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

Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS) – University of Arkansas

Research and development of solutions for cyber vulnerabilities across the United States' energy delivery systems

Background

In 2011, The Energy Sector Control Systems Working Group (ESCSWG) developed the revised "Roadmap to Achieve Energy Delivery Systems (EDS) Cybersecurity" in support of the Electricity Sub-sector Coordinating Council, the Oil and Natural Gas Sector Coordinating Council, and the Government Coordinating Council for Energy under the Critical Infrastructure Partnership Advisory Council (CIPAC) Framework. This project addresses objectives to meet or exceed the Roadmap vision. The Department of Energy Office of Electricity Delivery and Energy Reliability's (OE) Cybersecurity for Energy Delivery Systems (CEDS) program has the mission to develop capabilities enhancing reliability and resiliency of the Nation's energy infrastructure by reducing the risk of energy disruptions due to cyber-attacks. The University of Arkansas SEEDS Center is part of the CEDS academic R&D program focused on providing solutions outlined by this roadmap.

Barriers

- Threats change with time and are hard to quantify
- Difficult to provide actionable and timely information/visualization of security posture from vast quantities of disparate data
- Performance/acceptance testing of cybersecurity solutions without disrupting EDS operations is difficult
- Complexity of EDS
- Difficult to recognize incidents under way

Project Description

The goal of this Center is to conduct research and develop innovative cybersecurity technologies, tools and methodologies that advance the energy sector's ability to survive cyber attacks and incidents while sustaining critical functions. Part of this project is to verify and validate efficacy of the developed solutions and methodologies for transition to practice and commercialization in the energy sector. SEEDS will develop solutions for cyber vulnerabilities across the United States' energy delivery systems. This will protect hardware assets, make systems less susceptible to cyber threats and provide reliable delivery of electricity, oil and natural gas if such a cyber incident occurred. The management structure of the team includes a Project Leadership Team which includes the technical and campus leads as well as industry representation to discuss project progress, management of the center and industry outreach activities. The Center has a membership-based Industrial Advisory Board (IAB) which makes recommendations regarding industry relevance and alignment with the programmatic objectives. This membership-based model allows the center to be sustainable beyond DOE CEDS funding in order to continue to address ever-present cyber threats to energy delivery systems. This project is co-funded by the Department of Homeland Security (DHS) Science and Technology Directorate.

Benefits

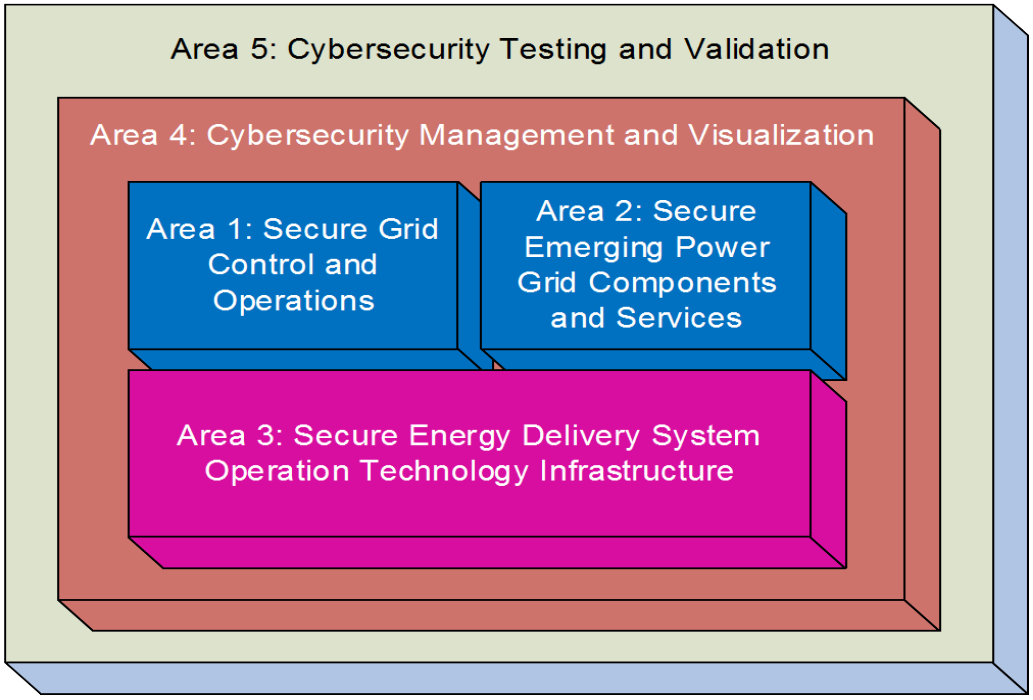
- All research receives industry feedback from the energy sector.
- Research university partners have rigorous testing facilities to evaluate cybersecurity tools prior to deployment to the energy industrial partners.
- All research is beta tested with an energy industry partner so other industry partners can evaluate results.
- Research solution efficacy is developed, verified and validated for transition to practice and commercialization in the energy sector.
- The intense research and development focus allows for the the involvement of students from all partner institutions to help provide industry a robust cybersecurity workforce.

Partners

- University of Arkansas (Lead)
- University of Arkansas, Little Rock
- Lehigh University
- Florida International University
- Carnegie Mellon University
- Arkansas Electric Cooperative Corporation

Website

- seedscenter.uark.edu



Technical Objectives

1)Secure grid control and operations; 2) Secure emerging power grid components and services; 3) Secure energy delivery system operation technology infrastructure; 4) Cybersecurity management and visualization; 5) Cybersecurity testing and validation.

Phase 1: Risk Assessment, Monitoring and Mitigation

- Analysis, modeling, and detection of data and topology manipulation attacks
- Real-time sensing, monitoring, and visualization for situation awareness
- Enhancing resilience through moving target defense
- Impact assessment of cyber attacks against time-critical communications and demand-side management

Phase 2: Advanced Protective Measure Development

- Defense-in-depth against data and topology manipulation attacks
- Detection of counterfeit devices and Botnet
- Integrated design of security-aware microgrid
- Security recovery in post-disaster power grid
- Visualization of network and control systems security

Phase 3: Intelligent and Automated Response

- Automated response to data manipulation attacks
- Optimization of security resource allocation
- Automated fusing of intrusion information for situation awareness
- Visualization for decision support
- Automated security management to mitigate cyber incidents

End Results

Project results will include:

- Achievement of industry relevant technical milestones.
- Successfully develop cyber technology and transition it for practice in the energy sector.
- SEEDS becoming a self-sustaining center in five years.
- A membership-based center with sufficient membership to continue industry relevant cybersecurity research and development.
- Rigorous research and development activity that propagates a highly quali-fied student workforce to be industry-ready in the area of cybersecurity for energy delivery

Content last updated: January 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

H. Alan Mantooth
Principal Investigator
University of Arkansas
479-575-4838
mantooth@uark.edu

Current Contact as of Aug. 2020

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