U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

Mark Hadley

Pacific Northwest National Laboratory (PNNL)

SSCP Commercialization

PNNL-SA-73897

Summary Slide: SSCP Commercialization

- **Outcomes:** Scalable, cost-effective methods to secure communication between remote devices and control centers.
- **Roadmap Challenge:** Poorly designed connection of SCADA and business networks can dramatically increase vulnerabilities of control systems.
- **Major Successes:** The task team provided Cisco with multiple SSCP implementation guidance sources and resources. The team also developed a protocol specification that describes deploying SSCP security objectives for routable control system communication.

- **Schedule:** Routable Protocol Specification, Implementation Guidance, Hallmark
- **Level of Effort:** $575k
- **Funds Remaining:** $287K
- **Performers:** PNNL
- **Partners:** SEL, CNP, Siemens, Industry Advisors, RTI, IBM, Cisco

Technical Approach and Feasibility

- **Approach**
  - Work with vendors to incorporate the SSCP into routers, network switches, gateways, and middleware products
  - Explore integration of SSCP security objectives in routable communication
  - Define a new “Routable SSCP”
  - Develop conformance and interoperability testing tools for routable protocol implementations
  - Work with standards bodies (IEEE, IEC) to make the SSCP an industry standard

Technical Approach and Feasibility

- **Approach**
  - Incorporate the SEL-3045 Cryptographic Daughter Card (CDC) into a product from another vendor
  - Create a PC-based key management solution for the CDC. The ability to manage keys is supported by the SSCP and is also a requirement for industry adoption and deployment of the SSCP. PNNL will provide security and interoperability testing of the key management application.
  - Support a second field test of the SSCP, preferably with a small electric utility or a utility in the oil and gas industry

Technical Approach and Feasibility

- **Metrics for Success**
  - Develop routable SSCP specification
  - Develop conformance and interoperability testing tools
  - Integrate SSCP-supporting CDC into third-party product
  - Provide SSCP key management solution
  - Complete second SSCP field test

Technical Approach and Feasibility

- **Challenge to Success**
  - Routable solutions (e.g., TLS) exist
    - Define security solution specific to control systems communication and security requirements – hence the new SSCP Routable Specification
  - Industry buy-in
    - Vendor participation
    - Standardization of SSCP

Technical Approach and Feasibility

- **Technical Achievements to Date**
  - Created routable SSCP specification
  - Provided vendors with SSCP implementation guidance
  - Working with IEEE 1711 co-chairs on convergence
  - Working with RTI for SSCP gateway design
  - Expanding SSCP to other industries

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Make the SSCP an industry standard
  - SSCP currently has momentum with commercial products available
  - Competing efforts – convergence required for legacy and embedded products
  - Focus on interoperability and security
- **Plans to transfer technology/knowledge to end user**
  - Target embedded system integration
  - Continue support of Hallmark project
  - Operational support
    - Protocol analyzer and test set products
    - Deployment guidance documents

Next Steps

- **Approach for the next year**
  - Complete current technology transfer efforts
  - Continue to explore making the SSCP an IEEE and/or IEC standard
  - Become an IEEE Compliance Institute validation entity for SSCP
  - Develop testing tools and functional prototype of routable SSCP