COORDINATED SCIENCE LABORATORY

ENGINEERING AT ILLINOIS

Information Trust Institute

David M. Nicol, Director

Franklin W. Woeltge Professor of ECE

ITI.ILLINOIS.EDU

INFORMATIONTRUST
INSTITUTE

Context

- ITI has been doing research and development for cyber-security in the power grid since 2004 (TCIP, TCIPG, CREDC, partnering on various DOE industry and lab calls)
- Current center (CREDC---DOE and DHS funded) has roughly 30 projects in the areas of
  - Cyber-protection Technology
  - Cyber Monitoring, Metrics, and Evaluation
  - Risk Assessment of EDS Technology and Systems
  - Data Analytics for Cyber Event Detection, Management, Recovery
  - Resilient EDS Architectures and Networks
  - Impact of Disruptive Technologies on EDS
  - Validation and Verification
- CREDC emphasis is on moving research results into practice
- ITI also supports DARPA RADICS program, with test-bed for development/evaluation/exercises

Areas needing attention

Business reasons for utilities to choose new security technologies

Need to be able to *quantify* benefit

    - Expensive protection for a a rare event is a hard sell
    - Classical definition of risk (probability x cost) is hard because quantifying probability is hard

Technologies that advance security while adding other (quantifiable) benefits

- Monitoring/analysis technologies that give better insight into system behavior
    - Data analytics
- Technologies that lower maintenance costs
    - Software defined networking

Areas needing attention

Information sharing

- (Tip of the hat to CRISP and CYOTE)
- Incentives and vehicles for sharing?
- Protections available
    - Anonymization and privacy protection with provable properties

Technology supporting rapid recovery from cyber intrusion

- Architectural support (e.g. virtualization)
- Intrusion detection
- “useable” response forensics tools
    - Close gap between expert knowledge and operational

Areas needing attention

Assessment

- (Tip of the hat to C2M2)
- Emerging technologies (e.g. Industrial Internet of Things, cloud computing) bring new capabilities, but change the attack surface
- How do we balance the economic benefits of emerging technologies with increased risks and added cost of security?

Improved trust in communications and provenance of digital artifacts

- Methodologies for increased checks, applied dynamically, yet lightweight