An Integrated Security System of Protecting Smart Grid against Cyber Attacks

Authors: Dong Wei, Yan Lu, Mohsen Jafari,
Paul Skare, and Kenneth Rhode

Presenter: Somo Peyechu

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Outline

- Introduction
- Background
- Smart Grid Security Requirements
- Development Challenges
- Proposed Security Framework
- Testing
- Summary

Introduction

- Smart grid is essentially an integration of electrical infrastructure with information infrastructure.

- This integration moves power systems from proprietary technology to more commonly available technologies.

Background

- Principal goal [1] of a power grid is to "deliver electricity economically subject to the constraints of capacity and reliability."

- Power grid automation systems are increasingly using public networks, increasing vulnerability to cyber attacks.
  - Use of proprietary protocols are now giving way to the cost effectiveness of using public networks.

Potential Network Attacks

- Cyber attacks are classified into three categories:
  - Component-wise: Field components which usually have a user interface for configuration or diagnostics.
    - Impact: 1) provide misleading data to SCADA operator
      2) damage field equipment
      3) loss of service if intruder shuts down device.
  - Protocol-wise: Almost all modern data communication adheres to well known protocols available to public.
    - Impact: 1) financial loss if attack leads to excess generation
      2) safety vulnerability if a line is energized while servicing is being done
      3) Equipment damage if control commands cause overloading

Potential Network Attacks

- Topology-wise: Any vulnerability in the network topology can be exploited by an intruder e.g. Denial-of-Service by flooding SCADA with valid protocol messages in order to saturate CPU computational power.
  - Impact: Control operators may fail to have a complete view of the entire power grid system leading to incorrect decisions being taken.

Security Differences between Smart Grid and IT systems

- Due to differences between both systems, IT security solutions cannot be directly deployed to secure the smart grid.

- Four major differences between IT and smart grid systems:
  - Security objectives
  - Security architecture
  - Technology base
  - Quality-of-Service (QoS) requirements

Security Differences between Smart Grid and IT systems

TEXAS A&M UNIVERSITY

➢ Different Security Objectives:

- Main objective of IT security is to protect data. Concerned mainly with data confidentiality, integrity, and availability.

- Current grid priorities:
  - Human safety
  - Functioning system under normal operating conditions
  - Protection of equipment and power lines

Security Differences between Smart Grid and IT systems

TEXAS A&M UNIVERSITY

➢ Different Security Architecture:

- IT network servers reside at the center and require more protection than edge nodes.

- For power automation system networks, the EMS is at the center but the edge nodes (RTUs, IEDs…) require same level of protection.

Security Differences between Smart Grid and IT systems

TEXAS A&M UNIVERSITY

➢ Different Technology Base:

- For IT networks, Windows, Unix, and Linux are widely used while Ethernet connects devices with IP-based protocols

- In power systems, vendors use proprietary operating systems and networks, and also many different communication protocols (DNP, ICCP…)

Security Differences between Smart Grid and IT systems

TEXAS A&M UNIVERSITY

➢ Different QoS Requirements:

- For IT networks, even though data volume is high, moderate tolerance exists for delay of data exchange. Occasional failures are not as strict as in power systems.

- In power systems, such delays are not tolerated and rebooting the system is not an option.

Challenges to Develop New Security for Smart Grid

- Many components are designed for performance, not security.
- Existing communication between devices was implemented without consideration of cyber security.
- Ability to integrate newly developed security solutions into existing legacy system.
- Allow for new requirements for data communication: bandwidth, delay of data transfers, and new protocols

Proposed Security Framework Design Criteria

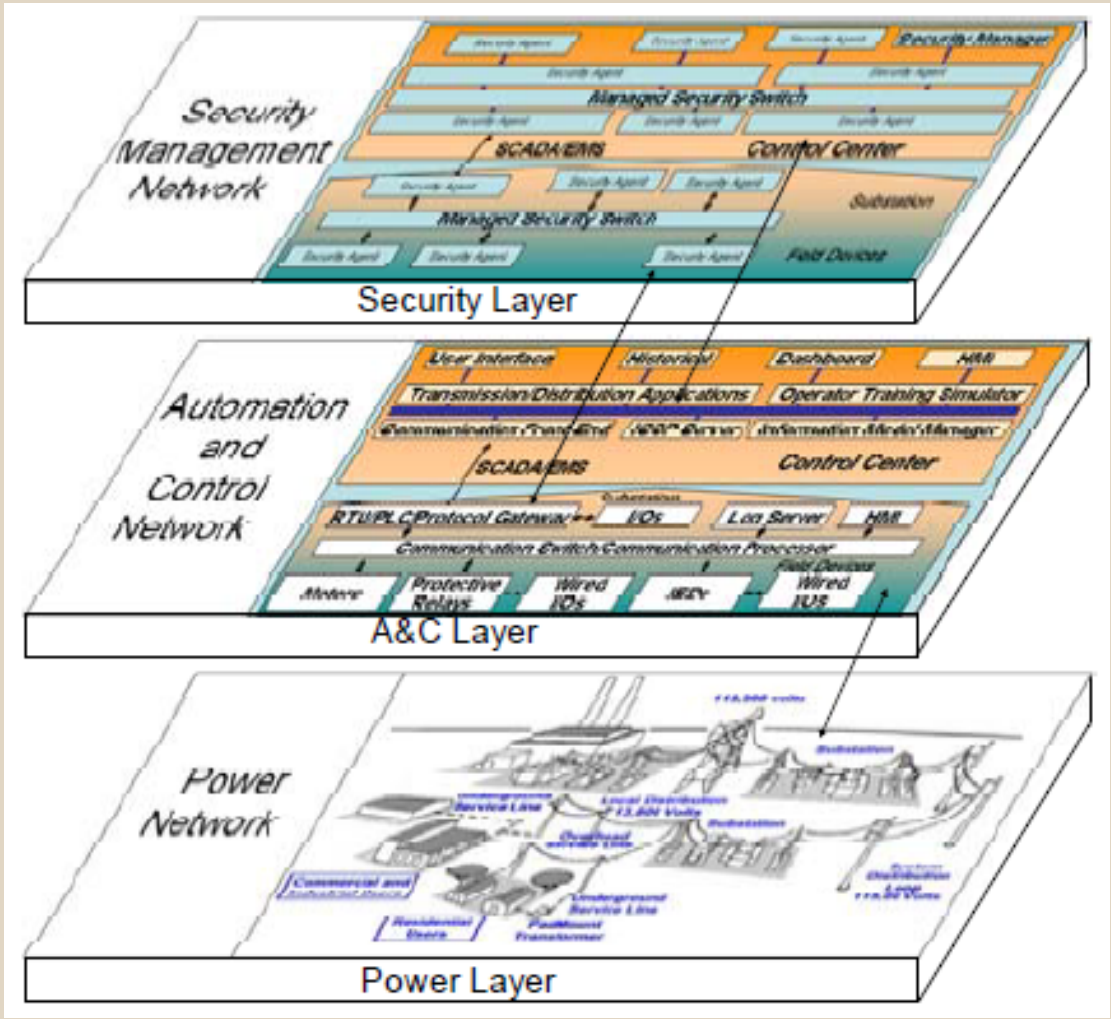
- Scalability: in order to maintain the same level of growth experienced by the power grid.
- Extendibility: such that the proposed solution can handle any future state of the power grid.
- Integration: new security melds with existing systems in non-intrusive manner without compromising control performance, reliability, stability, and availability.

Proposed Smart Grid Security Framework

TEXAS A&M UNIVERSITY

- An integrated security framework with 3 layers:
  - Power System
    - Power equipment and lines
  - Automation and Control
    - Monitors and controls transmission and distribution processes
  - Security
    - Provides clear demarcation of responsibilities

Proposed Smart Grid Security Framework



3-layered power transmission and distribution system[1]

Integrated Security Framework

- New solutions should be able to integrate security management (authorization, authentication), security operations (logging, auditing), and other security technologies (access control, intrusion) into the current standard security services.

- Integrated security framework consists of 3 major components
  - Security agents
  - Managed security switch
  - Security manager

Integrated Security Framework

Security Agents

- Extend security to system edges by providing protection at networked device level.
- Security agents only pass data packets whose information matches the ones in the access control list, and blocks all the rest.
- Its functions:
  - Translate between different protocols
  - Acquire and run latest vulnerability patches from security manager
  - Run host-based intrusion detection
  - Detect and send alarm messages to security manager
  - Encrypt and decrypt exchanged data

Integrated Security Framework

➢ Managed Security Switch

- Used across automation network to protect bandwidth and prioritize data.

- Its functions:
  - Run as a DHCP server (Dynamic Host Configuration Protocol)
  - Manage multiple VLANs
  - Run simple network-based intrusion detection
  - Provide QoS for data flow
  - Separates data by priority

Integrated Security Framework

➢ Security Manager

- Reside in the center of the power grid automation network and can be protected by existing IT security solutions.
- Able to connect to vendor servers and managed switches using VPN.
- Its functions:
  - Collect security agent information
  - Manage keys for VPN
  - Works as authentication, authorization, accounting server
  - Runs complex intrusion detection algorithms

Testing

- Small scale test carried out at Idaho National Laboratory (INL)
- Simplified power grid automation system was built; using penetration tests, all vulnerabilities were found and their respective impacts recorded.
- Proposed security framework then installed and same vulnerability penetration tests performed.

Test Results

- Security components do not impact SCADA communication in terms of extra delay on data exchange and bandwidth usage
- Some vulnerability is mitigated
  - Port scanning
  - Unused open ports
- Some vulnerability is partially mitigated
  - Flooding-based DoS attacks
- IDS mechanism reports some intrusion
  - Brute force key cracking
  - Access control violation
  - Flooding-based DoS

Summary

- Good job of differentiating IT system security with that required by power automation systems.
- Clear demarcation of security responsibilities.
- Test performed on legacy systems.
  - More tests need to be done with smart meters and other newer devices built with the smart grid in mind

References

- [1] D. Wei, Y. Lu, M. Jafari, P. Skare and K. Rohde, "An Integrated Security System of Protecting Smart Grid against Cyber Attacks," *Proc. Innovative Smart Grid Technologies (ISGT)*, Gaithersburg, Maryland, January 2010.

- [2] D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, and Michael Muller, "Power Infrastructure Security: Fundamental Insights of Potential Cyber Attacks and Their Impacts on the Power Grid," *Part of Project "Protecting Intelligent Distributed Power Grids against Cyber Attacks" for DOE.*

- [3] Sam Clements and Harold Kirkham, "Cyber-Security Considerations for the Smart Grid," *IEEE Power and Energy Society General Meeting*, July 2010, pp 1-5.

Thank You

TEXAS A&M UNIVERSITY

?