Smart Grid Security Efforts @ Illinois

**TCIPG: Trustworthy Cyber Infrastructure for the Power Grid**
- Drive the design of a resilient cyber infrastructure electric power which operates through attacks
- $18.8 M over five year, started Oct. 1, 2010
- Univ. Illinois, Cornell, Dartmouth, U.C. Davis, Wash. State Univ.
- Funded by DOE and DHS
- Follow-on to $7.5 M NSF CyberTrust Center

Illinois's Singapore Adv. Digital Sciences Center Smart Grid Subprogram
~$15M effort / 5 years
Projects in Microgrids, DERs, and HANs

**ETRI**
Korean National Smart Grid TestBed on Jeju Island.
Project concerning testbed and cyber security research (DDSOS)

**CACAIS Testbed**
Products tested & validated in CACAIS testbed: $1.2M FY10 funding from ONR

**Illinois Center for a Smarter Electric Grid**
Validation & Compliance Services
- $2.5M, YR1 DCEO funding
- Test bed & lab equipped with HW/SW to perform validation of Smart Grid systems
- Critical Infrastructure Protection (CIP): pre-audit check for compliance to NERC standards
- Prepare for NERC reliability compliance audits

4 New DOE Office of Electricity Security Projects with:

- EPRI
- Entergy
- DTE Energy
- Telcordia
- Pacific Northwest National Laboratory
- pjm
- Honeywell
- INL

tcipg.org
Vision: Drive the design of an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power, which 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
- Quantifying security and resilience
TCIPG Statistics

• Build upon $7.5M NSF TCIP CyberTrust Center 2005-2010
• $18.8M over 5 years, starting Oct 1, 2009
• Funded by Department of Energy, Office of Electricity and Department of Homeland Security
• 5 Universities
  – University of Illinois at Urbana-Champaign (20 Senior Investigators, 24 Graduate students)
  – Washington State University (5 Senior Investigators, 3 Graduate students)
  – University of California at Davis (2 Senior Investigators, 1 Graduate student)
  – Dartmouth College (2 Senior Investigators, 1 Graduate student)
  – Cornell University (1 Senior Investigator)
TCIPG Industry Interaction Board
TCIPG Clusters and Cross-Cutting Efforts

• **Clusters** integrate work in specific technical areas over the life of the project:
  – Trustworthy cyber infrastructure and technologies for wide-area monitoring and control
  – Trustworthy cyber infrastructure and technologies for active demand management
  – Responding to and managing cyber events
  – Risk and security assessment

• **Cross-Cutting Efforts** address issues that cross technical clusters:
  – Education and workforce development
  – Testbed and evaluation methodologies
  – Industry interactions and technology transition
TCIPG Technical Clusters and Threads

Clusters

- Trustworthy cyber infrastructure and technologies for wide-area monitoring and control
- Trustworthy cyber infrastructure and technologies for active demand management
- Responding to and managing cyber events
- Risk and security assessment

Threads

- Architectures design and tools for wide area communication networks
- Trust in PMU Networks
- Advanced monitoring and control for distribution networks
- Design of semi-automated intrusion detection and response techniques
- Model-based Assessment Tools
- Experiment-based Assessment Tools

tcipg.org
## Breadth of TCIPG Research Activities

### Cluster: Trustworthy cyber infrastructure and technologies for wide-area monitoring and control

- Secure Wide-Area Data and Communication Networks for PMU-based Power System Applications
- Real-time, Secure, and Converged Power Grid Cyber Networks
- Cooperative Congestion Avoidance in Power Grid Networks
- Direct Application of PMU Values into Power Flow Software
- Lossless Compression of Synchronization Measurement Data Archives
- Decentralized Sensor Networking Models and Primitives for the Smart Grid

### Cluster: Trustworthy cyber infrastructure and technologies for active demand management

- Smart-Grid-Enabled Distributed Voltage Support
- Specification-based IDS for Smart Meters
- Development of the Information Layer for the V2G Framework Implementation
- Non-Intrusive Load Monitoring
- Agent Technologies for Active Control Applications in the Power Grid
- Development of the Information Layer for the V2G Framework Implementation
Breadth of TCIPG Research Activities

**Cluster: Responding to and managing cyber events**

- RRE: A Game-Theoretic Response and Recovery Engine
- Assessment and Forensics for Large-Scale Smart Grid Networks
- Coordinating Black Start Operations Using Synchrophasors

**Cluster: Risk and security assessment**

- Trustworthiness Enhancement Tools for SCADA Software and Platforms
- Tools for Assessment and Self-assessment of ZigBee Networks
- Analysis of Impacts of Smart Grid Resources on Economics and Reliability of Electricity Supply
- Vulnerability Assessment Tool Using Model Checking
- Test-bed-Driven Assessment: Experimental Validation of System Security and Reliability
- Modeling Methodologies for Power Grid Control System Evaluation
- Automatic Verification of Network Access Control Policy Implementations
- Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components
- Towards Robust Power System Applications
TCIPG Testbed Effort

• TCIPG testbed aims to:
  – Provide experimental support and integration of TCIPG projects
  – Serve as national resource for experimental work in analysis of power grid system resiliency

• Testbed capabilities:
  – Equipment
    • Commercial Hardware and Software
    • Transmission, Distribution, Generation, and Home automation/control
  – Scalable simulation and emulation
    • Simulation of power generation/transmission, simulation/emulation of computer and communication systems
  – Coupling
    • Integration of simulation of electrical state, real equipment and cyber simulation/emulation of other grid components
TCIPG Summer School June 13-17, 2011

Tom Malec of the U.S. Department of Energy addresses the Summer School attendees.
TCIPG Webcasts: Technologies for a Resilient Power Grid

• Present topics on research, development, and design of a secure and resilient power grid
• Webcasts are open to the public and attract a broad audience from industry, academia, and government
• Webcast first Friday of each month at 1:00 p.m. CT
• Speakers so far:
  – Sept.: Manimaran Govindarasu, Iowa State
  – Oct.: Mathew Luallen, Sph3r3
  – Nov.: Alan Greenberg, Boeing, & Mark Enstrom, Neustar
  – Dec.: Robert Former, ITRON
For More Information

Bill Sanders

Director, DOE/DHS TCIPG Center (www.tcipg.org)
Director, Coordinated Science Laboratory
University of Illinois

217-333-2510

whs@illinois.edu