Roadmap to Secure Control Systems in the Energy Sector

Energy Sector Control Systems Working Group

ieRoadmap Workshop

Chicago, IL ♦ May 28-29, 2008

Dong Wei, Siemens Corporate Research, Inc.
Mohsen Jafari, Rutgers University
Protecting Intelligent Distributed Power Grids against Cyber Attacks

- **Outcomes:** Prototype of the integrated security system: 1) security agent; 2) managed security switch; 3) security manager; and 4) engineering system

- **Roadmap Challenges:** Open and flexible control leads to increased risks; Poorly designed connections to SCADA and business networks can dramatically increase vulnerabilities of control systems; Security upgrades hard to retrofit to legacy systems, may be costly, and may degrade system performance; Known technical risks can migrate from non-vendor supporting hardware and software

- **Approach:** An integrated and distributed security system which overlays across the intelligent power grid network in a hierarchical/distributed manner

- **Progress/accomplishments:**
  - Report is done
  - Architecture design specification + function design specification

- **Schedule:**
  - technical report – 05/15/08
  - specification – 09/30/08
  - test - 07/10/09
  - report – 07/17/09

- **Level of Effort:** high

- **Performers:** 4 researchers + 3 interns conducting the work

- **Partners:** SPTD, Rutgers, INL
Protecting Intelligent Distributed Power Grids against Cyber Attacks

- **Outcomes:** Risk and critical asset assessment models and software prototype

- **Roadmap Challenges:** Insufficient tools and techniques exist to measure risk (Measure and Assess Security Posture)

- **Approach:** Use of model based approach to assess vulnerabilities at control level, and use of simulations to measure the impacts of these vulnerabilities at the physical power grid level.

- **Progress/accomplishments:**
  - Literature review is done
  - Preliminary framework is done
  - Modeling & simulation is underway

- **Schedule:**
  - Technical report – 05/15/08
  - Modeling – 09/30/08
  - Testing – 06/30/09

- **Level of Effort:** Med

- **Performers:** 2 professors + 2 Ph.D students conducting the work

- **Partners:** SCR, SPTD, INL
Technology Transfer/Collaboration

Collaborate with the EMA (Energy Management Automation) Division, SPTD (Siemens Power Transmission and Distribution, Inc)
Next Steps – The Integrated Security System

1. Architecture design specification (conceptual model + software architecture) - 06/30/08
2. Function design specification (Algorithms) – 09/30/08
3. Version 1 – 03/06/09
4. First on-site test – 03/27/09
5. Version 2 – 06/26/09
6. Final Test – 07/10/09
7. Final Report – 09/30/09
Security Agent

- To translate between different protocol.
- To acquire and run the latest vulnerability updates from its security manager.
- To collect data traffic pattern, system log data and report to the security manager.
- To analyze traffic and access patterns with varying complexity depending on the hierarchical layer.
- To run host-based intrusion detection.
- To detect and send alarm messages to the security manager and designated devices, such as HMI.
- To acquire access control policies from the security manager and enforce them.
- To encrypt and decrypt exchanged data (end-to-end security).
Implementation of Security Agent

- An individual two-port module – the internal is connected to the protected device (such as PLC and HMI), the external port connected to a network device (such as switch, router).
- Agent resides in a managed security switch - a virtual security agent run on internal port connected to a protected device.
- Agent resides in all newly developed devices (such log server, PLC, RTU) – runs independently of control firmware.
Managed Security Switch

• To separate external and internal networks, trusted and non-trusted domains.
• To run as DHCP (Dynamic Host Configuration Protocol) server.
• To run as NAT/NPAT (Network Address Translation and Network Port Address Translation) and to hide the internal networks.
• To acquire bandwidth allocation pattern and data prioritization pattern from the security manager.
• To separate data according to prioritization pattern, such as operation data, log data, trace data and engineering data.
• To provide QoS for important data flow, such as operation data, guaranteeing its bandwidth, delay, etc.
• To manage multiple VLANs (Virtual Local Area Network).
• To run simple network-based intrusion detection.
Security Manager

• To collect security agent information.
• To acquire vulnerability updates from the vendor’s server and download them to the corresponding agents.
• To manage keys for VPN.
• To work as an AAA (authentication, authorization and accounting) server, validating user identifications and passwords, authorizing user access right (monitor, modify data), and recoding what a user has done to controllers.
• To collect data traffic pattern and performance matrix from agents.
• To collect alarms and events.
• To generate access control policies based on collected data (data mining technique used here) and download to agents.
• To run complex intrusion detection algorithms at control network levels.
• To generate bandwidth allocation pattern and data prioritization pattern (data mining technique may be used here) and download them to managed switches.
Next Steps – Risk Assessment Models and Software Prototype

1. Modeling – 09/30/08
   • Simulation – 03/13/09
   • Testing – 06/30/09
What is Risk?

Risk = \( f \) (threat, vulnerability, impact)

Calculated from IT network / Control Network

Calculated from physical grid
Final Analysis - Critical Asset Assessment

Vulnerabilities @ higher levels

Vulnerabilities @ substation level

Critical Asset assessment based on initial impact measures

Cyber Risk Assessment

Critical Asset assessment based on updated impact measures
Connection points between Physical Grid and Control/IT Networks

• Substations are where physical damages can be inflicted through cyber attacks:
  – Generation level
  – Transmission level
  – Distribution level
Impact?

- Must be in measurable terms; load reduction; economic loss, duration, etc.

- Multi dimensional impact vectors possible.

- Simulations (or historical data if available) can be used to measure impact vector.

- Traditional power grid stability / reliability analysis cab be used, e.g., N-1 analysis. This can be also extended to cascading effects?

- Initial analysis provides static impact measures for various combinations of substations losses. These values are obtained in the absence of cyber-attack, thus static values.

- These values can be updated incorporating cyber risks in some iterative fashion.
What could go wrong @ a substation level?

- Hacker interferes with the flow of the information
  - Incomplete or wrong information to the operator on process or input data
    - Failed states/conditions masked to the operator(s)
    - Normal states/conditions misrepresented as abnormal

- Hacker interrupts the controllability of the substation operation; the control center may lose the ability to properly control the substation operations.

- Hacker has the control of the substation
  - Failure or stoppage of components, e.g.,
    - Circuit breakers, motorized switches, etc.
    - Wrong state but correct information available to the operator
    - Disruption of normal sequence of events
How could it go wrong?

Two scenarios:

- Formal models of substation control logic, I/Os and database exist
- No formal models exist, e.g., legacy systems. (Domain expert view can be used to reverse engineer a subjective models of substation.)

- Categorization or classification of what could go wrong according to their initial impact. This could be an iterative process.

- Cause and effect analysis for each category – formal or informal methodologies

- Formal methodology – uses existing formalisms at substation level + domain expertise on power grid operation

- Informal methodology – uses only domain expertise on power grid operation
Cause & Effect Analysis

Control Model / Data model / Input & output model

Field device 1

Field device n

Field device N

What could go wrong
Scenario 1 – OPC XML service
Scenario 1 – OPC XML service
Scenario 1 – OPC XML service
Scenario 2 – TCP Connection