Lemnos Interoperable Security Project

Lemnos Participating Vendor Testing Report

Tennessee Valley Authority Test Laboratory

July 28-29, 2009

Contents

Figures

Tables

Lemnos Participating Vendor Testing Report
Tennessee Valley Authority Test Laboratory
July 28-29, 2009

1. Test Goals

There were four goals (tests) defined for this phase of the Lemnos Interoperable Security Project architecture testing:

(1) Establish a baseline connection between all vendor participants through the Cisco switch;
(2) Determine the ability to establish multi-vendor interoperability within a power provider utility process control laboratory test environment;
(3) Determine the level of security that could be established within this interoperable system;
(4) Determine the capability of the differing systems to produce and transmit Syslog messages to a common Syslog file storage.

2. Test Participants & Equipment

In addition to the Lemnos primary partners, Sandia National Laboratories (SNL) and Schweitzer Engineering Laboratories (SEL), four other vendor organizations participated in this phase of the Lemnos project testing: (1) Garrettcom, Inc., (2) n-Dimension, (3) Phoenix Contact, Inc., and (4) Industrial Defender, Inc. In the discussion to follow, a random assignment of vendor identifications has been assigned to each of the participants.

The specific vendor equipment systems that were used in this testing included:

- Sandia Lemnos/OPSAID Reference Architecture Prototype System (field & system units)
- Schweitzer SEL 3620 Ethernet Security Gateway
- n-Dimension nPlatform 340
- Garrettcom Magnum DX900
- Industrial Defender ESP (Electronic Security Perimeter)
- Phoenix Contact MGuard RS
- Industrial Defender SEM (Security Event Manager) use in test for Syslog files

A Cisco 2950 Switch was used throughout the testing for IP addressing of each of the equipment units included. After core goal testing was completed, additional testing was conducted utilizing a Cisco ASA 5520 Adaptive Security Appliance.

A diagram of the test network is shown in Figure 1. The description of the test units are simply identified as Units A-E, related to each of the five vendor organizations participating in the tests. In this system, the SNL-1 field unit served as both a standard control system unit and a gateway between the vendors and the Syslog file system (SNL-2) and the

Industrial Defender Syslog file system (SEM). The "hosts" identified were represented by each vendor's representative laptop computer for configuration definitions and view into message traffic & diagnostics throughout the testing.

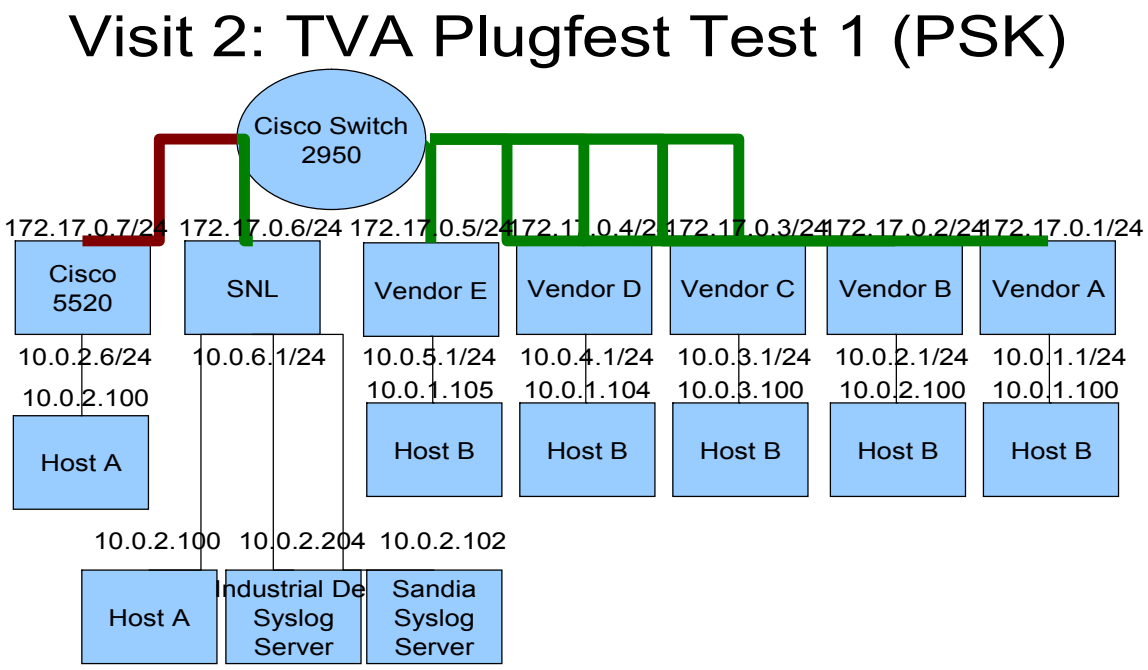

Figure 1. Test Network

3. Test Procedures & Results

The first step in conducting the tests was for each vendor to establish a Virtual Private Network (VPN) tunnel with Sandia and with each other. It was impressive that within two hours of the simple start of all units being connected to the Cisco 2950 and powering up all the equipment that 14 VPN tunnels for interoperability had been established (see Figure 2). One tunnel between two vendors (C & E) was not completed because one vendor had implemented DH Group 2 while the other had implemented DH Group 5 for IKEv1. This problem could be overcome by the inclusion of additional software along with possible dynamic configuration capability that would permit more than one group being implemented or by "standardizing" on a single specific DH group. This highlights one of the problems of vendors needing to meet the expectations of their customers needs and defining hard configurations.

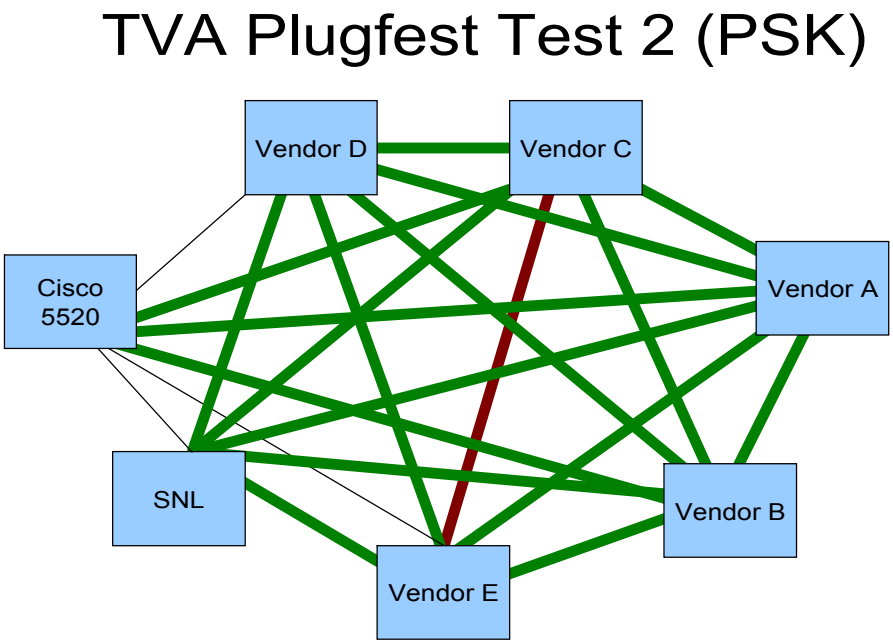

Figure 2. Virtual Private Networks Established

The next set of tests conducted addressed authentication between systems and the logging of Syslog messages. The tests began with each of the systems establishing communication with each other by using shared password keys (PSK) and that was accomplished.

During the testing, all vendor units were able to send Syslog messages to both the Sandia-2 unit Syslog files and the Industrial Defender SEM. All Syslog message traffic was also viewed by all participants, shown in Figure 3. Syslog is typically used for computer system management and security auditing. For example, authentication failures would be reported across the control system through the Syslog messages. Furthermore, Syslog is supported by a wide variety of devices and receivers across multiple platforms and through the Lemnos tests, Syslog can be used to integrate log data from many different types of systems into a central repository. Both interoperability and security are improved through the use of Syslog.

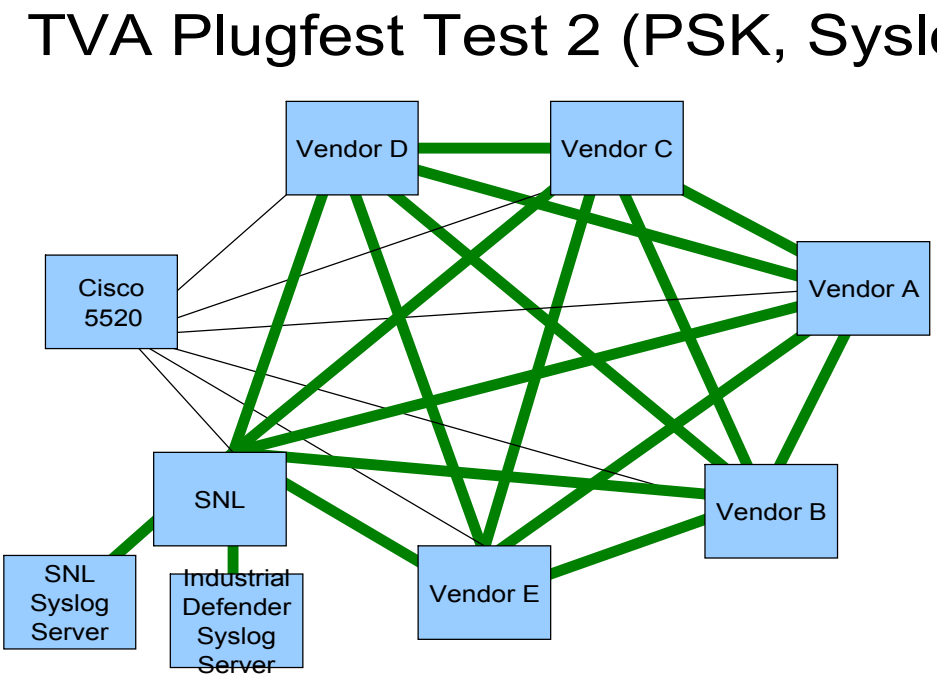

Figure 3. Distribution of Syslog messages with pre-shared keys

A second step was to utilize security certificates signed by a certificated authority (CA). The established links shown in Figure 4 were a combination of self-signed certificates and certificates authenticated by a CA (the Sandia system can provide that authentication for this testing).

Near the end of the test period, a Cisco Adaptive Security Appliance (ASA) 5520 unit was configured into the network and three vendor participants in the test were able to established connections to that unit. Due to testing time restrictions, the other two vendors and Sandia did not make connections to the Cisco unit, although all three noted that they had made such connections in the past.

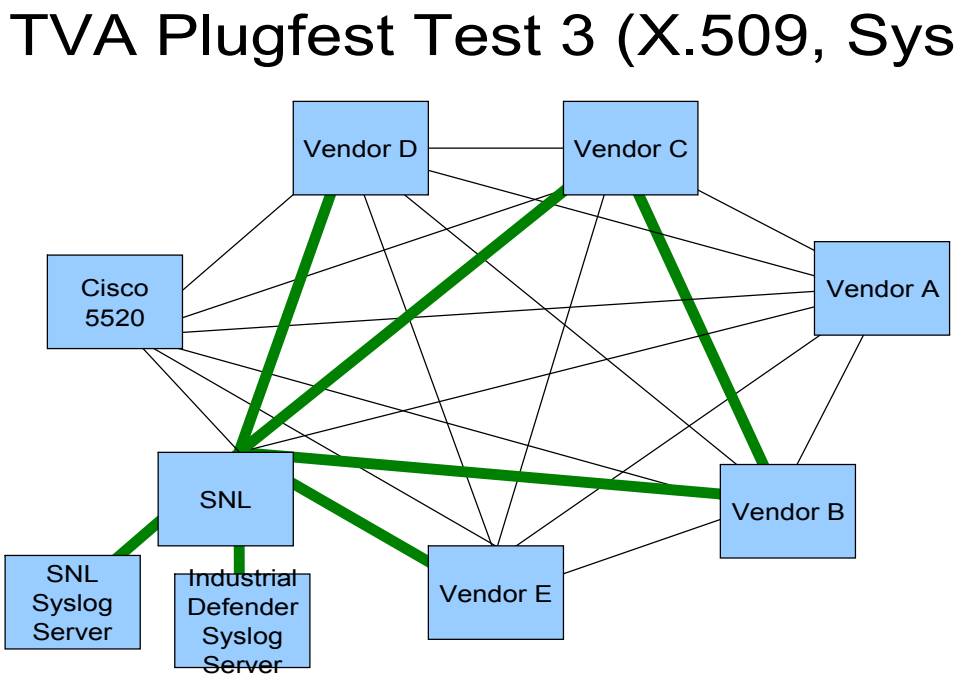

Figure 4. Distribution of Syslog messages with signed certificates

4. Test Observations

The key result from two days of testing by the six organizations represented at TVA is that it is possible to establish multi-vendor, secured interoperability and in a relatively short amount of time. This effort over the two day period included both actual floor testing time and several team meetings. Floor testing time totaled approximately 10 hours.

A major accomplishment of cooperation by all of the test participants was observed. All vendors worked around a table on their laptop computers connected to their respective control system (CS) units. These laptops provided the visualization, command, and configuration interfaces for the CS units. Discussions ranged from one-on-one to multiple-to-multiple. There was an excellent exchange of information about setting parameters and defining configurations throughout the entire testing process. Discussions were abundant about messages being sent/received, encryption codes being used, and parameters that were being used in assisting each other to establish interoperability. The cooperation among all participants was outstanding.

Nearly all of the testing procedures and steps required for the success of this testing were done in parallel. This permitted each of the participants to move ahead with next test stages as they completed each stage, permitting multi-way establishment of each level of interoperability and security testing.

	Vendor Settings for Interoperability Testing - July 28-29, 2009					
Vendor	**A**	**B**	**C**	**D**	**E**	**Sandia**
Parameter						
P1 Encryption	3DES, AES-128/256	DES, 3DES, AES-128/192/256	DES, 3DES, AES-128	DES, 3DES, AES-128/192/256	AES-128	DES, 3DES, AES-128/192/256
P1 Hash	MD5, SHA1, SHA2-256/512	MD-5, SHA1, Auto	MD-5, SHA1	MD-5, SHA1, Auto?	SHA1	MD-5, SHA1/160, SHA2-256/512
P2 Encryption	3DES, AES-128/256	DES, 3DES, Null, AES-128/192/256	DES, 3DES, AES-128	DES 3DES, Null, AES-128/192/256	3DES, AES-128/256	DES, 3DES, Null, AES-128/192/256
P2 Hash	SHA1, SHA2-256, MD5, Null	MD-5, SHA1, Auto	MD5, SHA1	DES, 3DES, Null	SHA1, SHA2-256	MD-5, SHA1/160, SHA2-256
PFS	no	yes/no, *need group	fixed on, 1024	yes/no/blank	1536 fixed	yes/no
Diffie Hillman (DH) Group	2,5,14-18	2,5,14-18	1,2	1,2,5	5	1,2,5
Key Lifetimes	auto	auto	auto	120-172860, auto	10800 - 36000	auto
DPD	yes	yes	yes	yes	yes	yes & no
IKE version	1	1	1	1	2	1&2
Vendor Version of SW	3.5	6.1.x	2.01	3MR6 (Maintainance Release)	X116	OPSAID v.2, strongswan v.4.2.14
DES = Data Encryption Standard						
AES = Advanced Encryption Standard						
SHA = Secure Hash Algorithm Standard						
PFS = Perfect Forward Secrecy						
DPD = Dead Peer Detection						
Key times "auto"=negotiable to lowest level						
3D=Triple DES						
IKE = Internet Key Exchange						
Question about government adoption of SHA2 as a requirement.						
Identified the gaps in some systems, but all systems are currently approved and acceptable for government standards & requirements.						

Table 1. Vendor Settings for Interoperability Testing

The entire test team met and defined the range of parameters and capabilities included with each of their respective systems which are summarized above in Table 1. From the discussions that ensued as a part of the creation of this cross-reference table, gaps were identified for different vendors and tasking was taken back to their respective organizations for implementation. Discussions also included the demonstration of capability during the Plug Fest planned for the ISA 2009 Expo being held on October 5-7, 2009. A question was asked about the possibility of repeating these tests a year from now to determine what has changed and how secured interoperability has improved; an interesting proposition to be considered for future Lemnos Project planning.

5. Conclusions

Through the cooperative trial and error exercises with each of the systems, this testing demonstrated that it is possible to establish a baseline level of common configuration parameters and settings for interoperability and security between multiple vendors and that it has been demonstrated. It became evident that the efforts to establish secured interoperability by experts is a necessary step towards creating the information needed for utility companies to install multi-vendor supplied equipments for secured interoperability. There are areas where each vendor needs to pay some attention in looking ahead for the next year.

The take-away from this set of testing and demonstration is that a major step has been taken to provide the information necessary to be shared amongst vendors and with utility companies for the establishment of secured interoperability.