Design Principles for Power Grid Cyber Infrastructure Protocols

Himanshu Khurana
University of Illinois, Urbana Champaign

ICSJWG, San Antonio, TX, April 2010

Joint work with Rakesh Bobba, Erich Heine, Tim Yardley and Pooja Agarwal

Trustworthy Cyber Infrastructure for Power Grid (TCIP; 2005-2010): Vision and Strategy

- Drive the design of *an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power*, which *operates through attacks* by:
  - Protecting the cyber infrastructure
  - Making use of cyber and physical state information to detect and respond to attacks
  - Supporting greatly increased throughput and timeliness requirements
- Support the provisioning of a new resilient “smart” power grid that
  - Enables advanced energy applications
    - High-speed monitoring and asset control, advanced metering, diagnostics & maintenance
- Research Partners
  - University of Illinois (UIUC), Cornell, Dartmouth College, Washington State University
- Sponsors
  - National Science Foundation, Department of Energy, Department of Homeland Security

TCIPG Effort Begins

Extend and **integrate** previously developed TCIP technologies and to develop new ones that collectively provide resilience in the nation's electric grid cyber infrastructure that ensures

- Trustworthy and timely operations,
- Survives malicious attacks while ensuring **continuous delivery of services**, and is built on an
- **Intrusion tolerant**, survivable architecture

- $18.8 M per over 5 years, starting Oct 1, 2009
- Funded by Department of Energy, Office of Electricity
  - With support from Department of Homeland Security
- 4 Universities
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - University of California at Davis
  - Dartmouth University
  - In addition, Bob Thomas will continue to work with TCIP as a consultant

More information at tcip.iti.illinois.edu

Introduction to Protocol Design for Power Grid

- **Cyber infrastructure is key to realization of a Smart Grid**
  - Introduces an additional threat element: cyber attacks
- **Cyber security protocols and their standardization are needed to protect against emerging cyber attacks**; e.g.,
  - Authentication protocols protect against attacks such as masquerading, spoofing, replay, etc.
  - Encryption protocols protect against eavesdropping attacks
  - Non-repudiation protocols protect against deniability
- **This work focuses on trustworthy designing of protocols for Smart Grids**
- **Publication**
  - Himanshu Khurana, Rakesh Bobba, Tim Yardley, Pooja Agarwal and Erich Heine, "Design Principles for Power Grid Authentication Protocols", in proceedings of HICSS, January, 2010.

The need for principles

Protocols	Attacks	Cause/Vulnerability
Authentication Protocol by Woo & Lam	Impersonation attacks	Lack of explicit names
STS by Diffie, Oorschot & Wiener	Impersonation attacks	Change in environmental conditions
Kerberos V4 by Steve & Clifford	Replay attacks	Incorrect use of timestamps
TMN by Tatebayashi, Matsuzaki, & Newman	Oracle attacks	Information flow

Research Focus

- **Specifically, this work presents and discusses key design principles**
  - Principles developed and applied, in part, for evaluation of DNP3 Secure Authentication Supplement V2.0*
    - Standardization efforts are in progress (V3 to be released soon)
    - However, principles are generic in nature
  - Principles leverage prior work in Internet authentication protocols but highlight key differences
  - Principles that will be needed as Smart Grid systems emerge

- **Disclaimers**
  - Principles are helpful but not sufficient
  - Recent updates to DNP3 Secure Authentication have not been evaluated

* Funded in part by EPRI

The Grid Today and Tomorrow

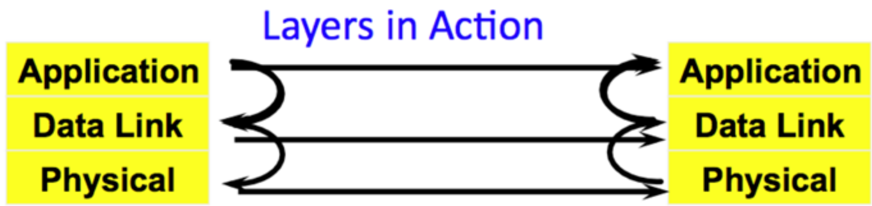
- **Today's Grid:**
  - Wide range of computation and communication technologies
    - E.g., serial to high-speed optic fiber, low-end to high-end microprocessors
  - Networks with limited surplus bandwidth
  - Prevalence of legacy protocols and systems
  - Lack of system-wide security infrastructure (e.g., PKI)

- **Tomorrow's Grid:**
  - High potential for major upgrades and deployment of security infrastructure

- **Perennial requirements**
  - High performance, high availability, timeliness, major attack target, adaptability

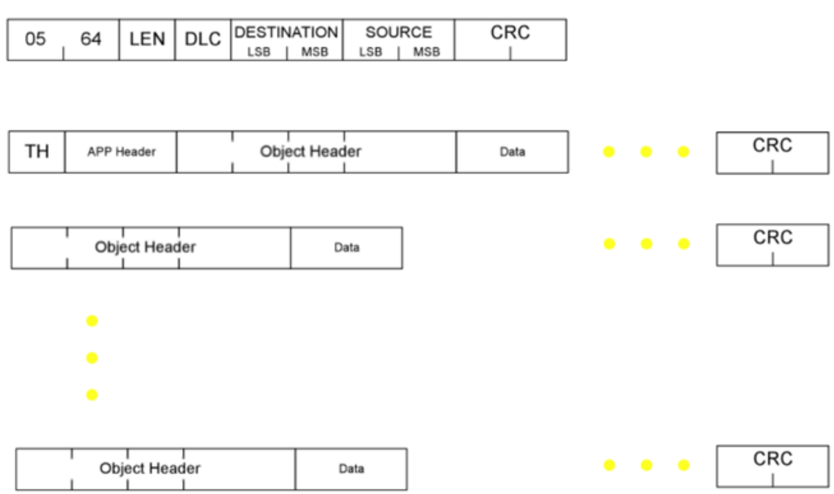
DNP Background

- **DNP Overview**
  - Transmits & receives
    - analog and digital values
  - Multi Master
  - Tens-of-millisecond update rate
  - Serial and Ethernet
  - *Extensively used in the Grid today*



- **DNP3 Secure Authentication Supplement**
  - Being developed by DNP Users Group to authenticate communication between a DNP3 master and outstation
  - Based on IEC 62351-1
  - Specification leverages ISO/IEC 9798-4 (HMAC based authentication)

DNP Message Structure



Selected Design Principles for Security Protocols

Principle	Attacks Mitigated	Applicability to Power Grid Authentication Protocols
Explicit Names	Impersonation attacks.	Need for explicit names for each entity in power grid.
Unique Encoding	Interleaving and parsing ambiguity attacks.	Insufficiency of legacy protocols to build security on them due to no protocol identifiers in them.
Explicit Trust Assumptions	Prevents errors due to unclear or ambiguous trust assumptions	Need to clearly state all trusted entities in power grid protocols and the extent of trust in them.
Use of Timestamps	Prevents replay attacks.	Need for high granularity for time synchronization.
Protocol Boundaries	Prevents incorrect function of protocol in it's environment.	Need for thorough analysis of the power grid environment.
Release of Secrets	Prevents blinding attacks and compromise of old keys.	Need to ensure that compromise of some remote devices should not compromise large number of keys.
Explicit Security Parameters	Prevents errors due to exceeding the limitations of cryptographic primitives.	Reduction in maintenance overhead by explicitly mentioning security parameters in remote devices.

Applying Known Authentication Principles

- **Principle of Explicit Trust Assumptions**
  - DNP3 Secure Supplement V2.0 claimed non-repudiation as a property using symmetric keys
    - Assumption: master is fully trusted
- **Principle of Protocol Boundaries**
  - DNP3 Secure Supplement v2.0 allows unauthenticated messages to preempt execution of ongoing operation
    - Limitation: DNP3 designed for serial environments
- **Principle of Explicit Names**
  - DNP3 does not use explicit names
    - Limitations: Globally unique names do not exist
    - Solution: (adopted by DNP3) use unique keys in each direction

Design for Efficiency

- **Real-time critical operations demand high efficiency**
  - Implication for cyber security: reduce computation and communication overheads
  - For example, efficient crypto operations, short message size, few rounds of messages
  - Must balance efficiency with security

- **DNP3 Secure Authentication Supplement v2.0 addresses this balance, though not optimally**
  - Message overhead: 4 bytes of sequence number + 4 bytes of nonce + 4 bytes truncated HMAC output
  - Optimal overhead: 2 bytes of sequence number + 8 bytes of truncated HMAC output

Design for Availability

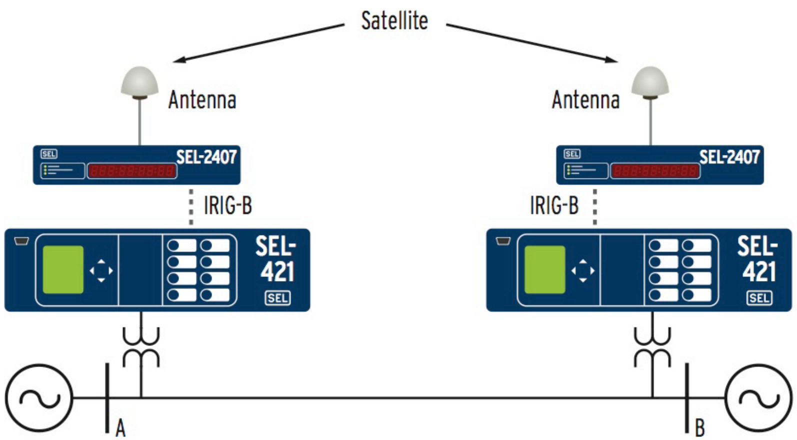
- **Availability often considered more important than confidentiality and integrity**
- To achieve good availability, the protocol must
  - Be efficient
  - Have good and fail-safe error management
  - Support auxiliary security functions

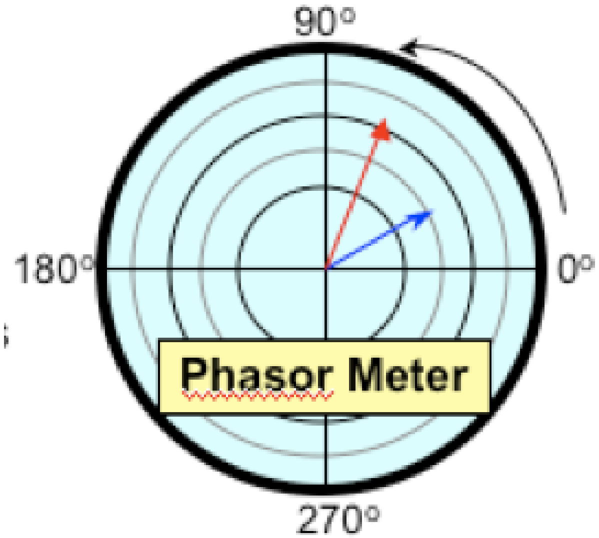
- **DNP3 Secure Authentication Supplement V2.0 allowed unauthenticated incoming messages to preempt ongoing operation**
  - Potential for Denial of Service attack
  - Limitation: underlying DNP3 designed for serial environments
  - Mitigation: authenticate new message prior to preemption (not easy to integrate)

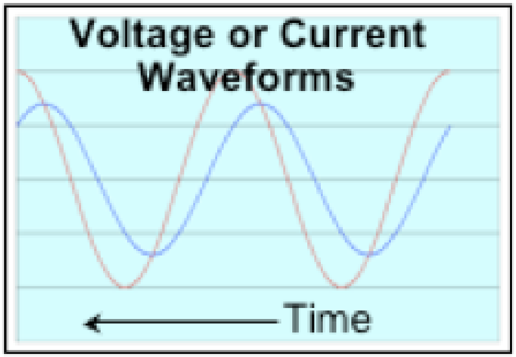
- **DNP3 Secure Authentication Supplement V2.0 did not have fail-safe error management**
  - Potential for Denial of Service attacks
  - Mitigation: better error management and support for auxiliary security functions

Looking Ahead to Emerging Smart Grid Systems and Applications: Synchrophasor Data Sharing

Background: PMUs and Synchrophasors







- Traditional SCADA data since the 1960's
  - Voltage & Current Magnitudes
  - Frequency
  - Every 2-4 seconds
- Data from Phasor Measurement Units (PMU's)
  - Voltage & current phase angles
  - Rate of change of frequency
  - Time synchronized using GPS and 30 - 120 times per second

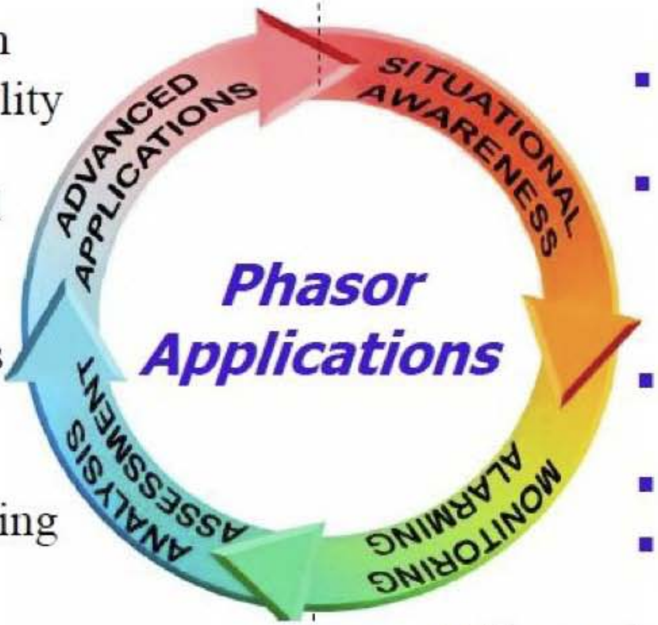
Background: SynchroPhasor Applications

RESEARCHERS

- Automatic alarming of RAS
- Out of step protection
- Short/long-term stability control
- FACTS feedback ctrl

PLANNERS

- Post-mortem analysis
- Model validation
- Phasor network performance monitoring & data quality
- Email notifications
- Test new real-time applications



RELIABILITY COORDINATORS

- Situational awareness dashboard
- Real time compliance monitoring
- Frequency Instability Detection/Islanding

OPERATORS

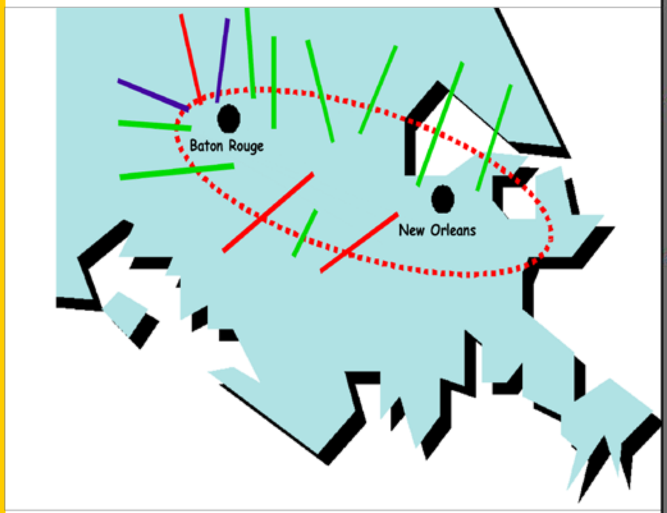
- Real time performance monitoring
- Real time alerts and alarms
- Event detection, disturbance location
- Suggest preventive action
- Interconnection state estimation
- Dynamic ratings

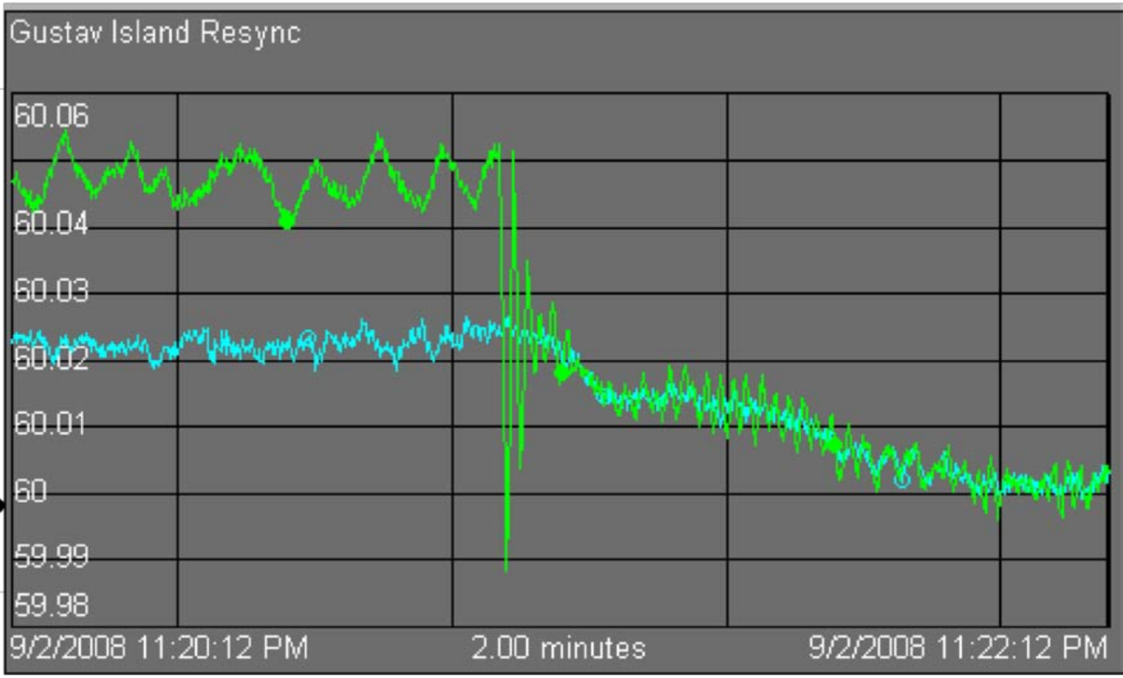
Credit: NASPI Operations Implementation Task Team (OITT)

Background: Real World Example

Entergy and Hurricane Gustav -- a separate electrical island formed on Sept 1, 2008, identified with phasor data

Island kept intact and resynchronized 33 hours later





Source: Entergy

Background: PMU Applications and Deployment

table 1. PMU deployment in different parts of the world.

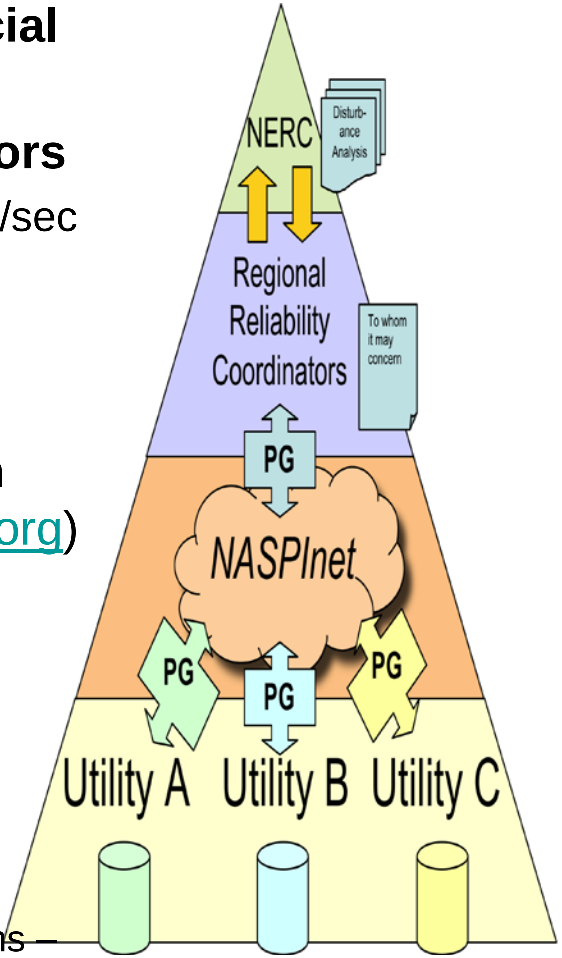
PMU Applications	North America	Europe	China	India	Brazil	Russia
Post-disturbance analysis	√	√	√	P	T	√
Stability monitoring	√	√	√	P	P	√
Thermal overload monitoring	√	√	√	P	P	√
Power system restoration	√	√	√	P	P	P
Model validation	√	√	√	P	T	√
State estimation	P	P	P	P	P	P
Real-time control	T	T	T	P	P	P
Adaptive protection	P	P	P	P	P	P
Wide area stabilizer	T	T	T	P	P	P

T = Testing phase; P = Planning stage

Source – Chakrabarti, Kyriakides, Bi, Cai and Terzija, “Measurements Get Together,” IEEE Power & Energy, January-February 2009

Background: PMU Data Applications and NASPI

- **Wide Area Measurement System (WAMS) is crucial for the Grid**
- **Promising data source for WAMS: Synchrophasors**
  - GPS clock synchronized; Fast data rate > 30 samples/sec
  - Phasor Measurement Unit (PMU)
- **Future applications will rely on large number of PMUs envisioned across Grid (>100k)**
- **WAMS Design and Deployment underway: North American Synchrophasor Initiative** - (www.naspi.org)
  - *Collaboration* - DOE, NERC, Utilities, Vendors, Consultants and Researchers
  - *NASPInet* – distributed, wide-area network
- **Applications with wide ranging requirements**
  - **Class A** - e.g., Frequency stability: 30-120 samples/second, 50-100ms latency
  - **Class B** - e.g., State Estimation: 20-60 sample/second, 200ms – 1 sec latency
  - **Class C** - e.g., Visualization: 10-30 sample/second, ~1second latency
  - **Class D** - e.g., Disturbance Analysis: 30-120 samples/second



Overview of PMU Systems and Data Networks

- **Substation systems and networks**
  - PMU, relays, clocks, Ethernet/similar, switches, routers,
- **Utility-wide systems and networks**
  - Phasor Data Concentrators, data historian, switches, routers, multiple networking technologies
- **NASPInet systems and networks**
  - Phasor gateways, data bus, management systems, wide area communication systems
- **Applications and users**
  - Monitoring, control, protection

Key cyber security requirements

- **Data security**
  - Desired properties: confidentiality, integrity and availability
  - Threats: eavesdropping, message insertion/modification, denial-of-service
- **System security**
  - Desired measures: protection, detection and response
  - Threats: intrusions, denial-of-service, malware, insider misuse, others
- **Regulation and compliance**
  - NERC CIP
  - Recent FERC response to petition and its implications for cyber security of synchrophasor systems

Select cyber security tools and technologies

- **Cryptographic protocols**
  - Encryption, authentication and key management
  - Symmetric vs. asymmetric cryptosystem approaches
- **Network security tools and technologies**
  - VPN, firewall, IDS, etc.
- **Enterprise security services**
  - Authentication, authorization, identity/key management
  - Data and messaging security
  - Incident management and forensics
- **Development and testing tools**
  - Secure development of software and hardware systems
  - Penetration testing/security evaluation

A crossroads in cyber security

- Today's approach*: physical and electronic perimeter protection, uniform security level, coarse-grained access control, auditing
  - Addresses baseline security requirements, common threats and attack modes
  - Aligned with current regulatory requirements

Where do we need to go?

- Risk-driven graded security levels, granular access control, cross-layer security designs
  - Address sophisticated attacks, provide strong assurances for decision making
  - In line with regulatory changes?
    - Recent proposed CIP changes point towards graded security levels and NIST 800-53 style security controls

* This is a generalization and not likely to be correct in all cases.

Example Implications and Challenges

- **Potential threat/attack: possible consequences of asset compromise or insider misuse**
  - Assets can include PDCs, PGWs, data bus routers, etc.
  - Significant damages with current approaches
  - *Mitigation*: granular access control at hosts, network devices, applications, databases
  - *Design techniques*: defense-in-depth, all-hazards approach, advanced protocol design
  - *Detection*: advanced intrusion detection systems with signature and anomaly based techniques

Example Implications and Challenges

- **Desired characteristic: trusted decision-making in control and protection**
  - Decisions based on received PMU data and analysis
  - Limited assurances with current approaches
  - *Enhancements*: strong data authentication, protocol security, auditing and accounting of data systems

Power Grid Cyber Security Resources

- NIST Smart Grid interoperability effort
  - http://www.nist.gov/smartgrid/
  - http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf
- NISTIR on Cyber Security
  - http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628
- National SCADA Testbed Program
  - http://www.oe.energy.gov/nstb.htm
- DOE OE Control System Security
  - http://www.oe.energy.gov/controlsecurity.htm
- FERC Smart Grid Policy
  - http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf
  - Recent petition: http://www.ferc.gov/whats-new/comm-meet/2009/121709/E-4.pdf
- NERC CIP
  - http://www.nerc.com/page.php?cid=2%7C20

Power Grid Cyber Security Resources

- NASPInet Specification
  - http://www.naspi.org/resources/dnmtt/naspinet/naspinet_phasor_gateway__final_spec_20090529.pdf, http://www.naspi.org/resources/dnmtt/naspinet/naspinet_databus_final_spec_20090529.pdf
- DHS Control System Security Program
  - http://www.us-cert.gov/control_systems/
- Roadmap to Secure Control Systems
  - http://www.controlsystemsroadmap.net/
- Trustworthy Cyber Infrastructure for Power Grid
  - http://www.**tcip.iti.illinois.edu**
- ARRA Cyber Security training material
  - https://www.arrasmartgridcyber.net/index.php

Conclusion

- Design principles for security protocol can be very helpful
- We adapt existing principles for authentication protocols and develop new ones for power grid cyber infrastructure authentication protocols
- In part, the principles were developed and applied to DNP3 Secure Authentication Supplement
  - Many recommendations have been adopted and work is still ongoing
- We then explored the need for advanced protocols in emerging Smart Grid systems such as WAMS
- Similar explorations of principles for encryption, key management, and other cyber security properties is needed

Questions?

- Contact
  - Himanshu Khurana, University of Illinois
  - hkhurana@illinois.edu