MIDDLEWARE DE SEGURIDAD PARA EL ACCESO A SERVICIOS IMS EN UN ENTORNO 802.11

EDGAR DE LA CRUZ ESPARZA

HERNÁN GEOVANNI TAIMAL

ANEXO B
HERRAMIENTAS DE LA IMPLEMENTACION DE REFERENCIA DE MIDSEG

UNIVERSIDAD DEL CAUCA
FACULTADA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN, MAYO DE 2009

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Anexo B
HERRAMIENTAS DE LA IMPLEMENTACION DE REFERENCIA DE MIDSEG

En el presente anexo se describe el conjunto de herramientas utilizadas para el desarrollo de MidSEG (ver Tabla 1), las cuales tienen licencia publica general (GPL, General Public License) que está orientada principalmente a proteger la libre distribución, modificación y uso del Software.

Tabla 1. Herramientas utilizadas en el MidSEG

Descripción	Licencia
Núcleo Linux	GPL
Java SE Development Kit - JDK	GPL
Eclipse	GPL
IPsec-Tools	GPL
racoon	GPL
iptables	GPL
JAIN-SIP	GPL
OpenIMSCore	GPL
bind9 (DNS)	GPL
Wireshark	GPL
MySQL	GPL
John the Ripper	GPL

B.1 Núcleo Linux

Definición: Linux es el núcleo del sistema operativo libre denominado GNU/Linux, desarrollado gracias a contribuciones provenientes de todo el mundo. Para la implementación de referencia se utilizó el S.O [1]. Ubuntu 8.04 y Kubuntu 8.04.

Uso: sobre el Linux se montaron los subsistemas (SCSWI, SSW y SSP) de la implementación de referencia de MidSEG.

Instalación: el proceso de instalación del núcleo Linux puede ser encontrado en [2].

B.2 JDK

Definición: Desarrollado por Sun Microsystems, es un software que provee herramientas de desarrollo para la creación de programas en java [3]. La versión utilizada para el desarrollo de los subsistemas del MidSEG es el jdk-1.6.

Uso: necesario para desarrollar las aplicaciones Java que se hicieron de los diferentes subsistemas de la implementación de referencia de MidSEG.

Instalación: el proceso de instalación puede ser encontrado en [4].

B.3 Eclipse

Definición: Es un entorno de desarrollo integrado (IDE) que facilita el desarrollo de software brindando un entorno de trabajo muy amigable, este se ejecuta sobre la maquina virtual de java [5]. La versión utilizada en la implementación de referencia de MidSEG es eclipse 3.2.

Uso: su IDE facilito el desarrollo de los subsistemas de MidSEG.

Instalación: el proceso de instalación puede ser encontrado en [6].

B.4 Herramienta IPsec-Tools

Definición: es una implementación de IPsec para sistemas operativos Linux y BSD. El paquete IPsec-Tools tiene una herramienta llamada setkey que permite manipular las políticas de seguridad de la base de datos de IPsec (SPD, Security Policy Database) y las asociaciones de seguridad de la base de datos de IPsec (SAD, Security Association Database) [7]. La versión utilizada para la implementación de referencia de MidSEG es ipsec-tools R0.7.1..

Uso: la herramienta le permite a MidSEG manejar de forma transparente para el usuario las SA y políticas de seguridad (SP) dinámicas de IPsec entre los diferentes subsistemas (SCSWI, SSP y SSW). Por medio de las SP y SA que define MidSEG se protegen los paquetes y se garantiza la confidencialidad entre los equipos, respectivamente. Para la configuración de las SA y SP entre SCSWI-SSP, MidSEG hace uso de las llaves CK e IK, resultado del autenticación AKA.

Instalación: el paquete es instalado con el comando que se expone en la Figura 1.

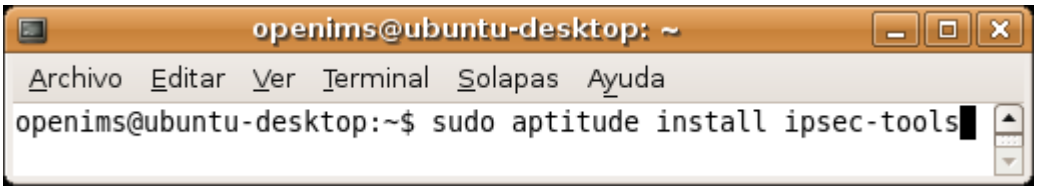

Figura 1. Instalación del paquete ipsec-tools

B.5 Racoon

Definicion: Es el software que permite la instalación dinámica de SA entre los subsistemas SSW y SSP por medio del protocolo IKE. Racoon soporta autenticaciones usando llaves compartidas o certificados X.509 [9]. La versión utilizada para la implementación de referencia de MidSEG es racoon.

El archivo principal de configuración es racoon.conf y se encuentran en el directorio /etc/racoon, las directivas del archivo de configuración racoon.conf se encuentran detalladas en [10].

Uso: Esta herramienta permite la configuración dinámica de las SA entre los subsistemas SSW – SSP y el núcleo IMS – SSP.

Instalación: el paquete es instalado con se muestra en la Figura 2.

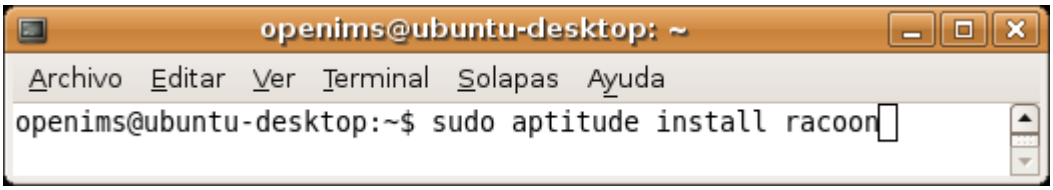

Figura 2. Instalación del paquete racoon

B.6 Iptables

Definición: es una herramienta que por líneas de comandos permite configurar un núcleo Linux 2.4.x y 2.6.x para filtrar paquetes IPv4 y hacer traducción de direcciones de red (NAT) de acuerdo a las políticas de filtrado de paquetes que se definan [11]. La versión utilizada para la implementación de referencia de MidSEG es iptables 1.3.8.

Uso: Las reglas que se definen en el filtro son agrupadas en cadenas (PREROUTING, POSTROUTING, INPUT, OUTPUT, FORWARD) para la manipulación de paquetes en diferentes estados de procesamiento (ver Figura 3). Las cadenas utilizadas por el MidSEG son PREROUTING, INPUT, FORWARD Y POSTROUTING, donde se determinan lo que se debe hacer con los paquetes IP de acuerdo a las reglas que se definan en estas y fueron utilizadas como se describe a continuación:

- PREROUTING: es la primera cadena en procesar el paquete en el núcleo Linux y es utilizada por el subsistema SSP para hacer NAT a la dirección de destino de los paquetes que van dirigidos hacia el puerto 5060.
- INPUT: a todos paquetes que deban ser procesados por la maquina se le aplican las reglas que aquí se definan. Es utilizado en los subsistemas SSW y SSP para permitir la relación entre estos subsistemas.
- FORWARD: todos los paquetes que deban ser reenviados hacia otro destino pasan por aquí y el subsistema SSW la utiliza para adicionar o remover reglas automáticamente que permitan desbloquear o bloquear el acceso a determinados dominios como resultado de un registro o des-registro SIP.
- POSTROUTING: es la última cadena en procesar el paquete en el núcleo Linux y es utilizada por el subsistema SSW para hacer NAT a la dirección de origen de los paquetes enviados por los clientes registrados de tal manera que puedan ser representados por una dirección IP pública.

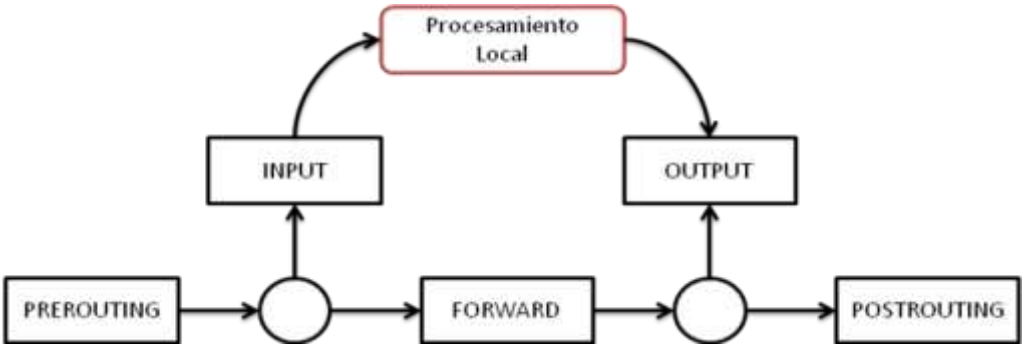

Figura 3. Estados de procesamiento del paquete con iptables

Instalación: por medio del comando que se expone en la Figura 4:

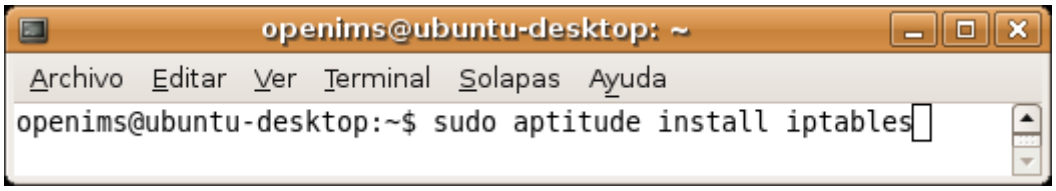

Figura 4. Instalacion del paquete iptables

B.7 JAIN-SIP

Definición: es un API desarrollado en el lenguaje Java del protocolo de inicio de sesión (SIP, Session Initiation Protocol). Es una implementación completa del RFC 3261 muy estable y ampliamente usada [12]. La versión utilizada para la implementación de referencia de MidSEG es jain-sip 1.2.

Uso: los subsistemas del MidSEG son construidos con este API, el cual contribuye con el soporte de SIP y permitió transportar AKA, adicionar nuevos encabezados (Realm, AH-Alg y ESP-Alg) y procesar los mensajes SIP (REGISTER, UNAUTHORIZED, OK) con el objetivo de cumplir con las funcionalidades de MidSEG.

Instalación: en el anexo C se explica cómo debe ser adicionado el API JAIN-SIP a la maquina virtual de java.

B.8 OpenIMSCore

Definición: Es una implementación de las funciones de control de llamada/sesión (CSCF, *Call Session Control Functions*) y del servidor local del subscriptor (HSS, *Home Subscriber Server*), que juntos forman el núcleo de la arquitectura IMS. En la Figura 5 se muestra los componentes OpenIMSCore, su ubicación dentro de la arquitectura IMS y los protocolos por medio de los que se comunican. Entre los componentes bases de este software de código abierto están SIP Express Router (SER) y MySQL [13].

Es importante tener en cuenta que este proyecto no tiene como objetivo convertirse o comportarse como un producto comercial, su fin es proveer una implementación de referencia para probar las tecnologías de IMS y facilitar la construcción de prototipos.

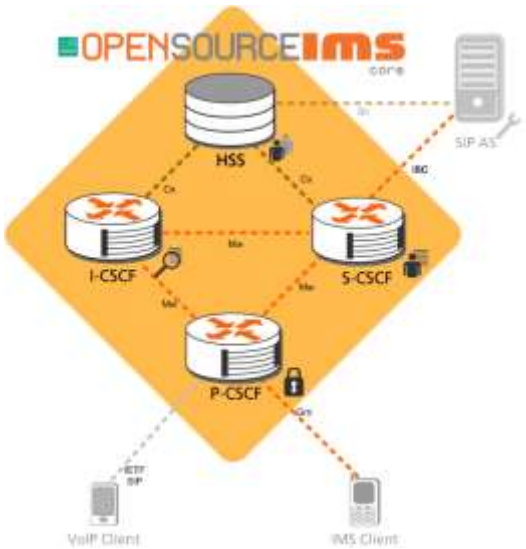

Figura 5. Arquitectura de implementación de OpenIMSCore [13].

Uso: esta herramienta permite obtener un ambiente IMS, necesario para las pruebas de funcionamiento de MidSEG que hace uso del registro realizado por el S-CSCF por medio de AKA.

Instalación: en [14] se encuentra la guía de instalación de OpenIMSCore.

B.9 bind9

Definición: es un servidor DNS comúnmente usado en Internet, especialmente en sistemas Linux, en los cuales es un estándar de facto [15]. La versión utilizada para la implementación de referencia de MidSEG es bind9 1:9.4.2.

Uso: en la implementación de referencia realizada del MidSEG, el servidor DNS permite resolver nombres de dominio del núcleo IMS.

Instalación: la instalación y configuración es realizada como se detalla en [14].

B.10 Wireshark

Definición: Es un analizador de protocolos de red, permite examinar de forma detallada la información de los paquetes capturados [16]. La versión utilizada fue Wireshark 1.0.0-1

Uso: esta herramienta permitió capturar los paquetes entre los diferentes subsistemas que conforman MidSEG para posteriormente hacer su análisis.

Instalación: el proceso de instalación puede ser encontrado en [17].

B.11 MySQL

Definición: Es un sistema de gestión de base de datos relacional que usa el lenguaje SQL estandarizado para el almacenamiento, actualización y acceso a información. El software MySQL tiene una doble licencia, los usuarios pueden elegir entre usar el software MySQL como un producto Open Source bajo los términos de la licencia GNU GPL o pueden adquirir una licencia comercial estándar de MySQL AB [18]. La versión utilizada para la implementación de referencia de MidSEG es mysql-server 5.0.51 y mysql-client 5.0.51.

Uso: el subsistema SSP utiliza esta herramienta como motor de base de datos para almacenar temporalmente los dominios a los que el usuario quiere ser registrado.

Instalación: por medio del comando que se expone en la Figura 6.

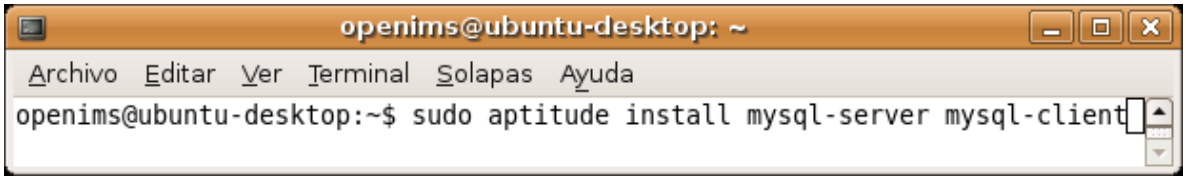

Figura 6. Instalación de MySQL

B.12 John the Ripper

Definición: Su principal propósito es encontrar contraseñas débiles de Linux utilizando los archivos donde se encuentran cifradas (passwd y shadow). Para lograrlo se puede usar diccionarios o un modo incremental [19].

Uso: Se utilizo esta herramienta para evaluar que tan seguras son las contraseñas utilizadas para los usuarios root en los servidores SMSP y SMSW.

Instalación: Un manual para usar esta herramienta puede ser encontrado en [20].

Bibliografía

[1] "Linux (núcleo)", http://es.wikipedia.org/wiki/Linux_(n%C3%BAcleo)
[2] "Instalación estándar Ubuntu", http://www.guia-ubuntu.org/index.php?title=Instalaci%C3%B3n_est%C3%A1ndar.
[3] "JDK – Java Development Kit", http://java.sun.com/javase/
[4] "Instalación Java", http://www.guia-ubuntu.org/index.php?title=Java
[5] "Eclipse", http://www.eclipse.org/
[6] "Instalación Eclipse", http://www.guia-ubuntu.org/index.php?title=Eclipse
[7] IPsec-Tools, http://ipsec-tools.sourceforge.net/
[8] "setkey - manually manipulate the IPsec SA/SP database", http://swoolley.org/man.cgi/8/setkey
[9] "racoon - IKE (ISAKMP/Oakley) key management daemon",http://netbsd.gw.com/cgi-bin/man-cgi?racoon++NetBSD-current
[10] "racoon.conf -- configuration file for racoon", http://netbsd.gw.com/cgi-bin/man-cgi?racoon.conf+5+NetBSD-current
[11] iptables, http://www.netfilter.org/projects/iptables/index.html
[12] "JAIN-SIP", https://jain-sip.dev.java.net/
[13] "Open IMS Core". http://www.openimscore.org/
[14] "OpenIMSCore Installation Guide", http://www.openimscore.org/installation_guide
[15] "bind9", http://www.bind9.net/
[16] "Wireshark", http://www.wireshark.org/about.html
[17] "Instalar Wireshark", http://diegosamuel.blogspot.com/2008/08/instalar-wireshark.html
[18] "MySQL", http://dev.mysql.com/tech-resources/articles/dispelling-the-myths.html
[19] "John The Ripper", http://www.openwall.com/john/
[20] "Analisis del John The Ripper 1.6", http://gseguridad.unicauca.edu.co/documentos/john1.txt