TCIPG: Trustworthy Cyber Infrastructure for the Power Grid

Bill Sanders
(on behalf of entire TCIPG team)

DHS Cyber Security Division R&D Showcase
December 16, 2014
The Challenge: Providing Trustworthy Grid Operation in Possibly Hostile Environments

• **Trustworthy**
  – A system which does what it is supposed to do, and nothing else
  – Availability, Security, Safety, …

• **Hostile Environment**
  – Accidental Failures
  – Design Flaws
  – Malicious Attacks

• **Cyber Physical**
  – Must make the whole system trustworthy, including both physical & cyber components, and their interaction.
Industry Roadmap – A Framework for Public-Private Collaboration

• Published in January 2006/updated 2011
• Energy Sector’s synthesis of critical control system security challenges, R&D needs, and implementation milestones
• Provides strategic framework to
  – align activities to sector needs
  – coordinate public and private programs
  – stimulate investments in control systems security

Roadmap Vision
By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
Trustworthy Cyber Infrastructure for Power (TCIPG) Summary

**Objectives**
- Identify and address critical security and resiliency needs at the cyber-physical junction in the evolving power grid
- Engage Industry (utility, control system vendors, technology providers)
- Research Excellence
- Education

**Technical Approach**
- Identify and take on important & hard problems
- Unique balance of long view of grid cyber security, with emphasis on practical solutions
- Work to get solutions adopted

**Schedule:** Sept 30, 2009 – Aug. 30, 2015

**Funded:** jointly by DHS S&T, DOE Office of Electricity, and the participating Universities

**Performers:** University of Illinois at Urbana-Champaign, Dartmouth College, Cornell University, University of California Davis, Washington State University

**Partners:** 9-Member External Advisory Board (EAB) from utilities and industry, as well as large Industry Interaction Board
Vision: Create technologies which improve the design of a resilient and trustworthy cyber infrastructure for today’s and tomorrow’s power grid, so that it operates through attacks

Research focus: Resilient and Secure Smart Grid Systems

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications and architectures
- Quantifying security and resilience
TCIPG Technical Clusters and Threads

Trustworthy Technologies for Wide Area Monitoring and Control
- Communication and Data Delivery (5 activities)
- Applications (2 activities)
- Component Technologies (2 activities)

Trustworthy Technologies for Local Area Management, Monitoring, and Control
- Active Demand Management (3 activities)
- Distribution Networks (1 activity)

Responding To and Managing Cyber Events
- Intrusion Detection and Response Techniques (6 activities)

Trust Assessment
- Model-based Assessment (3 activities)
- Experiment-based Assessment (5 activities)
## TCIPG Activities (1)
Trustworthy Technologies for Wide Area Monitoring and Control

### Current Efforts
- Cryptographic scalability in the smart grid
- Functional security enhancements for existing SCADA Systems
- GridStat middleware communication framework: Application requirements
- GridStat middleware communication framework: Management security and trust
- GridStat middleware communication framework: Systematic adaptation
- PMU-enhanced power system operations
- Real-time streaming data processing engine for embedded systems
- State-aware decentralized database system for smart grid
- Trustworthy Time Synchronous Measurement Systems

### Past Efforts
- CONES: Converged networks for SCADA
- Cooperative Congestion Control in Power Grid Communication Networks
- Decentralized Sensor Networking Models and Primitives for Smart Grid
- Lossless compression of synchrophasor measurement unit archives
- PMU Integration into Power Flow Software
- Secure Wide-Area Data and Communication Networks for PMU-based Power System Applications
Selected 2014 Accomplishment: Addressing Time Synchronization Challenges

- Continued study of potential impact of GPS spoofing on wide area measurement systems, and mitigation approaches
- Developed Position-Information-Aided Vector Tracking (PIA) – Award-winning paper at ION-GNSS 2014
- Developing hardware prototype to evaluate vulnerability and mitigation
OBJECTIVES

• Understand the timing and synchronization needs in power system applications.

• Investigate possible detection and mitigation schemes to harden PMUs against spoofing, jamming, and receiver errors.

• Develop a hardware-based testbed capable of investigating the resiliency of various PMUs to known GPS spoofing attacks.

• Develop a trustworthy GNSS-based timing source that is more spoofing-resilient than current GPS-based clocks.

RECENT ACHIEVEMENTS

• Created eight countermeasures to harden GPS-based timing for PMUs

• Theoretical analysis and experiments on [C2].

• Submitted an abstract to ION GNSS+ 2014 conference
Current Efforts

• Development of the information layer for the V2G framework implementation
• Password changing protocol
• Smart-grid-enabled distributed voltage support
• Trustworthy framework for mobile smart meters

Past Efforts

• Agent Technologies for Active Control Applications in the Power Grid
• Coordinated island operation and resynchronization
• Non-Intrusive Load Shed Verification
• SCADA Secure Wireless Networks
Selected 2014 Accomplishment: Trustworthy Framework for Mobile Smart Meters

**OBJECTIVES**

- Mobile Smart Meters as on-board units of electric vehicle
- Secure data transmission between mobile smart meter and charging station/charging pad
- Fast authentication for dynamic wireless charging of EV

**RECENT ACHIEVEMENTS**

- We have developed a key pre-distribution based approach for EV-charging pad authentication that supports roaming service and preserves EV’s location privacy
- Paper submitted to SmartGridComm’14
- As future work we will implement the protocol on portable computing device such as RaspberryPi and evaluate its performance in practice
TCIPG Activities (3)
Responding to and Managing Cyber Events

Current Efforts

- A game-theoretic response and recovery engine (RRE)
- Assessment and forensics for large-scale smart grid networks
- Detection/Interdiction of Malware Carried by Application-Layer AMI Protocols
- Intrusion Detection for Smart Grid Components by Leveraging of Real-Time Properties
- Specification-based IDS for smart meters
- Specification-based IDS for the DNP3 protocol

Past Efforts

- Coordinating Black Start Operations Using Synchrophasors
- Hardware-based IDS for AMI devices
- Usable management tools for the smarter grid’s data avalanche
OBJECTIVES

• Design an efficient monitoring architecture to detect and potentially prevent intrusions targeting or originating from an Advanced Metering Infrastructure (AMI)

• Implement a prototype of this monitoring solution and validate its accuracy and applicability

RECENT ACHIEVEMENTS

• Continued partnership with FirstEnergy to test prototype in a 36,000-meter AMI
  • Developed and tested a Web interface to enable operators to customize intrusion detection signatures

• Continued collaboration with EPRI to implement failure-driven security policy for AMI

• Collaboration with Fujitsu, UT Dallas, Honeywell, and Sandia to address the challenge of encrypted traffic
TCIPG Activities (4)

Trust Assessment

Current Efforts

- 802.15.4/ZigBee Security Tools
- Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components
- Security and Robustness Evaluation and Enhancement of Power System Applications
- Synchrophasor Data Quality
- Tamper-Event Detection Using Distributed SCADA Hardware
- Testbed-Driven Assessment: Experimental Validation of System Security and Reliability
- Trustworthiness Enhancement Tools for SCADA Software and Platforms
- Understanding and Mitigating the Impacts of GPS/GNSS Vulnerabilities

Past Efforts

- Automatic Verification of Network Access Control Policy Implementations
- Fuzz-testing of Proprietary SCADA/Control Network Protocols
- Modeling Methodologies for Power Grid Control System Evaluation
- Smart Grid: Economics and Reliability
- Tools for Assessment and Self-Assessment of 802.15.4/ZigBee Networks
- Vulnerability Assessment Tool Using Model Checking
Selected 2014 Accomplishment: 802.15.4/ZigBee Security Tools

OBJECTIVES

- Production of a cheap, easy-to-configure 802.15.4 radio peripheral
- Full support for popular 802.15.4 platforms accessible to SCADA asset owners
- Kismet-like GUI familiar to users of “wardriving” Wi-Fi auditing tools

RECENT ACHIEVEMENTS

- APImote v4 open source design donated by River Loop produced, released at Troopers.de industry conference & distributed to security industry researchers.
- Fingerprinting results & techniques for 802.15.4 digital radios confirmed, submitted to ACM WiSec & published in Dartmouth TR2014-746
- WIDS/WIPS evasion techniques utilizing PHY-level frame crafting confirmed, described in updated Dartmouth TR2014-749
Cross-Cutting Effort: Education and Engagement

**K-12 Education**
- Interactive lessons, hands-on activities, and curriculum materials
- Partnerships with teachers and schools
- Dissemination activities
- Connections with national curriculum endeavors

**Outreach and Workforce Development**
- Create interest in STEM related careers
- TCIPG summer schools
- Research opportunities for undergraduates

**Consumer Education and Public Information**
- Energy information for an informed public
- Consumer acceptance of smart grid technologies and policies
Selected 2014 Accomplishment: TCIPG
Education, Outreach, and Training

• Education of professionals versed in cyber and power is the core mission
  – Degree programs
  – Internships
  – Continuing Education
  – TCIPG Reading Group
• K-12 education and outreach
  – Power and Energy applets continue to evolve, and are integrated into curriculum projects nationwide
  – TCIPG Minecraft World
  – Encouraging interest in STEM education and careers
  – Teachers, parents learn too!
• Assisting community colleges in smart grid curriculum development under IGEN Consortium
Power and Energy applets
64,121 pageviews in the past year
1000 CD’s distributed

Tesla Town for the iPad
19,000 iTunes downloads
Available in Google play store

TCIPG Minecraft World
Available for download

Hands-on kits
Lesson plans
Posters
Trading cards
OBJECTIVES

• Span transmission, distribution & metering, distributed generation, and home automation and control, providing true end-to-end capabilities
• Provide foundational support for TCIPG projects
• Analyze research through varying fidelities and scales
• Serve as a national resource for experimental work in research and analysis of trustworthy power grid systems

RECENT ACHIEVEMENTS

• Brought in additional backup and disaster recovery options for the lab.
• Started new training/education based activity leveraging testbed prior work.
• Positioning testbed activities and resources for transition to practice.
Cross-Cutting Effort: Industry Interaction and Technology Transition

Activity Involvement
- Industry day posters and interest "post-its" follow-up
- PMU data NDAs and processes

Visits and Collaboration
- Company visits by students/faculty
- Guest industry lectures and seminars
- Student internships

Tech Transfer
- Software testing
- Formal adoption
Example Technology Transfer: Network Perception, Inc.

- Based on NetAPT technology developed under TCIPG
  - Static analysis of firewall rule sets
  - Tuned to utility systems, where identifying routable paths to critical cyber assets is an increasingly important problem
- Pilot deployment at major IOUs as technology matured
  - Demonstrated usefulness in NERC CIPS audits
- Used in security assessment of rural electric cooperative utility networks
- Transition of NetAPT from an academic project to a commercial product has been supported at UIUC by a one-year grant from DHS S&T

Network Perception is now a technology startup
Questions?

- www.tcipg.org
- Bill Sanders
  whs@illinois.edu
- Request to be on our mailing list
- Attend Monthly Public Webinars
- Attend our TCIPG Summer School June 2015