DOE/OE-0010

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

Padlock

Commercialization of a low-cost, low-power Ethernet security gateway for securing field devices

Background

Unlike generation and transmission networks, electricity distribution networks usually involve a small number of devices (attached to a pole or cabinet) located outdoors in populated areas that control the power and increasingly communicate to a concentrated point such as a substation or control center.

As distribution networks integrate a growing number of automation and communication components, there is greater potential for an unauthorized user to electronically or physically compromise a field device and then exploit the communication infrastructure to expand cyber access through the system.

Barriers

- Distribution system architectures are widely distributed and use a variety of communication media types and products
- Complexity increases exponentially with an increase in the number of nodes
- Field devices can be physically compromised and exploited, enabling cyber access to an upstream substations or control room
- Security solutions must be able to be applied to existing field installations

Project Description

This project will develop the Padlock security gateway, a commercial solution to help protect field device communications and sense physical tampering in order to enhance cyber and physical security at the distribution network level.

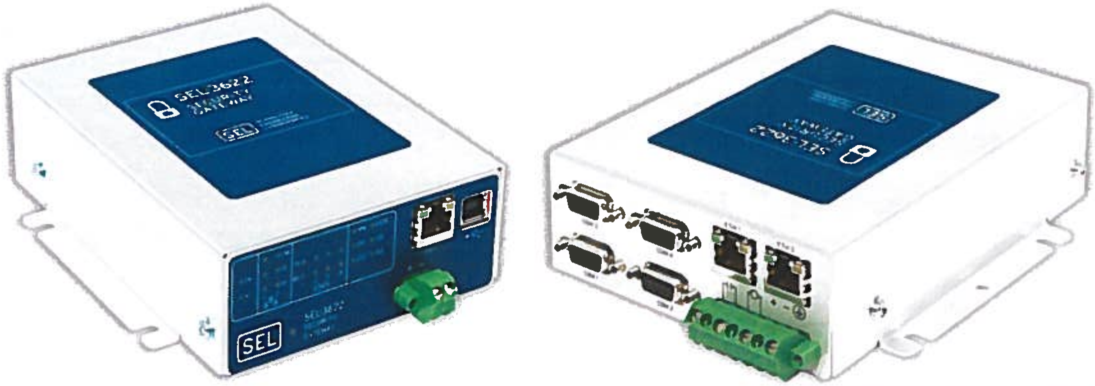
The low-power, low-cost Padlock Gateway will establish encrypted communication between central stations and field devices while enabling strong access controls, logging and secure communication with transparent access to the serial port of the existing energy system protection device. The Padlock gateway also serves as a demarcation point between electronic security perimeters.

Benefits

- Permits encrypted communication between central stations and field devices that support the Electronic Security Perimeter requirements of North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards
- Provides strong user-based access controls, logging and secure communication
- Produces a low-power, low-cost, interoperable solution
- Senses physical tampering to field device and takes cyber actions to prevent escalation of intrusions

Partners

- Schweitzer Engineering Laboratories
- Sandia National Laboratories
- Tennessee Valley Authority



Technical Objectives

The project will build on the technical foundation of the Schweitzer Engineering Laboratories (SEL) 3620 Ethernet Security Gateway developed under the Lemnos project for interoperable and robust substation cybersecurity.

Padlock will build a small low-power hardware platform, combine it with the SEL-3620 firmware, and advance the functionality by integrating physical tamper awareness with appropriate cyber responses. This new hardware platform is designed to secure SCADA, engineering access and real-time protection communications. The Padlock product will be developed in two phases.

August 2012

Phase 1: Research and Development

- Research and develop for commercialization a control system hardened Distribution Automation Security Gateway with the ability to identify physical and logical intrusions

Phase 2: Testing and Demonstration

- Laboratory test, field test and demonstrate the technology in real-world control system installations and prepare best practice guides for testing, deployment and long-term management of the technology

End Results

Project results will include:

- A small, low-cost low-power Ethernet Security Gateway designed to be installed in field cabinets with the ability to bridge the physical-cyber worlds
- Ability to upgrade distribution communications to use powerful cryptographic technology between a central station and field devices, establishing user access controls and audit trails that support NERC CIP compliance efforts
- Distribution networks that provide monitoring capabilities and near real-time logging of cyber and physical events
- Cyber controls preventing a physically compromised site from expanding access to upstream sites
- Enabling security architectures that allow asset owners freedom to install electronic devices close to large assets without security or compliance concerns

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) R&D Program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks.

For More Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Rhett Smith
Development Manager
Schweitzer Engineering Laboratories
509-336-7939
rhett_smith@selinc.com

Visit Our Website:

http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity