

Control System Authentication

Secure SCADA Communications Protocol

The Secure SCADA Communications Protocol (SSCP) is designed to secure serial control system communication through the use of symmetric key cryptography. The SSCP secures control system communication by encapsulating the original message with a header and authenticator. Two symmetric session keys are used to provide message authentication. The cryptographic key of the message originator is used to create a nonce that provides a unique value for the packet. The cryptographic key of the message recipient is used by a secure hash algorithm to calculate a hashed message authentication code based upon the header, nonce, and original message. In order to ensure perfect forward secrecy, each pair of communicating devices utilizes a Diffie Hellman method to generate ample cryptographic key material for authentication and encryption keys.

The operation of our nation's critical infrastructure—electricity, gas/oil, water/waste water, chemical, transportation, etc.—increasingly relies upon the use of control systems. These control systems were traditionally implemented with availability and personnel safety as primary considerations; security was an afterthought. With recent terrorist events still fresh in our memories, the lack of cyber security in control systems is of grave concern.



PROBLEM DOMAIN

- » Predictable
- » Vulnerable to attack
- » Does not ensure data integrity

SOLUTION

- » Authenticate communication
- » Utilize a unique identifier and authenticator for each communication

PNNL APPROACH

- » Develop technology with commercialization in mind
- » Form internal team comprised of multiple disciplines
- » Use an industry advisory board to guide efforts

WHY THIS SOLUTION IS BETTER

- » Integrity provides trusted communication
- » Availability supports operational requirements
- » Fewer points of failure due to embedded software
- » Lower cost to deploy than “bump in the wire” solutions
- » Integrates with traditional log analysis environments
- » Original message is left intact

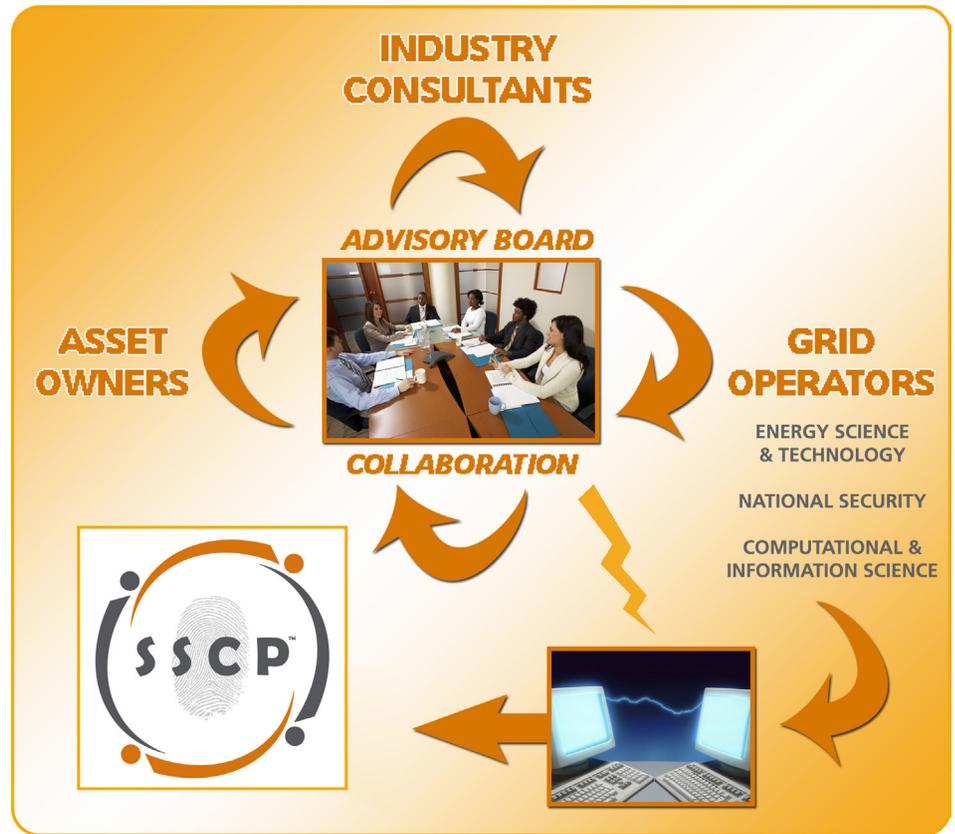
INDUSTRY COLLABORATORS

- » Schweitzer Engineering Laboratories(Hallmark Project)
- » Siemens
- » PNNL modified WireShark

Pacific Northwest National Laboratory draws upon vast industry relationships to form advisory boards to guide research the market will accept. One outcome of this collaborative research model is the Secure

SCADA Communications Protocol (SSCP) technology. This technology builds trust into Control Systems, allowing for the identification of malicious traffic and appropriate response without the use of encryption.

COLLABORATIVE DEVELOPMENT



For more information, contact:

Mark Hadley

Pacific Northwest National Laboratory

Mark.Hadley@pnl.gov



NSTB
National SCADA Test Bed


Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965