

Stan Pietrowicz

**Applied
Communication
Sciences**



CyberSecurity Intrusion Detection and Monitoring for Field Area Networks

Cybersecurity for Energy Delivery Systems Peer Review
August 5-6, 2014

CyberSecurity Intrusion Detection and Monitoring for Field Area Networks

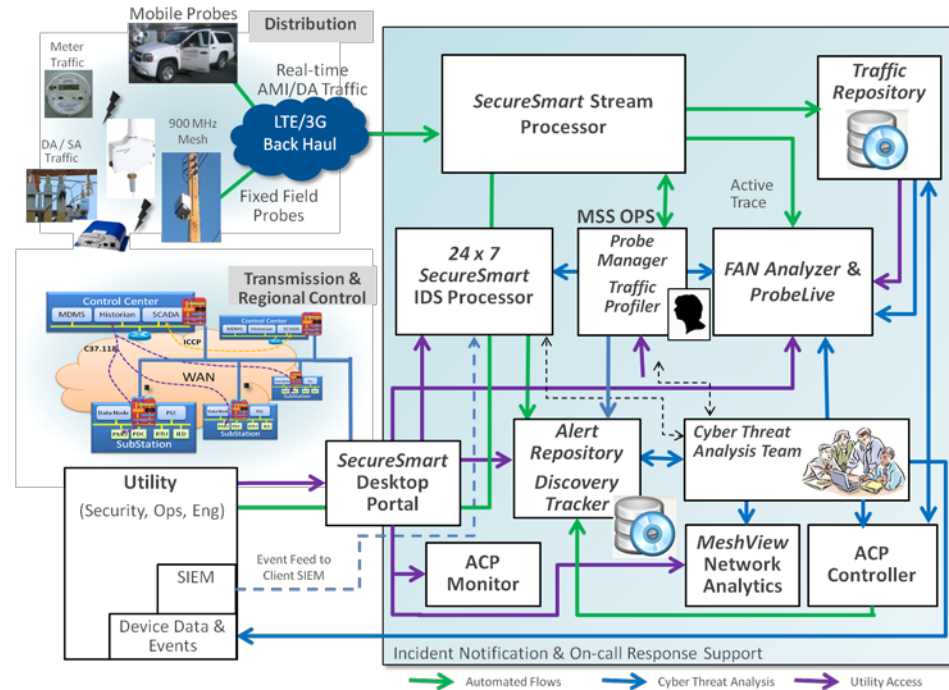
- **Objective**

- Improve Situational Awareness with a Continuous Monitoring and Intrusion Detection Solution

- AMI Wireless FANs
- DA Wireless FANs

- **Schedule**

- Phase I: 1/2014 – 12/2014
- Phase II: 1/2015 – 6/2015
- Wireless Traffic Research with Software Development (2014)
- Demonstration & Transition to *SecureSmart*™ MSS (2015)



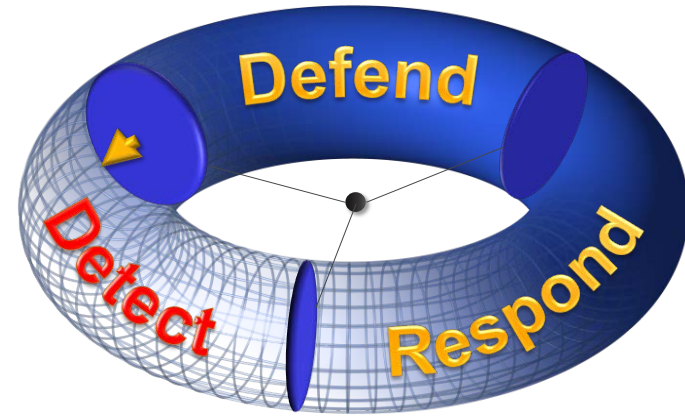
- **Total Value of Award:** \$1,280,766.00
- **% Funds expended (6/27/14):** 35.4%
- **Performer:** Applied Communication Sciences (ACS)
- **Partners:** Sacramento Municipal Utility District (SMUD)

Advancing the Start of the Art (S0A)

- **Accelerate research** on a sensor-based system to independently monitor wireless AMI and DA Field Area Networks (FANs)
 - Develop enhanced set of operational **capabilities to detect anomalous behavior** and improve asset owner **situational awareness and visibility** into FANs
 - **Integrate** enhanced intrusion detection analytics, monitoring and analysis tools into ACS's *SecureSmart*™ Managed Security Service
 - **Demonstrate** solution value and security benefits in our utility partner's (SMUD) operational environment
 - Advance first-of-its-kind technology to a **validated, full-scale monitoring solution** for the energy sector
-

Moving Beyond Defensive Controls with Continuous Detection and Monitoring

- Detect anomalous behavior and early signs of attack
- Detect exploitation of known weaknesses discovered in security assessments
- Provide continuous security validation and configuration compliance
- Ensure safeguards to customer privacy
- Provide multi-level, real-time view of FAN health and security
- Provide independent “ground truth” to help mitigate supply chain cyber threats
- Overlay onto AMI/DA Infrastructure at all stages of deployment
- Unobtrusive to AMI/DA operation



New Visibility and Situational Awareness into Field Area Networks

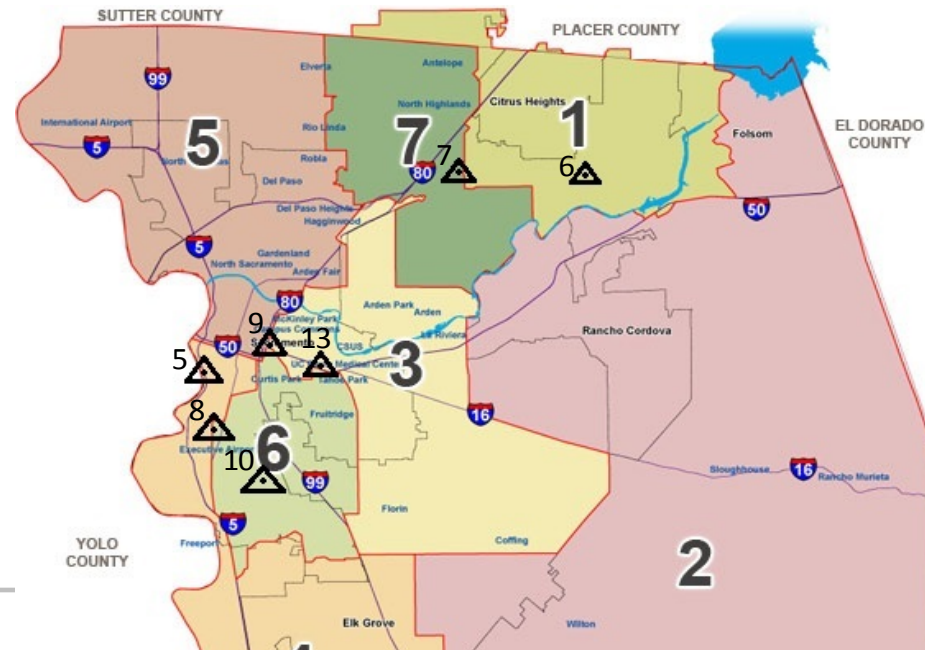
Challenges to Success

- **How do FAN security weaknesses manifest themselves in field communications?**
 - Conduct formal security analysis of AMI & DA communications
 - **What is normal FAN behavior and how do you measure it?**
 - Study production FAN traffic and develop a set of orthogonal indicators for real-time health monitoring
 - **How do we cover large service areas?**
 - Evaluate efficacy of mobile probes installed in fleet vehicles
 - **How do we abstract packet “bits and bytes” into situational awareness?**
 - Develop real-time dashboard and database-driven analytics to visualize current state, communication flows and network topology
-

Rich Production Traffic Environment at SMUD



- 625,000+ Meters
- 900 Square Miles with Diverse Population Density
- AMI and DA Wireless FANs in Operation
- 10 Field Probes Deployed
 - 7 Fixed Probes
 - 3 GPS-enable Mobile
 - 6 Sampling
 - 1 Full Band
- 24 x7 Traffic Streams
- 1 Year Traffic History
- Turn-up of New Smart Meter Applications
- Supportive Security, Meter Operations & DA Teams



Progress to Date

Wireless IDS Research

- Create a formal threat model to holistically identify targets and attack vectors
 - Analyze Production AMI and DA traffic for real-world weaknesses
 - Investigate, develop and test detection methods for top ranking threats
 - Deep Packet Inspection
 - Stateful Behavior Models
 - Statistical
 - White Lists
 - Consider differences among AMI systems and 802.15.4g standard
 - Task Report - 7/2014
 - **Example Discoveries**
 - Improper Traffic Flows
 - AMI and DA Production Systems
 - Bordering Utilities
 - Production and Test Environments
 - Unauthorized Protocols and Traffic Exchange
 - Insecure SCADA Traffic
 - Discovery of “Rogue” Networks
 - System Configuration Issues
 - FAN Security Issues with New AMI Application
 - Reappearance of Decommissioned Field Equipment
 - Gratuitous and Malformed Packets
 - Unknown Devices
 - Unexpected System Changes
-

Progress to Date

TrafficProfiler Dashboard Indicators

- A Multi-level, Real-Time Monitoring Strategy
 - System Wide
 - Service Area
 - Per Probe
 - Individual Device or Indicator
- Evaluated 27 of 40+ Potential Indicators using Filtered Fields, Field Logic and Analysis Operators
 - Count
 - Unique
 - Percent
 - Ratio
 - Latency
- Determined Optimal Sampling Intervals and Statistical Baselines for Alarm Generation
- **Prototype Indicators have already Detected a Variety of System Anomalies**
 - Router Failures
 - Mesh Routing Problems and Disturbances
 - Partial Backhaul Failure



Real-Time Warning of FAN Problems vs Today's 4-hr Meter Read "Health Indicator"

Progress to Date

MeshView NetAnalytics & Visualization

- **Sample Use Cases**

- Conduct a Security Forensics Investigation
- Troubleshoot a FAN Problem
- Investigate Node Connectivity
- Analyze a System or Routing Failure
- Investigate Meter Read Failures
- Improve, Re-engineer or Extend FAN
- Identify Overused Meters for Messages Relaying
- Monitor Traffic Mix for Service Integrity

- **Example Features**

- View Logical & Geospatial Routing Topology
- View Mesh Connectivity
- Time lapse Playbacks of Mesh Behavior
- Node Behavior Analysis
- “Top Talker”, Traffic Composition, and Other Statistics



Welcome to
MeshView™

Username:
stan

Password:

Sign in

© 2014, Applied Communication Sciences
A business of the ST.



Collaboration/Technology Transfer

Web Video

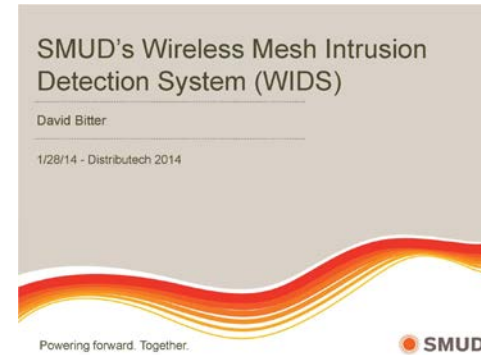


Press Releases



U.S. REP. LEONARD LANCE (NJ-7) VISITS ACS
NJ HQS TO REVIEW PROGRESS ON THE FIRM'S
SECURESMART MONITORING SOLUTION WITH
ACS PRESIDENT BRENT GREENE.

Conference Talks



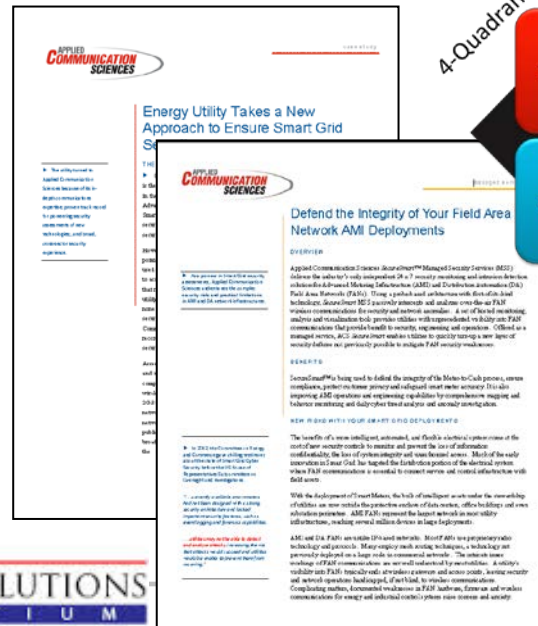
Conference Demos



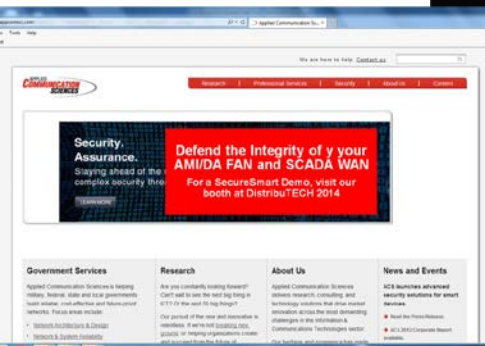
Direct Mail



Collateral



ACS Website



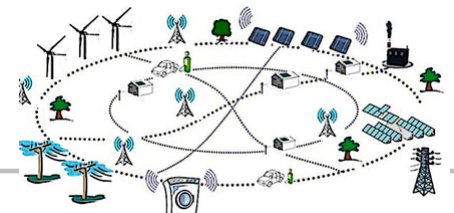
Technology Competitions



Technology Intro via Security Assessments



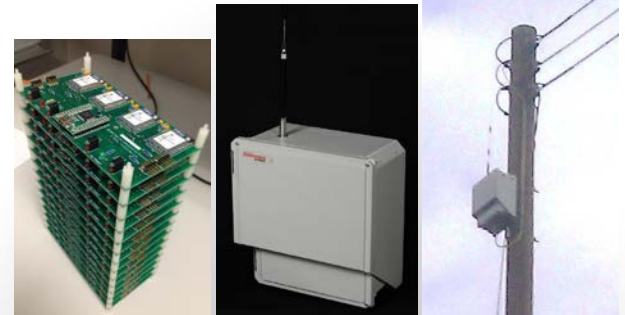
Smart Grid Pilots



Packaging The Technology into a Utility Solution

ACS *SecureSmart*™ Managed Security Service

- **Complete Continuous Monitoring as a Service (CMaaS) for Utilities that bundles:**
 - ACS First-of-its kind Sensor Technology
 - MSS Monitoring Infrastructure
 - Analysis and Visualization Applications
 - Network and Cyber Monitoring Services
- **24x7 Anomaly and Intrusion Detection**
 - AMI, DA, ICCP, DNP3, and PMU networks
 - Experience-driven and model-based IDS analytics
- **Daily Cyber Threat Analysis and Exchange**
 - Experts review bulk alerts and perform trace analysis, investigate and track suspicious activity
 - Threat Information Exchange
 - Incident notification, weekly calls, and monthly reports
- **Real-Time Network Health Monitoring**
 - Integrates with SIEM and NOCs



Next Steps for this Project

- **Complete Phase I Research**

- Continue developing intrusion detection deep packet inspection rules, stateful models, and statistical approaches
- Continue developing traffic indicators and formulating behavioral baselines
- Evaluate efficacy of Mobile Probes and upstream impacts

- **Phase II Demonstration**

- Prepare and deploy new capabilities at SMUD
 - Integrate into Operations Environment
 - Refine capabilities to support Use Cases
 - Complete Commercialization Plan
-