Lemnos Interoperable Security

A capability based on open-source specifications - demonstrated in a vendor product - that enables secured interoperability among energy control systems devices

A cost-shared effort between industry and

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

Cyber Security for Energy Delivery Systems

Lemnos Interoperable Security Program

Project Lead:
EnerNex Corporation

Partners:
Sandia National Laboratories (SNL)
Schweitzer Engineering Laboratories (SEL)
Tennesse Valley Authority (TVA)

Other Participating Vendors:
Industrial Defender
GarrettCom
Phoenix Contact
N-Dimension Solutions
Siemens
RuggedCom

The Concept

The Lemnos Interoperable Security Program began with one logical concept: If vendors develop control systems security products using an agreed-upon set of capability and operational requirements, energy asset owners can better evaluate product functions and purchase products from different vendors knowing they will be interoperable. Three years later, the Lemnos team developed those specifications—called interoperable configuration profiles—and one of the first products built to those profiles is in the market.

The Result

By developing and publishing interoperable configuration profiles for security products, Lemnos has made it possible for vendors to develop interoperable solutions - and they have built and tested commercial and proof-of-concept products that successfully demonstrate the approach. Aimed at energy control systems security products, Lemnos took four steps:

1. Defined functional requirements based on asset owner needs
2. Selected open-source specifications to meet the identified functional requirements.
3. Developed interoperable configuration profiles for these specifications tailored for the energy sector control systems environment.
4. Tested and validated the interoperable configuration profiles.

Lemnos work enables utilities and vendors to clearly communicate user needs, product features, and configuration parameters of control systems cyber security products. With extensive industry and government collaboration, Lemnos quickly brought R&D from a national laboratory into a commercially available, tested solution.

The Approach

Open PCS Architecture for Interoperable Design (OPSAID)

SNL
Created an interoperable security architecture for common process control system add-on security devices. Developed a reference implementation using open-source software and standardized hardware.

Funding: Originally funded internally at SNL, then funded by the Department of Energy's NSTB Program in 2006-2007.

Lemnos Interoperable Security Program

EnerNex
Developed interoperable configuration profiles and testing procedures for common security offerings (defined in OPSAID). Used TVA needs to determine the most valuable security features to demonstrate.

SEL and SNL
Independently developed counterparts of two security offerings—a VPN tunnel and logging capability. SEL developed a commercial prototype, while SNL developed a reference implementation using open-source software. After individual performance testing, the independent teams connected their devices—via the Internet and within the TVA lab—to demonstrate interoperability.

TVA
Provided SNL/SEL a utility testing environment and facilitated testing with other vendor devices.

Funding: EnerNex and participants cost-shared with a competitive DOE Financial Assistance Award in 2008-2010.

Commercialization

SEL
In December 2009, SEL released the SEL-3620 Ethernet Security Gateway, demonstrating that the Lemnos approach results in a scalable, robust, and interoperable security solution. The gateway secures routable protocols crossing electronic security perimeters and provides security logging in an easy-to-use Lemnos interoperable manner.

The Commercialized Solution

SEL-3620 Ethernet Security Gateway
As part of the Lemnos project, SEL developed a hardened security device for the energy sector built to the interoperable configuration profiles and testing procedures created by the Lemnos team. SEL rigorously tested the solution for functionality and security robustness, then tested it for interoperability by connecting it to SNL's independently developed reference implementation, and to other products from participating vendors.

Features:
SEL's solution, tailored specifically to secure smart grid communications, is now on the market. The Ethernet Security Gateway protects systems from malicious traffic with a configurable firewall and provides strong access control in and out of the electronic security perimeter with Lemnos interoperable VPNs. It additionally provides Lemnos interoperable security event reporting and precise time tagging of events through Syslog.

Now Available:
For more information on the features, benefits, and application of the Ethernet Security Gateway, visit http://www.selinc.com/SEL-3620/.

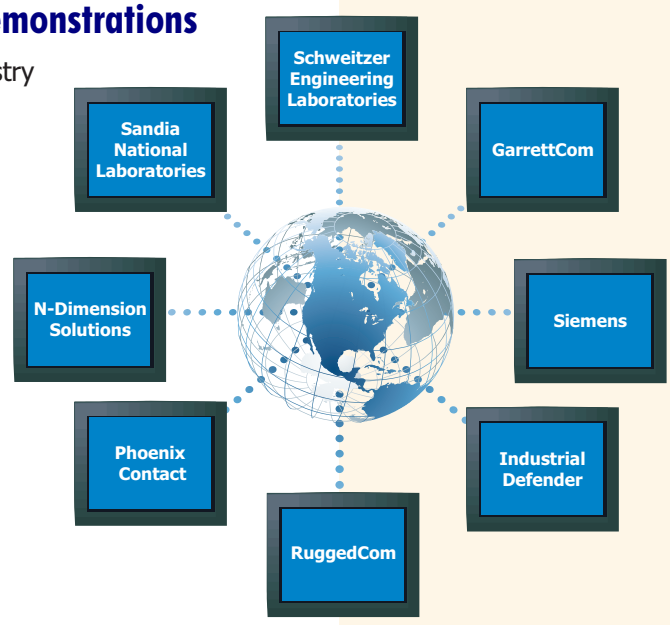
Benefits

- Published interoperable configuration profiles and testing procedures to guide vendor development
- Demonstrates, through interoperability testing, that building to universally accepted requirements is an effective way to achieve interoperability among solutions from different vendors
- Invites vendors to build and promote interoperable products
- Brings the first security device built to these requirements to market

Validating the Results: Interoperability Demonstrations

Through targeted outreach and presentations at industry events, the Lemnos team has cultivated interest from seven network security vendors in participating with Lemnos to build interoperability into their control systems solutions. To culminate the project, Lemnos researchers invited several of these vendors to demonstrate interoperability with the Lemnos product in public industry forums.

Vendors brought security solutions they developed against Lemnos requirements and connected them to the SNL reference implementation to test for product compatibility. The interoperability demonstrations have been performed at two public conferences to date.



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

Brian Smith
EnerNex Corporation
423-645-1214
brian@enernex.com

Ron Halbgewachs
Sandia National Laboratory
505-844-8054
rdhalbg@sandia.gov

Current Contactas of Aug. 2020

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