Hallmark Cryptographic Serial Communication

A cryptographic card and link module integrating the Secure SCADA Communications Protocol to provide secure serial communications for existing and new energy control systems

A cost-shared effort between industry and

U.S. DEPARTMENT OF ENERGY | Cybersecurity, Energy Security, and Emergency Response

Cyber Security for Energy Delivery Systems

Hallmark Cryptographic Serial Communication

Project Lead:
Schweitzer Engineering Laboratories

Partners:
Pacific Northwest National Laboratory
CenterPoint Energy Houston Electric

The Concept

Energy sector asset owners can safeguard serial SCADA communications between remote devices and the control center using the Secure SCADA Communications Protocol (SSCP). The protocol enables receiving devices to identify and authenticate the engineer requesting access, providing secure serial engineering access communications, like dial-up, with a focus on strong access control. Because the SSCP is protocol independent, this technology secures all legacy and new control systems designs.

The Approach

By uniting a national laboratory, asset owner, and vendor, the Hallmark team gained the expertise and resources necessary to develop, test, and rapidly commercialize a solution to secure serial communications reliably and economically. This successful approach began with the development of the SSCP, and has resulted in two commercialized products aimed at vendors and asset owners:

Secure SCADA Communications Protocol (SSCP)
Developed by Pacific Northwest National Laboratory (PNNL), the Secure SCADA Communications Protocol (SSCP) ensures control system data integrity through message authentication and optional encryption. It marks original messages with a unique identifier and authenticator; the receiving device will then scan the identifier and validate the message, ensuring that the information comes from a trusted source and has not been altered in transit. Unauthenticated commands are logged and reported as errors. The Hallmark team has successfully tested that this security protocol protects SCADA as well as engineering access communications.

Cryptographic Card (SEL-3045), aimed at original equipment manufacturers (OEMs), is an electronic hardware card that runs the SSCP. Control systems security OEMs can use the Cryptographic Card to jumpstart R&D to use the SSCP in building secure serial communication in their commercial products. The daughter card confidently provides interoperability and security assurance with Federal Information Processing Standard (FIPS) 140-2 Level 2 validated cryptography. The Hallmark team designed, developed, and tested the software and hardware functionality. OEMs can also access the hardware and software code libraries.

The Bump-In-The-Wire Link Module (SEL-3025), available to control systems asset owners, is the first hardware and firmware platform that integrates the SSCP cryptographic card to secure serial communications. The SEL-3025 adds only minimal latency while securing existing equipment and serial communication links, including dial up, radios, leased line, or most any serial communication network. As new products that support SSCP are developed, a forklift upgrade of all equipment is unnecessary; the SEL-3025 Link Module provides that transition by translating the secure serial communications for the legacy device.

Benefits

- Establishes secure serial communications by providing data integrity and message authentication
- Introduces minimal communication latency
- Easily incorporates into existing and new control system designs
- Offers OEMs flexible options to use the SSCP to develop secure serial products: reference design, code libraries, or FIPS-validated Cryptographic Card

The Commercialized Solution

The SEL-3025 Link Module and SEL-3045 Cryptographic Card, when available, will enable assets owners to secure existing and new control system designs across the energy infrastructure. Successful interoperability tests performed on the Link Module and Cryptographic Card prototypes have proven that multiple products are able to communicate and establish a secure communication using the SSCP.

The Hallmark team has worked closely with CenterPoint Energy, an end user and asset owner, to identify testing locations in CenterPoint's test energy management system. CenterPoint has also guided the team in providing a simple, manageable, and scalable deployment method.

Next Steps

The Hallmark team will perform field tests to validate physical and technical requirements at CenterPoint Energy. After testing is complete, the team will develop reports analyzing the impact of the technology on the control system and the end user. SEL will release the Link Module and Cryptographic Card in June 2010.

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads
Carol Hawk, Program Manager

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

Mark Hadley
Pacific Northwest National Laboratory
509-375-2298
mark.hadley@pnl.gov

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov