

Cyber-Physical Systems Security for Smart Grid

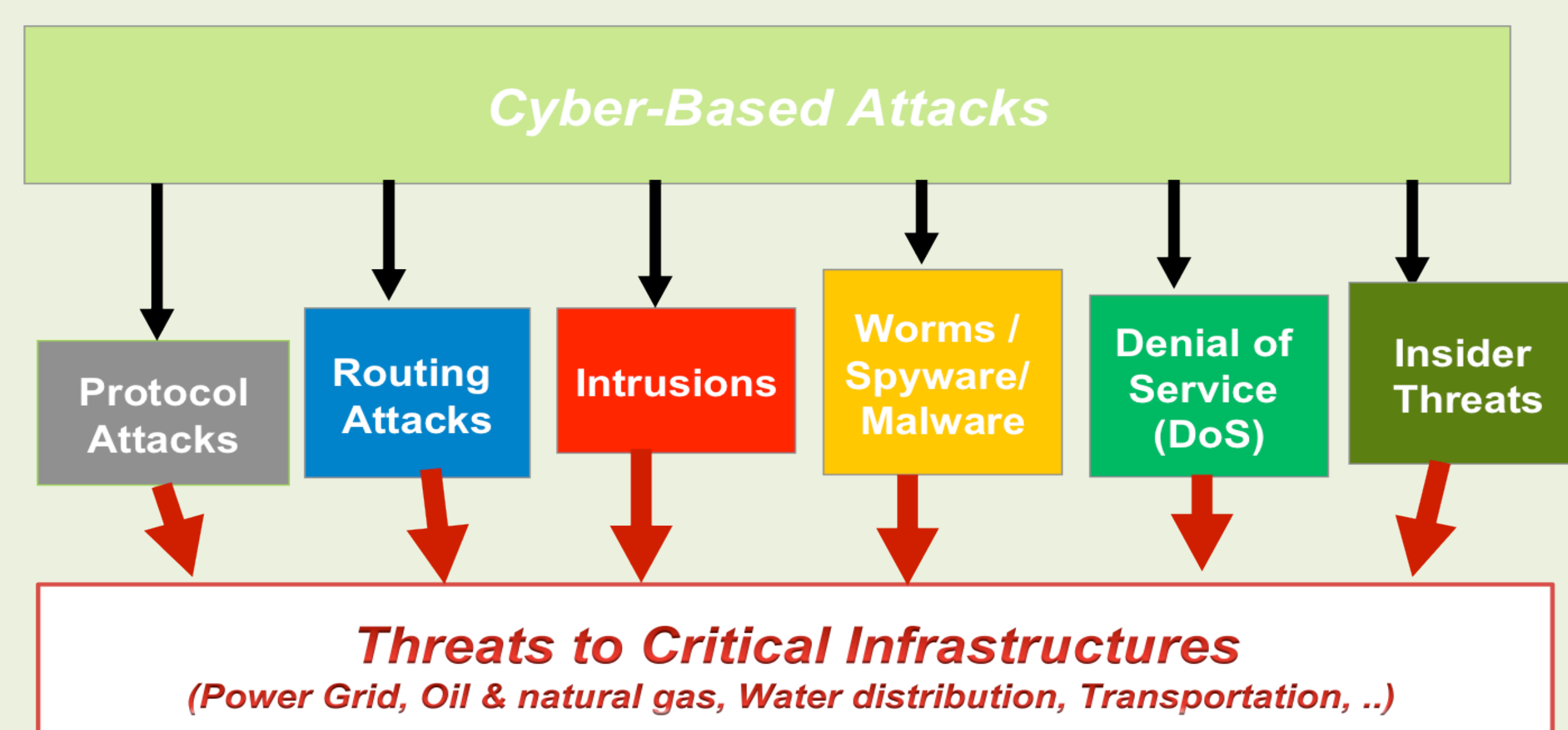
Manimaran Govindarasu, Aditya Ashok, Siddharth Sridhar, Adam Hahn, Iowa State University
Peter Sauer, University of Illinois, Urbana-Champaign



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 threats to the power grid



[General Accounting Office, CIP Reports, 2004 to 2010]; [NSA "Perfect Citizen", 2010]: Recognizes that critical infrastructures are vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

- Smart grid leverages existing network infrastructure which presents greater exposure to cyber threats
- Need to develop comprehensive cyber security architecture with robust models, algorithms, and analysis tools to improve the stability, security, and economic operation of the grid

Cyber-Physical System (CPS) Security

CPS Security = Information Security + Infrastructure Security + **Application Security**

	Information Security	Infrastructure Security	Application Security
NEEDS	- Information Protection - Confidentiality - Integrity - Authenticity - Authentication - Non-repudiation	- Infrastructure protection - Routers - DNS servers - Links - Internet protocols - Service availability	- Generation control apps. - Transmission control apps. - Distribution control apps. - Real-Time Energy Markets
MEANS	- Encryption/Decryption - Digital signature - Message Auth. Codes - Public Key Infrastructure 	- Traffic Monitoring - Dos, Defense measures - Authentication Protocols - Secure Protocols - Secure Servers - Firewalls/ IDS	- Attack-Resilient Control Algos - Model-based Algorithms - Anomaly detection - Intrusion Tolerance - Bad data elimination - Risk modeling and mitigation

Smart Grid Cyber Security requirements

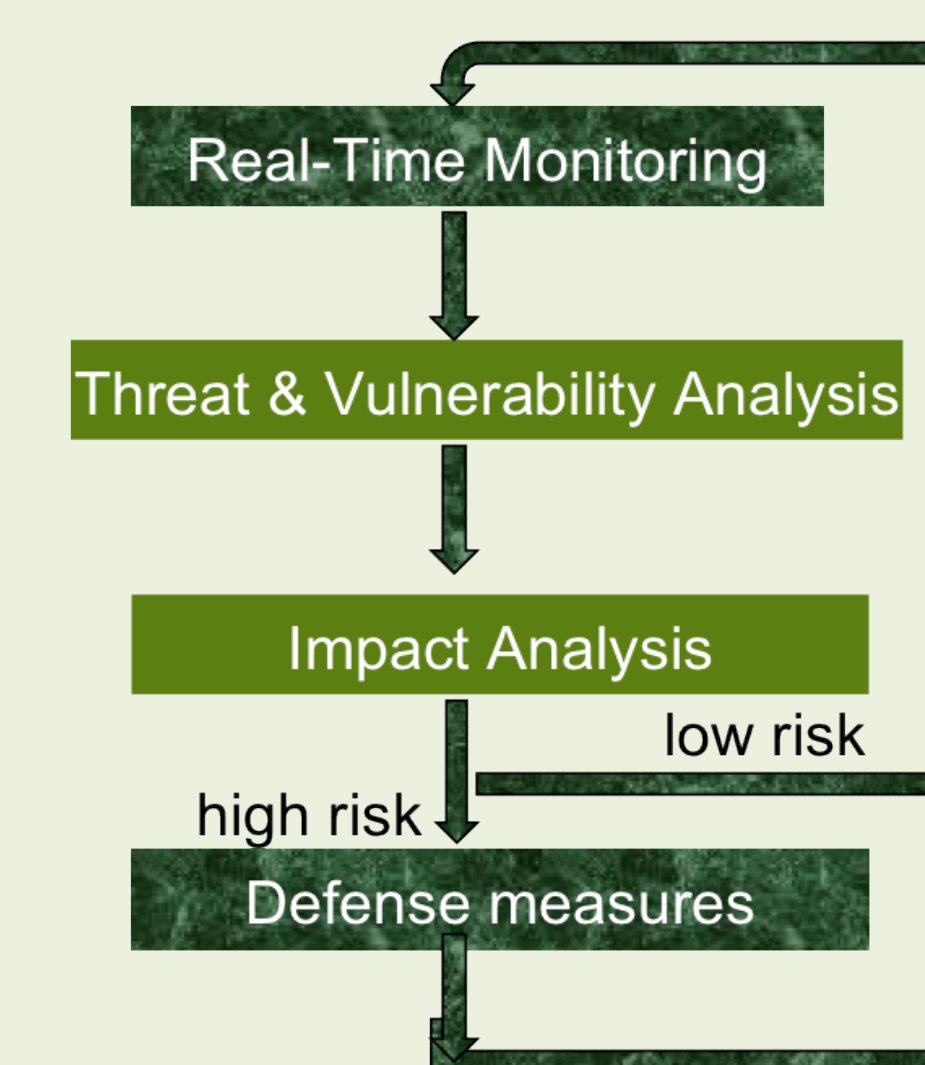
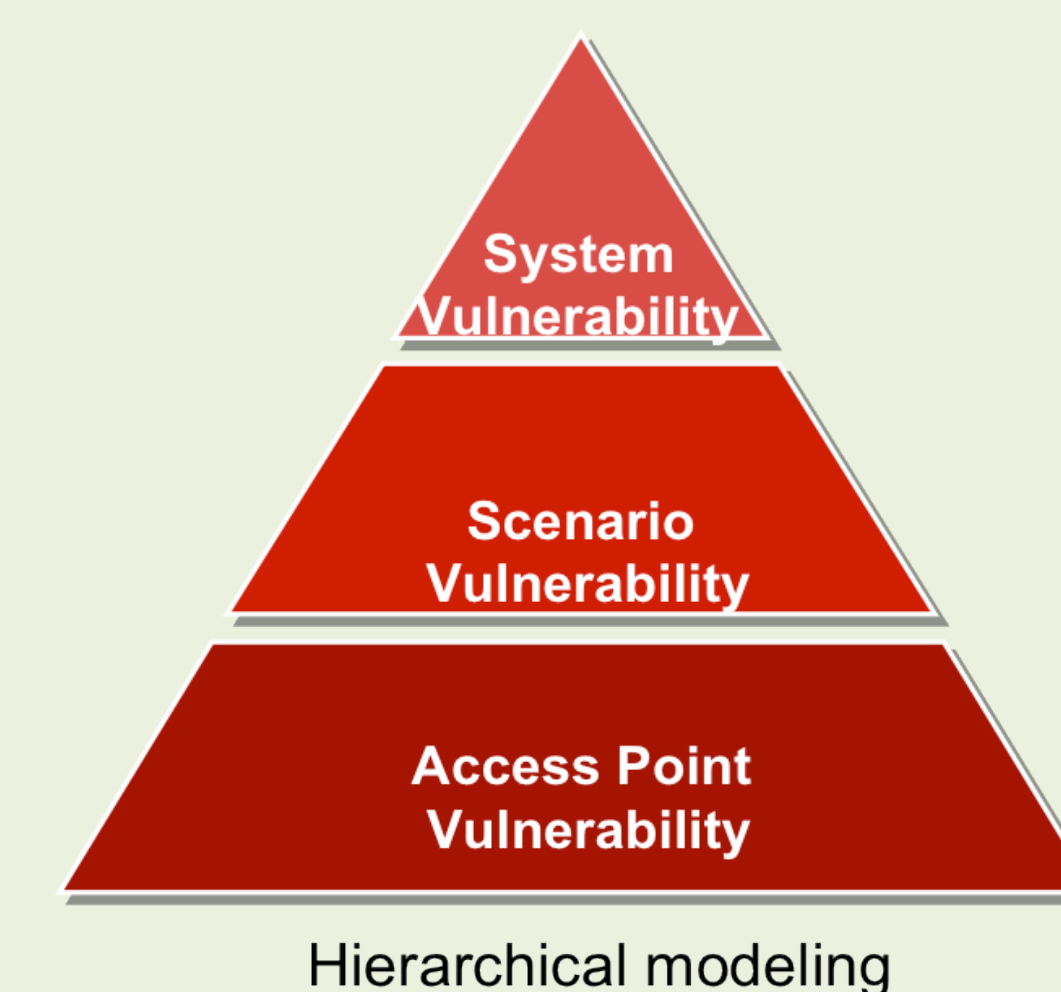
Confidentiality (C), Integrity (I), Availability (A), Authentication (AT), Non-repudiation (N)

Smart Grid Application	Information & Infrastructure Security	Application Security
AMI	I, AT, C	I, N
DMS	I, A, AT	I, AT
EMS	I, A, AT	I, AT
WAMPAC	I, A, AT, C	I, A
Power Markets	I, A, AT, C	I, N

Risk Modeling and Mitigation Framework

Risk = Threat x Vulnerability x Impacts

- Risk Assessment & Risk Mitigation (GAO CIP Report, 2010)
- Security Investment Analysis



Research Challenges

- **Risk Modeling and Mitigation**
 - Vulnerability Assessment
 - Impact Analysis
 - Novel metrics: Load loss, stability and reliability related, economic factors
 - Hierarchical risk modeling framework
 - Synergistic Cyber-Physical mitigation algorithms
- **Attack Resilient WAMPAC Algorithms**
 - e.g., Attack Resilient Wide-Area Measurement
 - Security of PMU networks and data
 - e.g., Attack Resilient Wide-Area Control
 - Robust Automatic Generation Control (AGC) Algo
 - e.g., Attack Resilient Wide-Area Protection
 - Adaptive, Intelligent Remedial Action Schemes
- **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