U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Cybersecurity Intrusion Detection and Security Monitoring for Field Area Networks

Continuous security validation, intrusion detection, and situational awareness for advanced metering infrastructure and distribution automation

Background

Advanced metering infrastructure (AMI) and distribution automation (DA) field area networks (FANs) are among the largest, possibly most complex, networks operated by utilities in the United States. Exploitable vulnerabilities in AMI and DA systems may arise from weaknesses in network functions, software, wireless communications, device hardware and firmware, and system configuration management.

Active security monitoring systems and tools are needed to continuously validate defensive and privacy controls, monitor for abnormal activity, and detect early signs of intrusion. Such systems are essential to maintain the integrity of SCADA and customer usage data, to avoid loss of control or power disruptions and to mitigate the financial and business risks of prematurely replacing a compromised system.

Barriers

- The impracticality of physically protecting and inspecting every field device in a distributed, service-territory-wide, multi-channel wireless network.
- Proprietary wireless technologies and protocols.
- Lack of commercial tools to provide visibility into wireless FAN communications.

Project Description

This project conducts research to accelerate development of a utility monitoring system to detect anomalous behavior, improve situational awareness, and provide visibility into wireless AMI and DA FANs. Working with utility partner Sacramento Municipal Utility District (SMUD), the project will demonstrate an enhanced FAN monitoring and intrusion detection system (IDS), a new real-time FAN health dashboard, and network analytics capabilities in an operational AMI and DA environment with 625,000 meters.

Developing the IDS involves studying the behavior of the wireless networks, nodes, and traffic patterns. A formal investigation of security weaknesses will sample over-the-air traffic in a production system. The application of deep packet inspection and behavioral and statistical methods will provide continuous validation of security and privacy controls. The effort will define and evaluate time series indicators for use in the real-time dashboard, and the database-driven network analytics will support engineering, troubleshooting, and security forensic use cases. Additionally, the research team will assess the efficacy of mobile probes mounted on utility vehicles for monitoring coverage of a service territory.

Benefits

- Protects integrity of delivering meter data to the billing system (meter-to-cash process)
- Protects the integrity of DA SCADA communications
- Delivers early warning of anomalous and malicious activity
- Provides multi-level, real-time view of FAN health and continuous validation of FAN security controls & configuration compliance
- Ensures safeguards to customer privacy
- Provides situational awareness based on ground-truth data from independent field probes
- Mitigates AMI and DA supply chain cyber threats
- Increases information and operational technology (IT/OT) effectiveness and efficiency
- Provides tools for AMI and DA operations, engineering, and security
- Overlays onto existing infrastructure unobtrusively

Partners

- **Applied Communication Sciences (ACS)**
- Sacramento Municipal Utility District (SMUD)

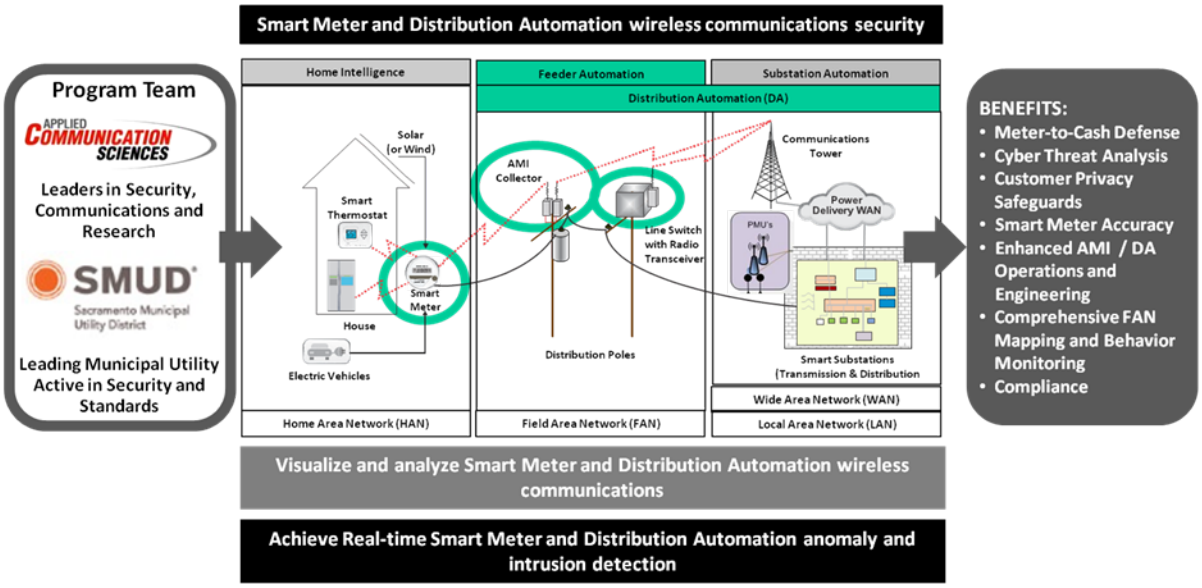

Figure 1: IDS for AMI and DA field area networks

Technical Objectives

This project consists of research, demonstration, and commercialization efforts that will result in the economical near-term realization of tools to monitor and defend AMI and DA FAN integrity. Specific core efforts are described below.

Phase 1: Research and Proof of Principle

- Collect and analyze production wireless AMI and DA traffic
- Define and implement new security analytics and heuristics
- Model FAN traffic to define an orthogonal set of security and performance indicators
- Define network operating baselines
- Advance monitoring software and visualization capabilities to deliver enhanced FAN situational awareness
- Assess efficacy of mobile probes

Phase 2: Demonstration and Commercialization

- Demonstrate new analytics, monitoring, and analysis tools in SMUD's daily operational environment
- Measure performance of analytics, investigate events, and take remedial actions
- Perform application and systems refinements
- Allow prospective utilities to test drive capabilities via interactive demonstrations
- Allow prospective utilities to learn the system's practical value from a utility that has deployed the system
- Make the capabilities available through ACS SecureSmart™ Managed Security Services

End Results

Project results will include the following:

- A commercially available advanced FAN IDS and continuous security monitoring system for AMI and DA networks
- One of the industry's first multi-level, real-time AMI and DA FAN situational awareness dashboards
- An integrated monitoring system that unobtrusively and independently provides packet-level visibility into FAN operation
- Database-driven network analytics that support security, engineering, and operations use cases

September 2014

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) 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 energy disruptions due to cyber attacks.

Contact Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Stanley Pietrowicz
Principal Investigator
Applied Communication Sciences
732-740-1021
spietrowicz@appcomsci.com

For More Information:

- http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity
- www.controlsystemsroadmap.net