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

Hallmark Project

Commercialization of the Secure SCADA Communications Protocol, a cryptographic security solution for device-to-device communication

Increased connectivity and automation in the control systems that manage the nation's energy infrastructure have improved system functionality, but left systems more vulnerable to cyber attack. Intruders could severely disrupt control system operation by sending fabricated information or commands to control system devices. To ensure message integrity, supervisory control and data acquisition (SCADA) systems require a method to validate device-to-device communication and verify that information has come from a trusted source and not been altered in transit.

The Secure SCADA Communications Protocol (SSCP) provides message integrity by marking original SCADA messages with a unique identifier and authenticator before sending. The receiving device will scan the identifier and validate the message before enacting the command. Unauthenticated commands are logged and reported as errors.

Over three years, the project team will implement this technology as a cryptographic daughter card (CDC), a hardware solution that Schweitzer Engineering Laboratories (SEL) will incorporate into a serial bump-in-the-wire device. This device can be applied easily to any legacy or existing control system without equipment reconfiguration or reprogramming. The team will validate the card under Federal Information Processing Standard (FIPS) 140-2, which accredits cryptographic technology. The CDC will also be available to other vendors, who can use it to increase security by adding cryptographic controls to both existing and future products.

The solution supports any byte- or bit-oriented protocol and will add only minimal latency. Current technologies in the market offer message confidentiality by encrypting text upstream of modem-sharing devices; this eliminates the operational ability of skilled personnel or protocol analyzers to read messages, and is often a vendor-specific technology. SSCP technology offers a standard approach to message authentication without encryption.

National SCADA Test Bed

Benefits

- Provides message integrity and authentication
- Can easily be incorporated into legacy and new control system designs
- Establishes secure serial communication
- Introduces minimal communication latency
- Allows protocol analyzers to read unauthenticated messages

Partners

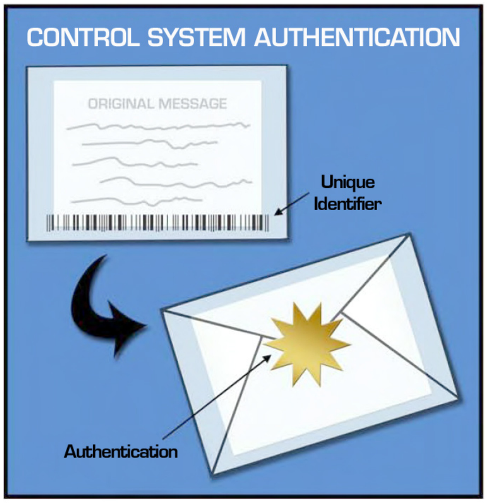
- Schweitzer Engineering Laboratories Inc.
- Pacific Northwest National Laboratory
- CenterPoint Energy

The CDC will be incorporated into a bump-in-the-wire link module, expanding SEL's current commercialized and FIPS 140-2-validated product line (SEL-3021) of serial cryptographic transceivers.

Technical Objectives

Phase 1: Development of CDC and Integration into Link Module

- Establish method to transfer Secure SCADA Communications Protocol (SSCP) technology to the cryptographic daughter card (CDC) hardware component
- Translate the SSCP technology into a protocol-independent CDC
- Develop the CDC into a new bump-in-the-wire link authenticator module, expanding the SEL-3021 Serial Encrypting Transceiver product line
- Commercially produce and test the product at SEL's facilities



The graphic illustrates the device's ability to authenticate each message and validate the unique identifier before enacting the message command.

Phase 2: Lab and Field Testing

- Conduct a laboratory test of the link module (with integrated CDC) at CenterPoint Energy's test energy management system
- Measure control system and operator impact and communication latency
- Perform a two-month field test at CenterPoint Energy to demonstrate interoperability and identify lessons learned from an asset owner's perspective
- Compile extensive reports analyzing: impact to the end user; impact to the control system; and best practices for implementing this new technology
- Achieve FIPS 140-2 validation

End Results

SSCP technology will be available as:

- A hardware daughter card that runs on a micro-controller platform (other vendors may purchase only this to incorporate into their own products)
- A bump-in-the-wire link module (incorporating the CDC), embedded between the input/output (I/O) server and its communication ports

Document deliverables include:

- A control system impact report
- An end-user impact report
- A best practices guide for implementing the new technology into existing control system environments

Next Steps:

The CDC will be available for use by any vendor and all federal and private organizations.

SEL plans on commercializing and honoring a 10-year warranty for its bump-in-the-wire link module. It can easily be incorporated into all legacy, existing, and new control system designs.

March 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

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

Visit Our Website:

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