

Analysis of the public domain software implementations of IPSec

Ban Ly

Objective:

The object of this project is to perform analysis on IPSec between public domain software (FreeSWan, KAME) and Cisco.

Language, Platform, etc:

Test bed will include two PCs, which are running either FreeBSD or Linux, and one or two Cisco router running IPSec IOS.

Input and output of the programs:

We will use a plain text file as an input file. This file will be encrypted and decrypted as it is being sent/received. The file can range from 50K to 1M byte.

Brief description of algorithms:

Internet Protocol Security (IPSec), developed by Internet Engineer Task Force (IETF) is open standards providing encryption and authentication service for IP traffic. IPSec use Internet Key Exchange (IKE) to provide exchange keys between peers, Authentication Header (AH) to provide data integrity, and Encapsulating Security Protocol (ESP) to provide encryption and confidentiality.

Procedures for testing:

- Perform clear text file transfer between two PCs to establish a baseline
- Insert a Cisco router with IPSec IOS in between the two PCs and perform file transfer. Compare the result with the baseline.
- Install FreeSWan on two PCs
- Perform file transfer under FreeSWan and compare the result to the baseline
- Insert a Cisco router between the two FreeSWan PCs. The Cisco need not perform any IPSec function. Purpose for this test is to see how much penalty it adds when sending IPSec traffic through the Internet.
- Connect a FreeSWan PC and a Cisco router and perform file transfer to verify the interoperability between FreeSWan and Cisco.

Time schedule:

- 10/01/03 – Project specification and research on related protocols
- 10/15/03 – Research on tools that needs to be use for testing
- 11/12/03 – Prepare the test bed by installing two FreeBSD/Linux machines and performs clear text file transfer to establish a baseline.
- 11/19/03 – Connect a Cisco router between the two machines. Enable IPSec on the Cisco router and perform file transfer. Capture the result.
- 11/26/03 – Establish IPSec connectivity between two machines (without Cisco IPSec) and perform file transfer. Capture the result and compare with the baseline.

12/03/03 – Reconnect the Cisco router into the test bed and perform IPSec file transfer.
This will demonstrate the interoperability between IPSec between Cisco and FreeBSD and FreeSWan.

List of literature:

<http://www.freeswan.org/>

<http://networking.earthweb.com/netos/article.php/1011451>

<http://www.conscoop.ottawa.on.ca/rgb/freeswan/ols2k/>

<http://www.strongsec.com/freeswan/install.htm>

<http://www.freeswan.ca/docs/freeswan-1.93/doc/testing.html>

<http://www.fedchik.org.ua/linux/ipsec/Introducing%20FreeS-WAN%20and%20IPsec.htm>

<http://www.x-itec.de/projects/tuts/ipsec-howto.txt>

<http://www.ietf.org/html.charters/ipsec-charter.html>

<http://www.forsitesolutions.com/Techstuff/freeswan/freeswan.html>

http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_tech_note09186a0080094203.shtml

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800d981f.html

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1826/products_feature_guide09186a0080080f59.html