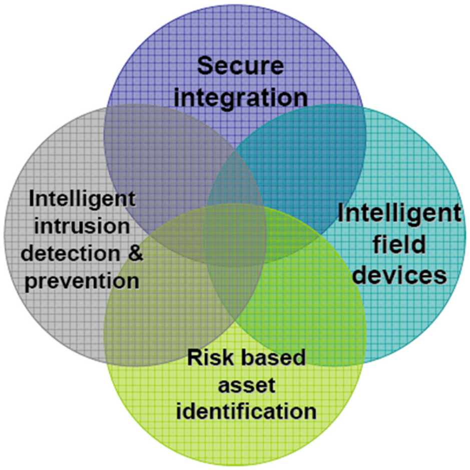
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Protecting Intelligent Distributed Power Grids Against Cyber Attacks

Development of a novel distributed and hierarchical security layer specific to intelligent grid design

Intelligent power grids are interdependent energy management systems—encompassing generation, distribution, IT networks, and control systems—that use automated data analysis and demand response capabilities to increase system functionality, efficiency, and reliability. But increased interconnection and automation over a large geographical area requires a distributed and hierarchical approach to cyber security.

This two-year project will develop three security components unique to intelligent power grids. The first is an automated risk assessment graph of the physical grid that, using advanced simulation and machine-learning capabilities, identifies threats and dynamically evolves based on simulation exercises and attack history.


Secure integration
Intelligent intrusion detection & prevention
Intelligent field devices
Risk based asset identification

The project team will then develop a hierarchical power grid security system, consisting of: security agents residing in or next to field devices and controllers; security switches at the substation control level; and security managers distributed across the grid at the enterprise layer. Security agents perform simple logging, reporting, and detection, while switches manage data traffic and detect intrusion using network rules. Security managers will be capable of generating new policies and updating existing ones based on simulation and historical information. These advanced managers connect to switches and agents, work as AAA (authentication, authorization, and accounting) servers, and acquire security patches and distribute them to control system components.

Finally, researchers will build a network topology optimizer, a model that determines the best location for agents, switches, and security managers. These technologies will ensure that each device, across the grid, actively contributes to network security. This distributed, hierarchical approach offers an unmatched security solution for advanced power grids.

National SCADA Test Bed

Benefits

- Protects components across a wide geographical area
- Ensures every intelligent node is responsible and aware
- Uses machine-learning and simulation to create an adaptive and evolutionary risk assessment graph
- Creates a distributed, hierarchical security layer encompassing enterprise systems, substation controllers, and field devices
- Distributes security devices to most critical assets based on system need
- Works with both legacy and open-source systems
- Identifies cyber attacks at the earliest stages and as far as possible from critical assets

Partners

- Siemens Corporate Research
- Center for Advanced Energy Systems at Rutgers University
- Idaho National Laboratory

Technical Objectives

Before beginning, the project team will assemble a technical advisory board with representatives from the power industry to guide R&D throughout. The three components will be created in two phases:

Phase 1: Design and Develop

- Investigate impact of cyber attacks in power control networks
- Analyze functional requirements of selected power grid networks
- Develop the risk-based critical asset identification system, including models and algorithms
- Create conceptual designs for security agents, security switches, and security managers
- Detail design specifications and develop models and algorithms specific for control networks in intelligent power grid systems

Phase 2: Test and Verify

- Conduct preliminary testing and verification of prototyped software for risk analysis and security configuration optimization
- Conduct two test rounds at Idaho National Laboratory on security agent, security switch, security manager, and security integration configuration software
- Develop technical reports summarizing tests and verification for security solutions
- Develop educational materials for a graduate seminar course to be taught at Rutgers University
- Establish commercialization strategies

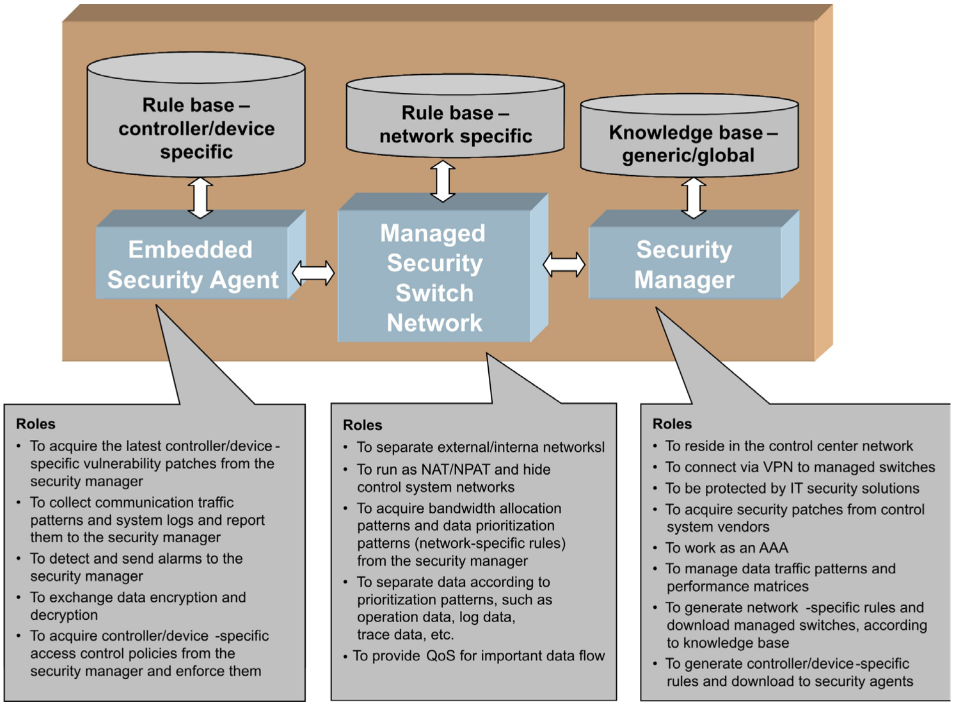
End Results

Project deliverables include:

- Critical asset risk evaluator software prototype
- Run-time and engineering software for security agents, switches, and managers
- Security layer optimization software prototype
- Technical reports and specifications for each device
- Educational materials for graduate course at Rutgers University

At the conclusion of the project, software and firmware prototypes will be available. The project team will work to establish general guidelines for future product development and commercialization.

The technology will become increasingly valuable as power suppliers begin converting to intelligent power grid networks, increasing system connection throughout the power grid and to the end user.


Rule base – controller/device specific
Rule base – network specific
Knowledge base – generic/global
Embedded Security Agent
Managed Security Switch Network
Security Manager

Roles

- To acquire the latest controller/device - specific vulnerability patches from the security manager
- To collect communication traffic patterns and system logs and report them to the security manager
- To detect and send alarms to the security manager
- To exchange data encryption and decryption
- To acquire controller/device -specific access control policies from the security manager and enforce them

Roles

- To separate external/interna networksl
- To run as NAT/NPAT and hide control system networks
- To acquire bandwidth allocation patterns and data prioritization patterns (network-specific rules) from the security manager
- To separate data according to prioritization patterns, such as operation data, log data, trace data, etc.
- To provide QoS for important data flow

Roles

- To reside in the control center network
- To connect via VPN to managed switches
- To be protected by IT security solutions
- To acquire security patches from control system vendors
- To work as an AAA
- To manage data traffic patterns and performance matrices
- To generate network -specific rules and download managed switches, according to knowledge base
- To generate controller/device-specific rules and download to security agents

May 2008

DOE National SCADA Test Bed (NSTB)

NSTB is a multi-laboratory resource that partners with industry and other government programs to test, research, and help design cyber security solutions to enhance control systems security in the energy sector and reduce the risk of energy disruption due to cyber attack.

For More Information:

Hank Kenchington
Program Manager
DOE NSTB
202-586-1878
henry.kenchington@hq.doe.gov

Dr. Dong Wei
Siemens Corporate Research
609-734-3525
dong.w@siemens.com

Visit Our Website:

www.oe.energy.gov/control security.htm