchav@sandia.gov

Current Contact as of Aug. 2020

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



A high-level overview of a single network during reconfiguration of the network node addresses.

Technical Approach

The project consists of research, development, and demonstration activities to build a vetted, open-source solution that incorporates a secure, scalable, resilient communications framework; enhanced security for energy sector protocols; and a framework for computation to support advanced situational awareness and analysis. Commercialization efforts will occur alongside development activities.

Phase 1: Prototype and Document

- Gather technical and operational requirements and capabilities from vendors
- Develop software defined network over WAN
- Integrate multiple project components into a single system
- Establish proof-of-concept within Sandia National Lab test setting

Phase 1 (cont.)

- Gather performance metrics from each component
- Hold independent 3rd party red team assessment.

Phase 2: Outreach and Test

- Complete laboratory environment setups and test R&D solution
- Integrate solution into an active microgrid to test interoperability with additional partners/participants.
- Document results

End Results

Project results will include the following:

- A more resilient and secure communications mechanism to support modern grid operation
- Improved security posture for utility infrastructure by (1) enhancing security of both known and unknown protocols and (2) extending security protection through internal perimeter protections for utility infrastructure
- An extensible platform that enables future computation, data analytics, and enhanced situational awareness
- A solution built with open source tools that is interoperable with commercially available products and can be retrofitted into existing systems already in operation