Application-driven Design for Secure and Timely Electric Grid Systems

Himanshu Khurana

Information Trust Institute, University of Illinois at Urbana-Champaign

TCIPG: Trustworthy Cyber Infrastructure for Power Grid

✧ Objective: Develop technologies that collectively provide resilience in the power grid cyber infrastructure
✧ Five-year effort: 2009 – 2014 ($18.8m); build on TCIP (2005 – 2010; $7.5m)
✧ Multi-University Research Team
  ❖ UIUC, Dartmouth, WSU and UC-Davis
  ❖ 25 faculty and scientist, 30 students, 10 developers and engineers
  ❖ Expertise in power systems, cyber security, communication systems, computing technologies
✧ Public-private Partnership
  ❖ Extensive industry partnerships include operators, utilities, vendors and providers
  ❖ DoE National Labs and the National SCADA Test Bed Program
✧ Research focus: Resilient and Secure Grid Systems
  ❖ Secure and real-time communication substrate
  ❖ Automated attack response systems
  ❖ Risk and security assessment
  ❖ Experimental Evaluation using an extensive testbed

University of Illinois • Dartmouth College • University of California - Davis • Washington State University

tcipg.org
Research Focus: Transmission and Distribution System

Color Key:
Blue: Transmission
Green: Distribution
Black: Generation

Transmission Lines
500, 345, 230, and 138 kV

Substation Step-Down Transformer

Primary Customer
13kV and 4 kV

Secondary Customer
120V and 240V

Balancing Authorities/Control Centers

As of August 1, 2007

USA Map

Regions and Balancing Authorities
NPCC
WECC
MRO
RFC
SPP
TRE
FRCC
SERC

Utility Network
WAN
NAN
Access Point

Meter
Risks Due to Cyber Attacks and Failures:

**Consequences**
- **Blackouts**
  - Significant economic disruption
  - Safety of the population
  - Secondary effects in other Cls
- **Market disruption – artificial congestion**
- **Equipment damage**
  - Transmission transformer - cost in millions, lead time in years
  - Potential long-term blackouts
- **Extortion**
- **Privacy violations**
- **Combined physical and cyber attacks**

**Adversaries**
- **Casual hacker**
  - Surprisingly capable antagonists
  - Knowledgeable community
- **Criminal extortionist**
  - Looking for return on investment
  - Willing to spend a lot of financial return is large enough
- **National government/organized terrorism**
  - Consequences sought may be non-financial
  - Large resources
- **Insiders (possibly used by attackers in other categories)**
Research Overview of Select Projects

- **Challenges**
  - Real-time critical operational environment
  - Bandwidth and connectivity constraints
  - Legacy protocols and systems
  - Emerging applications and systems

- **Problems addressed**
  - Authentication for SCADA protocol
  - Real-time middleware for SCADA systems
  - Tiered Architecture for Wide Area Measurement Systems

- **Approach**
  - Application-driven design
  - Eventually “science” of cyber security for power grid will emerge
SCADA Architecture

Overall Architecture (current)
SCADA Protocols

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

Authentication for SCADA Protocols

• Problem
  – Message authentication for SCADA

• Challenges
  – Bandwidth and computation constraints
  – Legacy integration (with DNP3)

• Approach
  – Evaluate industry proposal for DNP3 Secure Authentication Supplement (*funded by EPRI*)
  – Develop principles and improved protocol

> DNP3 Architecture

> DNP3 Secure Authentication
  > Based on ISO/IEC 9798 Standards (using HMAC)
Security Evaluation

- **Results**
  - Analysis of industry proposal:
    - *Bandwidth* reduction via HMAC truncation
    - *Legacy* integration via challenge-response
  - Issues with industry proposal
    - Recommend 32-bit truncated output &
    - Use both nonces and sequence numbers
      - Efficiency neither optimal nor correct
    - Insufficient resistance in design
      - Protocol-based DoS vulnerability
  - Our feedback
    - Proposed alternative HMAC truncation strategy
    - Proposed approach for DoS resistant design

- **Industry Interactions**
  - Participation in DNP Technical Committee
  - Feedback is being included in the standard
  - Participation in IEEE PSCC for IEC 62351-5 standard
Research Problem #1: Secure Protocol Design for the 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
## The need for principles

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Attacks</th>
<th>Cause/Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Protocol by Woo &amp; Lam</td>
<td>Impersonation attacks</td>
<td>Lack of explicit names</td>
</tr>
<tr>
<td>STS by Diffie, Oorschot &amp; Wiener</td>
<td>Impersonation attacks</td>
<td>Change in environmental conditions</td>
</tr>
<tr>
<td>Kerberos V4 by Steve &amp; Clifford</td>
<td>Replay attacks</td>
<td>Incorrect use of timestamps</td>
</tr>
<tr>
<td>TMN by Tatebayashi, Matsuzaki, &amp; Newman</td>
<td>Oracle attacks</td>
<td>Information flow</td>
</tr>
</tbody>
</table>
## Selected Design Principles for Security Protocols

<table>
<thead>
<tr>
<th>Principle</th>
<th>Attacks Mitigated</th>
<th>Applicability to Power Grid Authentication Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit Names</td>
<td>Impersonation attacks.</td>
<td>Need for explicit names for each entity in power grid.</td>
</tr>
<tr>
<td>Unique Encoding</td>
<td>Interleaving and parsing ambiguity attacks.</td>
<td>Insufficiency of legacy protocols to build security on them due to no protocol identifiers in them.</td>
</tr>
<tr>
<td>Explicit Trust Assumptions</td>
<td>Prevents errors due to unclear or ambiguous trust assumptions</td>
<td>Need to clearly state all trusted entities in power grid protocols and the extent of trust in them.</td>
</tr>
<tr>
<td>Use of Timestamps</td>
<td>Prevents replay attacks.</td>
<td>Need for high granularity for time synchronization.</td>
</tr>
<tr>
<td>Protocol Boundaries</td>
<td>Prevents incorrect function of protocol in it’s environment.</td>
<td>Need for thorough analysis of the power grid environment.</td>
</tr>
<tr>
<td>Release of Secrets</td>
<td>Prevents blinding attacks and compromise of old keys.</td>
<td>Need to ensure that compromise of some remote devices should not compromise large number of keys.</td>
</tr>
<tr>
<td>Explicit Security Parameters</td>
<td>Prevents errors due to exceeding the limitations of cryptographic primitives.</td>
<td>Reduction in maintenance overhead by explicitly mentioning security parameters in remote devices.</td>
</tr>
</tbody>
</table>
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
Research Problem #2: Real-time Middleware for SCADA Systems

- **Objective:** Enable network convergence for Control system applications
  - Multiple traffic paradigms
    - SCADA and other control
    - Monitoring
    - Engineering
    - Enterprise
  - Understand and support communications requirements/properties for existing and emerging applications

- **Implications for a range of emerging monitoring and control applications**

Joint work with Erich Heine and Tim Yardley
Research Challenges

• Technical Challenges:
  – Resource management
    • Quality of Service, Real-time scheduling, Wide area network optimization
  – Security
    • Access control, Integrity, Availability

• Development and Integration challenges
  – Use commercial, off-the-shelf platforms and tools
  – Minimal use of custom software
  – Support legacy devices and applications
  – Support existing and emerging applications
## Application Characterization with Industry Input

<table>
<thead>
<tr>
<th>Power Systems Application</th>
<th>Traffic Type</th>
<th>Traffic Path</th>
<th>Qualitative Quality of Service (QoS) Parameters</th>
<th>Packet Characteristics (size, timing) per device</th>
<th>Scalability considerations</th>
<th>Stream Bandwidth Characteristics (per device, total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection/Control</td>
<td>SCADA</td>
<td>IED(substation) -&gt; Control Center</td>
<td>Low latency, high priority, no loss</td>
<td>Size: 256B – 1KB Frequency: 1 packet every 2-4s</td>
<td>~5 devices per bus</td>
<td>.5KB/s per device 2.5-5KB/s per bus</td>
</tr>
<tr>
<td></td>
<td>SMV/GOOSE</td>
<td>IED -&gt; IED</td>
<td>High speed/lower latency, high priority.</td>
<td>Size: typically less than 1 Ethernet frame Frequency:</td>
<td>1 event per second per bus</td>
<td>1-15KB per protection event</td>
</tr>
<tr>
<td>Monitoring</td>
<td>PMU</td>
<td>IED/PMU -&gt; Phasor Data Concentrator (Control Center) IED/master -&gt; Control Center</td>
<td>Low latency, medium priority.</td>
<td>Size: 128 Bytes Frequency: 30 – 120 samples/sec</td>
<td>2 PMUs per bus</td>
<td>30Kbps per device, 60Kbps per bus</td>
</tr>
<tr>
<td></td>
<td>Other Monitoring Data</td>
<td></td>
<td>Low latency, medium priority.</td>
<td>Size: 32-64 Bytes Frequency: 1 sample/sec</td>
<td>20-25 Devices/substation</td>
<td>256-512Kbps per device 1-5 Mbps per substation (not all data leaves the substation)</td>
</tr>
<tr>
<td>Engineering</td>
<td>Interactive</td>
<td>Control Center &lt;-&gt; Substation</td>
<td>Medium latency, medium priority</td>
<td>N/A (these are not critical timings and can vary greatly)</td>
<td></td>
<td>1M per occasional request</td>
</tr>
<tr>
<td>Data Transfer</td>
<td>Control Center &lt;-&gt; Substation</td>
<td>Low priority</td>
<td>N/A (Big packets, but not a standard size)</td>
<td>A flow 1-2 times per day</td>
<td></td>
<td>1-5M per occasional request</td>
</tr>
<tr>
<td>Surveillance</td>
<td>Video</td>
<td>Substation -&gt; Control Center</td>
<td>Medium – High latency, medium priority.</td>
<td>Varied video frame sizes and rates</td>
<td>2-10 cameras per substation</td>
<td>100 Kb/s -1Mb/s per camera ~5Mbps per substation</td>
</tr>
</tbody>
</table>
Example Scenario

- Special purpose and Common Off The Shelf systems in datapath (*blue boxes*):
  - End-to-end deadlines (10s of ms for protection applications)
Results: Architecture
Results: Performance

Packet latency timings with CPU contention

Left: unenhanced host  Right: CONES enhanced host
Results: Performance

Network latency timings with network interface contention.

Left: unenhanced host
Right: CONES enhanced host
• Traditional SCADA data since the 1960’s
  – Voltage & Current Magnitudes
  – Frequency
  – Every 2-4 seconds
• Future 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
Why do Phase Angles Matter?

Wide-area visibility could have helped prevent August 14, 2003 Northeast blackout
Why do Phase Angles Matter?

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
Wide Area Measurement Systems and NASPI

- **Wide Area Measurement System (WAMS)** is crucial for the Grid
- **Promising data source for WAMS: Synchrophasors**
  - GPS clock synchronized
  - Phasor Measurement Unit (PMU)
  - Fast data rate ~ 30 samples/second
- **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](http://www.naspi.org)
  - *Collaboration* - DOE, NERC, Utilities, Vendors, Consultants and Researchers
  - *NASPI* – distributed, wide-area network
Conceptual NASPIInet Architecture

Source: NASPIInet Specification
tcipg.org
Research Problem #3: Towards a Distributed PMU Data Network

• Technical Challenges for NASPIInet
  – large distributed network - continental scale
  – quality of service (QoS) - prioritization of traffic, latency management etc
  – securing PMU data – integrity, availability and confidentiality, key and trust management, network admission control, intrusion detection, response, recovery
  – network management – performance, configuration, accounting, fault management, security management

• Business/Organizational challenges for NASPIInet
  – who owns/manages/provides the network
  – high initial costs

Exploring a Tiered Architecture

- Tiered Architecture
  - leverages data locality
  - leverages the existing hierarchy
    - power grid operators, monitors and regulators
      - allows for incremental growth/formation of NASPInet
      - can simplify trust and key management needed for securing PMU data
      - can simplify network management with localized providers
      - can simplify QoS management
      - provides distributed computing opportunities
Proposed Tiered Architecture

- Backup Internet Overlay
- Managed Secure Real-time Link
- Trusted Entity (e.g., Reliability Coordinator) acts as Hub
- DATA BUS
- PGW\(_1\)
- PGW\(_n\)
- Hub
- Managed Secure Real-time Network
- Optional Direct Link
- Storage Computation Content Router Services
Next Generation Smart Grid “Secure” Controls

- Multi-layer Control Loops
  - Multi-domain Control Loops
    - Demand Response
    - Wide-area Real-time control
    - Distributed Electric Storage
    - Distributed Generation
- Intra-domain Control Loops
  - Home controls for smart heating, cooling, appliances
  - Home controls for distributed generation
  - Utility distribution Automation
- Resilient and Secure Control
  - Secure and real-time communication substrate
  - Integrity, authentication, confidentiality
  - Trust and key management
  - End-to-end Quality of Service
  - Automated attack response systems
- Risk and security assessment
  - Model-based, quantitative validation tools

Note: the underlying Smart Grid Architecture has been developed by EPRI/NIST.
Thank you.
Questions?

Contact Information:
khurana@illinois.edu