Cyber-Physical Systems Security for Smart Grid
Manimaran Govindarasu, Aditya Ashok, Siddharth Sridhar, Adam Hahn, Iowa State University
Peter Sauer, University of Illinois, Urbana-Champaign

Problem definition
• Smart grid increasingly dependent on high-speed, automatic, monitoring and control technologies
• Adversaries can maliciously enter through the cyber infrastructure to inflict damage on the planning, operations, and market functions of the power grid
• Cyber attacks on critical infrastructures are increasing in number and sophistication (e.g., Stuxnet).

Asymmetric Threat: dynamic, evolving, speed, scale
• Several standards and roadmaps have been put out for ensuring cyber security compliance in Smart Grid
  - NERC CIP
  - NISTIR 7628
  - DoE 2011 Roadmap Energy Systems Cybersecurity

• Comprehensive Challenges: R&D, Deployment, Policy

Cyber-Physical System (CPS) Security
CPS Security = Information Security + Infrastructure Security + Application Security

Smart Grid Cyber Security requirements
Confidentiality (C), Integrity (I), Availability (A), Authentication (AT), Non-repudiation (N)

Risk Modeling and Mitigation Framework
Risk = Threat \times Vulnerability \times Impacts
- Risk Assessment & Risk Mitigation (GAO CIP Report, 2010)
- Security Investment Analysis

- Coordinated Attack-Defense
  - Risk modeling of coordinated attacks
  - Beyond N-1 criteria: Scope and planning
  - Robust cyber-physical counter measures

- Advanced Metering Infrastructure Security
  - Remote attestation of AMI components
  - Model-based anomaly detection methods
  - Security vs. Privacy tradeoffs

- Trust Management and Attack Attribution
  - Dynamic trust: Models, protocols, and validation
  - Insider threat: Models, metrics, mitigation algorithm
  - Attack attribution: Scalable architectures, algorithm

Data Sets and Validation
- Network models: SCADA, NASPInet, WAM, AMI, CIM
- Realistic attack models and attack data traces
- Realistic CPS Security Testbeds; Attack-Defense studies