Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA)

Cyber-physical security state estimation for power grid intrusion detection and control command validation and assessment

Background

The power grid is an energy delivery system comprising of individual power components and a geographically dispersed communications system. Power grid communications systems, components, and protocols must be secured from unauthorized access because adversarial manipulation could disrupt energy delivery.

The sensitivity and effectiveness of cybersecurity countermeasures can be improved using power grid models that evaluate the security of cyber-physical processes to provide more accurate information for safety-related decisions. Sharing this cyber-physical security information via security sensors distributed throughout the communications network will help identify and prevent adversarial manipulation of power grid control actions in a system-wide context and malicious activity across the power grid.

Barriers

Situational awareness technologies must:

- Provide operational insight into the expected functioning of the overall power grid.
- Flexibly adapt to diverse network architectures and changes to those architectures.
- Provide timely, security-relevant information system-wide while functioning within the constraints of power grid communications networks.
- Account for the varying security and processing capabilities of individual components.
- Offer extensible support for emerging sector best practices in planning, operational awareness, and cybersecurity.

Project Description

The CYMSA project is developing a cybersecurity situational awareness technology suite to detect adversarial manipulation of power grid components and communications networks. The project involves novel cyber-physical modeling and simulation research on communications networks and substations. Project researchers are developing network sensor technology based on "deep packet inspection" to assess command and control messages within the context of the power grid, as captured by system models and simulations.

Benefits

- Fast and security-relevant modeling and simulation of power grid operations and cyber control systems
- Power grid intrusion detection and prevention that dynamically evolves with power grid operation
- Cyber-physical vulnerability state estimation of power grid components
- Detection of malicious activity that "plays by the rules" through distributed security sensors and operational contexts

Partners

- **Georgia Institute of Technology**
- College of Electrical and Computer Engineering
- Cyber Technology and Information Systems Laboratory
- Strategic Energy Institute
- Southern Company
- Virgin Islands Water and Power Authority
- Burbank Water and Power
- Open Information Security Foundation

Technical Objectives

This research effort is prototyping a suite of cybersecurity technologies that enhance power grid situational awareness. The technologies will be demonstrated for commercial relevance and effectiveness in identifying malicious activity.

Phase 1: Research and Development

This phase will develop:

- Fast, real-time, security-relevant modeling and simulation algorithms and implementations that are capable of capturing and expressing operational power grid system state to distributed security sensors
- High-performance, latency-aware security sensors for power grid communications networks based on existing open-source intrusion detection and prevention systems capable of deep packet inspection
- Security rule consensus and synchronicity protocols
- Enhanced models of vulnerable power grid components to prioritize protective rule generation in bandwidth-constrained environments

Phase 2: Test and Validation

- Technology validation and testing against simulated malicious actor scenarios
- Continued and iterative refinement of technology based on performance against test threat scenarios

Phase 3: Technology Demonstration

- Deployment and demonstration of the technology suite at multiple power utility operator sites with the assistance of partnering utilities
- Continued commercialization and integration activity with power sector vendors as available

End Results

Research results will include the following:

- A cybersecurity situational awareness technology suite
- Enhanced modeling and simulation technologies based on co-simulation and distributed state estimation
- Network security sensors based on open-source intrusion detection and prevention systems
- Protective rule generation, consensus, and synchronicity protocols

Content last updated: September 2014

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

Seth Walters
Research Scientist
Georgia Tech Research Institute
404-407-8904
seth.walters@gtri.gatech.edu

Current Contact as of Aug. 2020

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