Cyber-Intrusion Auto-Response Policy and Management System (CAPMS)

A managed security system that integrates advanced cybersecurity algorithms with energy delivery systems to respond autonomously to cyber intrusions while sustaining critical energy delivery functions

Background

Cyber attacks are becoming more sophisticated every day. Electric utilities are faced with the challenge of detecting, analyzing, and responding to cyber incidents to protect public safety and preserve the integrity of grid assets. Cybersecurity solutions must account for legacy control systems, stand-alone operational systems, and increasingly distributed control systems.

These more complex systems have reached a level of sophistication such that automatic control system responses to cyber attack have an increasingly important role in defending against a coordinated attack. New, integrated approaches to cybersecurity are needed to combat these advanced threats.

Barriers

- Correlating seemingly unrelated events in both cyber and utility spaces is hampered by traditionally siloed systems.
- Utilities own and operate a mix of legacy and modern control systems, each controlled by isolated management systems.
- Signs of an intrusion can be hidden in massive volumes of data.
- Simple intrusion detection processing provides no guidance as to the goals of an attacker, nor does it define what should be done in the event of an attack.

Project Description

Security policies must be implemented as a part of grid control systems as well as the servers and networks that are part of traditional information technology (IT) security management. The CAPMS project is unifying both worlds and applying advanced cybersecurity incident behavioral models to analyze, predict, offer advice and, where appropriate, act autonomously to sustain energy delivery systems during a cybersecurity incident.

The CAPMS project is building on ViaSat's Trusted Network Platform (TNP) technology, a managed security service that protects utility network access and detects intrusions using a hybrid architecture for both centralized and distributed networks. Using this service, local control system devices are able to continually assess the trustworthiness of themselves and their peers, providing a global view of the network.

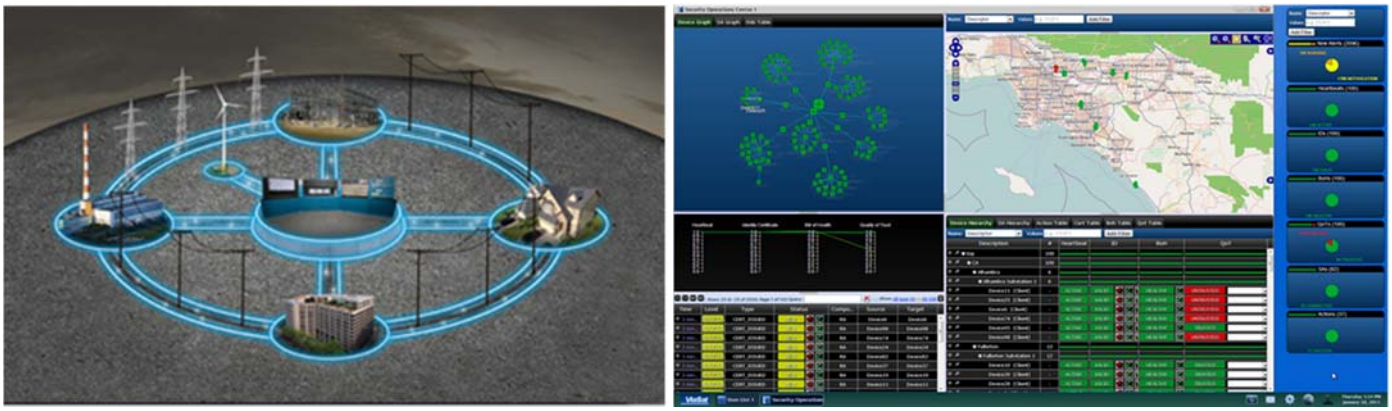
The distributed nature and design of the service provides high system availability in adverse conditions (i.e., cyber attacks). The CAPMS project takes a holistic defense-in-depth approach, providing several layers of detection of known and potentially new forms of cyber attack. The service uses behavioral and causal analysis algorithms to detect threats and then determines the most appropriate response method.

Benefits

- Unifies grid control systems with IT and operational system security policies
- Provides advanced policy-based threat modeling algorithms that enable proactive control system responses that can block intruders in the early stages of attack
- Provides global situational awareness and operator views of cybersecurity posture to help operators understand a cyber attack's effects on the energy delivery system
- Allows for automatic control system responses to attacks to help mitigate outages and damage to the grid
- Accommodates diverse energy delivery system architectures, operational policies, and legacy or modern devices of any vendor
- Enables ready sharing of threat scenario models among security experts, promoting best-of-breed techniques to defending against cyber attacks

Partners

- **ViaSat**
- Duke Energy
- Southern California Edison



Real-time monitoring and analysis of utility networks detect and respond to cyber attacks

Technical Objectives

The CAPMS project is developing techniques for detecting and responding to simulated cyber attacks at two utility partner test facilities. The demonstrations highlight areas that are unique to each partner but common enough across multiple electric utility company architectures. The project will use an agile development process and will be performed in the following phases.

Phase 1: Research and Analysis

- Phase 1 involves research and analysis of open-source and industry-wide techniques for detecting/ reporting events, as well as processing and responding based on policy.

Phase 2: Design, Development, Integration, and Testing

- In Phase 2, the project defines and implements a service-oriented architecture (SOA) that includes policy-based processing and expands cyber event processing. Development is iterative to clarify requirements and experiment with different threat scenarios, cyber events, and algorithms to determine best control system responses.
- Integration and testing verifies that the system performs the most basic functions and can be taken to the partner facilities for further development. The testing performed at ViaSat uses simulated interfaces that allow for corner cases and performance testing. Early code drops will be provided to the utility partner test laboratories, but final demonstration preparation with live equipment occurs in the last phase.

Phase 3: Demonstrations at Partner Utilities

- Final demonstration and experimentation for each threat scenario is conducted at utility partner test laboratories. Different techniques are used based on findings and what can be simulated in te test labs for each threat scenario/demonstration.

End Results

Project results will include the following:

- Implementations of behavioral and causal analysis algorithms to demonstrate the potential uses of grid cybersecurity posture as a safety input to operational control systems
- New techniques for visualizing the extent and root causes behind combined cyber and operational attacks
- Autonomous and near-real-time defensive and remediation responses
- Novel approaches for involving the CAPMS system as a full partner in grid operations workflow
- Security policy definition and simulation tools that allow for sharing and dissemination of emerging threat models
- Improvements to ViaSat's Trusted Network Platform for managing security policies that are defined in tandem with new grid control systems
- Support for both centralized and distributed management strategies with the ability to monitor/protect a variety of power grid networks

Content last updated: May 2015

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

Steve Lusk
Program Manager
ViaSat Inc.
508-229-6524
steve.lusk@viasat.com

Current Contact as of Aug. 2020

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