The Lemnos Interoperable Configuration Profile for IPSec

The Lemnos Interoperable Security Project

August 3, 2011

Rev 6


Lemnos Interoperable Security Project
Partners
Participating Vendors
EnerNex
SEL
TVA
Sandia National Laboratories
INDUSTRIAL DEFENDER
GarrettCom
Industrial Networking at its Best
PHOENIX CONTACT
CISCO
n-dimension solutions
RUGGEDCOM
INDUSTRIAL STRENGTH NETWORKS
SIEMENS
encore networks
DOE Cybersecurity for Energy Delivery Systems
Bringing Interoperability to the Control System Security Arena
Enhanced Ability to Meet Customer Needs
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
Participating R&D Organizations
EPRI
ELECTRIC POWER RESEARCH INSTITUTE
Sandia National Laboratories
NNSA

Table of Contents

Figures

Introduction

The effort required to achieve cyber security interoperability is often a barrier for utilities implementing technologies. Let's consider IP Security Protocol (IPSec) as an example, IPSec is a widely-used Internet Protocol to define Virtual Private Networks (VPN), or " tunnels", to communicate securely through untrusted public and private networks. The IPSec protocol, defined by the Internet Engineering Task Force (IETF)[1], has a significant number of configuration options and encryption parameters to choose from. The IETF has many Request for Comments (RFC) for the IPSec protocol. How would a utility decide on which IPSec configuration setting to use for a secure tunnel? The configuration options must be agreed upon and adopted by both parties prior to establishing the tunnel. The process of setting up a secure tunnel and getting different vendors to interoperate securely is labor intensive and may require a significant amount of security expertise by the end user. This whitepaper will document a secure configuration tunnel profile that will interoperate with different vendors.

Background

To obtain interoperability between proprietary security appliance units, one or both vendors must now write cumbersome "translation code." If one party changes something, the translation code "breaks." The Lemnos project is developing and testing a framework that uses widely available security functions and protocols, like IPsec, to exchange security log messages. Using this model, security appliances from two or more different vendors can clearly and securely exchange information, helping to better protect the total system.

The contributing Lemnos team for the IPSec Interoperable Configuration Profile can be found in Appendix A.

IPSec Configuration

As a utility would start a process to setup a VPN, there are a myriad a choices for the configuration. Initially, using the diagram from a popular IPSec tutorial on the Web, a nice decision tree exists to assist a utility in deciding basic VPN configuration parameters. See Figure 1, The IPsec Transform Creation Decision Tree. A good reference for an IPSec tutorial can be found at this link: http://www.eetimes.com/design/communications-design/4014693/IPsec-a-Tutorial-Part-VI.

With the Lemnos initial review, the team made the selections and tested the configurations with multiple vendors to insure they were interoperable and secure. For instance, the following choices are made from the flowchart by the Lemnos team:

- Use ESP (Encapsulating Security Payload)

[1] The EITF IPSec working group will develop mechanisms to protect client protocols of IP. A security protocol in the network layer will be developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality.

- Use TUNNEL mode (vs transport)
- Use a HMAC (Hashed Message Authentication Code)- needed for authentication and integrity. Use either MD5 or SHA1 (Secure Hash Algorithm 1)

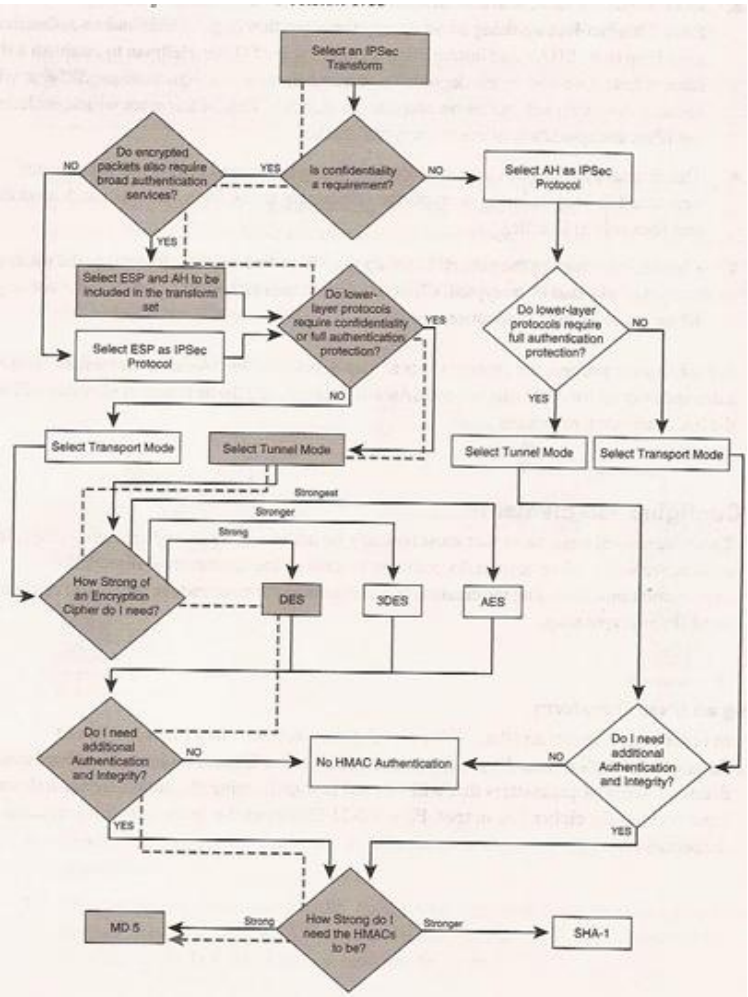

Figure 1 - The IPSec Transform Creation Decision Tree[2]

In a similar fashion, the Lemnos team reviewed the various IPSec RFCs, making secure interoperable choices and, very importantly, testing these choices with the variety of software that vendors on the team are using. Lemnos partners and participating vendors were using the following software at the time of testing:

- Strongswan on Linux platform
- Proprietary Stack on Wind River RTOS

[2] IPSec, a Tutorial—Part VI, Commsdesign, James Henry Carmouche Dec 28, 2006 (2:00 PM), URL: http://www.commsdesign.com/showArticle.jhtml?articleID=196800024, Reproduced from the book IPsec Virtual Public Network Fundamentals. Copyright [2006], Cisco Systems, Inc.

- Window XP embedded IPSec stack

The resulting list of the Lemnos team selections and testing is called an "Interoperable Configuration Profile". The Lemnos team in cooperation with Sandia National Labs and the following participating Lemnos vendors were part of the security and interoperability testing team:

- Schweitzer Engineering Laboratories
- Phoenix Contact
- N-Dimension
- Industrial Defender
- GarrettCom
- Siemens
- RuggedCom
- Encore Networks
- Cisco

The above listed team found the initial Lemnos IPSec interoperable configuration profile to be sound across multiple vendors. See Appendix B for the Draft Specification of the Lemnos IPSec Interoperable Configuration Profile.

Conclusion

This Lemnos recommended IPSec interoperable configuration profile is one of the initial deliverables for the project. The Lemnos project team welcomes additional input, other partner recommendations, and other vendor participation to ensure a broad base of testing and acceptance of this IPSec configuration profile.

If there are any questions or comments, please contact Dave Teumim, Lemnos Industry Outreach Facilitator, at dave431@enter.net.

Appendix A - Lemnos Contributing Team

Name	Organization
Rhett Smith	Schweitzer Engineering Laboratories
John Stewart	Tennessee Valley Authority
Brian Smith	EnerNex
Dave Teumim	Teumim Technical, LLC
Adrian Chavez	Sandia National Laboratory
Ronald Halbgewachs	Sandia National Laboratory
Sandy Bacik	EnerNex

Appendix B - Draft Specification of the Lemnos IPSec Interoperable Configuration Profile

Basic configuration decisions included:

- Using ESP (Encapsulating Security Payload)
- Using TUNNEL mode
- Using HMAC for authentication and integrity
- Using IKE Version 1 (moving to IKE Version 2 in future)
- Using DH-5 (Diffie-Hellman Group 5)

The specific configuration parameters for configuration the IPSec VPN tunnel are as follows:

- ike_life: 28,800s; (28,800 seconds life for key until exchange)
- ipsec_life: 3600s; (time till key re-negotiation)
- rekey_margin: 540s; (default value ?)
- rekey_fuzz: 100%; (default value ?)
- keyingtries: 3; (renegotiate keys 3 times)
- dpd_action: restart; (dead peer detection action)
- dpd_delay: 60s; (dead peer detection time "hello" interval in seconds)
- dpd_timeout: 150s; (dead peer detection time timeout interval in seconds)
- policy: PSK+ENCRYPT+TUNNEL+PFS+UP;
- Use PFS (perfect forward secrecy); for enhanced key exchange security (Use DH5 with PFS)The following is the Required, Recommended, and Deprecated list of Cryptographic Algorithms from the reference software configuration File

- 000 **List of registered IKE 1 Encryption Algorithms**:
  - 000 #7 OAKLEY_AES_CBC, blocksize: 128, keylen: 128(Required)
  - 000 OAKLEY_AES_CBC,blocksize:128, keylen: 192 or 256 (Recommended)
- 000 **List of registered IKE Hash Algorithms**:
  - 000 #1 OAKLEY_MD5, hashsize: 128 (Required)
  - 000 OAKLEY_SHA1, hashsize 128 (Required)
  - 000 #4 OAKLEY_SHA2_256, hashsize: 256 (Recommended)
- 000 **List of registered IKE DH Groups**:
  - 000 #2 *OAKLEY_GROUP_MODP1024, groupsize: 1024* ***(Deprecated)***
  - 000 #5 OAKLEY_GROUP_MODP1536, groupsize: 1536 **(Required)**
- 000 **List of registered ESP Encryption Algorithms**:
  - 000 #12 ESP_AES, blocksize: 8, keylen: 128-256
- 000 **List of registered ESP Authentication Algorithms:**
  - 000 #1 AUTH_ALGORITHM_HMAC_MD5, keylen: 128-128(Required)

- 000 AUTH_ALGORITHM_SHA1, Keylen 128-128 (Required)
- 000 #5 AUTH_ALGORITHM_HMAC_SHA2_256, keylen: 256-256 (Recommended)