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

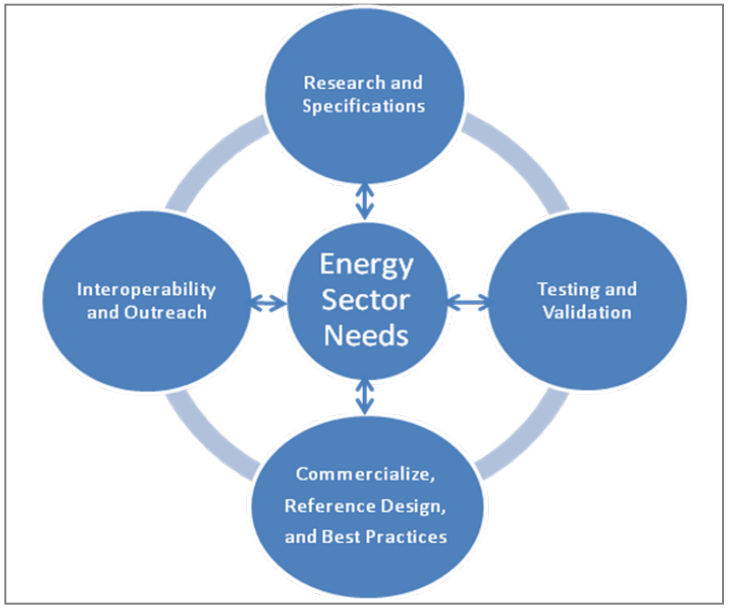
Brian Smith

EnerNex

Lemnos Interoperable Security

Summary Slide: Lemnos Interoperable Security

- **Outcomes:** Energy asset owners can better evaluate product functions, purchase, and install products supporting cyber security functions from multiple vendors knowing they will be interoperable
- **Roadmap Challenge:** Vendors do not have specific requirements or standards to build to
- **Major Successes:**
  - IPsec & Syslog protocols
  - Lab Testing & Public Plug-fests
  - Commercial product release (SEL)



- **Schedule**: Centralized Authentication, Secure Remote Access, and Syslog in 2010
- **Level of Effort: $**1.24M (2010)
- **Performers:** EnerNex
  Tennessee Valley Authority
  Sandia National Laboratories
  Schweitzer Engineering Laboratories

Technical Approach and Feasibility

- **Approach**

STEP 1 Define functional requirements based on asset owner needs

STEP 2 Select open source specifications (IETF RFCs) to meet the identified functional requirements

STEP 3 Develop interoperable configuration profiles for these specifications tailored for the energy sector control systems environment

STEP 4 Test and validate the interoperable configuration profiles

Technical Approach and Feasibility

- **Metrics for Success**

STEP 1 Verify commercial product against SNL reference implementation using the parameters specified in the Interoperable Configuration Profile

STEP 2 Validate that the configuration supports the utility control system environment

STEP 3 Verify interoperability between multiple commercial products using the parameters specified in the Interoperable Configuration Profile

Technical Approach and Feasibility

- **Challenges to Success**
  - Tailoring the work to support a utility control system environment
    - Looking at the use cases
    - End user testing
- **Technical Achievements to Date**
  - IPsec & Syslog protocols addressed in 2008/2009
  - Lab Testing at TVA (July 2009)
    - SNL, SEL AND 5 additional vendors
  - Public Plug-fests at ISA Expo (2009) & Distributech (2010)
  - Commercial product release by SEL (December 2009)

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Additional vetting of Interoperable configuration profiles
    - Additional “Participating” Vendors
    - Validates vendor neutrality
- **Plans to transfer technology/knowledge to end user**
  - Transfer stewardship of work completed by the project to the OpenSG Committee of the UCA International Users Group
    - Task Force under the SG Security Working Group created aimed at cyber security interoperability
  - Both vendors and utilities benefit

Next Steps

- **Approach For the Next Year**
  - Interoperable Configuration Profiles for:
    - Centralized Authentication
      - LDAP
      - Support BES asset owners NERC CIP efforts
    - Secure remote access (device to remote user)
      - SSH
      - Compliments the IPsec work (network to network)

Next Steps

- **Approach For the Next Year (continued)**
  - Syslog message standardization
    - Must address both RFC 3164 and RFC 5424
    - challenge to asset owners is that the contents of the Syslog messages is not standardized and typically varies by vendor and device
    - Utilize work from Quickdraw project (Digitalbond) to help identify events

Next Steps

- **Approach For the Next Year (continued)**
  - End User testing
    - Additional utility added as “Project Partner” for broader range of end user testing
  - Plug-fest
    - Additional “Participating Vendors” added in vetting and plug-fest efforts
  - Outreach
    - Continue support of OpenSG efforts
      - CyberSec Interop Task Force