TRANSMISSION & DISTRIBUTION WORLD

November 1, 2010

The Secure Connection

By John Wesley Stewart, Tennessee Valley Authority

Power system engineers used to stand around the water cooler discussing blackouts and faults; today, they stand around the printer discussing new cyber security regulations. As traditional power system engineers assume responsibilities in new areas of technology, new skill sets must be learned to securely design control systems that operate critical infrastructure. The external pressures about cyber security from regulatory bodies and increased attention from executives does not appear to be letting up. There must be a way to work smarter and not just harder - a way to engineer and configure security into the power system communications grid without having to become experts in network security.

If the power grid is ever going to enjoy built-in - instead of bolt-on - security, power system engineers have to be competent in security technologies in addition to power theory. Because most exploited vulnerabilities are the result of misconfigured systems, security implementations in process control devices should be easily configured to avoid such unnecessary exposure. True interoperability between security-enabled process control devices is needed to allow straightforward integration and secure communication. The Lemnos Interoperable Security Project, funded by the U.S. Department of Energy, is targeted at addressing these problems and improving the state of interoperability among secure devices in the energy sector.

The Lemnos project supports the U.S. federal government's "Roadmap to Secure Control Systems in the Energy Sector." Lemnos had its genesis in the original Open PCS (process control system) Security Architecture for Interoperable Design (OPSAID) project, which studied various security protocols and functionality for application in utility networks.

Lemnos project partners include EnerNex Corp., Tennessee Valley Authority (TVA), Sandia National Labs and Schweitzer Engineering Labs (SEL). This mix of participants provides a wide range of perspectives on the interoperability issue that exists in the security arena. Sandia and EnerNex contribute advanced security theory and a core knowledge of the current direction of this technology, while SEL brings the viewpoint of everyday reality. Representing asset owners in the project, TVA provides the functional security requirements.

Develop Requirements

The initial requirements were driven by the need for secure solutions to a wide range of problems. With the regulatory pressure and increased visibility, many types of functionality were identified as potential targets of the Lemnos work. These top-level requirements included issues such as the ability to filter malicious or illegal network traffic, cryptography and password management, and non-repudiation of network traffic. To focus on specific and achievable goals, the Lemnos team narrowed its focus to two of the most critical needs for energy sector networks.

The first need identified was for a secure communications channel to allow multiple remote locations to exchange data across a network. In the electric power industry, the most pressing need for this type of channel exists between a control center and various substations. With the critical nature of the data and the multiple flavors of data exchanged between the two locations, a mechanism to secure the communications channel is necessary. Among other requirements, the Lemnos team decided the channel should be agnostic to the different types of data that might traverse the path and that the creation of the channel should ensure the identity of both locations.

The second need identified was for simple messaging functionality to allow the exchange of short messages to report events associated with the security equipment or other pieces of information the system owner might need to know. An example of this functionality, driven by a specific North American Electric Reliability Corporation critical infrastructure protection requirement, is access logging. These messages could contain information about which user is remotely accessing a substation across the network or that an unauthorized user has attempted access.

To avoid duplication of effort and ensure the widest possible amount of support, the Lemnos team attempted to satisfy the identified requirements with known and proven standard protocols wherever possible. With this in mind, the secure communications channel requirement was mapped to Internet protocol security (IPSec), which is described in the Internet Engineering Task Force (IETF) request for comment (RFC) 4301. This protocol met all of the detailed requirements identified earlier in the project and is widely supported by vendors in the security space.

For the simple messaging requirement, the Syslog standard was identified as a solid solution to exchange the types of information needed to maintain situational awareness of the current state of control system networks. Syslog is also widely used protocol for this purpose and is defined by both IETF RFC 3164 and RFC 5424.

Develop Interoperability Configuration Profiles

Once the requirements were mapped to generally accepted security protocols, the real work began. As the team started examining IPSec implementations in detail, the true complexity of the protocol was exposed. Setting up an IPSec virtual private network between two networks with different vendors involved can be daunting. In one examination, more than 100 separate parameters needed to be configured to effectively allow the two endpoints to negotiate a connection. In many cases, complication is just a byproduct of flexibility and functionality, and a box that has a large number of configuration parameters is more likely to be adaptable to another vendor's product. This complexity can be a positive for those with an extensive networking background and understanding to navigate all the choices in a typical configuration, but for a power engineer with a limited networking background, this level of complexity is overwhelming.

To work toward eliminating the complexity and streamlining the configuration process, the Lemnos team began to develop an IPSec interoperability configuration profile (ICP). Exactly as it sounds, this document is a list of the selected configuration parameters and functionality found to be critical to interoperability. The information in this profile documents choices that historically would have been made by the asset owner for each separate installation. These configuration parameters include choices between encapsulating security payload versus authentication header, tunnel mode versus transport mode, and the identification of a common Diffie-Hellman group number. As each decision was debated and a specific setting was documented in the configuration profile, the requirements documented in an earlier project phase were consulted. The goal was to make the most secure choice that allowed for the widest possible range of interoperability.

In addition to documenting a standardized configuration for two interoperable devices, the ICP also provides guidance to vendors who are currently implementing security functionality. They are able to examine their existing implementation and identify a standard configuration that would allow them to interoperate with their peers in the industry. This helps to avoid the common occurrence where two different devices that are technically compliant with a given standard do not interoperate because different portions of the standard have been implemented.

Validate Through Multi-Vendor Testing

Once the parameters had been identified and a bridge had been built between the high-level standards and an actual device configuration, testing was performed to verify that the ICP could really be used to make two different vendors' products interoperate at an acceptable level. An independent third party was needed to provide a reference model that could be used for testing and validation.

With this goal in mind, Sandia National Labs created a reference model or golden board using open-source implementations of both IPSec and Syslog. Open-source tools like strongSwan were used because they are transparent and typically flexible. In addition to the reference model, more mainstream network security products also were added to the test bed alongside the control-system-specific devices. These were included in the test because of their widespread use in control centers. For the proposed ICP to be usable in a wide range of real-world situations, these mainstream products were critical to the test.

Finally, the commercial implementation of the Lemnos work was developed by SEL. This substation security gateway was designed using the requirements and documented functionality from the ICP.

Initial application and testing of the ICP was an iterative process. As the various devices were configured using the parameters identified in the ICP, issues were uncovered with configuration choices that did not exist. Over time, the Lemnos team overcame these problems. Once the profile was solidified within the Lemnos team, external vendors were approached to add their devices to the test bed for a wider perspective of control system security products.

As a new device was added to the test bed, it was configured using the parameters identified in the ICP. At this stage, several small issues were uncovered and addressed. To resolve each issue, any trade-offs between security and interoperability were debated and documented, with the end result being a solid and secure configuration that can be used in multi-vendor control system networks with a high level of assurance.

Integration with Open Smart Grid

To capture the Lemnos team effort and help integrate it into the wider efforts targeted at the tidal wave of new technology being deployed around the power grid, the output of Lemnos is being fed into a new task force in Open Smart Grid. The task force is made up of a cross section of utilities, vendors and subject matter experts from multiple areas. With its focus on interoperability and cyber security, it has been named OpenSG-Cybersec-Interop. The new task force allows the output of the Lemnos team to be fully vetted through a wider community and coordinated with other related efforts in the smart grid and power transmission sectors.

Looking Forward

As the first two years of the Lemnos project were coming to a close, the project was extended for an additional year with the mission to continue mapping out security protocols that meet the requirements documented through OPSAID and Lemnos. The new challenges chosen by the team include centralized authentication through directory services, secure engineering access and standardized messaging content.

The Lemnos team already has begun work on standard selection for this functionality. For centralized authentication, two separate implementations are being explored for inclusion with the reference model. OpenLDAP, because of its open-source origins, was the initial choice to provide standard directory services. As preliminary testing and investigation were done, the group has gravitated more toward Microsoft Active Directory Services (ADS) as the reference implementation of directory services. This is mainly due to the overwhelming majority of existing control system networks that already leverage MS ADS in each company's corporate network. The goal for interoperability in directory services is that one set of user credentials existing in a central system can be used to authenticate users across any vendor's equipment.

Secure engineering access is similar to the original secure communications channel requirement but with some distinct differences. This functionality is targeted more at user-to-device connections as opposed to network-to-network connections. Remote maintenance tasks such as reconfiguration or oscillography retrieval were used to generate the requirements for this area. Potential protocols being examined include secure shell and secure sockets layer/transport layer security (SSL/TLS). In this area, a subtly different vision is driving the work toward a different measure of interoperability. This work should build a model that would allow an end user to use a single application for engineering access to devices developed by different vendors.

Finally, the Syslog work that is slated for the final year of the Lemnos project is focused on bringing this functionality to a higher level of interoperability than earlier work. The first round of Syslog work was focused more on syntactic interoperability, which was limited to allowing some level of data exchange from a Syslog client to a server. The new work currently under way on Syslog is intended to bring interoperability to a higher level by standardizing the actual content and structure of certain important messages. This is increasingly important as the volume of messages increases and becomes more critical to compliance reporting. In real terms, this means alarms should be collected from each vendor's system and work with the system as they arrive, without translating each message into a common syntax.

Eliminating Islands

The Lemnos team has learned that interoperability can mean different things in different contexts. The most common use of the term refers to one system or component communicating or working with another without excessive integration work. Another angle to the interoperability problem involves a third-party communicating with both boxes in an identical way. In some ways, the second type of interoperability can be more challenging with greater returns to the asset owner.

The team also learned that most vendors will work together to improve interoperability when the opportunity arises. Also, asset owners cannot afford to deal with multiple proprietary systems when one interoperable system could do the job. Security continues to become more complicated by the day, with vendors adding functionality to meet a myriad of new requirements. With all the new technology being deployed to meet new security requirements and emerging smart grid applications, the industry has a choice. The infrastructure must be driven toward a more open and interoperable model. Islands are not satisfactory!

Acknowledgment

The author wishes to acknowledge that the work covered here is that of the Lemnos Core Team, which includes Brian Smith of EnerNex Corp.; Ron Halbgewachs and Adrian Chavez of Sandia National Laboratories; Dave Teumim, a Sandia contractor; and Rhett Smith of Schweitzer Engineering Labs.

John Stewart (jwstewart@tva.gov [jwstewart@tva.gov]) is a senior engineer in the architecture group of TVA's Transmission Power Control Systems organization. He has been the technical lead for multiple infrastructure and pilot projects focused on grid data, transport and control. Stewart is also vice-chair of the OpenSG Cybersec-Interop Task Force and was recently elected to the UTC Smart Networks Council Board. He holds a BSEE degree with a focus on telecommunications systems from Tennessee Technological University.

What is Lemnos?

Lemnos is an island in the northern part of the Aegean Sea. For ancient Greeks, the island was sacred to Hephaestus, the Greek god of technology, which back in those days was mostly about metallurgy. The equivalent Roman god was Vulcan. The reason Hephaestus had a special relationship with the island of Lemnos was because, as told in the Iliad, this is where he landed when his father, Zeus, hurled him headlong out of Olympus. So, one might understand the special attachment that Lemnos might hold for technology.

The Lemnos Interoperable Security Project is a multiyear U.S. Department of Energy National SCADA Test Bed effort highlighting a security interoperability framework for communications supporting the energy sector. It uses IPSec and Syslog for interoperable communication between security devices and will be expanded to use other popular Internet protocols like LDAP and SSL in coming years. This work is helping to foster the partnership between utilities and vendors by helping the two parties clearly communicate user needs, product features and configuration parameters relating to cyber security functions.

As in similar National SCADA Test Bed projects, DOE required that the Lemnos team commercialize the solutions developed through the project. Schweitzer Engineering Labs was tasked with producing the commercial implementation which has recently been released as the SEL-3620 Ethernet Security Gateway.

Companies mentioned:

EnerNex www.enernex.com

Microsoft www.microsoft.com

North American Electric Reliability Corp. www.nerc.com

Open Smart Grid www.osgug.org

Sandia National Labs www.sandia.gov

Schweitzer Engineering Labs www.selinc.com

Tennessee Valley Authority www.tva.gov

U.S. Department of Energy www.energy.gov