Cyber Security Interoperability - The Lemnos Project

Brian P. Smith, EnerNex
John Stewart, Tennessee Valley Authority
Ron Halbgewachs, Sandia National Laboratories
Adrian Chavez, Sandia National Laboratories
Rhett Smith, Schweitzer Engineering Laboratories
Dave Teumim, Teumim Technical

Keywords: Cyber Security, Interoperability, OPSAID, Interoperable Configuration Profiles, National SCADA Test Bed, NSTB

ABSTRACT

The energy sector is facing two major issues in securing control systems; 1) Cyber security is more important than ever before, and 2) Cyber security is more complicated than ever before. A key requirement for utilities and vendors alike in addressing these issues is interoperability. This paper introduces the Lemnos Interoperable Security Project, a multiyear DOE NSTB (National SCADA Test Bed) effort highlighting a security interoperability framework for communications supporting the energy sector[1]. Partners in the Lemnos project include EnerNex, Tennessee Valley Authority, Sandia National Laboratories, and Schweitzer Engineering Laboratories. It is built on the successes of OPSAID, a previous NSTB project. IPSec and Syslog are used in Lemnos for interoperable communication between security devices, and is expanding to use other popular Internet Protocols like LDAP and TLS/SSL. Lemnos partners and participating vendors produce "Interoperable Configuration Profiles" by consensus for Internet protocols and then verify the effectiveness of these profiles with comprehensive testing. This work is helping to foster the partnership between utilities and vendors by helping the two parties to clearly communicate user needs, product features, and configuration parameters relating to cyber security functions.

1.0 BACKGROUND

[1] Roadmap to Secure Control Systems in the Energy Sector, U.S. DOE and U.S. DHS, January 2006

The manner in which the energy sector is designing and operating control systems is undergoing some of the most significant changes in history due to the evolution of technology and the increasing number of interconnections to other systems. With these changes come two significant issues for the energy sector; 1) Cyber security is more important than ever before, and 2) Cyber security is more complicated than ever before. A key requirement in helping utilities and vendors alike in addressing these issues is interoperability. While interoperability has been present in much of the discussions relating to technology utilized within the energy sector and especially the Smart Grid, it has been absent in the context of cyber security.

1.1 CYBER SECURITY INTEROPERABILITY, NOT A NEW CONCEPT

In the *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, interoperability is defined as "The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user". [2] In theory, interoperability is possible with many of the cyber security solutions available to utilities today. The reality is that the effort required to achieve cyber security interoperability is often a barrier for utilities. For example, consider IPSec, a widely-used Internet Protocol to define Virtual Private Networks, or "tunnels", to communicate securely through untrusted public and private networks. The IPSec protocol suite has a significant number of configuration options and encryption parameters to choose from, which must be agreed upon and adopted by both parties establishing the tunnel. The exercise in getting software or devices from different vendors to interoperate is labor intensive and requires a significant amount of security expertise by the end user. Scale this effort to a significant number of devices operating over a large geographical area and the challenge becomes so overwhelming that it often leads utilities to pursue solutions from a single vendor which may inadvertently lock utilities into proprietary and closed systems. In other cases where equipment from multiple vendors is deployed, the robustness of the installed system may suffer by the fact that the solution is based on a least common denominator scenario dictated by the "weakest link in the chain".

1.2 LEMNOS IS ABOUT "*TACTICAL*" SOLUTIONS

[2] NIST Special Publication 1108 - NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, National Institute of Standards and Technology, January 2010

To better understand the focus of work being done within the Lemnos project, it is important to understand where it is applied to the problem space. The Lemnos work is aimed at providing lower level tactical solutions for specific needs identified by end user's and/or vendor's technology roadmap or other strategic efforts. Once the stakeholder navigates their way through one of many processes to determine their high level strategic picture, it will be left with a lower level set of requirements (i.e. "we need a secure communication channel between these two nodes" or "we need to support secure communication channel functionality in this device"). It is at this point is where the Lemnos work is applied. It is not intended to be prescriptive to the point of being used to define the utility's cyber security core functional requirements. The Lemnos work is instead intended to help the asset owners and vendors implement solutions to meet these requirements once they have been identified.

1.3 OPSAID

The work involved in the Lemnos project was built upon a foundation created by a previous NSTB project called Open PCS Security Architecture for Interoperable Design, or OPSAID. OPSAID was aimed at addressing technological, economic, and educational impediments to PCS owners implementing effective security on their systems by developing and testing an open source architecture for PCS security.

Sandia's work on the OPSAID project outlined an initial, high-level security functions as well as describing the initial OPSAID Component Modules (that implement the security functions). These OPSAID Component Modules formed the basis for the effort of the Lemnos project.

2.0 THE LEMNOS APPROACH

The ultimate output of the Lemnos work is artifacts referred to as *Interoperable Configuration Profiles* however the method to produce these profiles is just as important. The Lemnos work is formed around asset owner functional requirements relating to cyber security which means it is as much about the process as it is about the artifacts which it creates. By focusing the effort in this fashion, the process provides a linkage between these asset owner requirements and the technical solutions deployed to meet them by developing and publishing Interoperable Configuration Profiles for security products. Targeted at security products utilized within control systems deployed throughout the energy sector,

the approach taken by Lemnos to create the Interoperable Configuration Profiles covers four basic steps as show in Figure 1 that follows.

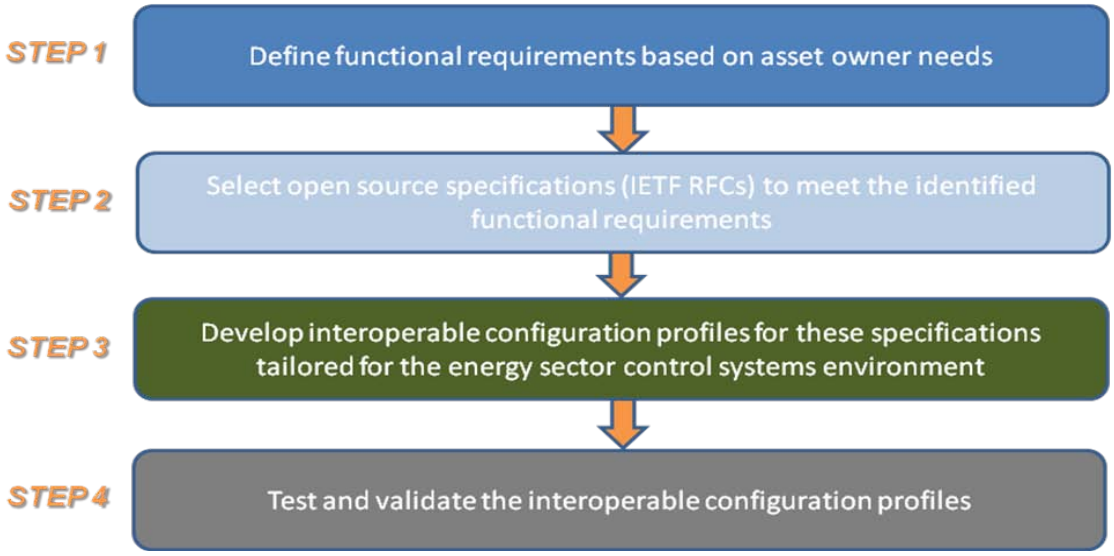

Figure 1 - The Lemnos Process

2.1 STEP 1 – DEFINE FUNCTIONAL REQUIREMENTS

The first step of the Lemnos process defines the problem in terms of core security functional requirements which may be needed by asset owners in various parts of their control system design. In short, we need to know what the problem is before jumping head first into solving it and risk missing the point altogether. It sounds simple but it's perhaps the most important step of the entire process. This step involves asking a set of binary questions. The subject either does something (performs a specific function) or it does not and there is no measurement involved. At the end of the step is a list of the core security functional requirements (i.e. the "problem") which can then be easily prioritized. For the initial Lemnos effort, numerous core functions were identified based on asset owner input as shown in Table 1that follows.

Table 1 - Core Security Functional Requirements

Core Security Functional Requirement
Secure communications channel *

Filter illegal network traffic
Notification, traceability, and troubleshooting *
Cryptography and password management
Detect malicious activity by monitoring network traffic
Monitor and analyze system processes

***** Selected for implementation in phase I of the Lemnos Project

In the end, phase I of the Lemnos project identified secure communications channel and notification, traceability, and troubleshooting as the highest priority items from the identified list of core security functional requirements.

2.2 STEP 2 – IDENTIFY OPEN SOURCE SOLUTIONS

The next step of the process takes each selected core security functional requirement and pairs it with a solution. For these solutions in the past, vendors may have developed their own proprietary solution or perhaps implemented a little known solution which did not effectively match the needs of the control systems environment. With Lemnos, the philosophy is to select the most commonly used, well-proven, open source solution for each requirement from within the IETF (Internet Engineering Task Force) library of RFC's (Request For Comments). For the two core security functional requirements identified in phase I of the Lemnos project, the selected solutions can be seen in Table 2 that follows.

Table 2 - Solutions for Identified Requirements

Functional Requirement	Component	Module
Secure communications channel	Virtual Private Network	IPsec (RFC 4301[3])
Notification, Traceability, Trouble Shooting	Audit Log	Syslog (RFC 5424[4]/3164[5])

[3] RFC 4301 - Security Architecture for the Internet Protocol, Internet Engineering Task Force, December 2005

[4] RFC 5424 – The Syslog Protocol, Internet Engineering Task Force, March 2009

[5] RFC 3164 - The BSD Syslog Protocol, Internet Engineering Task Force, August 2001

2.3 STEP 3 – INTEROPERABLE CONFIGURATION PROFILE DEVELOPMENT

If you are thinking that the decisions are over in step 2 of the process then think again. In reality, the selection of one or more IETF RFC's is just a starting point for many more decisions to come. Each RFC contains a myriad of choices that have to be made for implementation. Choices which cannot be made in a vacuum but which must be made with the supported utility applications and the underlying control system architecture in mind. By doing so, each Interoperable Configuration Profiles provide both a definition of cyber security interoperability and a minimum documented level of security for the targeted protocol(s). Table 3 illustrates a subset of parameters contained with the Interoperable Configuration Profile for IPsec.

Table 3 - Example Configuration Parameters for IPsec

Configuration Parameter
Use ESP (Encapsulating Security Payload)
Use TUNNEL mode
Use HMAC for authentication
Use IKE Version 1
Use DH-5 (Diffie-Hellman Group 5)

While the primary use of the Interoperable Configuration Profiles is to define interoperability for various IP protocols utilized for cyber security, they can also be utilized to communicate requirements and compare devices. The Lemnos work does not create a "one size fits all" structure which end users should require and vendors should implement in its entirety on each and every system device. Instead, the multiple Interoperable Configuration Profiles create a modular approach which allows users to require and vendors to support any combination of the Interoperable Configuration Profiles. What it means to end users and vendors is that as more Interoperable Configuration Profiles are created, they will have more choices (e.g. the addition of SSH/SSL in 2010/2011 will provide addition choices for VPN support). This modularity allows for the appropriate set of functionality to be applied on a case by case, device level based on the device's role in the overall system. Host device or network node, Interoperable Configuration Profiles can assist end users in communicating device requirements and

vendors in communicating device functionality for any networked device which must support a core security functional requirement.

2.4 STEP 4 – TEST AND VALIDATE

While testing is part of the standard development process for any device, the testing involved in the Lemnos process is aimed at two specific areas:

1. Validating the effectiveness of the Interoperable Configuration Profiles to clearly describe the parameters necessary to establish interoperability between two devices supporting covered security functionality.
2. Assess any potential impacts to the control systems environment from the addition of the specified technology. This is done by deploying this new technology into control system architectures and run simulated real world experiments. Various sites are used to test the Interoperable Configuration Profiles in differing control system architectures and under different data loads and different data protocols. This allows the team to analyze the system impact as well as the impact on the personnel that will be tasked with deploying and maintaining it.

Testing to date in the Lemnos project has been performed in two phases. The first phase involved only the project partners and covered the testing the reference design created by Sandia National Laboratories and commercial product produced by Schweitzer Engineering Laboratories within a simulated power system environment at facilities provided by the Tennessee Valley Authority. The second phase of the testing opened up participation to vendors outside the project partners and involved the addition of equipment from additional participating vendors within the same facilities.

In addition to the testing at the TVA facilities, public demonstrations involving both project partners and participating vendors were successfully conducted at the 2009 ISA Expo and 2010 Distributech conference.

Figure 2 - Lemnos Project Partners and Participating Vendors

3.0 SUCCESS FACTORS AND TANGIBLE BENEFITS

The objectives and guiding principles of the Lemnos Project have been clearly defined. It should provide vendors a clear target relating to user cyber security requirements based on open source solutions. It should provide asset owners the ability to choose “best in class” cyber security solutions for various points within their infrastructure. It should reduce the amount of effort in developing, specifying, selecting, and deploying cyber security solutions in the electric sector control systems environment.

If at the end of the project, the work ceases and is not utilized by either vendors or asset owners, then it can’t be considered a success even though all technical goals were achieved. The success factors which measure whether or not the project has provided tangible benefits to the energy sector need to confirm that:

- The Lemnos work has it made it easier for utilities to specify, select and deploy interoperable equipment and systems supporting cyber security functions.
- At the end of the Lemnos project, a long term steward has been identified and that the work would continue to be self sustained.
- Commercial products available on the market which directly support the Interoperable Configuration Profiles.

3.1 PROJECT STATUS

Started in 2008, the Lemnos project to date has produced Interoperable Configuration Profiles and completed testing for IPsec and Syslog protocols. Work is continuing on the project with the target for the 2010/2011 timeframe centered on three areas:

- Syslog format standardization - The challenge to asset owners is that the contents of the Syslog messages is not standardized and typically varies by vendor and device. These various log formats increase the time, effort, and complexity required to normalize data and detect or analyze security events in a multi-vendor environment.
- Central Authentication - To include management functionality and interoperability Lemnos will research, specify, and commercially develop the preferred method to centrally authenticate access to field devices. The LDAP RFC will be utilized and vetted for use in Energy sector control systems. LDAP provides a manageable and scalable solution to user based access controls and be interoperable with the two most popular domain controller environments, Active Directory and OpenLDAP.
- Secure Engineering Access - There is an industry need for cyber security to sit at the application layer to support engineering access to end devices. This supports the strong access controls required by NERC CIP. Combined with the central authentication effort, these solutions can fulfill the need for manageable and scalable solutions that improve the reliability of power systems while improving the cyber security.

At present, there is at least one commercially available product on the market (released Q4 2009) supporting the IPsec and Syslog Interoperable Configuration Profiles. More commercially available products are expected in the near-term supporting the existing Interoperable Configuration Profiles as well as those identified for development in 2010/2011.

4.0 CONCLUSION

Interoperability is not a new concept in the context of cyber security. It is however a difficult and challenging concept and one that poses a significant barrier to establishing and maintaining a secure posture for control systems deployed within the electric utility sector. The goal of the Lemnos project is to tackle this challenge by utilizing existing open source solutions tied together into a user friendly framework rather than creating yet another new standard for utilities and vendors alike to consider. It addresses the gap between vendors developing products and end users deploying these products where practical and robust cyber security interoperability in a multi-vendor environment has to date been difficult to achieve. Lemnos does this by producing "Interoperable Configuration Profiles" by consensus for Internet protocols and then verifies the effectiveness of these profiles within the context of a control systems environment through comprehensive testing. Ultimately, this work is helping to foster the partnership between utilities and vendors by helping the two parties to clearly communicate user needs, product features, and configuration parameters relating to cyber security functions.

It is a given that no two utilities core security requirements are going to be the same and there are many different paths that various asset owners will take to determine their individual core security requirements. No matter what the path, it is at that point that the work being down within the Lemnos Project will help them answer the questions: 1) Can my equipment support the needed core security function and if so; 2) How do I configure it properly. By defining cyber security interoperability by using the Interoperable Configuration Profiles, end users have greater assurance that any device which implements the profile will not only successfully communicate with other devices from the same vendor, but also other vendors' devices, providing a guaranteed, documented level of security.