CENTRO DE INVESTIGACIÓN CIENTÍFICA Y DE EDUCACIÓN SUPERIOR DE ENSENADA

División de Física Aplicada

Departamento de Ciencias de la Computación

Protocolos de Seguridad e Instrumentación de IPSec en Escenarios Experimentales de Internet 2 en México.

Tesis

Que para cubrir parcialmente los requisitos necesarios para obtener el grado de Maestro en Ciencias presenta:

María Concepción Mendoza Díaz

Ensenada, Baja California, México
Enero de 2002

Abstract of the thesis presented by María Concepción Mendoza Díaz, in order to obtain the Master Degree in Sciences in Computer Science, Ensenada Baja California, Mexico, January, 2002.

Security Protocols and Instrumentation of IPSec Experimental Scenarios on Internet 2 Mexico.

Approved by:

Dr. David H. Covarrubias Rosales
Thesis Director

Due to the global Internet growth and the appearance of new technologies requiring experimental escenarios before being introduced to comercial Internet, national projects have been created to create the next generation Internet (Internet 2). México has begun its Internet project in 1997, with the creation of the University Corporation for Internet Development (CUDI), begin formed by the most important academical institutions of out country. CICESE as CUDI's academical asociate has an active participation in the ejecutive committee and other committees for the network development.

Security is a very relevant aspect of actual networks, its considered a requirement for design and instrumentation processes of new networks, then involved in CICESE's contribution context to Internet 2 in Mexico, this thesis was developed to experiment with new security technologies using security protocols at the network level, particular to IP, giving an option to solve security problem at the transit layer.

IP Security Protocol (IPSec), also known as VPN Protocol, plays an important role for networks using IP as the fundamental communication protocol. IPSec gives a general solution to apply security mechanisms as authentication and confidentiality, independent of the applications used at the user level.

Funtionality and application of standard security protocols are described in this work. Experimental scenarios in Internet 2 were instrumented using IPSec, different configurations were evaluated executing video, audio and data applications. A numerical analysis has been done giving conclusions over the use of IPSec in a network like Internet 2, VPN uses and its real application.

Key words: Security protocolos, IPSec, security, VPN, IP, communication models.

Resumen de la tesis de María Concepción Mendoza Díaz, presentada como requisito parcial para la obtención del grado de **Maestro en Ciencias en Ciencias de la Computación**, Ensenada Baja California, México, Enero de 2002.

Protocolos de Seguridad e Instrumentación de IPSec en Escenarios Experimentales de Internet 2 en México.

Aprobado por:

Dr. David H. Covarrubias Rosales
Director de Tesis

Como consecuencia del crecimiento de Internet a nivel mundial y el surgimiento de nuevas tecnologías que requieren escenarios de experimentación antes de ser introducidos en los mercados comerciales, se han planteado proyectos a nivel nacional para crear las redes de Internet de siguiente generación (Internet 2). México inició su proyecto de Internet 2 en 1997, creando la Corporación Universitaria para el Desarrollo de Internet (CUDI), formada por las instituciones académicas más importantes del país. CICESE como asociado académico de CUDI participa activamente dentro del Comité Ejecutivo y los diversos Comités para el desarrollo de esta red.

La seguridad es un aspecto de gran relevancia en las redes de la actualidad, se considera un requisito en los planes de diseño e instrumentación de nuevas redes, por lo que, dentro del contexto de contribución del CICESE a Internet 2 en México, se desarrolló este trabajo de tesis para experimentar con las nuevas tecnologías de seguridad que plantean el uso de protocolos para brindar seguridad directamente al nivel de la capa de red, en particular al protocolo IP, proporcionando una opción para solucionar el problema de seguridad en la capa de tránsito.

El protocolo de seguridad IP (IPSec), también conocido como el protocolo VPN, juega un papel importante para las redes que utilizan como protocolo de comunicación fundamental a IP, brinda una solución general para aplicar mecanismos de seguridad como autenticación y confidencialidad, independientemente de las aplicaciones que se utilicen al nivel de usuario.

En este trabajo se describen los protocolos de seguridad estándares, su funcionalidad y aplicación. Se instrumentaron escenarios de experimentación en Internet 2 utilizando IPSec, se evaluaron diferentes configuraciones ejecutando aplicaciones de video, audio y

datos, se realizó el análisis numérico de las muestras obtenidas y se proporcionan conclusiones sobre el uso de IPSec en una red como Internet2, el uso de VPN y su ámbito real de solución.

Palabras clave: Protocolos de seguridad, IPSec, seguridad, VPN, IP, modelos de comunicación,

Agradecimientos

A mi director de tesis y amigo Dr. David H. Covarrubias Rosales. ¡Muchas gracias David! A mi jefe y amigo M.C. Jorge E. Preciado Velasco. ¡Muchas gracias jefe! Solo con su apoyo pude haber terminado este trabajo, mi respeto y cariño para ustedes.

A los miembros del Comité de tesis, gracias por sus contribuciones, apoyo e interés en este trabajo.

Al departamento de Ciencias de la Computación, gracias por aceptarme como estudiante y apoyarme para alcanzar esta meta.

A los profesores por compartir su conocimiento, sufrí en unas clases y otras las disfrute mucho.

Al Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE), mi segunda casa, aquí he aprendido casi todo lo que sé, me enorgullezco de ser parte de esta Institución, muchas gracias por apoyarme siempre.

Al Consejo Nacional de Ciencia y Tecnología (CONACyT) por todo el apoyo que me brindó.

A los estudiantes de Ciencias de la Computación, me tocaron varias generaciones, tuve la fortuna de reir, pachanguear y disfrutar la estancia de muchos de ellos, enriquecieron las clases, los proyectos, los días buenos y no tan buenos, aprendí mucho de ustedes y los llevo a todos en mi mente.

Al Grupo de Comunicaciones Inalámbricas (GCI) del Departamento de Electrónica y Comunicaciones, gracias por sus sonrisas, su apoyo

cuidando mis máquinas y su ejemplo de jóvenes emprendedores con muchas ganas de superarse.

A la Dirección de Telemática, mis compañeros y amigos, en especial... ¡Muchas gracias! al M.C. Raúl Rivera Rodríguez, por tus ideas, revisiones, amistad, compañerismo y orientación desde antes que empezara este trabajo. ¡Muchas gracias! a Abelardo Ozuna por tu apoyo con el diseño gráfico, figuras y tu disposición para ayudarme todo este tiempo. ¡Muchas gracias! al Ing. Enrique Elenes por tu apoyo siempre a tiempo en las conexiones de red que fueron necesarias en la instrumentación de los escenarios de pruebas, tus carrillas y por tus porras. ¡Muchas gracias! a Blanca Velázquez y a Sarita Vargas por su cariño, ustedes iluminan todos mis días. ¡Muchas gracias! a Saúl Velez, te quiero como mi hermanito, échale muchas ganas, tengo mucha fe en ti. Al grupo de trabajo de Internet 2, gracias por su interés, su apoyo y el ánimo que me brindan siempre.

Al grupo de trabajo de Seguridad del Comité para el Desarrollo de la Red de CUDI, en especial a mis compañeros y amigos, al M.C. Mario Farias-Elinos profesor investigador de la ULSA ¡Muchas gracias! por tus revisiones y contribuciones al trabajo, discusiones e ideas de lo mucho que podemos hacer por esta nueva red y por la organización a nivel nacional. ¡Muchas gracias! al Ing. Azael Fernández Alcántara técnico académico del Netlab-DTD-DGSCA-UNAM por tu disposición para apoyarme en la generación de pruebas de IPSec con IPv6.

A mi angel Carmelita Torres, a mis compañiebrios: My friend, Cristy, dianita.com, Danny, Carlitos, Guapo, Miriam, Zarinin y Erickin ¡los quiero mucho!

A la Federación de BPW y en especial al grupo de Mujeres Jóvenes Profesionales y de Negocios de Ensenada, gracias amigas por ser mi inspiración, es un lujo conocer mujeres brillantes que luchan todos los días por abrir espacios para la superación de la mujer.

A todos mis amigos y personas que quiero, sus huellas en mi vida han sido fundamentales para mi. ¡Muchas Gracias!

Alguna vez dije, no sé a quien agradecer tantas cosas buenas que me suceden... pues a Dios ¡Muchas gracias! por ponerme en los lugares adecuados, rodearme de gente maravillosa que me ha dado esta sonrisa de felicidad en mi rostro y tantísimos momentos hermosos y razones para agradecer estar viva.

Dedicatorias

Dedico este trabajo de tesis con todo mi corazón, admiración y respeto a los tres amores de mi vida:

A Juan Carlos Domínguez Valdez, tengo toda la vida por delante pedacito, para darte las gracias por estar conmigo, por hacerme tan feliz y ser todo lo que necesito, no hay palabras para decir lo mucho que te amo y todo lo que siento por ti. Estuviste en mi mente todo el tiempo, en cada página que escribí y en cada momento difícil en el que tu con tu sonrisa y palabras de aliento compusieron todo y siempre seguí. ¡TACH!

A mi mamá, una señora maravillosa que me enseñó los verdaderos valores de la vida, ha estado conmigo y para mí siempre y con su ejemplo me enseña todos los días la alegría de vivir. ¡Te quiero mucho mami!

A mi papá, que la vida me arrebató muy pronto, te extraño mucho y siempre te llevo conmigo, gracias a ti quise ser universitaria desde los 8 años, es también tuyo este logro. ¡Te quiero mucho papi!

Contenido

Contenido (Continuación)

Contenido (Continuación)

Contenido (Continuación)

Lista de Figuras

Lista de Figuras (Continuación)

Página

Lista de Figuras (Continuación)

Lista de tablas

Glosario

C

Cibertexto: Palabra o conjunto de palabras procesadas con un algoritmo de criptografía.

Cracker: Persona que de forma mal intencionada intenta explotar y/o engañar un sistema de cómputo.

CUDI: Corporación Universitaria para el Desarrollo de Internet. Corporación creada por el Gobierno federal de México para el desarrollo del proyecto nacional de Internet 2.

D

DES: Data Encryption Standard. Un algoritmo de criptografía simétrica desarrollado por IBM a mediados de 1970 y provisto por The National Bureau of Standards (NIST ahora).

DNS: Domain Name System. Conjunto de protocolos y servidores que proveen la traducción nombre/dirección para Internet. Estos servidores traducen nombres del tipo x.y.z en direcciones IP, y viceversa. La base de datos DNS ha sido expandida para almacenar atributos adicionales que son útiles para otros servicios de Internet.

DSA: Directory System Agent: Una entidad dentro de la especificación del sistema de directorios X.500. Un DSA es una base de datos que contiene registros para usuarios, roles, dispositivos, organizaciones, etc.

F

Firewall: Mecanismo de control de acceso para establecer políticas de control de flujo de información de un lado a otro de la pared de fuego.

FTP: File Transfer Protocol. Protocolo estándar para la transmisión de archivos.

H

Hacker: Persona que intenta descubrir las vulnerabilidades de un sistema de cómputo para protegerlo.

HMAC: Hashed MAC. Un código de autenticación de mensajes basado en una función hash de un solo sentido, asegurada con una llave secreta.

I

IDEA: International Data Encryption Algorithm. Un algoritmo de criptografía simétrica que emplea llaves de 128 bits y es utilizado en herramientas como PGP.

IETF: Internet Engineering Task Force. El grupo de individuos que participa en el desarrollo de los estándares de Internet. La IETF está compuesta por más de 50 grupos de trabajo que desarrollan dichos estándares.

IP: Internet Protocol. Protocolo de la capa 3 desarrollado bajo el financiamiento del Departamento de Defensa de Estados Unidos a mediados de los 1970s y principios de 1980s. Está instrumentado en una gran variedad de equipos y plataformas de sistemas operativos, haciéndolo el protocolo de este tipo, mayormente disponible e independiente de marcas comerciales.

ISO: International Standards Organization. Un grupo de estándares reconocido por la Unión Internacional de Telecomunicaciones de las Naciones Unidas y

responsable de la promulgación de una variedad de estándares, incluyendo comunicación y procesamiento de datos.

J

Jitter: Variación del retardo en una red de conmutación de paquetes.

K

Kerberos: Un mencanismo de autenticación de usuarios.

L

LAN: Local Area Network. Una red de comunicación de datos con una extensión geográfica limitada, típicamente un solo edificio o piso dentro de un edificio.

M

MAC: Mandatory Access Control. Se refiere a las políticas de control de acceso que son basadas por reglas o dirigidas de forma administrativa. MAC es un término muy popular en la comunidad de seguridad de computadoras ya que es utilizado en los Criterios de Evaluación de Sistemas de Computadoras Confiables (libro naranja) y sus derivados.

MD2/4/5: Message Digest 2/4/5. Una serie de algoritmos hash de un solo sentido desarrollados por los Laboratorios RSA y provistos como parte de sus productos ofrecidos.

MTA: Message Transfer Agent. Entidad que provee enrutamiento de correo electrónico y funciones de envío. El término se deriva de las series de estándares X.400 y puede ser aplicado a cualquier conmutador de mensajes.

N

Nessus: Proyecto de la comunidad de Internet, que provee un escudriñador (scanner) de dominio público. Una herramienta robusta, actualizada y sencilla para aplicar seguridad de forma remota.

O

OSI: Open System Interconnection. El área de ISO enfocada a los estándares de protocolos de comunicación de datos y sistemas distribuidos.

P

PDU: Personal Data Unit. Un elemento de datos emitido por una entidad del tipo protocolo, por ejemplo, un datagrama IP.

PGP: Pretty Good Privacy: Un protocolo de mensajes seguro para ser utilizado en mensajería informal. Utiliza los algoritmos RSA e IDEA.

Conjunto de Protocolos: una familia de protocolos que trabajan de forma conjunta y en una forma consistente entre sí.

Pila de Protocolos: un conjunto de protocolos por capas que trabaja de forma conjunta para proveer comunicación entre aplicaciones.

Protocolo: un conjunto de reglas que dictan la operación sobre alguna función de comunicaciones.

Q

QoS: Quality of Service. Calidad de Servicio, es la capacidad de ofrecer uno o varios servicos de red sometidos a los criterios y acuerdos de calidad de la(s) entidad(es) receptora(s) (Percepción Humana/ Requerimientos Técnicos).

R

RC2/4: Rivest Cipher 2/4. Algoritmos criptográficos simétricos, propiedad de Laboratorios RSA.

RSA: Ron **R**ivest, Adi **S**hamir, Len **A**dleman from MIT. El algoritmo de criptografía asimétrica más ampliamente conocido y patentado en Estados Unidos. Se utiliza para firmas digitales y distribución de llaves.

S

SHA: Secure Hash Algorithm. Un algoritmo no criptográfico que aplica una función hash de un solo sentido, fue diseñado para ser expresamente utilizado en DSA/DSS.

SILS: Standards for Interoperable LAN Security: Los estándares desarrollados por el comité 802.10 de la IEEE para ser utilizados en redes de area local (LAN IEEE).

SMTP: Simple Mail Transfer Protocol. Protocolo estándar para la transmisión de mensajes de correo electrónico.

Socket: Una interfaz entre el usuario y la red, cada interfaz puede soportar algun tipo particular de comunicación como: ráfaga de bytes orientados a conexión

confiable, ráfaga de paquetes orientas a conexión confiable y/o transmisión de paquetes no confiable.

SSH: Protocolo que provee una conexión segura de terminal remota.

T

Telnet: Protocolo estándar que provee una conexión de terminal remota.

TCP: Transmission Control Protocol: Protocolo de transporte orientado a conexión utilizado en Internet y utilizado por muchas aplicaciones como: Telnet, FTP, SMTP y HTTP para establecer comunicaciones confiables.

TCP-Wrappers: Mecanismo de control de acceso para sistemas operativos UNIX.

U

ULSA: Universidad La Salle. http://www.ulsa.edu.mx

V

VPN: Virtual Private Network. Una red privada configurada dentro de una red pública, lo que implica costos menores que una red privada dedicada. Ofrece servicios de integridad y confidencialidad.

Capítulo I

Introducción

El acceso a Internet es un recurso cada día más empleado para una amplia gama de servicios como telefonía, videoconferencia, búsquedas por el Web, comercio, y correo electrónico, entre otros. Por lo anterior, existe la gran necesidad de contar con un acceso más rápido a dicha red. Debido a la gran aceptación y penetración que Internet ha tenido en la población, se vislumbra un problema de saturación potencial.

En Estados Unidos, el 1o de octubre de 1996 se reunieron 36 universidades de ese país y crearon un proyecto conjunto llamado Internet2. El propósito de este proyecto es hacer posible una siguiente generación de la red Internet creando la infraestructura de comunicación y las aplicaciones que darán un impulso a la investigación científica, al concepto de bibliotecas virtuales, telemedicina, entre muchas otros. El día 8 de abril de 1999 se estableció oficialmente el proyecto en México bajo la administración de la Corporación Universitaria para el Desarrollo de Internet (CUDI) [CUDI, 2001].

La nueva red Internet2 ya está en operación en Estados Unidos, Canadá y México. En este proyecto se encuentran varias instituciones académicas del país, entre ellas el CICESE.

Una de las grandes diferencias que existen entre Internet convencional e Internet2 es la velocidad de interconexión lograda entre sus nodos principales, mediante la utilización de tecnologías y protocolos que permiten dichas velocidades y ambientes de operación deseables para la ejecución de aplicaciones de siguiente generación. La mayoría de dichos protocolos son experimentales. Se formaron diversos grupos de trabajo para la investigación y experimentación de nuevas tecnologías, en búsqueda de instrumentar una red de siguiente generación que brinde conexiones rápidas y eficientes para la ejecución efectiva de aplicaciones demandantes de recursos de comunicación.

La motivación principal de este trabajo de tesis es contribuir a Internet2 en México, también conocida como Red-CUDI, y proponer una plataforma segura a través de recomendaciones y mecanismos de seguridad acordes a las necesidades de una red de alto rendimiento sobre la que se espera se ejecuten aplicaciones de primer nivel.

Objetivo general

Investigar protocolos estándares de seguridad y la aplicación de VPN e IPSec en el medio de experimentación de los equipos y protocolos involucrados en la red de Internet2 en México.

Objetivos específicos

- Investigar la arquitectura, protocolos, interfaces y equipos asociados a la Red CUDI particularizando en aspectos tales como: pruebas de vulnerabilidad y administración.
- Investigar las fortalezas y debilidades de los protocolos de seguridad propuestos por el área de seguridad de la IETF, en especial los trabajos desarrollados sobre IPSec y VPN.
- Conceptualizar e instrumentar escenarios reales de pruebas dentro de Red CUDI.
- En acuerdo a las especificicaciones dictadas por el área de seguridad de la IETF, instrumentar y probar IPSec en el enrutamiento de VPN, y desarrollar pruebas en Red-CICESE y en Red-CUDI.
- Aplicar los resultados de forma inmediata en el contexto de la Red CUDI.

Marco de referencia de la tesis

El tema es la Seguridad en Redes e Informática, un área de reciente aparición en los mundos de la Computación y las Comunicaciones. Con el crecimiento exponencial del uso de Internet se han creado intereses de muchas índoles sobre los recursos disponibles en las redes, lo que ha obligado a invertir en mecanismos de Seguridad, para proteger la información y equipos de accesos no autorizados que puedan afectar su funcionamiento.

Ante el planteamiento nacional de Internet 2 en México, la seguridad resulta un área de oportunidad de gran interés y desarrollo. El proyecto cubre aspectos tecnológicos y de investigación importantes en el área de Telemática, concretamente aquéllos relacionados con el diseño de protocolos y algoritmos enfocados a proporcionar servicios de seguridad en una red con características como la Internet 2.

Características principales de la tesis

En este trabajo de tesis se está abordando un tema que es el estado del arte en Seguridad en Redes, donde la investigación y el desarrollo de Protocolos de Seguridad son actividades a nivel mundial en la actualidad. El trabajo es el primero en su tipo en el CICESE y a nivel nacional es precursor en el ambiente de Internet en México. Sus características principales se citan a continuación.

- Trabajo de investigación con alto grado de actualidad.
- Los resultados esperados se aplicarán directamente en el escenario de Internet2 México.
- Contribuye al fortalecimiento de la vinculación entre grupos de investigación en el CICESE.
- ***Resultados originales susceptibles a ser publicados en revistas especializadas en el tema.***

Organización del trabajo

Como parte inicial de este escrito, se presenta una revisión de diferentes conceptos teóricos fundamentales para la comprensión del funcionamiento de protocolos de seguridad y el área de su aplicación (Capítulo II). El concepto más importante y relevante es la instrumentación de servicios de seguridad en la capa de red, de tal manera que su ejecución sea transparente al usuario e independiente de las plataformas de software utilizadas, obteniendo en consecuencia una solución general, aunque no total.

En el capítulo III se describe el protocolo de seguridad aplicado en este trabajo, IPSec, el protocolo de seguridad para IP, su diseño, arquitectura, componentes y funcionamiento para las dos versiones de IP utilizadas actualmente IPv4 e IPv6.

En el capítulo IV se presenta la metodología que siguió el análisis de IPSec y se describe el procedimiento empleado para la realización e instrumentación de los escenarios de pruebas. El diseño e instrumentación del experimento se desarrolló para la Red-CICESE, elaborando una VPN entre el Laboratorio de Redes Inalámbricas y Telemática, un escenario en Internet2 e Internet1 creando conexiones seguras entre instituciones del Grupo de Trabajo de Seguridad de Internet2 [GTS, 2001], y uno especialmente conceptualizado y diseñado para la reunión de Otoño de CUDI.

En el capítulo V se presenta la discusión de los resultados obtenidos a partir de las muestras obtenidas de los escenarios experimentales, al igual que un análisis numérico de éstos.

En el capítulo VI se presentan las conclusiones, líneas de investigación futuras y comentarios de los resultados obtenidos en este trabajo de tesis.

En tecnología hay una serie de términos en inglés para los cuales es difícil encontrar una traducción al español sin perder el concepto correcto, por lo que en este escrito se usarán los términos originales.

Capítulo II

Introducción

La seguridad ha sido un elemento que tomó relevancia en la última década en los mundos de la Computación y las Comunicaciones, esto como un efecto natural en los ambientes que crecen de forma exponencial y que pierden las características de conocimiento y confianza entre quienes interactuan. Conviene mencionar que en el medio académico y restringido donde surgió Internet y permaneció algunos años, la Internet es actualmente un ambiente de más de 60 millones de computadoras conectadas, de más de 200 países de todos los continentes, millones de usuarios, de diferentes culturas, con diferentes propósitos, inquietudes, edades, etc. En el año 2000 se registraron con respecto al año 1999, el doble de incidentes de seguridad, y el doble de computadoras afectadas por estos incidentes, 9 millones 350 mil computadoras [CERT, 2001].

La seguridad no fue un aspecto considerado en el diseño inicial de los protocolos de comunicación y sistemas operativos, lo que ha ocasionado oportunidades diversas para acceder de forma no autorizada a redes y sistemas y ha dado lugar a una de las actividades más populares en estos días en el ciberespacio: la intrusión de sistemas.

En los últimos años se han desarrollado una gran variedad de herramientas, metodologías y técnicas para contarrestar estas deficiencias de origen y proteger a los sistemas de intrusos, sobre todo al nivel de aplicaciones del usuario o del administrador.

El interés de este trabajo es en particular sobre los esfuerzos por proporcionar mecanismos de protección en capas de comunicación intermedias, técnicas aplicadas directamente a los protocolos de comunicación para proporcionar la transmisión segura de información. Con la idea anterior, en este capítulo se definirán conceptos básicos de seguridad para describir posteriormente los protocolos estándares de seguridad.

Seguridad de información

Las objetivos fundamentales en Seguridad son: prevenir la revelación, la modificación y la utilización no autorizada de datos, recursos de computadora y de red. La definición del estándar ISO 7498-2 [ISO, 1989] define cinco elementos básicos que constituyen la seguridad de un sistema: la **confidencialidad** de los datos, la **autenticación** de los datos, la **integridad** de los datos, el **control de acceso** (disponibilidad) y el **no repudio**.

Confidencialidad implica que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas. **Autenticación** define mecanismos para garantizar la procedencia de la información, ya sea a nivel de usuario o de computadora. **Integridad** implica que los datos no han sido modificados o corrompidos de manera alguna

desde su transmisión hasta su recepción. El **control de acceso** establece la forma en que el recurso está disponible cuando es requerido. El **no repudio** es la garantía de transmisión y recepción de información, busca proteger al emisor de que el receptor niegue haber recibido el mensaje, y proteger al receptor de que el transmisor niegue haber enviado el mensaje.

En seguridad de información, se consideran seis elementos sobre los cuales se han hecho desarrollos en busca de proporcionar ambientes protegidos [Kent, 2001]:

1. ***Seguridad física*:** un elemento de atención básica, los recursos deben ser protegidos físicamente de accesos no autorizados, accidentes, robos, etc.
2. **Segu*ridad de procedimientos*:** elemento enfocado a las medidas de protección en los procesos y procedimientos.
3. ***Seguridad de personal*:** elemento enfocado a la definición de privilegios, y accesos de personal involucrado con los recursos.
4. ***Seguridad de emanación de compromisos*:** elemento enfocado a la definición de responsabilidades y compromisos en el manejo de la información.
5. ***Seguridad de sistemas operativos*:** elemento enfocado a la protección de servicios y usuarios, accesos no autorizados al sistema operativo de una computadora.
6. ***Seguridad de comunicaciones*:** elemento enfocado a la transmisión segura de información a través de medios de comunicación.

Prevención es la palabra clave en Seguridad, se han desarrollado una gran diversidad de técnicas y herramientas de prevención a nivel de aplicaciones, siempre dependientes del sistema operativo o la aplicación que se utilice. Los protocolos de seguridad buscan brindar servicios de seguridad en la transmisión de información, sin importar el tipo, procedencia, sistema operativo o aplicación que la genere, son este tipo de esfuerzos el objeto de estudio de este trabajo.

Terminología

Dentro del área de Seguridad, se manejan diversos términos para identificar los factores que intervienen, los conceptos principales son: vulnerabilidades, ataques, contramedidas y amenazas [Kent, 2001].

Vulnerabilidades.

El software está desarrollado por humanos, quienes modelan e implantan programas a su criterio, concepto y conocimiento del lenguaje de programación que utilizan, es común, en consecuencia, encontrar imperfecciones en los sistemas. Son estas imperfecciones las que propician oportunidades para accesos no autorizados, las que se conocen como vulnerabilidades de los sistemas.

Ataques.

Los ataques son los medios por los cuales se explotan las vulnerabilidades, se identifican dos tipos de ataques: extracción (wiretapping) pasiva y extracción activa.

En la extracción pasiva el atacante escucha, sin modificar mensajes o afectar la operación de la red. Generalmente no puede detectarse este tipo de ataque, pero sí prevenirse mediante mecanismos como la encriptación de información.

Los objetivos del atacante son la intercepción y el análisis de tráfico en la red. Al estar escuchando el tráfico, el atacante puede identificar:

- el origen y destino de los paquetes de comunicación, así como la información de cabecera.
- Monitorear el tráfico y horarios de actividad.
- Identificar el uso de protocolos y observar la transferencia de datos entre protocolos que no utilicen encriptado, por ejemplo la versión no segura de telnet o ftp que transfieren la clave de usuario en texto simple.

En la extracción activa el atacante modifica los mensajes o irrumpe la operación de la red. El atacante tiene como objetivo modificar datos o bien crear tráfico falso. Este tipo de ataque, generalmente puede detectarse, pero no prevenirse. La gama de actividades identificadas sobre ataques conocidos puede clasificarse en cuatro categorías:

1. *Modificación de mensajes*: al interceptar mensajes, se altera su contenido o su orden para irrumpir su flujo normal.
2. *Degradación y fraude del servicio*: tiene como objetivo intervenir el funcionamiento normal de un servicio, impide el uso o la gestión de recursos en la red. Ejemplo de este

ataque es el de negación de servicio (DoS, Denial of Service), donde se suprimen los servicios de SMTP, HTTP, FTP, DNS, entre otros.

3. *Reactuación*: al interceptar mensajes legítimos, se capturan y repiten para producir efectos diversos, como el ingresar dinero repetidas veces en una cuenta de banco.
4. *Suplantación de identidad*: Este es uno de los ataques más completos y nocivos. El intruso o atacante adopta una identidad con privilegios en una red y explota esos privilegios para sus fines. Un ataque con prioridad de atención para todo administrador de red es el "spoofing" donde el intruso obtiene servicios basados en la autenticación de computadoras por su dirección IP. Es recomendable seguir una estrategia y de preferencia tener una herramienta para combatirlos [Baluja, 2000].

Todos estos ataques tienen un impacto relativo a la política de seguridad de un sistema, aunque en Internet dentro de los más temidos se encuentra el DoS por su relevancia al suprimir el funcionamiento de un sistema, y el *Spoofing* al obtener privilegios de acceso de forma fraudulenta. La autenticación de IPSec ESP/AH (Encapsulating Security Payload/Authentication Header), que será descrito en el capítulo III, provee protección en contra de *spoofing* ya que cualquier paquete fraudulento será identificado y descartado [Kriwaniuk, 2001].

Contramedidas.

Lo más importante es contar con una Política de Seguridad, un documento legal y con apoyo directivo, que define la misión, visión y objetivos de los recursos de red e información en cuestión. En una política se define lo que es permitido y lo que no, las necesidades de confidencialidad, autenticación y otros servicios de seguridad para los recursos involucrados. Toda red debe contar con una política de seguridad, el CICESE tiene su Política de Seguridad autorizada por el Director General [PolCICESE, 2001]. La política de seguridad para Red-CUDI o Internet 2 en México se encuentra en elaboración por el grupo de trabajo del Comité para el Desarrollo de la Red [GTS, 2001] en conjunto con la Comisión de Seguridad de CUDI.

Las contramedidas son entonces, las políticas de seguridad apoyadas por todos los medios técnicos o de procedimientos que se aplican y desarrollan para atender vulnerabilidades y frustrar ataques específicos. Ejemplos: reglamentos, *firewalls*, nessus,

ssh, *tcp-wappers*, antivirus, kerberos, radius, entre muchos otros comerciales o de dominio público.

Amenazas.

Las amenazas están dadas por condiciones de entorno, dada una oportunidad y adversarios motivados y capaces de montar ataques que explotan vulnerabilidades, podría producirse una violación a la seguridad (confidencialidad, integridad, disponibilidad y/o uso legítimo) [Cripto, 2001]. Los perfiles de capacidades de los atacantes se identifican como sigue:

- Inserción de mensajes solamente.
- Escuchar e introducir mensajes.
- Escuchar y obstruir.
- Escuchar, obstruir e insertar mensajes.
- Escuchar y remitir un mensaje ("hombre en el medio")
- Capacidades activas y pasivas de forma unidireccional o bidireccional

Cada enlace en una red y cada recurso es susceptible a diferente tipo de amenazas, de ataques, y quizá a diferentes atacantes. El análisis de riesgos y el monitoreo constante de vulnerabilidades pueden identificar las amenazas que han de ser contrarestadas, así como especificar los mecanismos de seguridad necesarios para hacerlo.

De acuerdo a la figura 1, las cuatro categorías generales de amenazas que se utilizan en la actualidad son las siguientes:

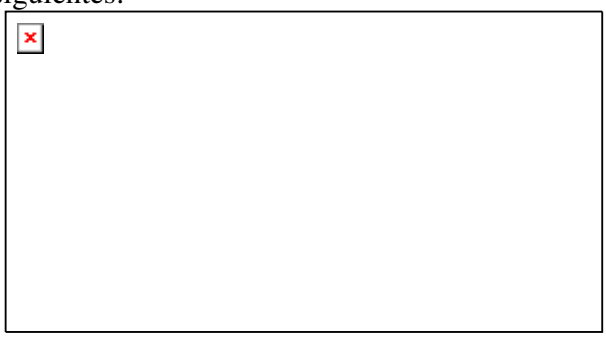


Figura 1. Categorías de amenazas a la seguridad. a) Interrupción, b) Intercepción, c) Modificación, d) Falsificación.

De acuerdo a la figura 1, las cuatro categorías generales de amenazas que se utilizan en la actualidad son las siguientes:

1.*Interrupción*: es una amenaza contra la disponibilidad, el ataque ocasiona que un recurso del sistema deje de estar disponible. Ejemplos: DoS, destruir un elemento de hardware o cortar una línea de comunicación.

2.*Intercepción*: es una amenaza contra la confidencialidad, el ataque produce la captura no autorizada de información en el medio de transmisión. Ejemplos: *Sniffers*, lectura de cabeceras, intercepción de datos.

3.*Modificación*: es una amenaza contra la integridad, el ataque produce no solo el acceso no autorizado a un recurso sino también la capacidad de manipularlo. Ejemplos: modificación del contenido de mensajes interceptados, alterar programas para modificar su funcionamiento.

4.*Falsificación*: es una amenaza contra la autenticidad, el ataque produce que una entidad no autorizada inserte mensajes falsos en el sistema. Ejemplos: sustitución de usuarios, alterar archivos, inserción de mensajes espurios en la red.

Servicios y protocolos por capas de red.

El desarrollo de protocolos está basado en los servicios definidos en las capas de comunicación del modelo estandar OSI-ISO [Briscoe, 2000], para entender apropiadamente las características de los protocolos de seguridad y su intervalo de aplicación, se ha elaborado una marco de trabajo que esquematiza una relación entre los servicios y las capas de protocolos [Kent, 2001]. En la Tabla I puede observarse que los servicios de seguridad pueden aplicarse completamente en la capa 7, parcialmente en las capas 3 y 4, mucho menos ingerencia en las capas 1 y 2, y prácticamente ninguna función en las capas 5 y 6.

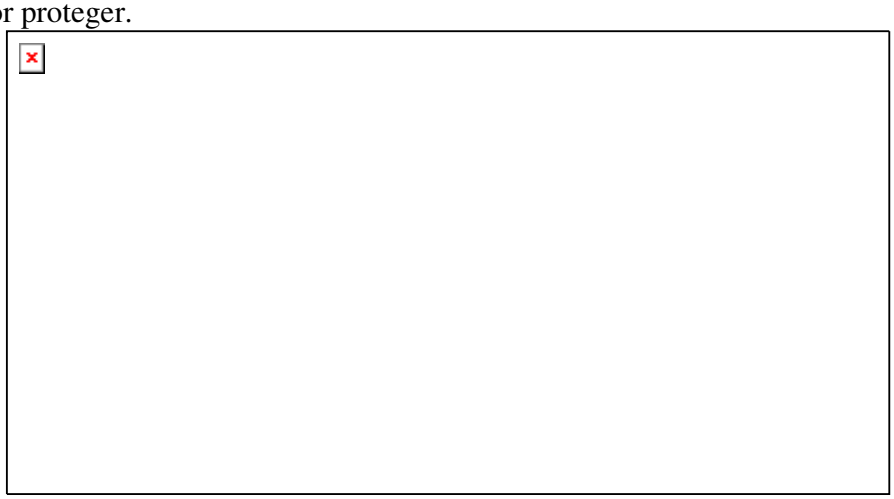
Tabla I. Relación de Servicios a Capas de Protocolos.

	Capas de comunicación						
Servicio	***1***	***2***	***3***	***4***	***5***	***6***	***7***

Autenticación de entidad extremo (Peer Entity)	-	-	✔	✔	-	-	✔
Autenticación del origen de los datos	-	ND	✔	✔	-	-	✔
Servicios de Control de acceso	-	ND	✔	✔	-	-	✔
Confidencialidad de la conexión	✔	✔	✔	✔	-	-	✔
Confidencialidad orientada a no conexión	-	✔	✔	✔	-	-	✔
Confidencialidad de un campo selectivo	-	-	-	-	-	✔	✔
Confidencialidad del flujo de tráfico	✔	-	✔	-	-	-	✔
Integridad orientada a no conexión	-	ND	✔	✔	-	-	✔
Integridad de un campo selectivo	-	-	-	-	-	-	✔
Origen, no repudio	-	-	-	-	-	-	✔
Recepción, no repudio	-	-	-	-	-	-	✔

Seguridad en la Capa Física.

En esta capa se tiene una dependencia significativa de la tecnología de red que se utilice. El equipo y todo lo demás cambia si hay modificación de tecnología de comunicación: Ethernet, SDH, SONET, etc. Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de trafico), no se provee servicio, pero se da soporte a las capas superiores para control de acceso, autenticación del origen de los datos e integridad orientada a no conexión. La granularidad de protección es individual o a nivel de circuitos conmutados. En la Figura 2 se esquematiza un escenario común de componentes de capa física, se distinguen con la letra S aquellos componentes con capacidad de protección de datos y cifrado, y con la letra D aquellos que son los puntos débiles por proteger.

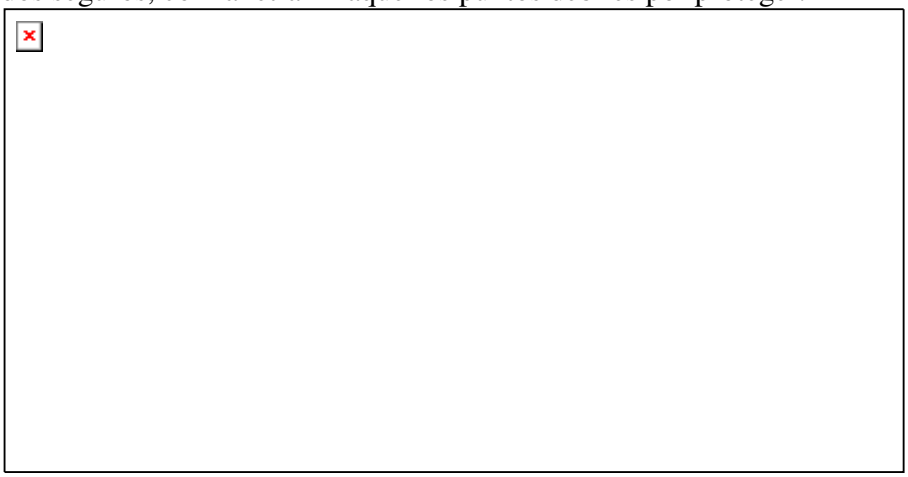


MTA:Message Transfer Agent.
MUX: Multiplexor.

Figura 2. Ejemplo de seguridad en la capa física en una red de paquetes.

Seguridad en la Capa de Enlace

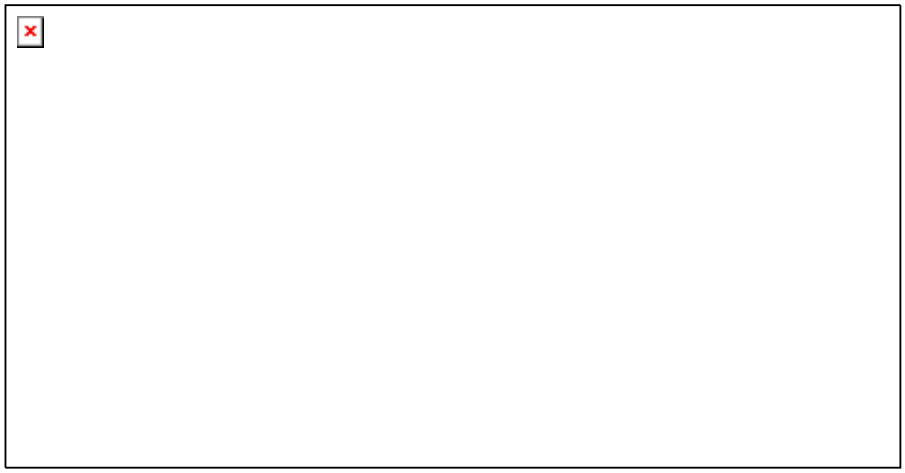
En esta capa se tiene una dependencia ligera de la tecnología (IEEE LANs) y del conjunto de protocolos que se utilice. Los servicios de seguridad son: confidencialidad, control de acceso, autenticación del origen de los datos e integridad orientada a no conexión. La granularidad de protección es en los *hosts* individuales y en los segmentos de la LAN. En la Figura 3 se esquematiza un escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.



MTA:Message Transfer Agent.

Figura 3. Ejemplo de seguridad en la capa de enlace en una red de paquetes.

En la Figura 4, se muestra la conjunción de los ejemplos de la capa 1 y 2, se aprecia su complemento y necesidad de aplicación de seguridad en las capas superiores.

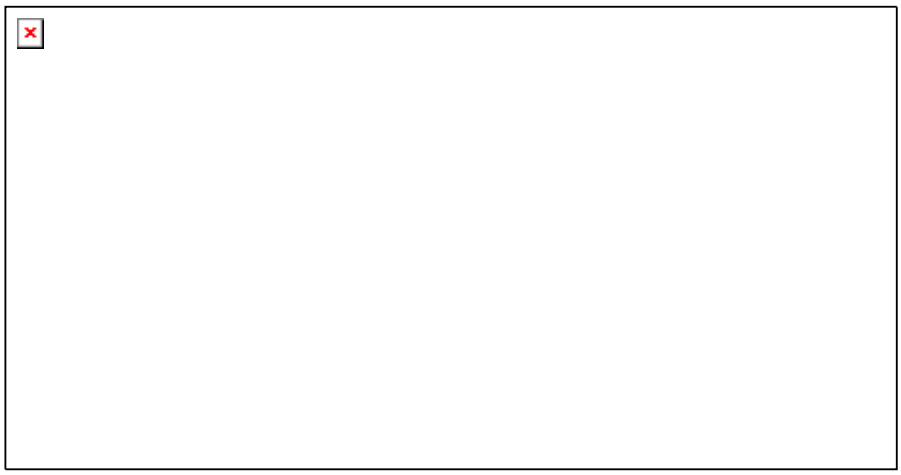


MTA:Message Transfer Agent.

Figura 4. Ejemplo de seguridad en las capas física y de enlace en una red de paquetes.

Seguridad en la Capa de Red (inferior).

En la subcapa inferior de esta capa se tiene una alta dependencia de la tecnología de red y menor sobre el conjunto de protocolos que se utilicen. Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de tráfico limitado), control de acceso, autenticación del origen de los datos e integridad orientada a conexión y a no conexión (dependiente de la red). La granularidad de protección radica en los hosts (por conexión) y en el enrutador (LAN). En la Figura 5 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

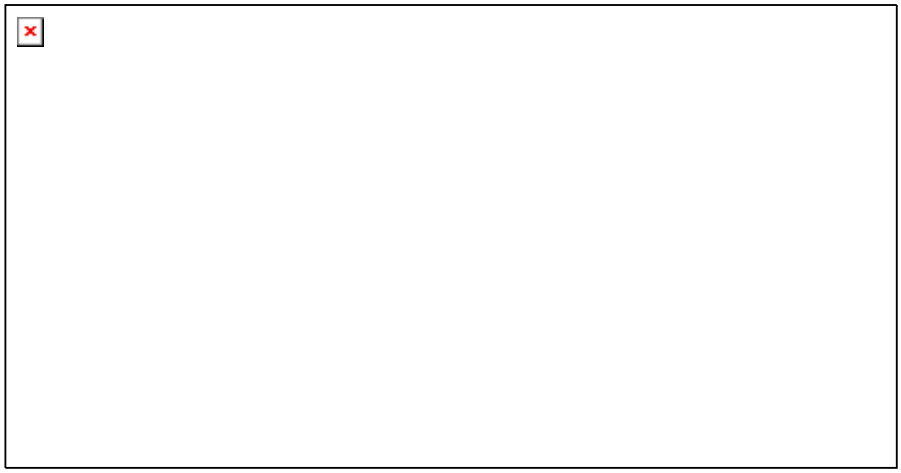


MTA:Message Transfer Agent.

Figura 5. Ejemplo de seguridad en la capa de red (inferior) en una red de paquetes.

Seguridad en la Capa de Red (superior)

En la subcapa superior de esta capa no se tiene dependencia de la tecnología de red, aunque sí moderada sobre el conjunto de protocolos que se utilicen (el tunelaje de IP disminuye esto considerablemente). Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de tráfico limitado), control de acceso, autenticación del origen de los datos e integridad orientada a no conexión y a secuencia parcial. La granularidad de protección radica en los hosts, en la red o seguridad de calidad de servicio (QoS). En la Figura 6 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquellos componentes considerados seguros, con la letra D aquellos puntos debiles por proteger.

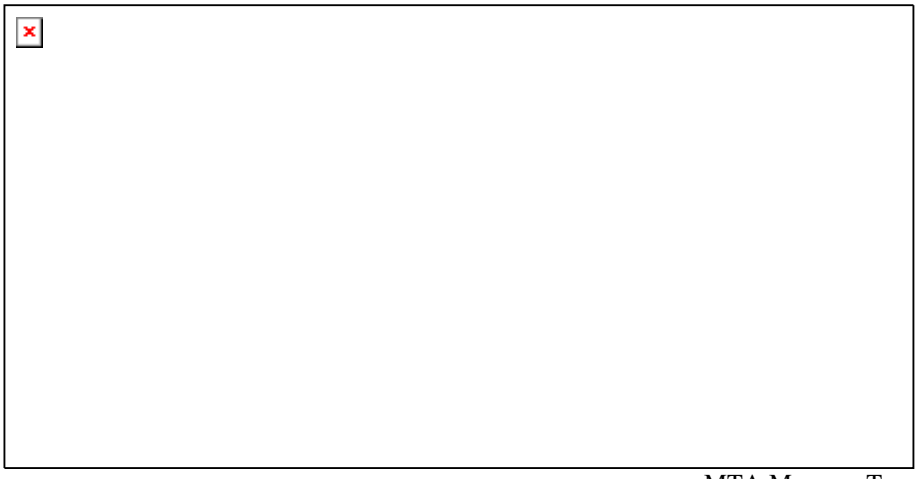


MTA:Message Transfer Agent.

Figura 6. Ejemplo de seguridad en la capa de red (superior) en una red de paquetes.

Seguridad en la Capa de Transporte.

En esta capa no se tiene dependencia de la tecnología de red, aunque sí alta dependencia sobre el conjunto de protocolos que se utilice. Los servicios de seguridad son: confidencialidad, control de acceso, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orientada a no conexión e integridad orientada a conexión con recuperación de datos. La granularidad de protección radica en los hosts por conexión. En la Figura 7 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquellos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.



MTA:Message Transfer Agent.

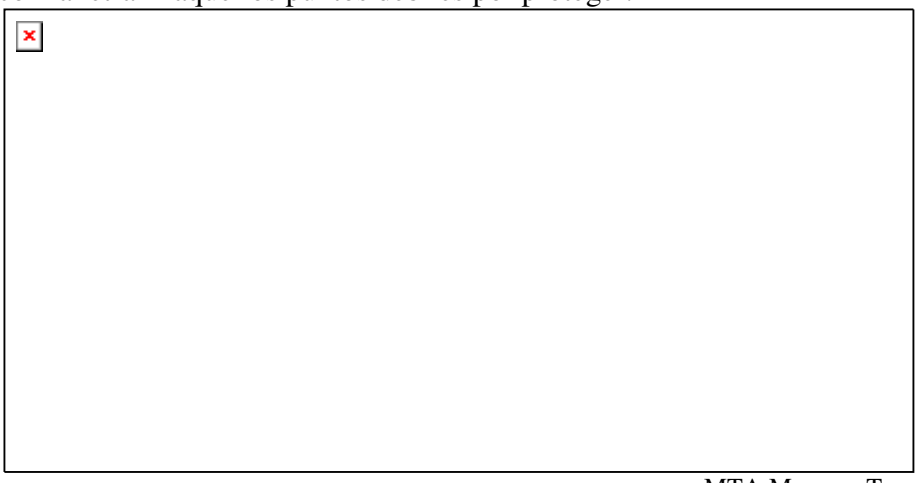
Figura 7. Ejemplo de seguridad en la capa de transporte en una red de paquetes.

Seguridad en la Capa de Sesión.

En esta capa no se tiene dependencia de la tecnología de red, aunque sí alta dependencia sobre el conjunto de protocolos que se utilice. Los servicios de seguridad son: integridad orientada a conexión, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orientada a conexión y control de acceso. La granularidad de protección radica en las sesiones. El escenario de componentes y riesgos para esta capa es igual al de la capa de transporte mostrada en la Figura 7.

Seguridad en la Capa de Aplicación.

En esta capa no se tiene dependencia de la tecnología de red. La dependencia es significativa sobre las aplicaciones. Los servicios de seguridad son: confidencialidad (orientado a conexión, a no conexión, o a un campo selectivo), autenticación del origen de los datos, autenticación de la entidad extremo, integridad (orientada a conexión y a no conexión, con opción a recuperación) y no repudio (en el origen y recepción). La granularidad de protección radica en los usuarios, aplicaciones y PDUs (Protocol Data Unit). En la Figura 8 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.



MTA:Message Transfer Agent.

Figura 8. Ejemplo de seguridad en la capa de aplicación en una red de paquetes.

Mecanismos específicos de seguridad.

Se han desarrollado una gran variedad de algoritmos, mecanismos y técnicas para brindar protección a los recursos informáticos, y garantizar la integridad, confidencialidad y control de acceso de información.

La confidencialidad es necesaria para mantener un secreto, pero sin autenticación, no puede saberse que la persona con la que se está compartiendo ese secreto, es quien dice ser, y sin la confianza de la integridad del mensaje recibido, no se sabe si el mensaje es el mismo al que fue enviado. Los mecanismos descritos en esta sección están enfocados a garantizar estos aspectos.

Criptología.

La Criptología es un área de estudio de las Matemáticas con gran aplicación en las Ciencias de la Computación, se divide en dos ramas: la criptografía, que involucra lo relacionado al diseño de sistemas para encriptar o cifrar información, y el criptoanálisis sobre el proceso inverso, involucra los sistemas para desencriptar o descifrar códigos [Grosek, 2001].

Los algoritmos criptográficos proveen confidencialidad de datos al convertir un mensaje (texto plano) en garabatos (cibertexto) y visceversa.

Los sistemas de criptografía se han clasificado como se muestra en la figura 9. Los sistemas simétricos basan su cifrado y descifrado en una sola llave, los sistemas asimétricos o de llave pública, basan su seguridad en llaves diferentes, una privada para descifrar y una pública para cifrar. Los algoritmos de bloque (Block) no poseen memoria interna, los mismos bloques utilizados para el texto plano son siempre relacionados a los bloques del cibertexto. Los sistemas de ráfaga (Stream) poseen memoria interna, los bloques del texto plano, no siempre son transformados a bloques idénticos de cibertexto. Los algoritmos criptográficos, sin importar su simetría, son conmutativos:

texto plano = Desencriptar (Encriptar (texto plano))

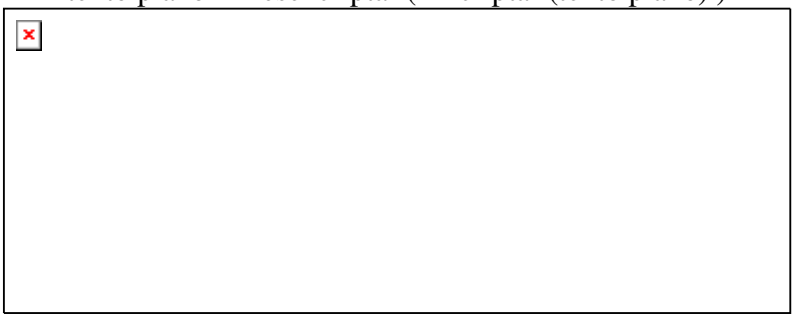


Figura 9. Clasificación de Criptosistemas.

Hablando de criptología, el ejemplo común involucra a quien envía el mensaje encriptado (Alicia), el que recibe el mensaje y lo descifra (Bertha), y el intruso en algún

punto de la transmisión, intentando descifrar mensajes (Oscar), como se muestra en la figura 10.

Para caracterizar un algoritmo seguro o robusto se manejan tres categorías: a) **incondicionalmente seguro**, solo hay un algoritmo de este tipo y no es implementable, ya que no existe manera de generar números realmente aleatorios, siempre dependen de una semilla, b) **probablemente seguro**, el problema matemático para descifrarlo es altamente complicado ($O(2^n)$), c) **computacionalmente seguro** (2^{70}), se requiere gran capacidad de cómputo para descifrarlo.

Figura 10. Esquema de una comunicación segura.

De los Block Ciphers el más comercial es quizá el DES (Data Encryption Standard), no es robusto pero es simple de instrumentar. Una mejor opción para sistemas más seguros es el 3DES o bien, IDEA (International Data Encryption Algorithm) más robusto aunque costoso de recursos. De los sistemas asimétricos, RSA (nombre por sus autores) es el más popular.

La selección del algoritmo de criptografía a ser utilizado en las herramientas de seguridad, se realiza en los mismos términos que otros algoritmos de computación, en base a su complejidad y robustez, acordes al nivel de seguridad deseado en el sistema.

Los algoritmos robustos son considerados de alta confidencialidad y valor, por ello, países como Estados Unidos[1] tienen leyes muy estrictas con respecto a la exportación de la tecnología criptográfica [BXA, 2001].

Mecanismos de integridad de datos.

La integridad, como se ha referido antes, se refiere a la garantía de que la información no ha sido alterada durante su transmisión. Asi como hay cibersistemas simétricos y asimétricos, también hay métodos simétricos y asimétricos para garantizar la integridad de mensajes [Naganand, et al., 1999]. Los MAC (Message Authentication Codes), son códigos que utilizan funciones hash[2]. El MAC se genera al aplicar la función hash a una llave privada con el mensaje, el resultado se transmite en conjunto con el

[1] La US Commerce Department's Bureau of Export Administration administra la regulación de exportación que controla, entre otras cosas la criptografía.

[2] un algoritmo criptográfico de un solo sentido que cambia una variable de tamaño arbitrario y la convierte en una variable de tamaño fijo.

mensaje, y la verificación del MAC permite aplicar la función hash a la llave secreta con el mensaje para producir un compendio temporal, y comparar este compendio con el atado al mensaje. Este proceso se llama transformación fundamental o *keyed hashing*. Es importante realizar el proceso completo, porque solo aplicar la función hash a unos datos no provee autenticación, es como una comprobación de paridad (checksum), una función *keyed hash* es un MAC.

HMAC es un método especial. Fue diseñado por Hugo Krawczyk, Ran Canetti y Mihir Bellare [RFC2104, 1997]. Es un método mejorado de manejo de llaves con funciones Hash, y brinda protección adicional a otros algoritmos, de tal forma que SHA (Secure Hash Algorithm) se convierte en HMAC-SHA, MD5 (Message Digest 5) se convierte en HMAC-MD5. La construcción de HMAC es criptográficamente más fuerte que otras funciones hash. Por ejemplo, MD5 es susceptible a un ataque del tipo colisión, donde es posible encontrar dos entradas diferentes que produzcan el mismo compendio, HMAC-MD5 no es susceptible a este ataque.

Mecanismos de control de acceso y autenticación.

La autenticación es uno de los problemas más complicados en seguridad. Implica reconocer y garantizar que alguien (persona o computadora) es quien dice ser. La autenticación es un servicio básico de seguridad. Puede hablarse de autenticación con criptografía o sin criptografía, los grandes problemas radican en la autenticación de personas y los mecanismos de distribución de llaves y certificados.

Las firmas digitales es uno de los mecanismos más utilizados para el intercambio de mensajes en el correo electrónico. Los mecanismos de llaves digitales implican esquemas de confianza, el esquema común es que una persona cree su llave digital, y solicite que al menos otras dos firmen su llave, de esta manera hay al menos dos testigos de que esa llave le pertenece a esa persona. La generación de llaves para computadoras, son esquemas actuales, en sistemas seguros a nivel de red, no de usuario [Cooper, et al, 1995].

En lo que se está actualmente trabajando y buscando establecer, es la Infraestructura de Llaves Públicas (Public Key Infraestructure, PKI). Una infraestructura que forma un sistema en el que participan entidades certificadoras que garantizan la identidad digital de personas, instituciones o aplicaciones. El sistema es a través del manejo de certificados, documentos digitales para autenticar personas, servidores o aplicaciones. Es un esquema complicado, donde intervienen entidades generadoras/revocadoras de certificados, solicitantes de certificados y solicitudes de legalidad de certificados. Es un esquema que exije la participación del gobierno o de entidades oficiales para validar la identidad de personas y organizaciones. Cabe mencionar, que a la fecha, en México no existe ninguna entidad certificadora oficial.

Protocolos de Criptografía.

Dentro del contexto del modelo de interconexión OSI-ISO, la tabla II muestra la ubicación de algunos de los protocolos de criptografía más utilizados y reconocidos como estándares por la IETF. Las dos primeras capas están sujetas a los estándares de interoperabilidad de seguridad de LAN (SILS, Standard for Interoperable LAN Security) [IEEE, 1998].

Los protocolos de la capa de red son objeto de estudio de este trabajo de investigación, como se describe en los objetivos, en particular AH y ESP que son parte del conjunto de protocolos denominado IPSec.

Los protocolos de la capa de aplicación se describirán brevemente, sin profundizar, solo describiendo conceptos relevantes para el posterior entendimiento de su interoperabilidad con IPSec.

Tabla II. Capas y protocolos de criptografía.

Capa	***Nombre***	***Protocolos***
7	Aplicación	X.400, MSP, PEM, S/MIME, PGP, X.500, DNSSEC, Administración de certificados y llaves
6	Presentación	
5	Sesión	SSL
4	Transporte	TLSP
3	Red	NLSP, ESP, AH
2	Enlace de datos	SILS
1	Física	Enlace síncrono

Protocolo Secure Sockets Layer (SSL)

El protocolo SSL fue diseñado originalmente por Netscape Development Corporation©, la versión 3.0 fue diseñada con apoyo público y sugerencias de la industria con el siguiente objetivo: establecer una conexión segura (con criptografía) entre cliente y servidor, proveer privacidad y confidencialidad en la comunicación de dos aplicaciones [SSL, 2001].

SSL está compuesto por dos capas. En la capa inferior, se encuentra el protocolo SSL de registro, trabaja sobre algun protocolo de transporte (TCP y UDP por ejemplo), este protocolo se utiliza para encapsulamiento, encriptamiento, autenticación, servicios de secuencia y compresión. En la capa superior se encuentran 4 protocolos: el protocolo SSL de inicio de comunicación entre dos entidades o handshake, negocia mecanismos de encriptamiento, autenticación, secuencia y compresión y establece los parámetros clave entre cliente y servidor. El protocolo Change Cipher Spec, invoca cambios síncronos de mecanismos de seguridad y parámetros clave entre cliente y servidor. El protocolo de datos de aplicación para transportar los mensajes de aplicación entre los pares de cliente y

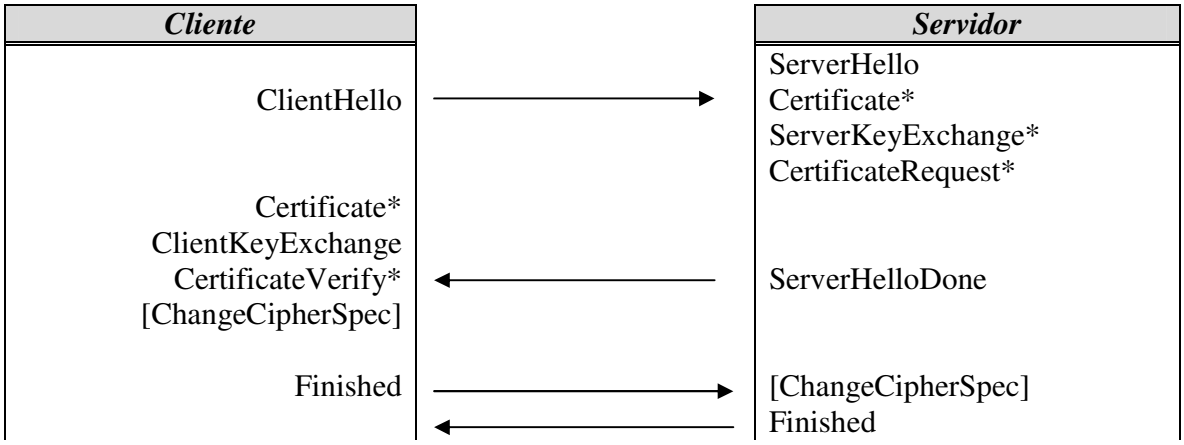
servidor, y el protocolo de Alerta, que comunica mensajes de cierre y error de conexión [Kent, 2001].

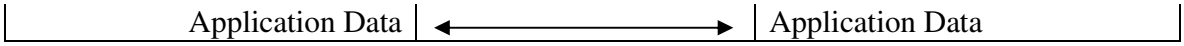
El protocolo SSL provee una conexión segura con los siguientes servicios:

1. La conexión es privada, en el handshake inicial se define la llave secreta, y el algoritmo simétrico (DES, RC4, por ejemplo).
2. El cliente puede autenticarse utilizando algun algoritmo asimétrico o de llave pública (RSA, DSS, etc.). Esto es opcional, depende de si los certificados de cliente estan disponibles.
3. El servidor se autentica utilizando certificados X.509.
4. La conexión es confiable. Se garantiza la integridad del mensaje utilizando funciones hash seguras MAC (SHA, MD5, etc.).
5. Se garantiza una secuencia estricta de mensajes, confia en TCP.
6. La compresión es opcional.

En la figura 11 se muestra el diálogo del protocolo SSL de Handshake. el intercambio de mensajes del tipo "hello" entre cliente y servidor, para establecer versión, algoritmos, certificados y llaves de autenticación, antes de la transmisión de la información.

SSL ha sido ampliamente utilizado, tanto en productos comerciales como de dominio público (Open_ssl/mod_ssl para apache por ejemplo) para el protocolo HTTP. Fue sometido el internet-draft a la IETF y propuesto como estándar en 1996, la IETF redefinió su construcción y estableció TLS 1.0 como estándar, que corresponde a la versión 3.1 de SSL.





* Indica mensajes opcionales o dependientes de la situación y que no son enviados siempre.

Figura 11. Protocolo SSL para establecer una conexión segura entre cliente y servidor.

Protocolo Transport Layer Security TLS.

TLS es el estándar creado por la IETF[3] como el protocolo de la capa de transporte. Surgió como respuesta a SSL de Netscape y PCT de Microsoft©, se consideró negativo para la industria el manejo de dos protocolos similares, asi que se estableció TLS [RFC2246, 1999]. Está basado en SSL, de hecho se considera una actualización, versión 3.1 de SSL y presenta las siguientes modificaciones:

- Requiere soporte para el algoritmo DSA y D-H, RSA es opcional.
- El algoritmo de generación de llaves está modificado, utiliza MD5 y SHA-1 con HMAC como función pseudo aleatoria, a diferencia del algoritmo de llaves MAC definido en SSL.
- Contiene un conjunto más completo de alertas.

TLS es la propuesta por el grupo de trabajo de la IETF, sin embargo, ha habido mayor desarollo sobre SSL.

Protocolo Network Layer Security (NLS).

NLSP es un protocolo de seguridad desarrollado en el seno de ISO-OSI, y diseñado para utilizarse en la capa superior de la capa 3 (capa de red). Se ofrece para versiones orientadas a conexión y a no conexión. [ISO, 1995].

[3] Internet Engineering Task Force.

Protocolos Authentication Header AH, Encapsulating Security Payload (ESP).

Los protocolos AH y ESP son parte del conjunto de protocolos de seguridad conocidos como IPSec. IPSec es un estándar de seguridad de la capa de red. Ofrece servicios de seguridad como encriptamiento y protección de integridad para los paquetes IP. IPSec es considerado hoy en día como el mejor protocolo de seguridad, se encuentran algunas implementaciones funcionando y diversos proyectos de experimentación y desarrollo. Dada su relación con el protocolo de siguiente generación de IP (IPv6) se considera el protocolo de seguridad para las redes de siguiente generación.

Se genera un encabezado extra entre las capas 3 y 4 (IP y TCP) para ofrecer al destino suficiente información para identificar asociaciones de seguridad. AH autentica e incluye direcciones de fuente y destino. ESP encripta y autentica.
Además de AH y ESP, utiliza ISAKMP/IDE para el manejo de llaves, que se encuentran documentados en varios RFC y documentos que circulan en Internet. IPSec se encuentra descrito a profundidad en el capítulo III de este trabajo.

Protocolos de la capa de aplicación.

En esta capa se encuentran protocolos destinados a la seguridad de alguna aplicación específica, por lo que existen una gran variedad de propuestas, tanto comerciales como de dominio público para ofrecer servicios de seguridad, se mencionan algunos reconocidos como estándares a manera de referencia.

DNS es el sistema de nombres que mantiene nombres como www.cicese.mx, DNSSEC [RFC3130, 2001] es el sistema que contiene contramedidas a las vulnerabilidades encontradas, más servicios de seguridad. PGP (RFC2440, 1998] es un protocolo ampliamente utilizado para el encriptamiento de mensajes de correo electrónico y firmas digitales. S/MIME es un protocolo ampliamente utilizado para la seguridad de mensajes ya sea de correo electrónico o en servicios de directorio. Los protocolos X.400, X500 son estándares de ISO/CCITT para mensajes y directorios respectivamente, el X.509 es la porción del estándar X.500 para autenticación, en particular para certificados de llave pública y listas de revocación de certificados [ITU, 2001].

El protocolo de seguridad de mensajes (MSP, Message Security Protocol), es un protocolo de mensajes para ser utilizado con X.400 y protocolos de correo definidos en el RFC 822/SMTP, fue adoptado como protocolo estándar seguro para el sistema de mensajes de la Defensa de Estados Unidos.

Conclusiones.

En este capítulo se han descrito conceptos importantes, que serán utilizados a lo largo del escrito de tesis y cuya comprensión fue escencial para el desarrollo del trabajo. Esta documentación es resultado del desarrollo de los objetivos de investigación de protocolos de seguridad, conceptos de seguridad y ubicación del tema dentro del área de Seguridad. El siguiente capítulo describirá el funcionamiento de la aplicación de servicios de seguridad para el protocolo IP, tanto para la versión 4 como para la versión 6 de este protocolo.

Capítulo III

Introducción

La nueva tendencia en seguridad es crear protocolos que funcionen a menor nivel que el de aplicaciones, de tal forma que se brinde seguridad tanto a IP como a protocolos de capas superiores de forma transparente para el usuario; protocolos que funcionen sin que el usuario deba hacer o instalar algo particular en su computadora, y protejan su tráfico sin importar la aplicación que lo genere. El Grupo de Seguridad de la IETF [SWA, 2001] desarrolló mecanismos para proteger al protocolo IP al cual se denomina ***IP Security Protocol*** (IPSEC) [SWG, 2001], el cual es un protocolo de seguridad de la capa de red para ser instrumentado y proveer servicios de encriptación con flexibilidad para soportar combinaciones de autenticación, integridad, control de acceso y confidencialidad.

IPSec es considerado el mejor protocolo de seguridad en la actualidad, representa un gran esfuerzo del grupo de trabajo de la IETF, aunque existen controversias al respecto, como los resultados de una evaluación criptográfica donde se presentan una serie de recomendaciones y observaciones [Niels99], es considerado una excelente opción para implementar VPN (Virtual Private Networks), de hecho se le conoce también como el protocolo VPN. Actualmente hay proyectos para explotar otras características y crear aplicaciones que faciliten y expandan su utilización hasta usuarios finales, con características deseables como: facilidad de uso y sencillez al alcance de todos. Son este tipo de proyectos los que están marcando el estado del arte en seguridad en redes.

Uno de los retos y diferencias entre Internet e Internet2 es la instrumentación de IPv6, se busca que esta nueva red esté basada en IPv6 y en base a ello aprovechar los beneficios directos de tener un protocolo de comunicación con características mejores, entre ellas un diseño que contemple seguridad aplicando IPSec, de forma integrada en las cabeceras de extensión, no como adición forzada en el caso de IPv4.

Este capítulo contiene la definición de conceptos importantes relacionados directamente con el protocolo de seguridad IPSec: la pila TCP/IP, IPv4, IPv6, VPN, así como la definición a profundidad del conjunto de protocolos conocido como IPSec.

Internet Protocol versión 6.

Si bien el uso de Classless Inter-Domain Routing (CIDR) se puede alargar unos pocos años más de tiempo, es opinión generalizada que los días del protocolo IP en su forma actual (IPv4) están contados. Actualmente Internet se utiliza por millones de personas con necesidades diferentes, produciendo miles de millones de máquinas utilizando la red. En la década de los 90's y previendo esta explosión del interés por la Internet, se hizo evidente que el IP tenía que evolucionar y volverse más flexible.

Al ver en el horizonte estos problemas, el IETF comenzó a trabajar en 1990 en una versión nueva del IP, una que nunca se quedaría sin direcciones, resolvería varios otros problemas y sería más flexible y eficiente también. Sus metas principales fueron:

5. Manejar miles de millones de hosts, aún con asignación eficiente de espacio de direcciones.
6. Reducir el tamaño de las tablas de enrutamiento.
7. Simplificar el protocolo, para permitir a los enrutadores el procesamiento más rápido de los paquetes.
8. Proporcionar mayor seguridad (verificación de autenticidad y confidencialidad) que el IP actual.
9. Prestar mayor atención al tipo de servicio, especialmente con datos en tiempo real.
10. Ayudar a la multitransmisión permitiendo la especificación de alcances.
11. Posibilitar que un host sea móvil sin cambiar su dirección.
12. Permitir que el protocolo evolucione.
13. Permitir que el protocolo viejo y el nuevo coexistan por años.

El protocolo IPv6 presenta atractivas ventajas: mantiene las buenas características del IP, descarta y reduce sus inconvenientes, agrega además nuevas funciones donde se necesitan. En general, IPv6 no es compatible con IPv4, pero es compatible con todos los demás protocolos de Internet, incluidos TCP, UDP, ICMP, IGMP, OSPF, BGP y DNS, a veces requiriendo pequeñas modificaciones (principalmente para manejar direcciones más grandes). Las características principales del IPv6; son de 16 bytes de longitud, lo que resuelve el problema que se buscaba resolver: proporcionar una cantidad prácticamente ilimitada de direcciones Internet.

La segunda mejora principal del IPv6 es la simplificación de la cabecera, que contiene sólo 7 campos (contra 13 en el IPv4). Este cambio permite a los enrutadores procesar con mayor rapidez los paquetes y mejorar, por tanto, el rendimiento.

La tercera mejora importante fue el mejor apoyo de las opciones. Este cambio fue esencial con la nueva cabecera, pues campos que antes eran obligatorios ahora son opcionales. Además, es diferente la manera de representar las opciones, haciendo más sencillo que los enrutadores hagan caso omiso de opciones no dirigidas a ellos. Esta característica mejora el tiempo de procesamiento de paquetes.

Una cuarta área en la que el IPv6 representa un avance importante es la seguridad. La IETF tenía infinidad de historias sobre preadolescentes precoces que usaban sus computadoras personales para meterse en bancos e instalaciones militares por todas partes de Internet. Se tenía la fuerte sensación de que había que hacerse algo para mejorar la seguridad. El soporte a las verificaciones de autenticidad y la confidencialidad son características clave del IP nuevo. Para manejar estas características, IPv6 utiliza IPSec y requiere su implementación para un funcionamiento completo e interoperable.

Por último, se tenía que prestar mayor atención al tipo de servicio que en el pasado. El IPv4 de hecho tiene un campo de 8 bits dedicado a este asunto, pero con el crecimiento esperado del tráfico multimedia en el futuro, se requiere mucho más.

Uno de los planteamientos en Internet2 es precisamente la instalación de este nuevo protocolo, y que sea la plataforma de experimentación para la evolución gradual de la Internet.

Arquitectura de protocolos de red TCP/IP.

En los inicios de las redes de comunicaciones se plantearon varias arquitecturas de red diferentes (OSI/ISO, SNA/IBM, DECNET, TCP/IP, entre otras), sin embargo, la más simple y abierta fue el conjunto de protocolos TCP/IP, sobre cuya arquitectura se han hecho grandes desarrollos e implementaciones, y han dado lugar a lo que ahora conocemos como Internet. Es común hoy en día, hacer referencia teórica al modelo de capas de OSI/ISO, pero para cuestiones prácticas de implementaciones en redes e Internet, el modelo de capas más utilizado es TCP/IP. Existen algunas propuestas para implementar la arquitectura OSI sobre TCP/IP [RFC1085, 1988], sin embargo, no es común este tipo de implementaciones, existe también documentación que relaciona un modelo con otro [Feit, 1993].

La arquitectura TCP/IP consta de tres componentes [Naganand, et.al., 1999]:

- Una pila de protocolos, cuatro capas que se comunican entre sí para transmitir paquetes[4].
- Un esquema de direccionamiento, con capacidad de identificar de manera única un destino.
- Un esquema de enrutamiento, con capacidad de determinar de forma eficiente el camino que debe seguir un paquete para llegar a su destino.

[4] Un paquete es una unidad de datos, organizada en diferentes campos: cabecera, carga útil y fin de paquete.

La pila de protocolos de TCP/IP.

Se denomina una pila, por su esquema de capas y funcionamiento, la entrada y salida siempre es por la misma capa, la capa inferior. La figura 12 muestra la pila de protocolos, el diseño es simple, cada capa interactúa únicamente con las inmediatas superior e inferior, cada capa tiene servicios e interfaces bien definidas, el diseño para cada capa puede ser independiente.

Figura 12. Pila de protocolos TCP/IP

La capa de Aplicación.

En la capa de aplicaciones se especifica el protocolo por servicio, tales como el HTTP, SNMP, SMTP, etc. Por el cual las aplicaciones en diferentes hosts podrán comunicarse entre sí. También define las interfaces para la capa de transporte, esta interfaz es dependiente del sistema operativo. La interfaz más popular es el socket[1], que se provee en todos los tipos de sistemas operativos que soporten TCP/IP.

La capa de Transporte.

La capa de Transporte provee los siguientes servicios:

1. Transporte orientado a conexión, y orientado a no-conexión. En un esquema orientado a conexión, una vez establecida, la conexión permanece hasta que la aplicación se interrumpe, o bien termina voluntariamente. La aplicación establece el destino de la conexión una sola vez, un ejemplo perfecto es una llamada telefónica. En el esquema

[1] Una interfaz entre el usuario y la red, cada interfaz puede soportar algun tipo particular de comunicación como: ráfaga de bytes orientados a conexión confiable, ráfaga de paquetes orientas a conexión confiable y/o transmisión de paquetes no confiable.

orientado a no-conexión, la aplicación debe establecer el destino de la conexión para cada transmisión de información, un ejemplo es un fax. TCP (Transport Layer Protocol) es un protocolo orientado a conexión, UDP (User Datagram Protocol) es un protocolo orientado a no-conexión.

2. Transporte confiable y no-confiable. Si por cualquier razón un paquete se pierde (mal direccionamiento, problemas con la red, algun nodo sin funcionar, etc.), en una conexión confiable (orientada a conexión), este paquete será retransmitido, esta capa asume la responsabilidad de garantizar el envío del paquete. En una conexión no confiable (orientada a no-conexión), esta capa no asume esa responsabilidad y la aplicación deberá manejar los casos en que se pierdan paquetes en la red.
3. Seguridad. Este servicio es nuevo, la integración de servicios de seguridad es reciente. En IPv4 es un elemento impuesto y que prácticamente no se utiliza, en IPv6 está considerado en el diseño y es instrumentado en las cabeceras de extensión.

La capa de Red.

La capa de Red provee el servicio orientado a no-conexión. Esta capa es responsable del enrutamiento de paquetes, de la definición de rutas para su transmisión y de definir el esquema de direccionamiento para identificar cada destino sin ambiguedades.

En el conjunto de protocolos TCP/IP, hay dos protocolos de red: IPv4 e IPv6. IPv4 (Internet Protocol versión 4) es el protocolo de capa de red más popular hoy en día y tiene la infraestructura de enrutamiento muy madura. El direccionamiento es uno de los componentes más importantes de un protocolo de red, IPv4 maneja direcciones de 32 bits (2^{32} computadoras[5]) representadas en notación decimal separada por puntos A.B.C.D, cada símbolo es un byte y representa una parte de dirección de red y otra de computadora. La dirección de red se obtiene con un AND lógico con la máscara de red, todas las direcciones IP van acompañadas de una máscara de red [Feit, 1993]. Por ejemplo, una dirección IPv4

[5] Menos las direcciones reservadas.

válida de Red-CICESE es 158.97.28.12/255.255.252.0 o bien en otra notación, 158.97.28.12/22., es la computadora 12 de la subred 28, de la red 158.97.0.0. asignada de forma única al CICESE y a la computadora dentro de Red-CICESE.

Una dirección IPv6 es de 128 bits de longitud y su representación es diferente, números hexadecimales separados por dos puntos, el concepto de máscara es similar y se ha implementado una jerarquía mucho más rica para disminuir los problemas de enrutamiento y direccionamiento. Por ejemplo, una dirección IPv6 válida de Red-CICESE es 3ffe:8070:100f:1:a00:20ff:fec6:ba27/64 que indica la región geográfica, la institución, subred y computadora de forma única en la red mundial experimental de IPv6 [6BONE, 2001].

Existe un control universal por los organismos de Internet [NICMX, 2001] para la asignación de direcciones, de igual forma se está construyendo el direccionamiento para IPv6.

Los componentes del encabezado de IPv4 se muestran en la figura 13, no todos son utilizados para efectos de seguridad.

Figura 13. Encabezado IPv4.

La definición de componentes se describe a continuación:

Versión: es un campo de 4 bits utilizado para indicar la versión, un 4 para IPv4, se utiliza para validar compatibilidad.

Longitud de encabezado: indica la longitud del encabezado en 32 bits. La longitud máxima de un encabezado IPv4 es de 60 bytes. Esta es una de las limitantes resueltas en IPv6.

Tipo de servicio (TOS): se utiliza para indicar los requerimientos de tráfico de un paquete, no ha sido utilizado y se encuentra en revisión por la IETF.

Longitud total: la longitud total del datagrama[6] en bytes, incluyendo el encabezado. Indica el tamaño total del datagrama a la capa de red en el extremo receptor.

Identificación: es un campo de 16 bits para identificar de manera única un datagrama IP. Este campo se utiliza principalmente para fragmentación, identifica de manera única cuál paquete IP pertenece a un datagrama IP.

Banderas: Solo han sido definidos dos bits de los tres reservados. El primer bit especifica la no fragmentación del paquete. El segundo bit indica si es el último fragmento de un

[6] Un datagrama IP se refiere a la carga útil más el encabezado IP, dentro del contexto de computadoras clientes.

datagrama o si hay otros, este bit se utiliza también para la reconstrucción de los datagramas fragmentados.
Offset de fragmentación: indica el offset del paquete IP dentro del datagrama IP.
Tiempo de vida (TTL): un contador para eliminar ciclos, se asigna un valor por omisión, y cada enrutador en la trayectoria lo decrementa en 1.
Protocolo: indica el protocolo de transporte.
Checksum del encabezado: se utiliza para validar la integridad del encabezado IP.
Dirección fuente y dirección destino: indica las direcciones de 32 bits del fuente y destino del paquete, respectivamente.
Opciones: Información adicional, no utilizada para cuestiones de seguridad.

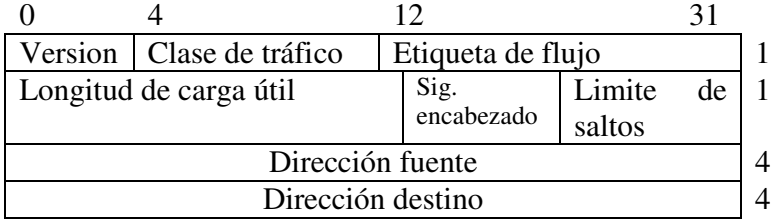


Figura 14. Encabezado de IPv6.

Los componentes del encabezado de IPv6 se muestran en la figura 14, la utilidad de los componentes se describe a continuación:
Versión: indica la versión, 6 para IPv6.
Clase de tráfico: campo de 8 bits para indicar los requerimientos de tráfico del paquete, similar a TOS de IPv4.
Etiqueta de flujo: campo de 20 bits, experimental.
Longitud de carga útil: campo de 16 bits que indica la longitud de la carga útil sin incluir el encabezado IPv6.
Siguiente encabezado: campo de 8 bits, para indicar el uso de cabeceras de extensión.
Límite de saltos: campo de 8 bits similar al TTL de IPv4.
Dirección fuente y destino: campos de 128 bits para las direcciones fuente y destino del paquete, respectivamente.

Las Cabeceras de Extensión, son una de las modificaciones más relevantes del protocolo IP de siguiente generación, las extensiones de opción se insertan entre el encabezado de IPv6 y el encabezado de transporte como se muestra en la figura 15. Cada cabecera de opción recibe un identificador único y se codifica con el formato que se muestra en la figura 16.

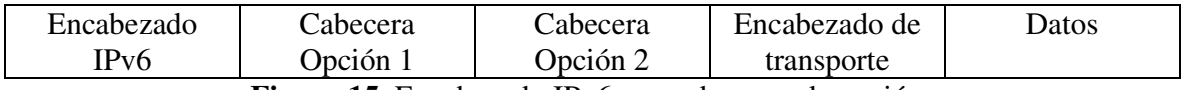


Figura 15. Encabezado IPv6 con cabeceras de opción.

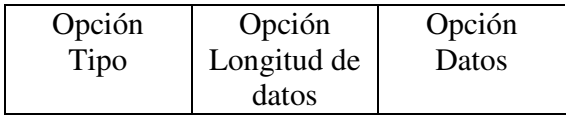


Figura 16. Formato de las opciones de IPv6

Capa inferiores.

Las capas inferiores son responsables de la transmisión de paquetes por el medio físico. La transmisión es entre dos dispositivos que están físicamente conectados. Ejemplos: Ethernet, ATM.

Flujo de los datos.

Cada capa en la pila de protocolos tiene funciones específicas y la división por capas debe prevalecer, la capa de aplicación no puede hablar con la capa de red directamente, se requiere hacerlo a través de la capa de transporte. Para ejemplificar el modelo, se asumirá que el protocolo de transporte es TCP y el protocolo de red es IP. De acuerdo a la figura 17, la secuencia de la comunicación sería la siguiente:

1. Una aplicación en la computadora fuente de la comunicación, genera datos que requieren ser transmitidos sobre una interfaz del tipo socket a la capa de transporte. La aplicación identifica el destino con el que desea comunicarse. El destino incluye la aplicación y dirección de la computadora receptora de los datos.
2. La capa de transporte, que en este caso sería TCP, toma los datos y agrega el encabezado de transporte, en este caso el encabezado TCP a la carga útil, los datos, y los envía a la capa de red. Los campos en el encabezado de transporte especifican los servicios requeridos por la aplicación.

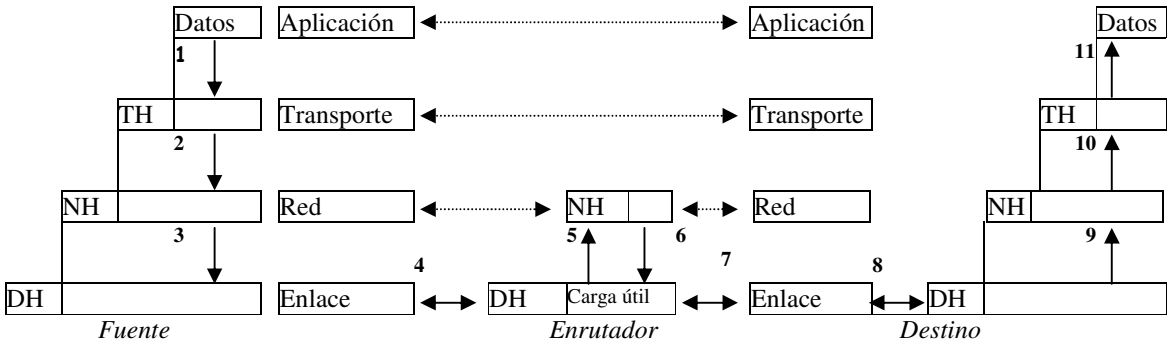


Figura 17. Flujo de datos en una arquitectura TCP/IP.

3. La capa de red recibe la carga útil de la capa de transporte. Agrega el encabezado IP y lo envía a las capas inferiores de enlace, la capa de red identifica el vecino (enrutador) o siguiente salto en la ruta para que el paquete llegue a su destino.
4. Las capas inferiores de enlace agregan el encabezado de enlace de datos a la carga útil procedente de la capa de red, e identifica la dirección física del siguiente salto hacia el que debe enviarse el paquete.
5. Las capas inferiores de enlace en el siguiente salto reciben el paquete, extraen el encabezado de la capa de enlace y envían el paquete a la capa de red.
6. La capa de red revisa el encabezado de red, decide el siguiente salto al que debe enviarse el paquete en la ruta de destino, y lo regresa a las capas inferiores de enlace.
7. Las capas inferiores de enlace agregan el encabezado de enlace y lo envían al siguiente salto.
8. Se repiten los pasos 6 y 7 hasta que el paquete alcanza el destino.
9. En el destino, las capas inferiores de enlace extraen el encabezado de enlace y envían el paquete a la capa de red.
10. La capa de red, extrae el encabezado de red y envía el paquete a la capa de transporte.
11. La capa de transporte verifica el encabezado de transporte para garantizar que la aplicación está siendo atendida apropiadamente, extrae el encabezado de transporte, identifica la aplicación a la que va destinada el paquete y lo envía a la aplicación.
12. La aplicación en el destino, recibe la información que le fue enviada.

El funcionamiento de la pila de protocolos utilizada en Internet, es importante para la implementación de seguridad del tipo BITS (Bump In The Stack) que se analizará en el capítulo IV.

Redes Privadas Virtuales.

Una VPN (Virtual Private Network) es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de encriptación y/o autentificación criptográfica. Una VPN es *virtual* porque no es físicamente un red distinta, es *privada* porque la información que transita por los túneles es encriptada para brindar confidencialidad, y es una *red* porque consiste de computadoras y enlaces de comunicación, pudiendo incluir enrutadores, switches y gateways de seguridad.

VPN es una tecnología punto a punto, ampliamente adoptada en ambientes de transacciones financieras, y/o redes que requieren confidencialidad permanente, tanto en redes privadas como entre proveedores de Servicio de Internet y sus clientes. En el mercado existe una gran variedad de soluciones VPN, la figura 18 ilustra un ejemplo de interconexión de oficinas sucursales de un corporativo, interconectadas vía VPN usando la Internet como dorsal de su red. Cada oficina tiene un gateway de seguridad que provee una interfaz con Internet y la red interna del corporativo. Los gateways de seguridad se configuran para definir las políticas de control de acceso para cada oficina. Los servicios de seguridad de IPSec son ampliamente utilizados para la implementación de VPNs [Davis01].

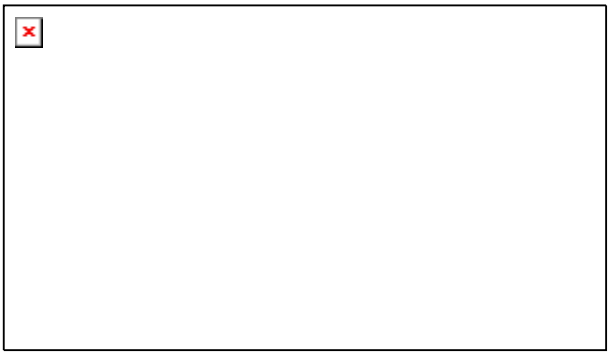


Figura 18. VPN interconectando las oficinas A, B, y C, utilizando a la Internet como *backbone* de su red.

Las VPNs tienen cierto nicho de aplicación, en ambientes punto a punto que requieren canales seguros de forma permanente (transacciones de dinero, por ejemplo), sin embargo, Internet 2 tiene características variadas, es importante que además de existir alternativas como ésta, haya flexibilidad para aplicar diversos niveles de seguridad que puedan adaptarse a las distintas necesidades.

Protocolo de Seguridad IP.

IPSec (Internet Protocol Security) es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de Red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones, y es mucho más poderoso. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores [Dan99].

La arquitectura de IPSec.

La arquitectura de IPSec define la granularidad con la que el usuario puede especificar su política de seguridad. Permite que cierto tráfico sea identificado para recibir el nivel de protección deseado (Figura 19).

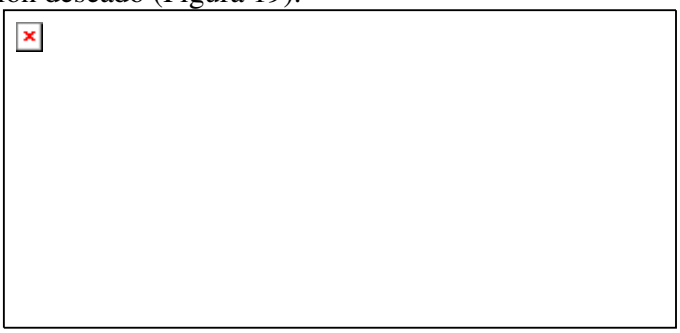


Figura 19. Túneles de comunicación protegidos por IPSec entre redes separadas.

IPSec está diseñado para proveer seguridad interoperable de alta calidad basada en criptografía, tanto para IPv4 como para IPv6 [RFC2401, 1998]. Está compuesto por dos protocolos de seguridad de tráfico, el Authentication Header (AH) y el Encapsulating Security Payload (ESP), además de protocolos y procedimientos para el manejo de llaves encriptadas. AH provee la prueba de los datos de origen en los paquetes recibidos, la integridad de los datos, y la protección contra-respuesta. ESP provee lo mismo que AH adicionando confidencialidad de datos y de flujo de tráfico limitado.

En la figura 20 se aprecia la arquitectura de IPSec. Al utilizar el mecanismo de AH se aplican algoritmos de autenticación, con la aplicación del mecanismo ESP, además de autenticación, también algoritmos de encriptación. El esquema de interoperabilidad se maneja a través de Asociaciones de Seguridad (SA), almacenadas en una base de datos. Los parámetros que se negocian para establecer los canales seguros se denominan Dominio de Interpretación IPSec (Domain of Interpretation, DOI), bajo políticas pre-establecidas dentro de un esquema de funcionamiento estático con valores fijos y previamente establecidos, o bien, en un esquema de funcionamiento dinámico utilizando un protocolo de manejo de llaves, Interchange Key Exchange (IKE).

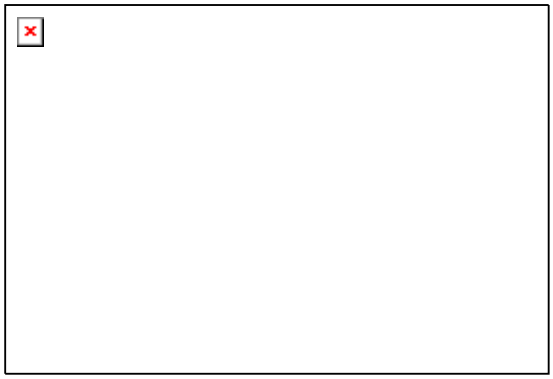


Figura 20. Arquitectura de IPSec.

Modos de funcionamiento de IPSec.

El diseño de IPSec plantea dos modos de funcionamiento para sus protocolos: transporte y túnel, la diferencia radica en la unidad que se esté protegiendo, en modo transporte se protege la carga útil IP (capa de transporte), en modo túnel se protegen paquetes IP (capa de red) y se pueden implementar tres combinaciones: AH en modo transporte, ESP en modo transporte, ESP en modo túnel (AH en modo túnel tiene el mismo efecto que en modo transporte).

El modo transporte se aplica a nivel de hosts. AH y ESP en este modo interceptarán los paquetes procedentes de la capa de transporte a la capa de red y aplicarán la seguridad que haya sido configurada. En la figura 21 se aprecia un esquema de IPSec en modo transporte, si la política de seguridad define que los paquetes deben ser encriptados, se utiliza ESP en modo transporte, en caso que solo haya sido requerida autenticación, se utiliza AH en modo transporte.

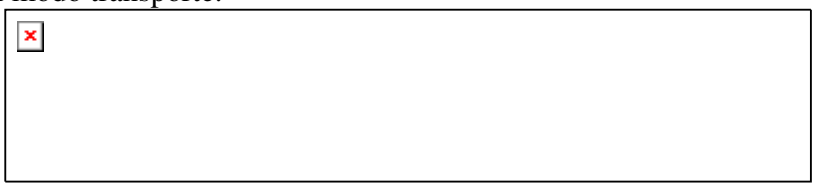


Figura 21. Hosts A y B implementando ESP en modo transporte.

Los paquetes de la capa de transporte como TCP y UDP pasan a la capa de red, que agrega el encabezado IP y pasa a las capas inferiores; cuando se habilita IPSec en modo transporte, los paquetes de la capa de transporte pasan al componente de IPSec (que es implementado como parte de la capa de red, en el caso de sistemas operativos), el componente de IPSec agrega los encabezados AH y/o ESP, y la capa de red agrega su encabezado IP. En el caso que se apliquen ambos protocolos, primero debe aplicarse la cabecera de ESP y después de AH, para que la integridad de datos se aplique a la carga útil de ESP que contiene la carga útil de la capa de transporte, esto se ilustra en la figura 22.

Encabezado IP	Encabezado AH	Encabezado ESP	Carga útil TCP

Figura 22. Formato del paquete con AH y ESP.

El modo túnel se utiliza cuando la seguridad es aplicada por un dispositivo diferente al generador de los paquetes, como el caso de las VPN, o bien, cuando el paquete necesita ser asegurado hacia un punto seguro como destino y es diferente al destino final, como se ilustra en la figura 23, el flujo de tráfico es entre A y B, e IPSec puede aplicarse con una asociación de seguridad entre RA y RB, o bien, una asociación de seguridad entre A y RB.

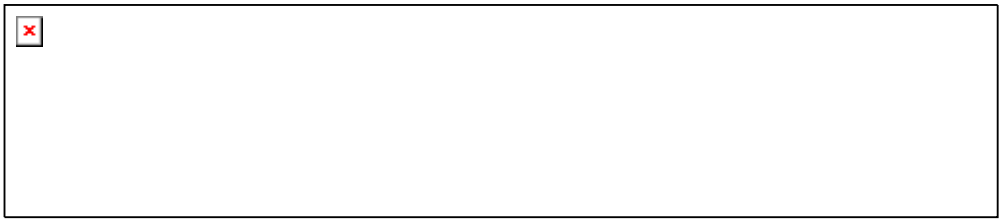


Figura 23. Aplicación de IPSec en modo túnel.

IPSec en modo túnel, tiene dos encabezados IP, interior y exterior. El encabezado interior es creado por el host y el encabezado exterior es agregado por el dispositivo que está proporcionando los servicios de seguridad. IPSec encapsula el paquete IP con los encabezados de IPSec y agrega un encabezado exterior de IP como se ilustra en la figura 24.

Encabezado IP	ESP	Encabezado IP	Carga útil de la red

Figura 24. Formato del paquete aplicando IPSec en modo túnel.

IPSec también soporta túneles anidados, aunque no son recomendados por lo complicado de su construcción, mantenimiento y consumo de recursos de red. La figura 25 muestra dos túneles, A envía un paquete a B, la política indica que debe ser autenticado con el enrutador RB, además existe una VPN entre RA y RB, de tal forma que el paquete que ve RB es el que se muestra en la figura 26, el encabezado exterior es un paquete ESP entunelado y contiene un paquete AH entunelado, el paquete AH contiene el paquete IP para el host B generado por el host A.

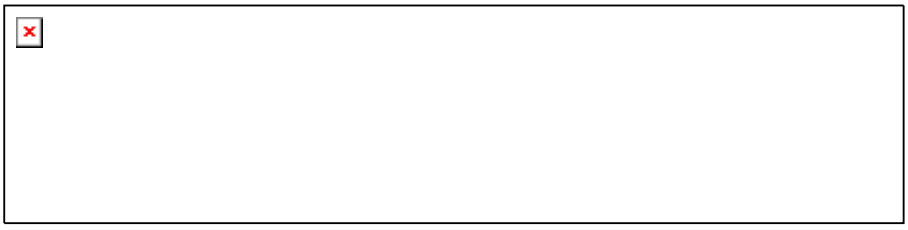


Figura 25. Ejemplo de túneles anidados.

Encabezado IP	ESP	Encabezado IP	AH	Encabezado IP	Datos
Fuente: 158.97.2.1		*Fuente*: 158.97.1.1		*Fuente*: 158.97.1.1	

Destino:	*Destino*:	*Destino*:
158.97.3.3	158.97.3.3	158.97.4.2

Figura 26. Formato del paquete del túnel anidado.

Asociaciones de seguridad.

Una asociación de seguridad (SA) es la forma básica de IPSec, es el contrato entre dos entidades que desean comunicarse en forma segura. Las SA determinan los protocolos a utilizar, las transformaciones, las llaves y la duración de validéz de dichas llaves. Las SA son almacenadas en una base de datos (SADB), son de un solo sentido, es decir, cada entidad con IPSec tiene una SA para el tráfico que entra, y otra SA para el tráfico que sale. Además de ser unidireccionales, también son específicas al protocolo, hay SA separadas para AH y para ESP.

Indice de parámetros de seguridad (Security Parameter Index, SPI).

El SPI es una entidad de 32 bits que identifica de manera única una SA. Es el mecanismo concebido para que en una comunicación segura, la fuente identifique cual SA utilizar para asegurar un paquete por enviar, y el destino identifique cual SA utilizar para verificar la seguridad del paquete recibido. El SPI se incluye en los encabezados ESP y AH, el destino utiliza la tupla <spi, dst, protocol> para identificar de forma única la SA.

Gestión de las SA.

Para el manejo de SA se establecen dos tareas: creación y borrado; estas actividades pueden ser manuales o a través del protocolo de manejo de llaves (IKE).

La creación es un proceso de dos etapas: 1) negociación de parámetros de la SA, 2) actualización de la SADB. El manejo manual de llaves es obligatorio en toda implementación, el proceso de definición de SPI y parámetros es totalmente manual, y permanecerán hasta que sean manualmente borrados. En el manejo dinámico de llaves, se utiliza un protocolo de manejo de llaves en Internet como IKE. El kernel con IPSec habilitado, invoca IKE si se trata de una comunicación segura y no encuentra una SA. IKE negocía la SA con el destino o con el siguiente salto (host o enrutador), dependiendo de la política y crea la SA en la SADB.

Igualmente las SA pueden ser borradas manualmente o con IKE, los criterios de borrado pueden ser: tiempo de vida expirado, llaves comprometidas, solicitud explícita para borrarse, el número de bytes utilizado excede un umbral especificado en la política.

Parámetros.

Los parámetros por negociar en una SA, tanto para AH como para ESP son los siguientes:
Número de secuencia: un campo de 32 bits utilizado en el procesamiento de paquetes de salida, es parte de los encabezados de AH y/o ESP, su valor inicial es 0, se incrementa en uno cada vez que la SA es utilizada, se utiliza para detectar ataques del tipo "replay".
Sobreflujo del número de secuencia: campo utilizado en el procesamiento de paquetes de salida y se establece cuando hay sobreflujo del campo de número de secuencia. La política determina qué hacer si este campo está activado.
Ventana de antireply: campo utilizado en el procesamiento de paquetes de entrada. Se activa si IPSec detecta paquetes retransmitidos por hosts sospechosos.
Tiempo de vida: El tiempo de validéz de una SA, se especifica en términos de bytes asegurados con la SA, no se recomienda enviar más de 4Gb de paquetes utilizando la misma SA. Para evitar la pérdida de la conexión segura, se manejan dos límites, soft y hard. Al llegar al límite soft el kernel es notificado para que inicie una nueva negociación antes del límite hard que es cuando la SA expira.
Modo: los valores son: túnel, transporte o indistinto. Si el valor es indistinto la SA puede ser utilizada para modo túnel o modo transporte.
Destino del túnel: campo utilizado para modo túnel, indica la dirección IP de destino del encabezado exterior.
Parámetros PMTU: IPSec no fragmenta o reensambla paquetes, sin embargo, agrega un encabezado IPSec y por lo tanto impacta la longitud del PMTU. IPSec debe participar en la determinación del PMTU (Protocol Maximum Transfer Unit), una SA mantiene dos valores: el PMTU y el campo de edad.

Políticas de seguridad en IPSec.

La política es uno de los componentes más importantes de la arquitectura de IPSec, determina los servicios de seguridad que serán aplicados a un paquete. Las políticas de seguridad son también almacenadas en una base de datos (Security Policy Database, SPD) indexada por seleccionadores.

La SPD es consultada tanto para el procesamiento de salida como el de entrada, se propone un administrador de la SPD para agregar, borrar y modificar; no hay un estándar que lo defina, pero se propone que los seleccionadores contengan los siguientes campos:
Dirección fuente: puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica. Indistinta en el caso de que sea la misma política para todos los

paquetes con un mismo host de origen, el rango de direcciones y prefijo de red, para los gateways de seguridad y para VPNs, la dirección específica para un host con varias direcciones, o en un gateway cuando los requerimientos de algun host sean específicos.
Dirección destino: puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica (homologada o no). Los tres primeros para gateways de seguridad, la dirección específica como índice para la SPD.
Nombre: nombre de un usuario o sistema sobre el cual se aplique la política de forma específica.
Protocolo: el protocolo de transporte.
Puertos de capas superiores: los puertos del fuente y destino sobre los que se aplica la política.

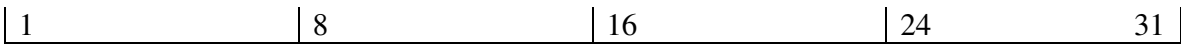
IP Encapsulating Security Payload (ESP).

ESP es un encabezado de protocolo insertado en el datagrama IP para proveer servicios de confidencialidad, autenticación del origen de los datos, *antireplay* e integridad de datos a IP [Naganand, et al. 1999]. Es un estándar definido en el RFC 2406. El encabezado ESP se inserta después del encabezado IP y antes del encabezado del protocolo de capa superior (modo transporte) o antes del encabezado IP encapsulado (modo túnel) [RFC2406, 1998].

El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado ESP contendrá el valor 50 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6) [RFC1700, 1994].

El formato de los paquetes ESP para una SA dada es fijo durante la duración de la SA. El encabezado ESP tiene la forma definida en la figura 27, el SPI y número de secuencia ya fueron definidos, la carga útil de datos son los datos protegidos, el relleno (de hasta 255 bytes) se utiliza en ESP por varias circunstancias: algunos algoritmos criptográficos requieren que el elemento de entrada sea un múltiplo del tamaño de su bloque, si no se especifica confidencialidad en la SA, se utiliza el relleno para justificar los campos *Longitud de relleno* y *Siguiente cabecera* del encabezado ESP, para esconder el tamaño real de la carga útil; el contenido del relleno es dependiente del algoritmo de criptografía, el algoritmo puede definir un valor de relleno que debe ser verificado por el receptor para el proceso de desencriptado. El campo de longitud de relleno define cuánto relleno se agregó, el campo de siguiente cabecera indica el tipo de dato contenido en la carga útil de acuerdo al conjunto de Números de Protocolo IP definidos por IANA (Internet Assigned Numbers Authority) [RFC1700, 1994]. El campo de datos de autenticación contiene el valor de verificación de integridad calculado sobre el paquete ESP menos los datos de autenticación.

ESP aplicado en modo transporte solo se utiliza en implementaciones del tipo host y provee protección a los protocolos de capas superiores, pero no al encabezado IP.



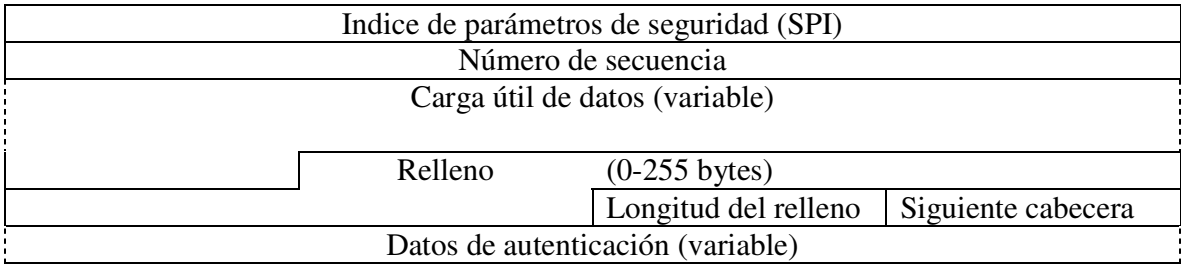


Figura 27. El encabezado ESP.

El encabezado ESP se inserta después del encabezado IP y antes del protocolo superior (TCP, UDP, ICMP, etc.) o antes de cualquier encabezado IP que haya sido previamente insertado. En la figura 28 se ilustra la transformación del paquete IP al aplicar ESP en modo transporte para IPv4; en la figura 29 se muestra el caso para IPv6.

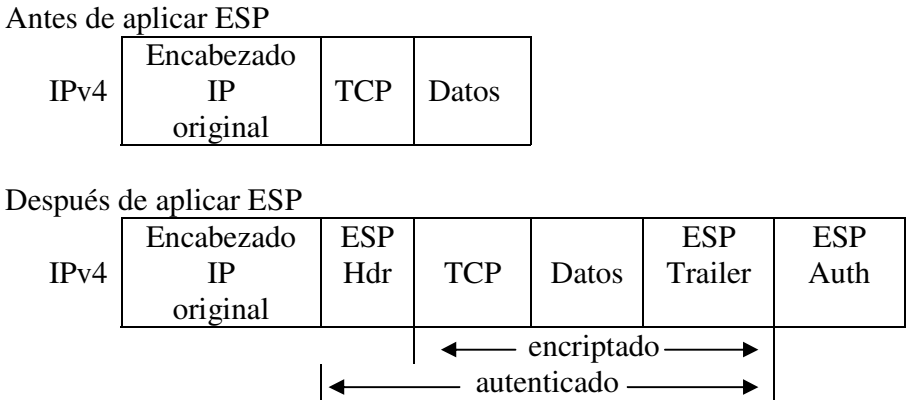


Figura 28. Transformación del paquete IPv4 al aplicar ESP en modo transporte.

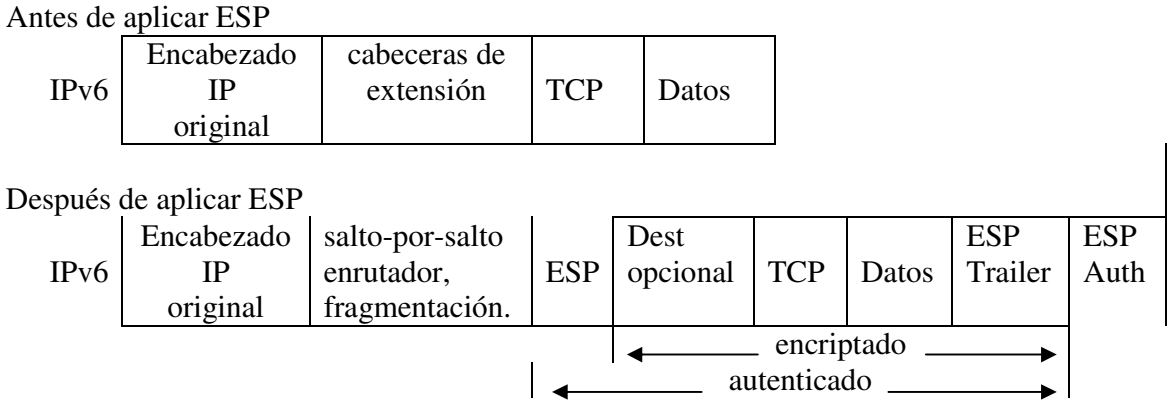


Figura 29. Transformación del paquete IPv6 al aplicar ESP en modo transporte.

En modo túnel, ESP puede ser empleado en hosts o en gateways. El encabezado IP interior contiene las direcciones del destino y origen del paquete, y el encabezado exterior puede contener direcciones diferentes, comunmente direcciones de gateways de seguridad en el camino entre el origen y destino. La posición de los encabezados ESP en modo túnel con respecto a los encabezados IP exteriores es igual que en modo transporte. En la figura 30 se muestran los encabezados ESP para IPv4 e IPv6.

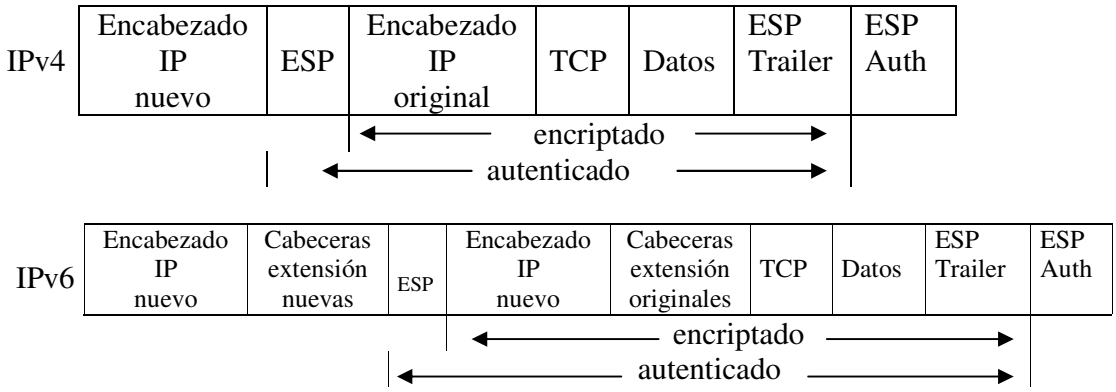


Figura 30. Transformación del paquete IP al aplicar ESP en modo túnel.

En caso de no haberse indicado la confidencialidad en la SA, el algoritmo de criptografía es Nulo, en caso de aplicar confidencialidad a un paquete que se envía, el proceso aplicado en general es el siguiente:

1. Encapsular en el campo de carga útil de ESP:
   - para modo transporte, solo la información original del protocolo de capa superior.
   - para modo túnel, el datagrama IP original completo.
2. Agregar el relleno necesario.
3. Encriptar el resultado (carga útil de datos, relleno, longitud del relleno y la siguiente cabecera) usando la llave, el algoritmo de criptografía, el modo indicado en la SA y si existe, datos de sincronización criptográfica.

En la parte del receptor se sigue en general el siguiente procedimiento para desencriptar los paquetes recibidos:

1. Desencriptar la carga útil de ESP, relleno, longitud del relleno, y siguiente cabecera, utilizando la llave, el algoritmo de criptografía, el modo y en su caso, los datos de sincronización criptográfica, indicados en la SA.
2. Procesar el relleno según haya sido especificado por el algoritmo utilizado.
3. Reconstruir el datagrama IP original:
    - para modo transporte, el encabezado IP original más la información del protocolo de capa superior original en el campo de carga útil de ESP.
    - para modo túnel, el encabezado IP entunelado, más el datagrama IP completo en el campo de carga útil de ESP.

Es importante mencionar que el encriptamiento no debe ser sustituto por la autenticación, la autenticación es el servicio básico de una comunicación segura, reforzada con el encriptamiento de datos.

IP Authentication Header (AH).

AH es el protocolo IPSec utilizado para proveer servicios de integridad de datos, autenticación del origen de los datos, y *antireplay* para IP [Naganand, et al. 1999]. Es un estándar definido en el RFC 2402 [RFC2402, 1998]. La principal diferencia entre la autenticación provista entre ESP y AH tiene que ver con la cobertura, ESP no protege los campos del encabezado IP, a menos que sean encapsulados por ESP (modo túnel). El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado AH contendrá el valor 51 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6) [RFC1700, 1994].

La figura 31 muestra el encabezado AH, todos los campos son obligatorios, tienen funciones similares a las explicadas en ESP, el campo reservado no se utiliza y su valor debe ser cero.

1	8	16	24	31
Siguiente cabecera	longitud de carga útil	reservado		
Indice de parámetros de seguridad (SPI)				
Número de secuencia				
Datos de autenticación				

Figura 31. El encabezado AH.

Al igual que ESP, AH puede aplicarse tanto en modo túnel como transporte. Las figuras 32 y 33 muestran la ubicación de AH al aplicar IPSec en modo transporte en los paquetes IP.

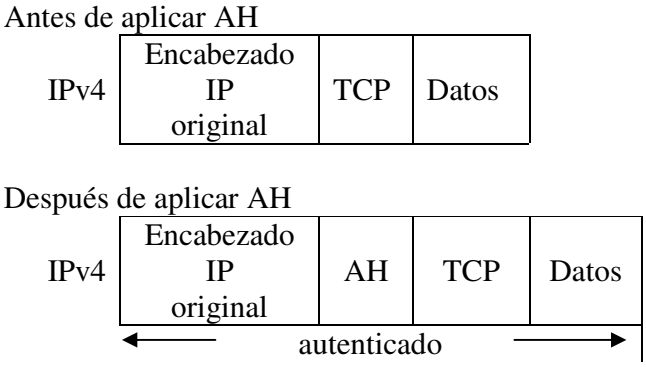


Figura 32. Transformación del paquete IPv4 al aplicar AH en modo transporte.

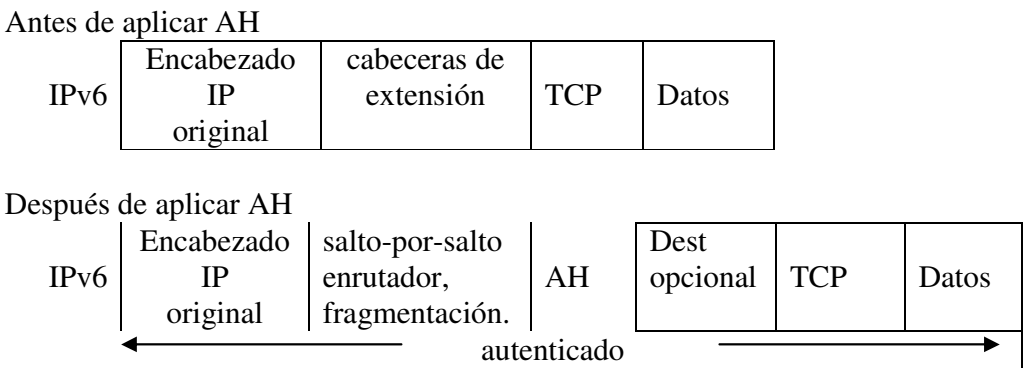
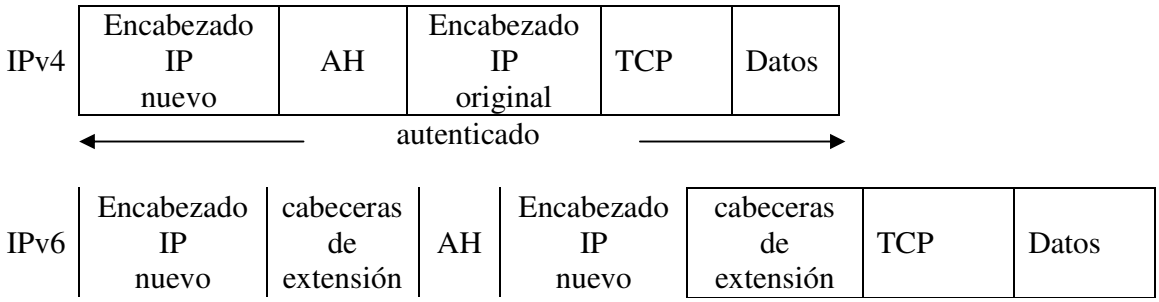


Figura 33. Transformación del paquete IPv6 al aplicar AH en modo transporte.

La aplicación de AH en modo túnel, tiene una ubicación similar a la de ESP, en la figura 34 se muestra la transformación de los paquetes IP al aplicar AH en modo túnel.



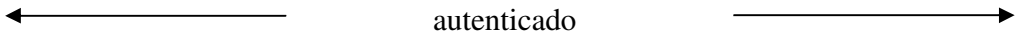


Figura 34. Transformación del paquete IP al aplicar AH en modo túnel.

El proceso de cálculo del valor de verificación de integridad (Integrity Check Value, ICV) que utiliza AH, llena con ceros los campos vulnerables a cambios en tránsito (TOS, Flags, Fragment, TTL, Header checksum en un encabezado IPv4) y se calcula sobre lo siguiente:

- los campos del encabezado IP que sean inmunes a cambios en tránsito o pueda predecirse su valor (Version, longitud de carga útil, longitud total, identificación, dirección de fuente y destino en un encabezado IPv4).
- el encabezado AH (siguiente cabecera, longitud de relleno, reservado, SPI, número de secuencia y datos de autenticación (que es puesta a cero para este cálculo), y bytes de relleno en caso que existan.
- los datos del protocolo de capa superior, que se asume son inmunes a cambios en tránsito.

Internet Key Exchange (IKE).

El protocolo IKE no es parte de IPSec, es una alternativa para crear las Asociaciones de Seguridad de forma dinámica, está definido en el RFC 2409 [RFC2409, 1998]. IKE es un protocolo híbrido basado en el marco definido por el Protocolo de manejo de llaves y asociaciones de seguridad de Internet (Internet Security Association and Key Management protocol, ISAKMP) definido en el RFC2408 [RFC2408, 1998], y otros dos protocolos de manejo de llaves Oakley[7] y SKEME[8]. Las implementaciones de IPSec están forzadas a soportar el manejo manual y solo algunas de ellas consideran IKE, que ha resultado demasiado complejo e inapropiado. El uso de IKE en el 2001 fue congelado por la IETF, el planteamiento sobre manejo dinámico en el 2001 es llamado “son of IKE” o IKE versión 2 y se encuentra en discusión en el área de seguridad de la IETF.

[7] protocolo creado por Hilarie Orman de la Universidad de Arizona.

[8] protocolo creado por Hugo Krawczyk que utiliza encriptación de llave pública.

Implementación de IPSec.

La implementación de IPSec puede hacerse en hosts, gateways/enrutadores, y/o firewalls, resultando conveniente la implementación en éstos últimos al complementar mutuamente sus funciones. Típicamente modificando la pila de IP para soportar IPSec de forma nativa, cuando esto no es posible, puede implementarse como interceptor que extrae e inserta paquetes en la pila de IP "Bump in the Stack" (BITS), o bien utilizando un dispositivo de encriptación externo dedicado "Bump in the Wire" (BITW) como se esquematiza en la figura 35.

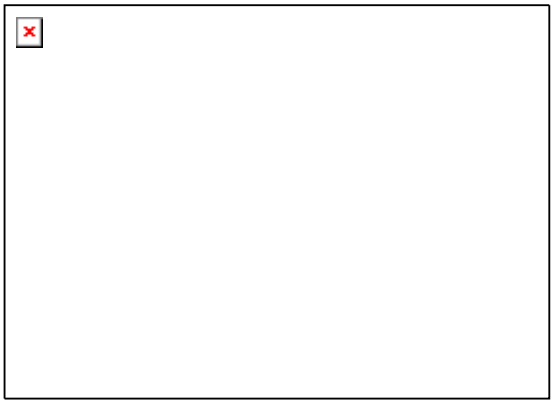


Figura 35. Tipos de implementaciones de IPSec.

IPSec está diseñado para operar en hosts y/o en gateways, en modo túnel para proteger datagramas IP completos (VPN), o en modo de transporte para proteger protocolos de capas superiores. A la fecha existen algunas implementaciones, sin embargo, la mayoría limitadas a la aplicación de VPN únicamente, sobre todo en implementaciones de forma nativa, de hecho es denominado por algunos como el "protocolo VPN" . En los últimos años han emergido los proyectos para implementar seguridad en sistemas operativos, esquemas BITS, en busca de brindar una plataforma base de seguridad independiente de las aplicaciones preferidas por el usuario.

Configuraciones de IPSec.

Cuando la implementación de IPSec radica en un host o sistema final, los paquetes pueden ser asegurados de extremo-a-extremo, es decir desde el origen de los datos hasta su destino final. La figura 36 muestra este esquema, donde cada paquete que sale del host es asegurado y puede inclusive determinarse que todo paquete que no haya sido asegurado por IPSec sea eliminado. El resultado de un esquema de seguridad extremo-a-extremo, IPSec en modo transporte generalmente, donde todo el tráfico (Telnet, SMTP, HTTP, etc.) entre ambos extremos puede ser asegurado, o bien, de forma particular a través de la definición explícita de SA.

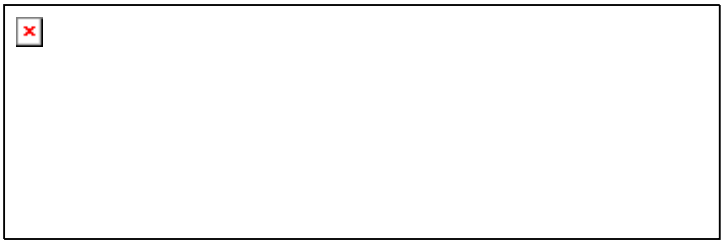


Figura 36. Seguridad extremo-a-extremo a través de la red.

Algo importante de mencionar de la seguridad extremo-a-extremo, es que puede afectar el funcionamiento de otras aplicaciones que requieran inspeccionar los paquetes en tránsito (Firewalls, QoS, etc.), y no puedan hacerlo, ya que verán solo paquetes ESP. Quizá la implementación más común son las VPN descritas en la sección III.3, que han sido vistas como una excelente alternativa de ahorro, en lugar de contratar líneas dedicadas, utilizar la red pública con servicios de seguridad. Cuando IPSec se aplica a enrutadores en modo túnel, y dos enrutadores establecen túneles a través de los cuales envían tráfico desde una subred localmente protegida hacia otra subred remotamente protegida se denomina una VPN, la figura 37 muestra un esquema de este tipo.

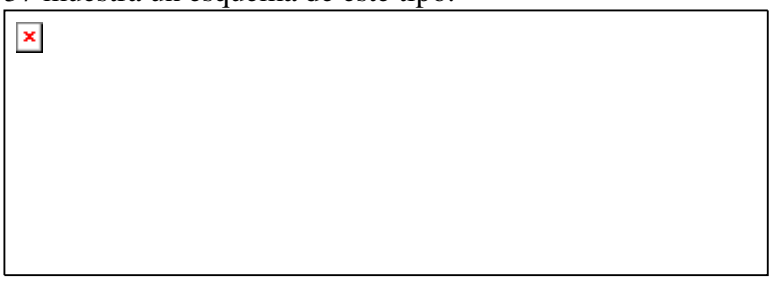


Figura 37. Una VPN a través de Internet.

Existe otro tipo de implementación que es una combinación de la extremo-a-extremo donde un host encripta y desencripta tráfico que envía y recibe, y la VPN en donde es un enrutador el que hace este trabajo. En la configuración del tipo "*Road Warrior*", una computadora implementa IPSec y es capaz de asegurar los paquetes que envía y verificar la seguridad de los paquetes que recibe, su extremo IPSec es un enrutador que protege la red con la cual se desea establecer la comunicación. La figura 38 ilustra este esquema.

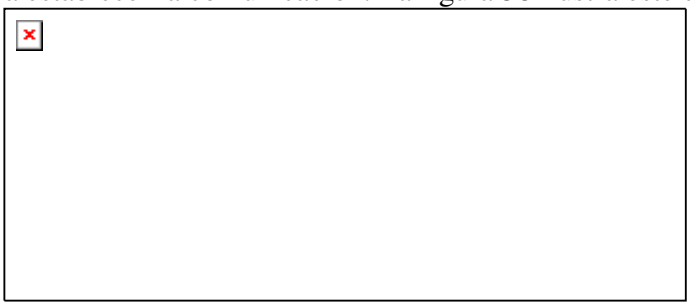


Figura 38. Esquema de configuración de un road warrior.

También es posible la implementación de túneles anidados, un ejemplo podría ser una institución que tiene un gateway de seguridad para proteger su red de ataques del exterior, pero además tiene otro gateway de seguridad en su red interna para protección de

ataques internos. La figura 39 muestra este esquema, difícil de mantener y establecer, pero quizá útil y necesario para ciertas necesidades entre instituciones con instalaciones remotas.

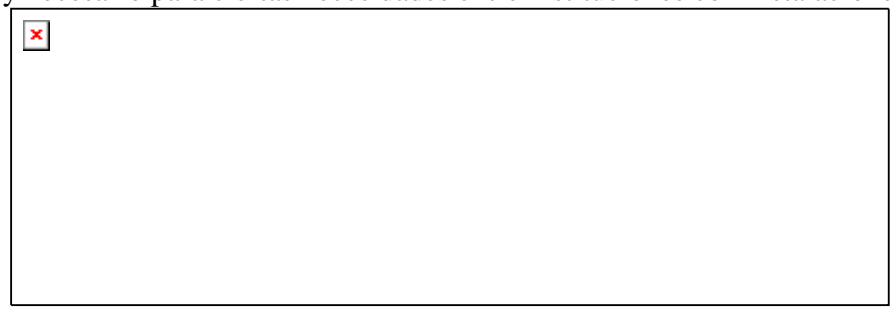


Figura 39. Esquema con túneles anidados.

Conclusiones.

En este capítulo se ha descrito IPSec, su funcionamiento, configuraciones y potencial. Los aspectos más importantes del capítulo se pueden sintetizar como sigue: la arquitectura modular de IPSec que brinda servicios independientes de autenticación y cifrado, la inclusión de encabezados IPSec en paquetes IPv4 e IPv6 y sus diferencias, y la diversidad de arreglos para su instrumentación cubriendo necesidades de diferente índole.

En el capítulo IV se describirá la metodología utilizada para la instrumentación de IPSec en los escenarios de pruebas y las configuraciones con las cuales se estuvo experimentando para evaluar el comportamiendo de IPSec en sus diferentes modos de operación.

Capítulo IV

Introducción.

Para analizar el funcionamiento de IPSec se consideraron dos metodologías igualmente válidas y muy utilizadas en el mundo: simulación y experimentación. Dado que la motivación principal de este trabajo es contribuir directamente al proyecto nacional de Internet2, cuya red se encuentra en fase de desarrollo en vivo con nuevas tecnologías, la creación de escenarios experimentales presenta ventajas sustantivas para la realización de este trabajo de tesis, desarrollando el interés por aplicar servicios de seguridad con base en un modelo por capas, en particular en la capa de Tránsito de paquetes IP, fortaleciendo en consecuencia las capas interiores donde se ubican las aplicaciones, bases de datos, es decir, los aspectos de mayor interés de los usuarios de esta nueva red, como se muestra en la figura 40.

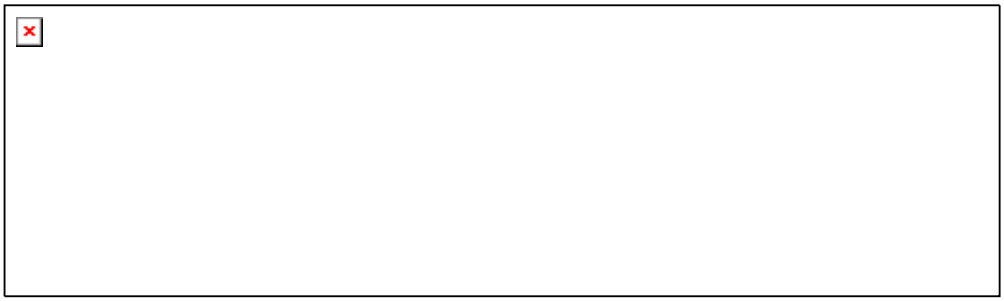


Figura 40. Modelo de seguridad por capas: perimetral (enrutadores), tránsito (protocolos como IP), host (seguridad propia por computadora), almacenamiento (seguridad de las BD, RAIDs, etc) y la seguridad en las aplicaciones (desarrollo, calidad, etc).

El experimentar en un ambiente real, e interactuar directamente con otras nuevas tecnologías, permitirá obtener resultados igualmente válidos en comparación con esquemas simulados, pero mejores y más apegados a la realidad, aplicables directamente en una red funcional. Dichos resultados podrán contribuir de forma inmediata para la consideración de IPSec, como una alternativa para brindar servicios de seguridad en la siguiente generación de Internet en nuestro país. El método seleccionado de análisis para este trabajo de tesis es el de experimentación.

El proceso de análisis tuvo tres enfoques: los servicios de seguridad y su resistencia a los ataques más dañinos (DoS, Spoofing), el rendimiento de la instrumentación de IPSec, bajo distintas configuraciones y la Calidad de Servicio.

Se conceptualizaron, diseñaron e instrumentaron varios escenarios de experimentación: a)usando la Red-CICESE como red pública insegura, b) a través de Internet 2 en México, y c)en un ambiente controlado, un Laboratorio de Interoperabilidad

expresamente diseñado e instrumentado para la Reunión de Otoño de CUDI 2001. Cada uno de estos escenarios serán descritos a lo largo de este capítulo.

Metodología.

Para el planteamiento de la metodología a seguir en el análisis de IPSec se investigaron varias iniciativas sobre cómo probar que un sistema es seguro, principalmente el manual de recomendaciones con licencia GNU, Open Source Security Testing Methodology Manual [Herzog, 2001]. Con base en dichas referencias, se plantea en este trabajo un proceso basado en los dos tipos de ataques: pasivo y activo (descritos en el capítulo II) y cuatro conceptos perfectamente aplicables a IPSec:

Visibilidad: cuánto puede verse en Internet, es decir, puertos abiertos, tipo de sistema, arquitectura, aplicaciones instaladas, direcciones de correo, nombres de empleados, etc.

Acceso: qué accesos se brindan al exterior, es decir, servicios públicos como páginas web, servidores DNS, video, correo, etc.

Confianza: tipo y cantidad de mecanismos de autenticación, no repudio, control de acceso, contabilidad, confidencialidad de datos, e integridad de datos.

Alarma: Registro y monitoreo en tiempo y propiedad en búsqueda de actividades que violen los conceptos anteriores, como bitácoras, tráfico, acceso a puertos, etc.

Una metodología debe plantear un flujo a través del cual se recolectan datos, se analizan y se obtienen resultados. En la figura 41 se encuentra la representación gráfica del proceso que se siguió en este trabajo.

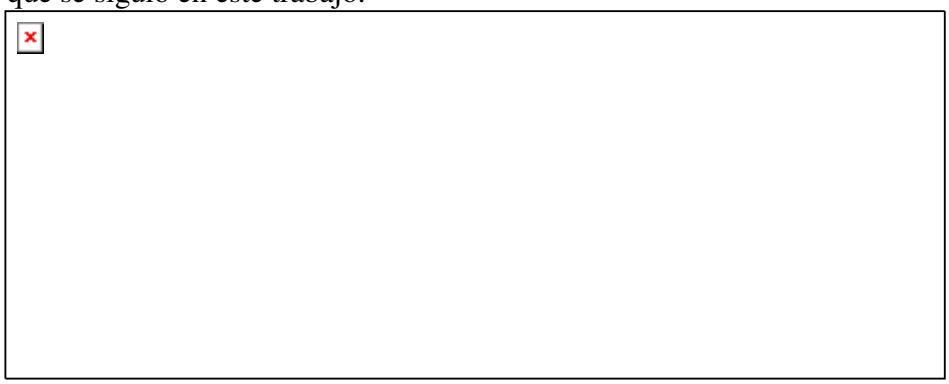


Figura 41. Representación gráfica del flujo de la metodología de análisis.

La metodología incluye la instrumentación de escenarios diversos que cubran las diferentes configuraciones de IPSec, generación de pruebas de seguridad y rendimiento para cubrir los enfoques planteados. Las fases se describen a continuación:

1. Conceptualización y diseño de los Escenarios de Pruebas.

2. Instrumentación de los Escenarios de Pruebas en Red-CICESE, en Internet 2 y en un ambiente controlado. Lo anterior incluye:

- Definición de requerimientos de hardware y software para instalación de IPSec sobre IPv4 e IPv6.
- Definición de los puntos apropiados para instrumentar IPSec en la red.
- Definición de políticas y asociaciones de seguridad relevantes para el funcionamiento de IPSec.
- Instrumentación de escenarios funcionales considerando la modularidad para cumplir las configuraciones requeridas: VPN, host-to-host, host-to-gateway.
- Selección de software para analizar el tráfico para recolectar datos y estadísticas.

3. Definición de los parámetros de evaluación del sistema de pruebas.
   - Contenido de los campos de los paquetes IP, encabezados ESP y AH.
4. Definición de Plan de pruebas.
   - Considerar las diferentes configuraciones de operación de IPSec, así como modos de funcionamiento, para evaluarlas de forma independiente.
   - Selección de ataques para verificar vulnerabilidades en el campo de acción de IPSec (Confianza, Acceso en la capa de red): DoS, *sniffer* sobre medios, principalmente para demostrar las ventajas de las conexiones seguras con IPSec, intercepción de paquetes de diferentes servicios (H.323, DNS, etc), y falsificación de paquetes hacia un destinatario específico.
   - Ejecución de aplicaciones para verificar el comportamiento en cada una de las configuraciones propuestas, con servicios de seguridad y sin servicios de seguridad para hacer un análisis comparativo.
   - Análisis del comportamiento del sistema mediante la relación entradas/salidas.

- Verificar el funcionamiento de servicios de Calidad de Servicio, *Firewalls* y listas de acceso, en teoría estos dispositivos podrían deshechar los paquetes al no poder abrirlos.
- Generación de tráfico para medir el rendimiento de los *gateways* de seguridad de las diferentes plataformas elegidas.

5. Ejecución de Plan de pruebas.
    - El registro de datos y estadísticas debe hacerse distinguiendo los esquemas de pruebas con servicios de seguridad y sin servicios de seguridad.
6. Generación del comportamiento gráfico de los diferentes escenarios.
7. Análisis numérico y documentación de resultados.
8. Evaluación del sistema.
9. Conclusiones y recomendaciones.

Escenarios de Pruebas.

Como resultado de la investigación de proyectos similares, se experimentó con implementaciones del tipo BITS, en Sistemas Operativos. Se eligieron dos sistemas diferentes, populares y utilizados en el entorno de Internet 2: MS-Windows2000© y Linux.

Las conexiones seguras *host-to-host* fueron probadas sobre MS-Windows2000© y su versión experimental IPSec6 con IPv6, y Linux con IPv4. Los *Gateways* de Seguridad fueron instrumentados en GNU/Linux en su variante Slackware con el proyecto FreeS/WAN (Free Security Wide Area Network) [FSWAN, 2001]. Este proyecto tiene como principal objetivo hacer la Internet segura y privada, apoyar la difusión y uso de IPSec, produciendo tecnología bajo esquemas de libre distribución para GNU/Linux y no sujeto a restricciones de exportación. Se considera una excelente alternativa para ser utilizado como plataforma base de desarrollo, de tal forma que este trabajo de tesis complemente una iniciativa ya con camino recorrido, y la contribución a Internet2 sea un sistema funcional, de inmediata instalación y uso.

El código fuente y documentación del proyecto se distribuye bajo licencia GPL (General Public License o GNU Library General Public License), de tal manera que es una buena plataforma de arranque para experimentar y evaluar la potencialidad de IPSec, su aplicación en VPN e IPv6, así como implementar servicios más allá de túneles predefinidos de protección, servicios que le permitan al usuario la libertad de decidir los niveles de seguridad deseados y que la infraestructura de protección sea dinámica y adaptable a las necesidades.

FreeS/WAN soporta varias aplicaciones, entre las más importantes:
a) VPN, permite la comunicación segura entre múltiples sitios sobre una red insegura (Internet) mediante la encriptación de toda la comunicación entre los sitios.
b) Road Warriors, permite la comunicación segura para sitios con direcciones IP de asignación dinámica.
c) Encriptación Oportuna, permite la habilidad para configurar FreeS/Wan gateways de tal manera que entre ellos negocien el establecimiento de encriptación, de forma dinámica.

El proyecto FreeS/WAN está apegado a los estándares, tiene estrecha relación con el grupo de trabajo de IPSec de la IETF para la validación de la implementación y nuevas iniciativas como la de encriptación oportuna.

Se conceptualizaron e instrumentaron tres escenarios de experimentación: uno dentro de Red-CICESE, otro a través de Internet2 e Internet y el último expresamente creado para la Reunión de Otoño de CUDI 2001. En todos los escenarios experimentales se obtuvieron una serie de datos, con los cuales se generaron estadísticas asociadas, matrices de datos que fueron procesados para la discusión de resultados, no están incluidos en este documento de tesis, pero sí en la copia electrónica en la que se almacenó todo el trabajo.

Escenario VPN.

Se conceptualizó y diseñó una conexión de IPSec del tipo *gw-to-gw* para evaluar una VPN con gateways de seguridad (SG) (GNU/Linux en su variante Slackware con FreeS/WAN) dentro de la Red-CICESE. Se crearon dos redes protegidas con este esquema, considerando la Red-CICESE como una red pública insegura, el diagrama se muestra en la figura 42.

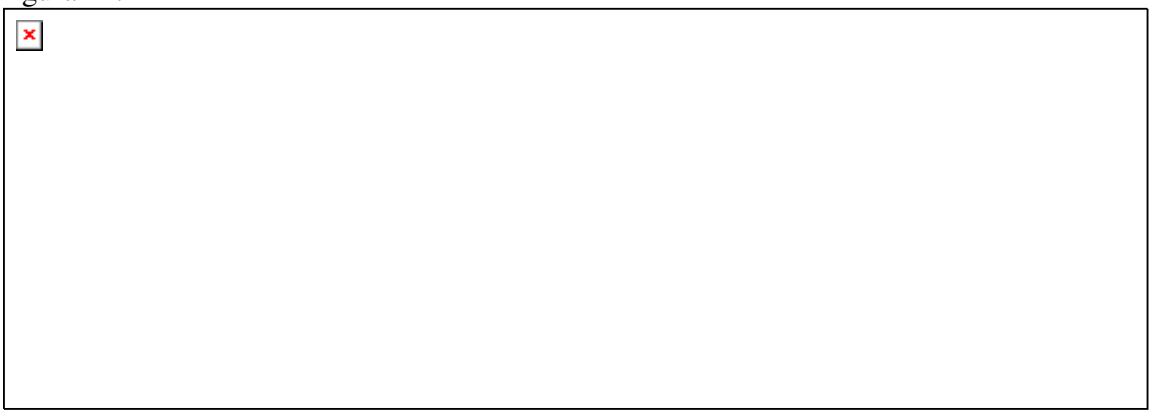


Figura 42. Escenario de pruebas que instrumenta una VPN dentro de la Red-CICESE, utilizando ésta como una red pública insegura.

La VPN fue construida entre los gateways de seguridad (pc-comedi y pc-simula4), asegurando de esta manera todo el tráfico generado entre la subred 158.97.92.0 y la subred 158.97.24.0. Se creó la asociación de seguridad para trabajar en modo túnel, aplicando autenticación y ESP. La relevancia de este escenario radica en la evaluación del concepto de VPN, su funcionamiento y experimentación. Se configuraron dos gateways de seguridad de forma similar, el IPSec es incrustado directamente en el kernel, en la pila IP y las asociaciones de seguridad son negociadas por *demonios* del sistema operativo. La creación del escenario implicó esfuerzos de conectividad, enrutamiento, definición de los puntos IPSec, diseño del esquema, pruebas de funcionamiento sin servicios de seguridad, configuración de la VPN y pruebas con servicios de seguridad. De los elementos obtenidos más relevantes, fue la comprobación del cifrado de la información por los protocolos de IPSec, colocando un elemento del tipo "man-in-the-middle" en la red pública insegura, analizando el tráfico, abriendo paquetes antes y después de activada la VPN, así como pruebas de falsificación de tráfico y ataques del tipo de Denegación de Servicio (DoS). Se observó también la transformación de los paquetes al aplicar IPSec en modo túnel.

Escenario host-to-host.

Se instrumentaron conexiones IPSec del tipo *host-to-host* para experimentar con IPv6, se establecieron túneles de conexión con dos instituciones académicas en México a través de la infraestructura de Internet2 y de Internet, utilizando la pila IPv6 experimental proporcionada para MS-Windows2000© que incluye IPSec6, el diagrama se muestra en la figura 43.

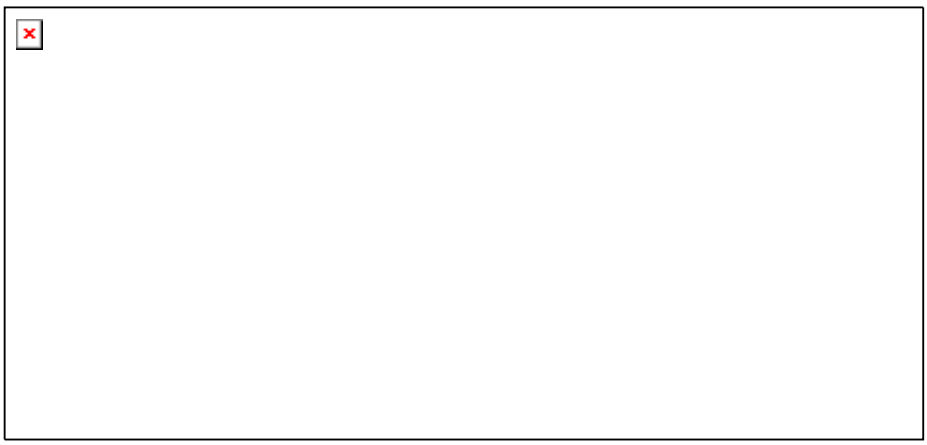


Figura 43. Escenario de pruebas de conexiones seguras a través de Internet 2 e Internet 1 con instituciones del Grupo de Trabajo de Seguridad de Internet 2 [GTS, 2001].

Se realizaron pruebas de funcionamiento de los túneles IPv6 hacia sitios con este protocolo habilitado en Internet, capturando los tiempos de respuesta con IPv4 y al aplicar encapsulamiento para IPv6. Se probaron dos conexiones seguras con IPSec creadas en modo transporte, una conexión CICESE-UNAM y otra conexión UNAM-ULSA, capturando los tiempos de respuesta al aplicar el encapsulamiento de IPv6 e IPSec y la transformación de los paquetes en modo transporte.

Escenario controlado.

Se conceptualizó, diseñó e instrumentó un escenario controlado para pruebas, expresamente para la Reunión de Otoño de CUDI 2001, primera ocasión en que se probó la interoperabilidad de tecnologías, se demostró el funcionamiento de una VPN y conexión segura y su impacto en las aplicaciones multimedia. Fue un esquema para evaluar los protocolos y aplicaciones utilizadas en Red CUDI con y sin servicios de seguridad. La figura 44 muestra el escenario de pruebas completo, la figura 45 resalta las configuraciones de IPSec.

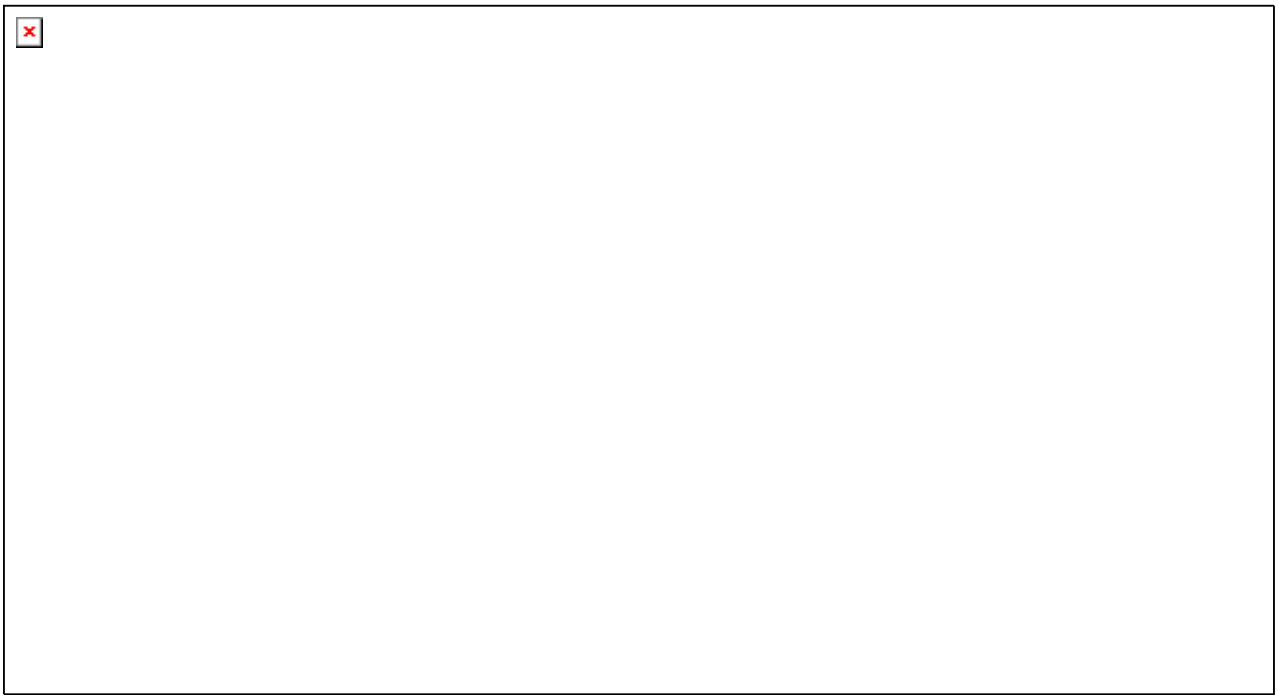


Figura 44. Escenario de pruebas diseñado para la Reunión de Otoño de CUDI 2001.

Se creó una VPN con dos gateways de seguridad instrumentando IPSec en modo túnel, con IPv4, creando asociaciones de seguridad para las subredes izquierda y derecha de la siguiente forma: se aplicó ESP, manejo de llaves manual, SPI 200, y se generaron

para cada SG, llaves para autenticación y para encriptación. El algoritmo de encriptación es 3DES-MD5-96. Adicionalmente una conexión segura con IPSec6 en modo transporte, IPv6, políticas de seguridad para todo el tráfico y autenticación como servicio de seguridad, también fueron complemantadas.

La VPN se resalta con un tubo grueso entre los gateways de seguridad centrales, y la conexión segura se resalta con una línea punteada entre un host de la subred central y un host de la subred derecha.

Figura 45. Pruebas de IPSec en el escenario de pruebas de la Reunión de Otoño de CUDI 2001.

Este escenario entregó resultados muy interesantes, se tuvo la oportunidad de probar otros protocolos como multicast, H.323 y otros, con y sin servicios de seguridad, las pruebas realizadas y resultados se describen a detalle en los siguientes apartados de este capítulo.

Definición de pruebas.

Las pruebas se fueron desarrollando de forma gradual, considerando las diferentes configuraciones de IPSec y modos de funcionamiento. En el escenario VPN se enfocó el análisis sobre las vulnerabilidades de los SG, de una red de conmutación de paquetes sin servicios de seguridad, y verificar la transformación de los paquetes al aplicar IPSec. En el

escenario host-to-host, además de observar la transformación de paquetes, se observó la sobrecarga al aplicar encapsulamiento al utilizar IPv6 e IPSec6, y se verificó el funcionamiento atravesando el Firewall de Red-CICESE. En el escenario controlado el interés principal fue la ejecución de aplicaciones, la generación de tráfico para analizar el rendimiento, generación del comportamiento gráfico y verificación de calidad de servicio.

Escenario VPN.

El objetivo fue interceptar tráfico, mostrar las vulnerabilidades de una red local de datos basada en IP sin servicios de seguridad y observar las diferencias al habilitar un protocolo de seguridad como IPSec en una configuración de VPN. Las pruebas se realizaron de extremo a extremo del escenario de la figura 42, a través de transmisiones de paquetes con un patrón definido (feedfacedeadbeef) para que fueran fácilmente reconocibles al analizar el tráfico, así como la captura general del tráfico en la Red-CICESE como pública insegura, para observar diferencias al aplicar servicios de seguridad del tipo de IPSec y medir sus alcances y protección sobre ataques del tipo de falsificación de paquetes (spoofing) y denegación de servicio (DoS).

Adicionalmente, para demostrar las vulnerabilidades de una LAN basada en IP sin servicios de seguridad, se capturó el tráfico de forma indiscriminada en el segmento donde fue instalado el *sniffer*, los datos obtenidos se discuten en el siguiente capítulo.

Escenario host-to-host.

El objetivo de este escenario fue probar IPSec en modo transporte, aplicado a hosts, creando conexiones seguras punto a punto, conexiones host-to-host con IPv6 en una WAN[9]. Se realizaron dos conexiones seguras probadas sobre Internet e Internet 2, para apreciar el sobreflujo al aplicar el encapsulamiento, primero para IPv6 y después para IPSec. Las políticas de seguridad y las asociaciones de seguridad se construyeron para aplicar modo de transporte y el protocolo AH. Al establecer conexiones hacia Internet e Internet2, se atravesó el *firewall* de Red-CICESE, se probó para manejar paquetes con IPv6 encapsulado y con IPSec, los resultados son discutidos en el capítulo V.

Escenario controlado.

La red mostrada en la figura 44 ilustra el escenario general instalado para la Reunión de Otoño de CUDI 2001. Se generó tráfico *multicast*, video por paquetes (H.323), entre otros. Las muestras fueron obtenidas con la VPN desactivada, 100 muestras de tres

[9] Wide Area Network o Red de cobertura amplia.

tamaños de paquete distintos: 64, 1024 y 2024 bytes, y con la VPN activada, 100 muestras con los mismos tamaños de paquete. El tamaño de paquete es importante para observar el comportamiento por fragmentación, al manejar datos, voz y video, más esquemas de encapsulamiento que aumentan la carga útil de un paquete y obligan su división para ser transmitidos. Se transmitieron paquetes pequeños de 64 bytes, paquetes de 1024 bytes (la unidad máxima de transmisión (MTU) en Ethernet es 1518 bytes) y paquetes grandes de 2024 bytes.

La dirección IP de la LAN fue 148.202.245.0, se crearon tres subredes: 148.202.245.0/27 para el segmento de conexión a I2, 148.202.245.32/27 para la subred derecha, y 148.202.245.64/27 para la subred izquierda. En cada subred se encontraba un equipo de Calidad de Servicio, para probar el comportamiento de éste con paquetes IPSec en la conexión segura con IPv6 e IPSec6 y la VPN con IPv4.

Definición de pruebas a nivel sistema.

Además de la definición de pruebas de seguridad en los diferentes escenarios, un aspecto importante es la definición de pruebas a nivel del sistema de red, medidas éstas en términos de: retardos, variación del retardo (jitter) y caudal eficaz (throughput). El retardo punto a punto es el tiempo que transcurre desde que un paquete es enviado por un nodo fuente hasta que éste es recibido por el nodo destino. La variación del retardo o *jitter* es la diferencia en el retardo encontrado por paquetes consecutivos con un mismo destino de red, cuando un paquete arriba a un buffer y encuentra paquetes delante de él, o arriban posteriormente pero con mayor prioridad, el paquete de interés tiene que esperar a que los primeros sean atendidos, lo que aumenta el retardo para paquetes del mismo tipo. El caudal eficaz o *thoughput* es la porción del tráfico ofrecido que es recibido exitosamente en el punto destino.

En todos los casos, se utilizaron herramientas de análisis de tráfico, para obtener retardos y *throughput*, con ello se calculó el *jitter* para evaluar el sistema, con y sin servicios de seguridad, para definir si los valores resultantes cumplen los valores permitidos de parámetros de desempeño para los servicios sensibles del tiempo: un retardo de 400ms y *Jitter* de 20ms para voz, mismo retardo y 30ms de *jitter* para video [Cruz, 2001].

Conclusiones.

En este capítulo se describieron las pruebas realizadas con el protocolo IPSec, cubriendo los tres enfoques planteados: la relevancia de aplicar servicios de seguridad ante una evidente y comprobada vulnerabilidad de IP, extraer tráfico de una LAN es sencillo y representa problemas serios. La resistencia de IPSec a las estrategias de ataques, las prestaciones de una red en donde se ha instrumentado IPSec, bajo distintas configuraciones

y la evaluación de dichas prestaciones para garantizar la calidad de servicios, sobre todo aquellos que se están manejando en Internet2, servicios sensibles al tiempo como son voz y video. En el siguiente capítulo se desarrollará el análisis numérico, se discutirán los resultados que serán la base para las conclusiones y recomendaciones de este trabajo de tesis.

Capítulo V

Introducción.

Los resultados que se analizarán a continuación, arrojan conclusiones interesantes, en contra de lo que se hubiera esperado en un principio sobre la degradación del sistema al aplicar servicios de seguridad. Se encontraron resultados donde los mecanismos de *buffering* en un *gateway* de seguridad facilitan el control de los paquetes e impactan de forma positiva los servicios sensibles del tiempo de transmisión. Se comprobó la vulnerabilidad de una LAN basada en IP, los efectos de encapsulamiento, entre otros parámetros analizados en este capítulo.

Escenario VPN.

De acuerdo a la figura 42 del capítulo anterior, las pruebas sobre este escenario mostraron las vulnerabilidades en una LAN sin servicios de seguridad. En la figura 46 se muestra el envío de pings (paquetes de 64bytes) del host sunrise (158.97.24.1, subred derecha) al host sunset (158.97.92.1, subred izquierda), adicionalmente se generaron algunas consultas al servidor web de sunset. El tráfico fue interceptado en tránsito de una subred a otra, y lo capturado de forma indebida se muestra en la figura 47.

```
[comedi@sunrise comedi]$ ping -p feedfacedeadbeef sunset
PATTERN: 0xfeedfacedeadbeef
PING sunset (158.97.92.1) from 158.97.24.1 : 56(84) bytes of data.
64 bytes from sunset (158.97.92.1): icmp_seq=0 ttl=29 time=3.4 ms
64 bytes from sunset (158.97.92.1): icmp_seq=1 ttl=29 time=1.9 ms
64 bytes from sunset (158.97.92.1): icmp_seq=2 ttl=29 time=1.9 ms
```

Figura 46. Envío de pings con un formato definido del host sunrise en la subred segura de un extremo al host sunset en la subred segura del otro extremo del escenario de la figura 42.

```
[root@sniffer comedi]# /usr/local/sbin/tcpdump -x host sunset
tcpdump: listening on eth0
03:16:00.994977 158.97.24.1 > sunset.cicese.mx: icmp: echo request
        4500 0054 560a 0000 3f01 74da 9e61 1801
        9e61 5c01 0800 920c 7d18 382b 49f5 7a3b
        5a5f 0600 feed face dead beef feed face
        dead beef feed
03:16:00.996362 sunset.cicese.mx > 158.97.24.1: icmp: echo reply
        4500 0054 18.....
03:16:12.463399 sunset.cicese.mx.1039 > pc-simula4.cicese.mx.http: S 11610724:11610724(0) win 8192 <mss 1460> (DF)
        4500 002c 242a 40.....
03:16:12.463672 pc-simula4.cicese.mx.http > sunset.cicese.mx.1039: S 2052540348:2052540348(0) ack 11610725 win 32120
<mss 1460> (DF)
        4500 002c b7f4.....
```

Figura 47. Tráfico interceptado, filtro definido para tráfico cuyo destino fuera el host sunset.

Al habilitar la VPN, la transmisión entre sunset y sunrise fue asegurada con servicios de autenticación y encriptación, por lo tanto al transmitir de nuevo paquetes con el patrón definido, ya no fue posible su extracción, como había sido el caso sin la VPN, lo único observable por un intruso es el encabezado resaltando el protocolo número 50 asignado a ESP (la VPN fue construida para utilizar este protocolo IPSec). El resultado se muestra en la figura 48, donde se observa la transmisión de paquetes entre pc-simula4 y pc-comedi (los gateways de seguridad) no la fuente y destino de los paquetes originales, sino la información necesaria para su enrutamiento, el contenido ya no es apreciable y el encabezado lleva ahora en el campo de protocolo, el número 50 indicando que son paquetes IPSec.

```
[root@sniffer comedi]# /usr/local/sbin/tcpdump host pc-simula4
tcpdump: listening on eth0
03:31:37.972204 pc-simula4.cicese.mx > pc-comedi.cicese.mx: ip-proto-50 116
03:31:37.974409 pc-comedi.cicese.mx > pc-simula4.cicese.mx: ip-proto-50 116
```

Figura 48. Tráfico entre *sunset* y *sunrise* después de habilitada la VPN, solo puede observarse el protocolo 50 que corresponde a ESP, el encabezado de IPSec.

En la captura de tráfico de forma indiscriminada en el segmento donde fue instalado el *sniffer*, se observaron comunicaciones entre los usuarios de esa subred, los datos obtenidos se muestran en la figura 49, donde puede observarse que las aplicaciones transmiten su información en plano, es decir, en texto simple, dicha información (mensajes, claves de usuario, etc.) puede fácilmente ser capturada, analizada, robada, etc.

```
POP: pc-juancon.cicese.mx => matrix.cicese.mx jcontrer:claveenascii
============
pc-cscw.cicese.mx:cera-bcm > matrix.cicese.mx:telnet [RESET] [AF]
 ^X^_#'$^_#'$^XANSI^A^C^A^Ayhernand
 claveenascii
 set term=vt100;
 pine
 einzunza@cicese.mx
 para que no pongas ninguna objecion yo invito
 ============
sunset.cicese.mx:imgames > 158.97.24.1:telnet [RESET] []
 ^X #'^XANSI^C^A^_^E!^A^Acomedi

 claveenascii

 exit
 ============
pc-cscw.cicese.mx:vocaltec-admin > matrix.cicese.mx:telnet [RESET] []
 ^X^_#'$^_#'$^XANSI^A^C^A^Ayhernand

 claveenascii
 set term=vt10;^Hterm=vt100;
   pine
 write jjuarez
 Que quieres^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^Hfinger
 talk jjuarez
 clear
 mail jjaurez@cicese.mx
 Que?
 Que quieres?
```

Figura 49. Tráfico interceptado en una subred de Red-CICESE (las claves que aparecieron fueron reemplazadas por "claveascii").

Esta situación quizá no es del conocimiento de muchos usuarios, sin embargo, representa riesgos altos para quien requiere de confidencialidad al utilizar su red. Ciertamente, el análisis de tráfico tiene un alto potencial para los intrusos, cifrar el contenido no representa una solución total puesto que los encabezados viajan sin encriptación, las habilidades de inteligencia y deducción de un intruso quedan libres de acción.

Para los ataques *spoofing* y DoS se utilizaron herramientas disponibles en Internet. El ataque *spoofing* que busca falsificar la identidad de paquetes en la red, se inhabilita en un ambiente protegido con IPSec, consecuencia de la autenticación por medio de llaves aplicada a cada paquete que transita por una conexión segura. Sin embargo, los ataques de negación de servicio tienen objetivos diferentes, buscan que un sistema se sobrecargue, sature o se confunda de tal forma que los servicios que ofrece dejen de estar disponibles para usuarios legítimos del sistema. El destino de este tipo de ataques son sistemas, fuera del ámbito de acción de IPSec, por lo que prácticamente no hay protección y cada sistema debe habilitar los *parches*, actualizaciones y recomendaciones para evitar ataques DoS dependiendo del tipo de sistema y aplicaciones corriendo en él.

Escenario host-to-host.

De acuerdo a la figura 43 del capítulo anterior, al probar IPSec en modo transporte con IPv6, se apreció el sobreflujo al aplicar el encapsulamiento, primero para IPv6 y después al insertar el encabezado IPSec, al transmitir información en la conexión segura CICESE-UNAM. El firewall instalado en Red-CICESE, como se esperaba, deshecha los paquetes IPv6 e IPSec. Para el caso de IPv6 hay que habilitar el sistema operativo y actualizar el producto que se utiliza (SunScreen EFS 3.0), para manejar IPSec hay que crear reglas y habilitar filtros para los protocolos 50 y 51. La tabla III muestra los datos promedios obtenidos de las pruebas (paquetes de 64 bytes), en donde puede notarse el sobreflujo al utilizar IPv6 e IPSec, con cada encapsulamiento los milisegundos necesarios para transmitir un paquete aumentaron considerablemente.

Tabla III. Promedios de transmisión entre CICESE y UNAM, sobre Internet y sobre Internet 2, con los protocolos IPv4, IPv6 e IPSec.

Red	IPv4 (ms)	IPv6 (ms)	IPSec6 (ms)
Internet	220	380	460
Internet 2	112	288	312

La observación de los paquetes al habilitar la conexión segura, reflejó la diferencia entre la transformación de los mismos en modo transporte, pudo verse como se muestra en la figura 50, el encapsulamiento de IPv6 en IPv4 (la dirección subrayada es la dirección IPv6 del host en CICESE, la dirección en negrita es la dirección IPv6 del host en la UNAM), al aplicar IPSec6 no hubo cambio en el encabezado IP dado que en modo

transporte, el encabezado AH se agrega al encabezado TCP, el encabezado IP no sufre alteración, situación distinta al aplicar IPSec en modo túnel, donde el encabezado IPSec se agrega al encabezado IP, y al analizar el tráfico, el campo protocolo corresponde a IPSec.

```
12:42:40.035332 pc-vrico.cicese.mx > unam-ipv6-1.ipv6.unam.mx:  ip-proto-41 108
0x0000   4500 0080 548e 0000 8029 395f 9e61 1c10        E...T....)9_.a..
0x0010   84f8 6cfe 6000 0000 0044 3380 2002 9e61        ..l.`....D3....a
0x0020   1c10 0000 0000 0000 9e61 1c10 3ffe 8070        .........a..?..p
0x0030   0001 0008 0000                                 ......
```

Figura 50. Paquete IPSec con IPv6 encapsulado en IPv4, a través de una conexión segura del tipo host-to-host entre CICESE y UNAM sobre Internet2.

Es importante mencionar que los datos obtenidos son sólo una muestra que refleja el estado de la red en un momento determinado, los tiempos de transmisión dependen de muchos factores como estado del enrutamiento, carga en Red-CICESE, carga en Red-UNAM, nivel de congestionamiento en Internet e Internet2, etc. De hecho, para hacer mediciones por Internet comercial, se aprovechó una interrupción del servicio de Internet2, ya que el esquema de enrutamiento normal entre CICESE y UNAM es a través de Internet2. Lo relevante de estos datos es el sobreflujo al aplicar encapsulamiento. En la actualidad se está experimentando con IPv6 en modo túnel, lo que degrada las prestaciones de una red, sin embargo, ayuda a probar aplicaciones mientras se construyen redes con equipo IPv6 puro. En el caso de IPSec su instrumentación es mediante este método en IPv4, pero mediante cabeceras de extensión en IPv6 que sean procesables de forma rápida. No es factible a la fecha hacer pruebas reales en Internet (comercial o 2) a nivel de aplicaciones y evaluar el comportamiento de IPSec con IPv6, dado que IPv6 se encapsula en IPv4 y los resultados son afectados por ello.

Escenario controlado.

Refiriéndose a la figura 44 del capítulo anterior, las figuras 50 y 51 son muy ilustrativas para observar la transformación entre lo que puede ver un intruso analizando tráfico con y sin servicios de seguridad. Como se describió en el capítulo anterior, el escenario fue instrumentado con 3 subredes, una VPN (IPSec con IPv4) y una conexión segura (IPSec6 con IPv6). El rango de direcciones local fue 148.202.245.0-148.202.245.94. En la figura 51 se muestra el tráfico sin servicios de seguridad entre hosts de la subred izquierda y hosts de la subred derecha, adicionalmente tráfico local hacia Internet e Internet2, para efectos de este análisis el interés radica en el tráfico que atravesó la VPN únicamente. Se observan una gran cantidad de líneas que representan comunicación entre esos hosts. Las líneas más gruesas muestran el tráfico más demandante de recursos, servicios de video entre la 148.202.245.65, la 148.202.245.66 (izq) y la 148.202.245.35 (der) por ejemplo. La figura 52 muestra el tráfico después de haber activado la VPN, muestra de forma muy ilustrativa el tubo de tráfico entre la 148.202.245.20 (SG izquierdo) y la 148.202.245.21 (SG derecho), incluyendo todo el tráfico generado entre la subredes izquierda y derecha, es decir, el tráfico visible en la figura 50, deja de serlo y todo el tráfico generado entre la subred izquierda y la subred derecha es cifrado y autenticado con los

mecanismos definidos en la VPN. El intruso observando tráfico queda inhabilitado para obtener mayor información.

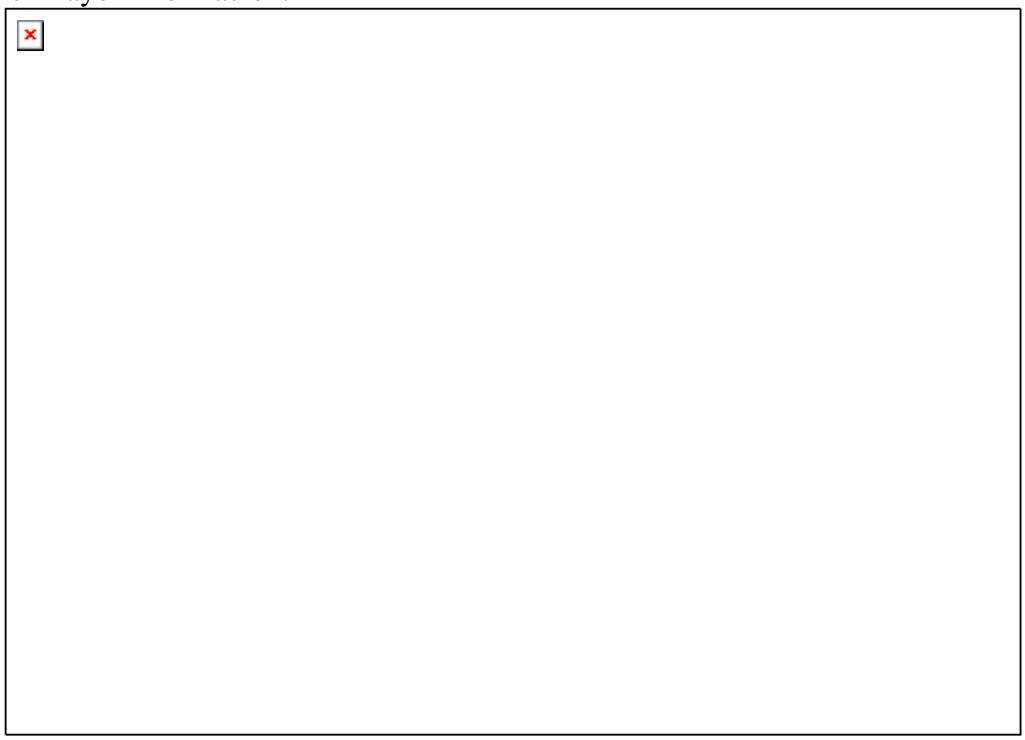


Figura 51. Muestra de tráfico sin aplicar servicios de seguridad (tomada en la subred de conexión a Internet2).

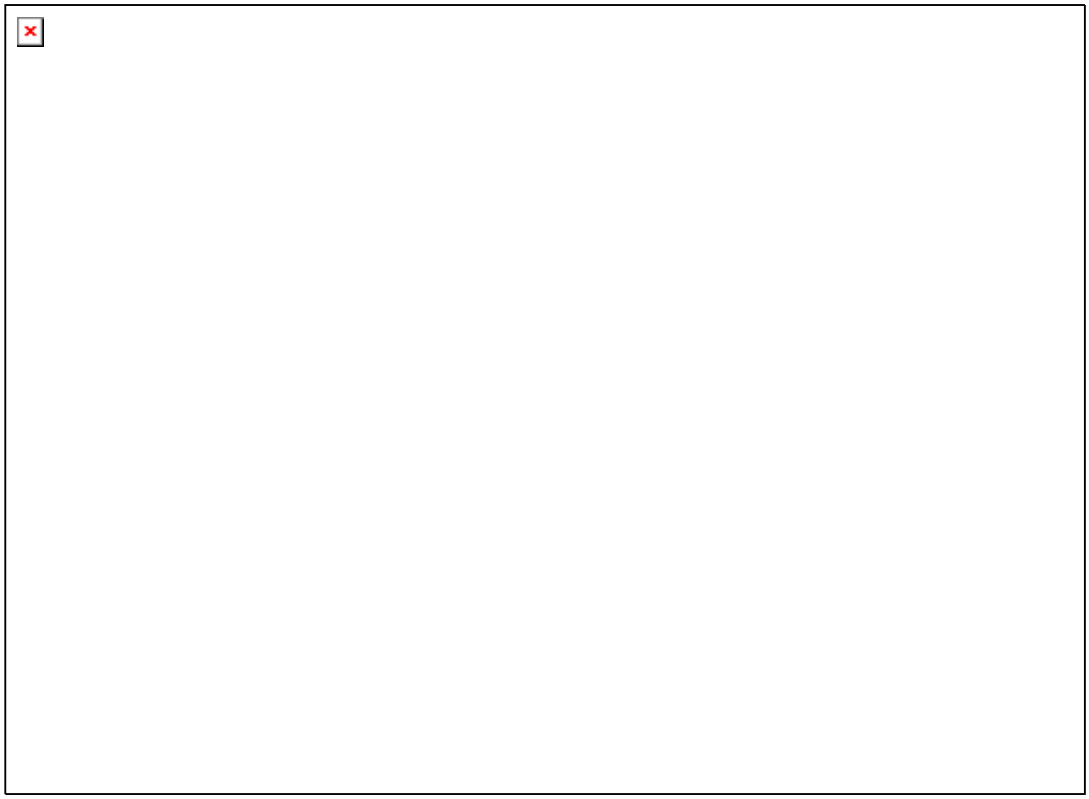


Figura 52. Muestra de tráfico al haber aplicado servicios de seguridad (tomada en la subred de conexión a Internet2).

Se generó tráfico *multicast*, video por paquetes (H.323), entre otros. Los datos fueron obtenidos con la VPN desactivada, y con la VPN activada, 100 muestras para cada tamaño de paquete como se describió en el capítulo anterior.

La figura 53 muestra la gráfica resultante de los datos obtenidos en la transmisión de paquetes de 64bytes con y sin servicios de seguridad de la VPN, de donde puede observarse el contraste de comportamiento del retardo y caudal eficaz al aplicar la VPN y sin aplicarla.

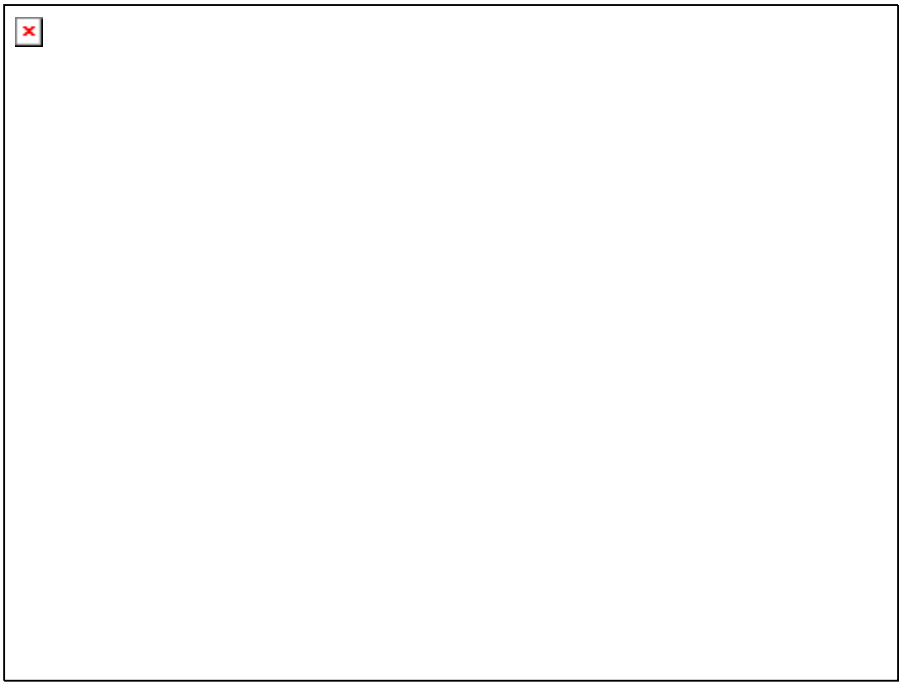


Figura 53. Gráfica de throughput vs retardo para la transmisión de paquetes de 64bytes con y sin servicios de seguridad.

De acuerdo a la figura anterior, al transmitir paquetes sin la VPN, los retardos fueron altos alcanzando un máximo de 406 ms con un caudal eficaz de 2.2 Kbps y un mínimo retardo de 82 ms con un caudal eficaz de 10.92 Kbps, es decir, una comunicación bastante mala. El retardo máximo para la calidad en transmisión de voz y video es de 400ms [Cruz, 2001], en este esquema se rebasa. Esta situación fue observable en las aplicaciones que se estaban ejecutando de multimedia, al activar la VPN el cambio fue totalmente notorio, el aumento en la calidad del servicio fue inmediato y sorprendente, al analizar los datos obtenidos, se ratificó el comportamiento observado, con servicios de seguridad, se tuvo un máximo retardo de 10 ms alcanzando un caudal eficaz de 89.6 Kbps, y un mínimo retardo de 1 ms alcanzando un caudal eficaz de 896 Kbps. Es decir, muy por debajo de los límites permitidos para voz, video y datos que se muestran en la tabla IV [Cruz, 2001].

Tabla IV. Valores permitidos de parámetros de desempeño para diferentes servicios.

Servicio	Retardo	Variación en el retardo
Voz	400ms	20ms
Video	400ms	30ms
Datos	1400ms	--

Este comportamiento se atribuye a la intervención de los gateways de seguridad sobre cada paquete transmitido y recibido, al dar un tratamiento especial para insertar encabezados de autenticación y secuencia de los mismos. Este mecanismo mejoró la

recepción reflejada en la disminución de retardos que además se mantuvieron estables produciendo un *Jitter* también bajo.

Uno de los elementos que da mayor información para evaluar el comportamiento de una red, es la variación del retardo (Jitter). Los datos estadísticos obtenidos, en base a las variaciones del retardo para cada uno de los tres muestreos realizados se encuentran en la tabla V, de donde las variaciones son notables entre los datos sin la VPN activa con respecto a los datos con la VPN activa. Variaciones que respaldan lo observado durante las pruebas en las pantallas de aplicación, al mejorarse de forma evidente el video y el audio, servicios que son sensibles al tiempo.

El comportamiento se mantuvo para los tres escenarios de prueba, en cada caso las prestaciones del sistema con la VPN activada, fueron por mucho superiores a los obtenidos sin la VPN activada.

Tabla V. Determinación de los momentos centrales del *Jitter*.

Eventos	Media	Desviación Estándar	Área
Tamaño paquete: 64B			
Sin VPN	65.88855	99.42132	1133.03484
Con VPN	0.00805	0.06014	9.44581
Tamaño paquete: 1024B			
Sin VPN	19.66815	96.43093	2161.60285
Con VPN	0.37322	1.17755	33.53168
Tamaño paquete: 2024B			
Sin VPN	12.44351	42.36587	1200.58529
Con VPN	2.07721	4.8416	51.5161

Para el caso de paquetes de 64bytes, el histograma resultante del *Jitter* calculado para el muestreo sin la VPN se muestra en la figura 54, el comportamiento del *Jitter* con la VPN activa, se encuentra en la figura 55. La media sin la VPN fue de 65 ms en contraste con 0.008 ms con la VPN, la desviación estándar y el área de la curva establecieron diferencias muy fuertes, los valores sin la VPN muy dispersos con variaciones muy altas, lo que indica una comunicación degradada.

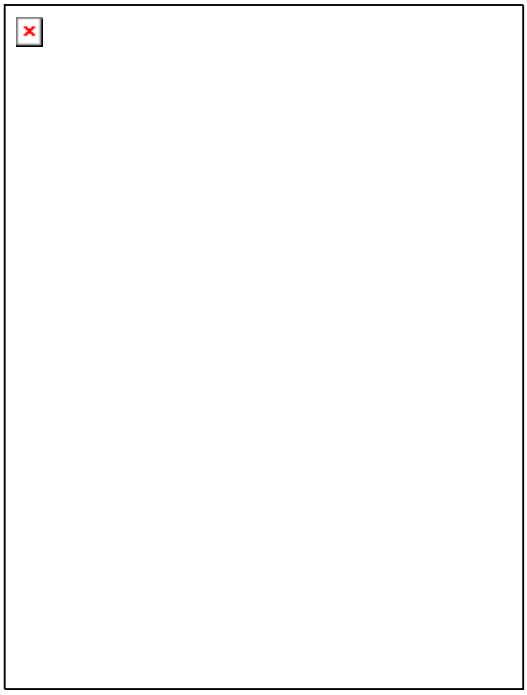


Figura 54. Histograma de la variación de retardo sin servicios de seguridad para paquetes de 64bytes.

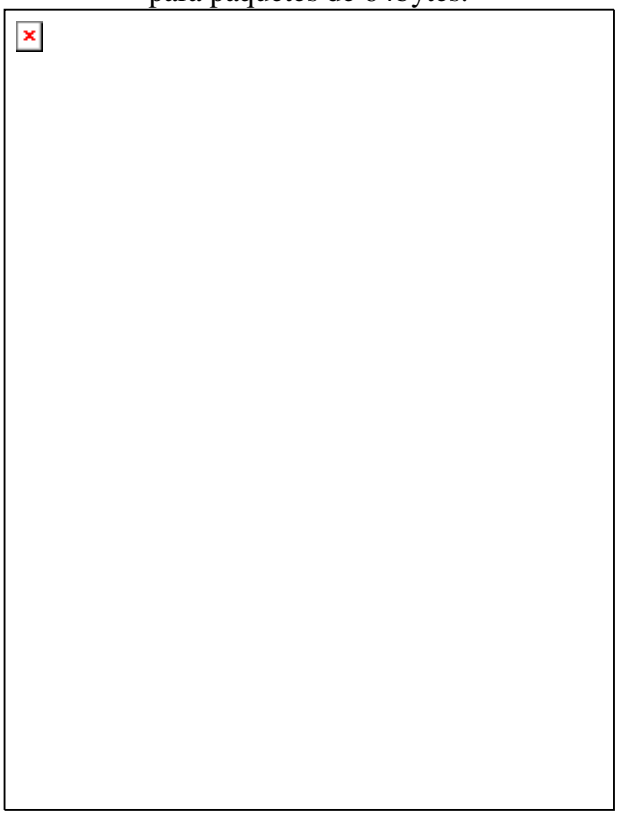


Figura 55. Histograma de la variación de retardo con servicios de seguridad para paquetes de 64bytes.

El siguiente muestreo se realizó con paquetes de 1024bytes, mismas 100 muestras, mismo tráfico generado en la red, con y sin servicios de seguridad de la VPN. La figura 56 muestra la gráfica *throughput* vs retardo, donde el caudal eficaz sin VPN fue mucho mejor que en el caso anterior, sin embargo, el contraste se mantuvo, el máximo retardo sin la VPN fue de 484 ms con un caudal eficaz de 20.69 Kpbs, un mínimo retardo de 7ms alcanzando un caudal eficaz de 2Mbps. Con la VPN el máximo retardo fue 18 ms alcanzando un caudal eficaz de 352Kpbs, y un retardo mínimo de 1 ms con un caudal eficaz de 896Kpbs, el máximo caudal eficaz fue de 5.8Mb (casi el 60% de utilización) con un retardo de 2 ms.

La figura 57 muestra el histograma de la variación del retardo sin VPN y la figura 58 el histograma de la variación del retardo con la VPN activada.

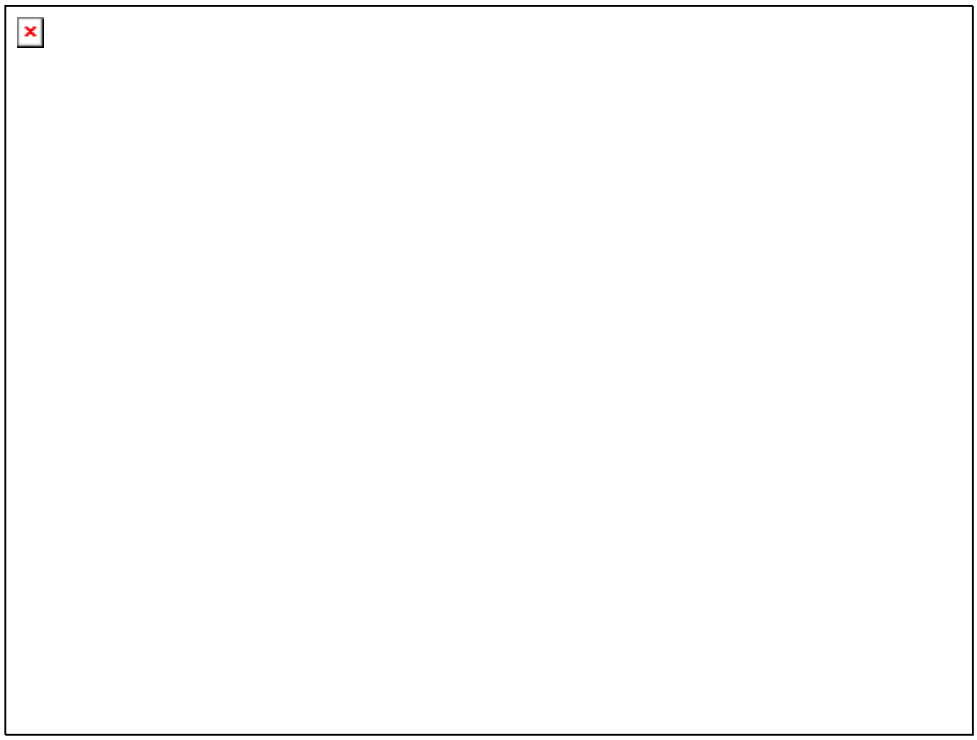


Figura 56. Gráfica de throughput vs retardo para la transmisión de paquetes de 1024bytes con y sin servicios de seguridad.

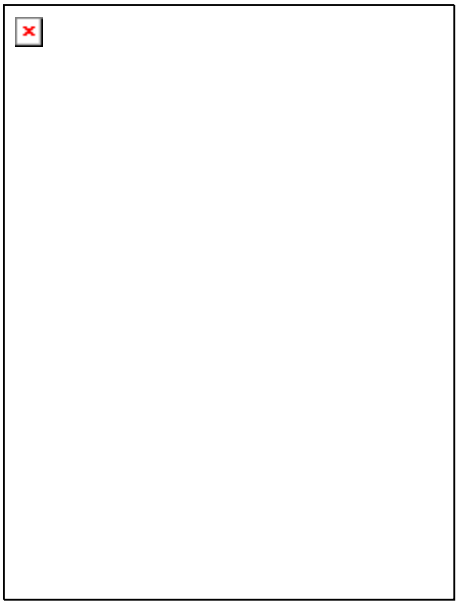


Figura 57. Histograma de la variación de retardo sin servicios de seguridad para paquetes de 1024bytes.

El comportamiento del *Jitter* se mantuvo en este escenario, de nuevo la mejoría de la comunicación fue visible al habilitar los servicios de seguridad de la VPN, los datos estadísticos de la tabla IV, marcan de nuevo la dispersión de los datos, alta variación del *Jitter* en el muestreo sin la VPN, y valores estables y buenos en el muestreo con la VPN.

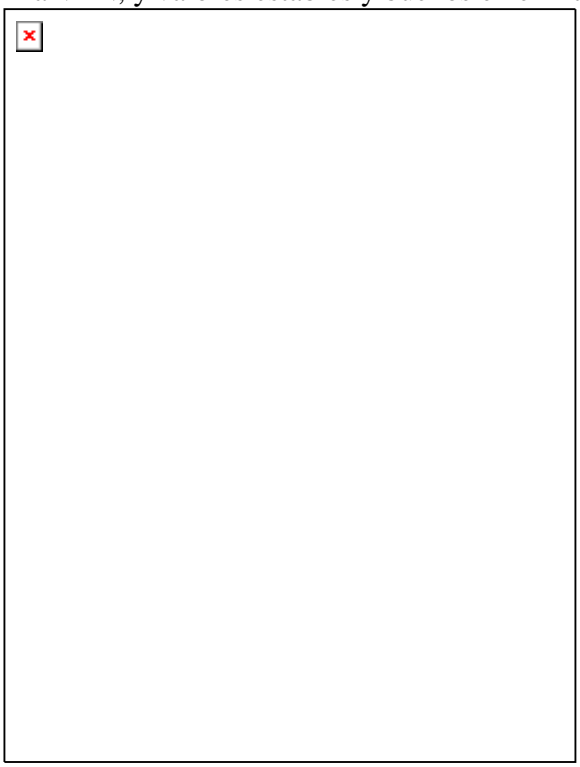


Figura 58. Histograma de la variación de retardo con servicios de seguridad para paquetes de 1024bytes.

El último muestreo se aplicó con paquetes de 2024bytes, paquetes grandes que rebasan el MTU para provocar fragmentación, bajo las mismas circunstancias que los muestreos anteriores, con y sin servicios de seguridad. La figura 59 muestra la gráfica obtenida de *throughput* vs retardo, donde también se observa un comportamiento similar a los casos anteriores, retardos y *Jitter* altos, poco caudal eficaz para la red sin servicios de seguridad, y retardos pequeños y variaciones mínimas del retardo con caudal eficaz casi al 60% de utilización al tener los servicios de seguridad activos. En la figura 60 se muestra el histograma del *Jitter* sin habilitar la VPN , donde se muestra de nuevo un comportamiento similar a los casos anteriores, un área amplia de la envolvente con una media de 12.44 ms.

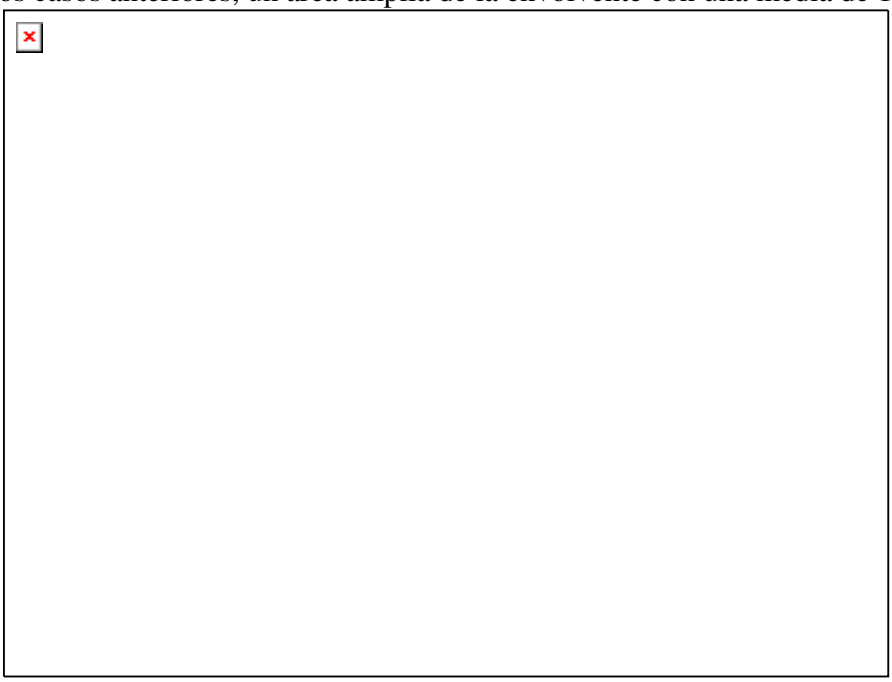


Figura 59. Gráfica de throughput vs retardo para la transmisión de paquetes de 2024bytes con y sin servicios de seguridad.

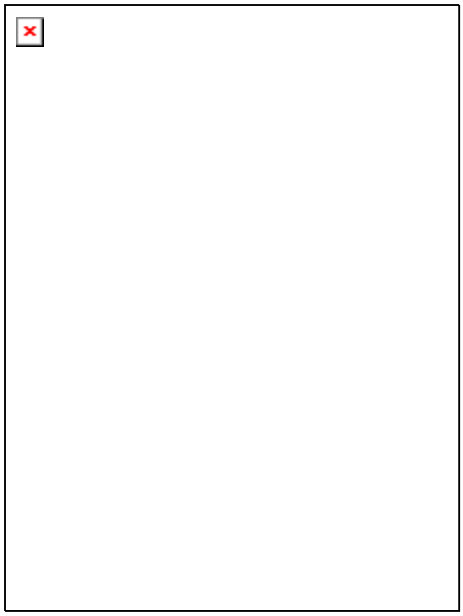


Figura 60. Histograma de la variación de retardo sin servicios de seguridad para paquetes de 2024bytes.

En la figura 61 se muestra el histograma del *Jitter* con la VPN activada, en este caso la variación es muy pequeña con una media de 2 ms. Es importante mencionar que en este escenario el sistema llegó a un punto de saturación, debido al tamaño forzado de los paquetes superior al máximo definido para una red de este tipo, por lo que el número de muestras fue inferior al de los casos anteriores.

El comportamiento se mantuvo para los tres escenarios de prueba, en cada caso las prestaciones del sistema con la VPN activada, fueron por mucho superiores a los obtenidos sin la VPN activada.

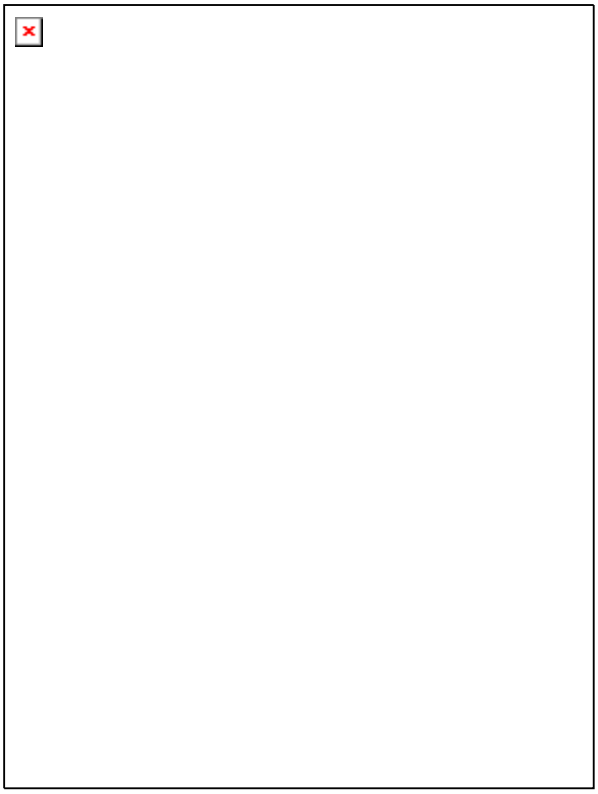


Figura 61. Histograma de la variación de retardo con servicios de seguridad para paquetes de 2024bytes.

La conexión segura fue establecida host-to-host con IPv6 e IPSec6, no estaba anidada en la VPN para poder extraer información y visualizar el tráfico, un extremo se encontraba en la subred central (148.202.245.15) y el otro extremo en la subred derecha (148.202.245.34). Por último, en la figura 62 se muestra un paquete interceptado, con una herramienta habilitada para IPv6, en donde puede observarse además del encabezado normal de IP con protocolo 41 de IPv6, la información encapsulada de IPv6: las direcciones IPv6 y el valor de la siguiente cabecera, 51 correspondiente a AH. En otras herramientas que no manejan IPv6 solo es visible el encabezado IP, no es posible leer el encabezado IPv6 encapsulado, por lo que en conexiones como ésta, IPSec en modo transporte, no es evidente que el contenido es IPSec, no se visualiza ningún cambio, el campo protocolo mantiene su valor 41.

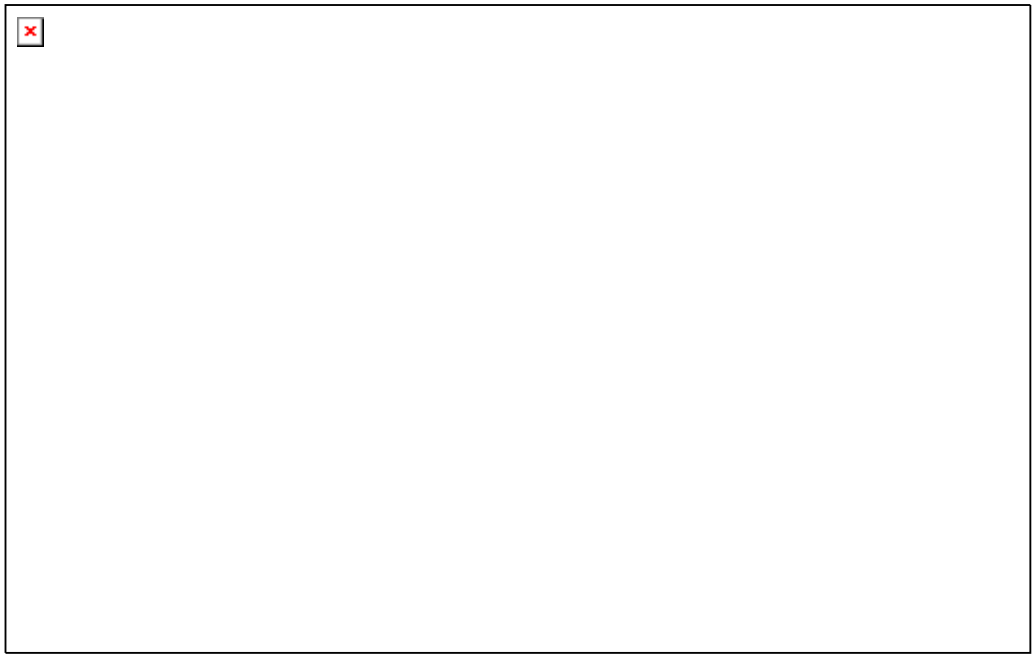


Figura 62. Paquete encapsulado IPSec6 con IPv6 de la conexión segura host-to-host utilizando AH en modo transporte.

Conclusiones.

Algunos de los resultados obtenidos fueron sorprendentes, comúnmente se considera que aplicar servicios de seguridad implica sacrificar prestaciones de la red o de un sistema, ya que los métodos de seguridad implican costo de procesamiento, de sobreflujo en la red, relleno, etc. Para el caso de servicios sensibles al tiempo, resulta interesante conocer que los mecanismos de *buffering* que aplica un *gateway* de seguridad para autenticar y ordenar paquetes cifrados impacta de forma positiva a aplicaciones multimedia.

Considerando las cotas para servicios sensibles de tiempo mostradas en la tabla IV, en los casos sin la VPN, donde los retardos fueron altos y la media del *Jitter* fue arriba de los 20ms, se encuentran en la cota máxima de calidad de servicio para voz, y cerca de la cota máxima de 30ms para video. En los casos con la VPN, los parámetros de desempeño tuvieron valores mínimos con prestaciones excelentes para la transmisión de video y voz. En la tabla VI se muestra un resumen de las estadísticas obtenidas.

Tabla VI. Resumen de las estadísticas obtenidas.

Eventos	**Throughput (Kbps)**		**Jitter (ms)**		**Retardos (ms)**	
	Mínimo	**Máximo**	**Mínimo**	**Máximo**	**Mínimo**	**Máximo**
Paquete: 64B						
Sin VPN	2.2	298.66	1.02	346.01	2.07	406.3
Con VPN	81.45	896	0	8.95	1	10.03

Paquete: 1024B						
Sin VPN	3.26	2120	0.08	214.98	6.06	484.03
Con VPN	300.8	5800	0	17.04	1.01	20.05
Paquete: 2024B						
Sin VPN	29.81	2940	0.02	349.06	11	850.06
Con VPN	1500	5780	0	9.04	4.01	13.06

Las intrusiones fueron interesantes, y resaltaron las deficiencias de IP con respecto a seguridad, la transmisión de datos se realiza sin considerar que puede haber “un hombre en el medio”. Los esfuerzos a nivel de aplicaciones para cifrar sus datos son importantes y funcionales, aunque IPSec resulta ser un excelente complemento para todas aquellas aplicaciones que no integran servicios de seguridad por sí mismas.

Conclusiones

Introducción.

En este trabajo se ha abordado el estado del arte de la aplicación de mecanismos de seguridad a través de protocolos, que representan las nuevas iniciativas de los grupos de trabajo de la IETF.

Se ha considerado un escenario real de pruebas con las ventajas inherentes de experimentar en un ambiente real, e interactuar directamente con otras nuevas tecnologías, los resultados obtenidos han contribuido a la consideración de IPSec, como una alternativa para brindar servicios de seguridad en la Internet de siguiente generación en nuestro país.

El proceso de análisis tuvo tres enfoques: los servicios de seguridad y su resistencia a los ataques más dañinos (DoS, Spoofing), el rendimiento de la instrumentación de IPSec, bajo distintas configuraciones y la Calidad de Servicio.

Con el fin de entender la aplicación y funcionamiento de protocolos de seguridad, se estudiaron los modelos de comunicación OSI y TCP/IP, las vulnerabilidades documentadas del protocolo IP, la clasificación de mecanismos y modelos de aplicación de Seguridad en Redes, el concepto de Red Privada Virtual (VPN) y los protocolos de seguridad estándares, en particular IPSec.

Como parte de la estrategia de evaluación de protocolos de seguridad, se diseñaron e instrumentaron tres escenarios de experimentación: dentro de Red-CICESE, en Internet2 y en la Reunión de Otoño de CUDI. Se desarrollaron configuraciones de VPN y host-to-host con implementaciones de IPSec del tipo BITS en modo túnel y modo transporte. Se realizaron actividades para observar el comportamiento sobre los dos aspectos importantes al aplicar mecanismos de seguridad: seguridad y costo. Actividades de intrusión, análisis de tráfico, evaluación del sistema y la calidad de servicios sensibles del tiempo de transmisión con y sin servicios de seguridad.

La aplicación de Seguridad es indispensable en las redes públicas. IPSec tiene enfoque diferente a otros protocolos de seguridad más populares como SSH y SSL, que funcionan en la capa de transporte y están ligados con una aplicación particular. Con IPSec pueden establecerse comunicaciones seguras extremo a extremo, de forma flexible y bajo diversas configuraciones, sin importar la aplicación del nivel de usuario.

Resumen de los logros más importantes del trabajo a partir de la instrumentación de IPSec.

IPSec es un protocolo punto a punto, es decir, establece una comunicación segura entre dos puntos únicamente, y no es un protocolo end-to-end, es decir, no hay protección de sistema a sistema, o de usuario a usuario. Este protocolo, como los otros estudiados, no ofrecen una solución única para combatir las diferentes vulnerabilidades, es parte de la solución para brindar seguridad en una red, pero no es una solución general, un complemento, por ejemplo, puede ser SSH para establecer conexiones seguras a nivel de usuario.

Contrario a lo que comúnmente se maneja, una VPN no es solamente una red virtual (conmutada), es además privada, no representa una solución completa, y no brinda

protección total a una red, una VPN protege únicamente el canal por donde transita la información de un extremo a otro de la VPN, si uno de los extremos de la VPN o de una conexión segura host-to-host se compromete, se perdió la protección. Más aún, una VPN o conexión segura no brinda ninguna protección con respecto a intrusiones a una computadora, es decir, el hecho que se apliquen VPN o conexiones seguras no sustituye el esfuerzo que debe hacerse por instrumentar mecanismos de seguridad en sistemas, sobre todo si la implementación de IPSec es del tipo BITS en sistema operativo.

IPSec no detiene los ataques del tipo DoS, aunque sí representa una solución para ataques *spoofing*. IPSec cifra y autentica paquetes IP, como se pudo constatar, contra el análisis de tráfico se protege el contenido pero los encabezados quedan visibles, pudiendo representar información útil para los intrusos.

El aspecto más importante al buscar proteger una red, es la Política de Seguridad, que establece la misión de los recursos informáticos y define los niveles de protección deseados, en el caso de Internet2 la política se está estableciendo en el seno del Grupo de Trabajo de Seguridad y la Comisión de Seguridad de CUDI. Las recomendaciones implican: crear una Política de Seguridad donde se contemplen todos los usuarios y recursos de una red, instrumentar IPSec en las conexiones que requieran confidencialidad, instalar un *Firewall* como apoyo al control de acceso, utilizar sistemas de detección de intrusos (IDS), instalar *parches* al software y mantenerlos al día, monitoreo de la red y de bitácoras de sistemas. Los usuarios por su parte: cifrar sus archivos sensibles de confidencialidad, aplicar candados o *screenlocks*, claves para inicializar su computadora, claves robustas de usuario.

La evaluación del sistema (con IPv4) se desarrolló en un escenario controlado, con un número pequeño de asociaciones y políticas de seguridad de IPSec, los resultados en el comportamiento de aplicaciones multimedia (RealServer©, MeetingPoint© con H.323) fueron sorprendentes, no se esperaba ver los contrastes de retardo y caudal eficaz entre las muestras obtenidas con y sin la VPN, los datos obtenidos (tablas V y VI) enmarcan la mejora de la calidad de servicios observada durante las pruebas en el laboratorio y comprobada con el análisis numérico.

En la experimentación con IPv6 se obtuvieron datos sobre el retraso producido por el encapsulamiento de IPv6 en IPv4 a través de Internet2, el encapsular merma la evaluación real del funcionamiento de IPSec y aplicaciones, sin embargo, los datos obtenidos muestran que el costo de encapsular es considerable, bajo este esquema no se están obteniendo los beneficios esperados de IPv6 mientras Internet2 no maneje este protocolo como protocolo fundamental de comunicación.

Los resultados obtenidos en este trabajo de tesis abrieron una línea de investigación para los Grupos de trabajo de Seguridad, IPv6, End-to-End y Calidad de Servicio del Comité del Desarrollo de la Red de CUDI en busca de tecnologías que permitan proporcionar un medio seguro y con la mejor calidad a las aplicaciones de sus usuarios.

Principales aportaciones de la tesis.

Este trabajo de tesis representa para mi un fuerte crecimiento profesional y personal al abordar uno de los temas que representan el estado del arte de Seguridad en redes. IPSec es motivo de investigación y experimentación en núcleos de desarrollo importantes en el mundo, sobre todo en proyectos nacionales de redes de siguiente generación. CICESE ha contribuido a través del desarrollo de este trabajo de tesis, participando en las reuniones nacionales de CUDI con la activación del Grupo de Seguridad de CUDI, un tutorial de IPSec, el diseño e instrumentación de un laboratorio de prueas y el desarrollo de pruebas de IPSec sobre enlaces a través de Internet 2 entre diferentes instituciones.

IPSec es sin duda un excelente candidato para ser utilizado en redes de siguiente generación que utilizan el Protocolo Internet (IP) como protocolo de red, como es la Internet2 en México, su aplicación radica en la capa de Tránsito del Modelo de Seguridad por capas (figura 40) propuesto por el Grupo de Seguridad para Internet 2 en México.

Con este trabajo de tesis, se inicia la labor de consultoría del Grupo de trabajo de Seguridad de CUDI para la instrumentación de IPSec en sus diferentes configuraciones en Internet2 y en las instituciones académicas que pertenecen a ella.

Líneas futuras de investigación.

El protocolo IPSec está en etapa de exploración y comprensión, es un estándar de la IETF en proceso de re-evaluación sobre la cual se han sometido propuestas de simplificación a nivel de *drafts*, hay mucho trabajo por hacer sobre el análisis de vulnerabilidades de la arquitectura de IPSec y sobre todo del protocolo para manejo dinámico de llaves IKE donde la propuesta se está gestando con el nuevo protocolo son-of-IKE o IKE versión 2.

Existen diferentes iniciativas de instrumentación de IPSec en diversas plataformas para ampliar su uso, hay mucho trabajo de desarrollo por hacer con respecto a la integración de nuevos protocolos en las redes de siguiente generación como Multicast, MultiProtocol Levels Switching (MPLS), PKI, Multicast Key Management Protocol (MKMP), entre otros.

En el Grupo de Trabajo de Seguridad hay fuerte interés por la interoperabilidad de IPSec sobre diferentes plataformas para establecer conexiones seguras y/o VPN entre las instituciones con equipo de diferente arquitectura. En varios grupos de trabajo del CDR se están gestando planes para hacer pruebas exhaustivas de las tecnologías (entre ellas IPSec), sobre la infraestructura de Internet2 en busca de fronteras de calidad de servicio para aplicaciones End-to-End.

En el CICESE están en proceso de pruebas los Sistemas Administrativos en ambiente WWW, por el grado de confidencialidad de la información es de suma importancia contar con un ambiente seguro, se está considerando IPSec como base tanto en el campus CICESE como en la comunicación inter-campus con La Paz, Monterrey y la oficina en el D.F., o bien conexiones remotas de los directivos y/o jefes de proyectos.

Referencias

Baluja, García Walter. *Los ataques spoofing. Una estrategia general y una herramienta para combatirlos.* Tesis de Maestria. ISPJAE, Habana, Cuba. 2000.

Briscoe, Neil, *Understanding the OSI 7 Layer Model*. Briscoe. PC Network Advisor. Num. 120. Julio 2000. Pag. 13. http://www.itp-journals.com/search/t04124.htm

BXA, 2001**.** *US Commerce Department's Bureau of Export Administration.* http://www.bxa.doc.gov/Encryption

CERT, *2000 Annual Report,* CERT Coordination Center, Abril 2001. http://www.cert.org/annual_rpts/cert_rpt_00.html

Cooper, Frederic J., Goggans Chris, Halvey John K., Hughes Larry, Morgan Lisa, Siyan Karanjit, Stallings William, Stephenson Peter. *Implementing Internet Security.* New Riders Publishing. 1995.

Cripto, 2001. *Amenazas deliberadas a la seguridad de la información*, http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html

Cruz, Patiño Héctor Raúl. *Análisis y modelado de mecanismos para la implementación de redes con calidad de servicio*. Tesis de Maestría, Departamento de Electrónica y Telecomunicaciones, CICESE. Agosto 2001.

CUDI, 2001. Corporación Universitaria para el Desarrollo de Internet, http://www.cudi.edu.mx

Feit, Sidnie. *TCP/IP Architecture, protocolos, and implementation*. McGraw-Hill Series on Computer Communications. 1993.

FSWAN, 2001. Linux FreeS/WAN Project. http://www.freeswan.org.

Grosek, Otokar, Herrera-Garcia Sergio. *Cryptology or " What Kama sutra did suggested"*. FEI Slovak Technical University/CITEDI-IPN. Material de curso. Abril 2001.

GTS, 2001. Grupo de Trabajo de Seguridad del Comité para el Desarrollo de la Red de CUDI. http://seguridad.internet2.ulsa.mx

Herzog, Peter Vincent. Abril 2001.*Open-Source Security testing methodology manual*. http://www.ideahamster.org.

IEEE, *Supplement to Standard Interoperable LAN/MAN Security (SILS).*IEEE Std. 802.10 Integrated Services. IEEE Standards for local and metropolitan Area Networks. LAN-MAN Standards Committee. 1999. http://standards.ieee.org/getieee802/802.10.html

ISO, 1995. *Network layer security protocol.* ISO International Organization for Standardization. Information technology -- Open Systems Interconnection -- ISO/IEC 11577:1995.

ISO, 1989. *Basic Reference Model: Part 2: Security Architecture.* ISO International Organization for Standardization. Information technology -- Open Systems Interconnection -- ISO-7498-2.

ITU, 2001. *Protocolos Series X.* International Communications Union. Data Networks and open system communication. http://www.itu.int/rec/recommendation.asp?type=products&parent=T-REC-x

Kent, Stephen. *Network Security Protocol Standards.* Seminar. Network & Distributed System Security Symposium of the Internet Society. NDSS'2001.

Krywaniuk, Andrew. *Security Properties of the IPSec Protocol Suite.* Internet Draft (Trabajo en proceso). draft-krywaniuk-ipsec-properties-00.txt. Julio 2001, expira Febrero 2002. http://www.ietf.org/ietf/lid-abstracts.txt

Naganand, Doraswamy, Harkins Dan. *IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Prentice Hall. 1999.

NICMX, 2001. *Network Information Center* Sección México. http://www.nic.mx/.

PolCICESE, 2001. Política de Seguridad en Informática del CICESE. http://telematica.cicese.mx

RFC1085, M. Rose. TWG.*ISO Presentation Services on top of TCP/IP-based internets.* Network Working Group. Request for Comments: 1085 December 1988.

RFC1700, Reynolds, J., and J. Postel, *Assigned Numbers,* STD 2, Request for Comments 1700, Octubre 1994. Información adicional: http://www.iana.org/numbers.html.

RFC2104, H. Krawczyk. IBM M. Bellare UCSD. R. Canetti IBM.*HMAC: Keyed-Hashing for Message Authentication*. Network Working Group. Request for Comments: 2104. Category: Informational February 1997.

RFC2246, T. Dierks. C. Allen Certicom. *The TLS Protocol Version 1.0*. Network Working Group. Request for Comments: 2246 Category: Standards Track. January 1999.

RFC2401, S. Kent. BBN Corp. R. Atkinson. @Home Network. *Security Architecture for the Internet Protocol.* Network Working Group. Request for Comments: 2401 Category: Standards Track. November 1998.

RFC2402, S. Kent. BBN Corp. R. Atkinson. @Home Network. *IP Authentication Header.* Network Working Group. Request for Comments: 2402 Category: Standards Track. November 1998.

RFC2406, S. Kent. BBN Corp. R. Atkinson. @Home Network. *IP Encapsulating Security Payload (ESP).* Network Working Group. Request for Comments: 2406 Category: Standards Track. November 1998.

RFC2409, D. Harkins, D. Carrel, Cisco Systems. *The Internet Key Exchange (IKE).* Network Working Group. Request for Comments: 2409 Category: Standards Track. November 1998.

RFC2440, J. Callas. Network Associates. Track L. Donnerhacke. IN-Root-CA Individual Network. e.V. H. Finney Network Associates. R. Thayer EIS Corporation. *OpenPGP Message Format*. Network Working Group. Request for Comments: 2440. Category: Standards. November 1998

RFC3130, E. Lewis. NAI Labs. *Notes from the State-Of-The-Technology: DNSSEC.* Network Working Group. Request for Comments: 3130 Category: Informational. June 2001.

SSL, 2001. *SSL 3.0 Protocol Specification*. http://home.netscape.com/eng/ssl3/index.html

SWA, 2001. *IETF Security Working Area* http://web.mit.edu/network/ietf/sa/

SWG, 2001. *IETF IP Security Protocol Working Group.* http://www.ietf.org/html.charters/ipsec-charter.html

6BONE, 2001. *Testbed for deployment of IPv6*. http://www.6bone.net/