UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS.

FACULTAD DE INGENIERÍA ELÉCTRICA.

DPTO. TELECOMUNICACIONES Y ELECTRÓNICA.

CONSIDERACIONES SOBRE LA SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES SOPORTES DE VOZ SOBRE IP (VOIP) EN CUBA.

TESIS PRESENTADA EN OPCIÓN AL TÍTULO ACADÉMICO DE MÁSTER EN **TELEMÁTICA.**

Maestría de Telemática

Autor: Ing. Aslan Santana Vázquez

Tutor: Dr. Armando Sarmiento Rojas

Consultante: M.Sc. Humberto Beceiro García

2007

Agradecimientos

A mis familiares por la paciencia que en estos años me ha permitido dedicar tiempo a mi preparación profesional.

A mi compañero y nuevo amigo Beceiro, por su paciencia y ayuda en el desempeño del presente trabajo.

Al Dr. Armando Sarmiento Rojas, en su doble condición de Tutor y Director del Centro de Capacitación de ETECSA, y al excelente colectivo de trabajadores del Centro, que nos han proporcionado las mejores condiciones para desarrollar la Maestría.

A los profesores de la Universidad Central de Las Villas, que nos han impartido los conocimientos y las experiencias necesarias para escalar en la montaña del conocimiento.

A mis compañeros de aula, por la amistad que recordaré siempre.

Tampoco puedo dejar de mencionar a mi colega y amigo Nelsito, por su apoyo en los momentos mas necesitados.

Para mi esposa **Baby** y mis hijos **Amanda** y **Wilfre**,
que son la razón de mi trabajo diario.
Para **mi familia**,
por estar siempre ahí generando una tranquilidad ideal.
:-)

Resumen

El creciente tráfico de datos producido por las aplicaciones que hoy se desarrollan en Internet, así como nuevas posibilidades tecnológicas en el procesamiento de la voz y otros medios, han impulsado al cambio de paradigma de conmutación de circuitos sobre el cual se sustentaba el tráfico de voz en la Red Telefónica Publica Conmutada (RTPC), hacia la conmutación de paquetes. Los operadores de telecomunicaciones más importantes del mundo, han apostado a la utilización de la Voz sobre IP (VoIP), para abaratar el costo de las Inversiones y de la Operación y Mantenimiento de las Redes.

Muchas ventajas se pusieron rápidamente de manifiesto, aprovechando las infraestructuras que para el transporte de datos estaban creadas. No obstante, la VoIP desde sus inicios, ha presentado aspectos que requirieron atención especial. Estos son: Calidad del Servicio (QoS) y Seguridad.

En el primer caso, muchas han sido las innovaciones realizadas en esa área de la ingeniería para satisfacer a los usuarios, teniendo en cuenta que en la RTPC, se logra una excelente Calidad y adicionalmente una elevada Disponibilidad. El otro aspecto, o sea, la Seguridad constituye un enorme reto para el despliegue de la VoIP, ya que aparecen nuevos elementos que pueden ser vulnerables a los ataques de virus, denegación de servicio y otros. La propia omnipresencia de IP, es a su vez un verdadero reto para aplicaciones como VoIP.

El presente trabajo una vez que muestra una visión general de VoIP, centra su atención en las vulnerabilidades y ataques que asechan la seguridad de dicha red y que pudiesen ser predecibles en el despliegue de la VoIP en las redes de telecomunicaciones de Cuba. También aborda los aspectos de seguridad que están presentes en los distintos protocolos de señalización que han sido desarrollados. El trabajo aborda las afectaciones, que las soluciones de seguridad que se requieren para VoIP, provocan en la QoS, originadas tanto por la introducción de nuevos elementos en la red como Firewalls y NATs y la utilización de encriptación, protocolos y algoritmos, que se han desarrollado con fines de proveer seguridad a los datos que cruzan las distintas redes, es especial a la voz.

Además analiza los aspectos posibles que ETECSA, puede considerar sobre la seguridad en el despliegue de VoIP, centrándose en tres áreas claves: protección, privacidad y control.

El trabajo constituye el marco inicial para la implementación de seguridad en el desarrollo de la Telefonía IP en el país, mostrando las vulnerabilidades potenciales en un entorno VoIP, al tiempo que perfila los pasos necesarios para asegurarla. Mucho se ha trabajado en cuanto a la seguridad en redes IP, pero aún son muchos los aspectos pendientes de solución e investigación, por lo que no seguir el curso de este perfeccionamiento y aun peor no tomar en cuenta la seguridad en las inversiones, puede conducir a errores de trascendencia futura.

Tabla de Contenido

Introducción.....*1*
CAPITULO 1:Situación de la Seguridad en las Redes de VoIP.....*4*
1.1 Generalidades sobre VoIP.....4
1.2 Aspectos de Seguridad en los distintos protocolos de VoIP.....6
1.2.1 Protocolo H.323.....6
1.2.2 Protocolo SIP.....7
1.2.3 Protocolo MEGACO/H.248.....9
1.3 Vulnerabilidades y ataques en Redes VoIP.....10
1.3.1 Confidencialidad y privacidad.....12
1.3.1.1 Vulnerabilidad de la contraseña por defecto del conmutador.....13
1.3.1.2 Vulnerabilidad clásica de intervención de la línea telefónica para escuchar llamadas.....13
1.3.1.3 Corrupción de la caché ARP y desborde ARP.....13
1.3.1.4 Interfaz servidor Web.....13
1.3.1.5 Vulnerabilidad de la mascara de red Teléfono VoIP.....14
1.3.1.6 Vulnerabilidad de mapeo de direcciones IP a extensiones.....14
1.3.2 Problemas de integridad.....14
1.3.2.1 Ataque de inserción al Servidor DHCP.....15
1.3.2.2 Ataque de inserción servidor TFTP.....16
1.3.3 Accesibilidad y denegación de servicio.....16
1.3.3.1 Ataque de agotamiento de recursos CPU sin ninguna información de cuenta.....16
1.3.3.2 Vulnerabilidad de la contraseña por defecto.....17
1.3.3.3 Defecto en el software utilizado.....17
1.3.3.4 Vulnerabilidad de cierre forzoso de cuenta.....18
1.4 Calidad del Servicio (QoS) y Seguridad en Redes VoIP.....18
CAPITULO 2: Afectaciones a la VoIP provocadas por las Soluciones de Seguridad.....*24*
2.1 Firewalls y NATs.....24
2.1.1 Firewalls.....24
2.1.2 Necesidades de Firewalls específicos para VoIP.....26
2.1.3 Traductores de Direcciones de Red (NAT).....27
2.1.4 Mecanismos para solucionar los problemas NAT.....29
2.1.5 Consideraciones sobre el establecimiento de la llamada con NAT y Firewalls.....31
2.1.6 Efectos de los Firewall y los NATs sobre QoS.....34

2.2 Encriptación e IPSec. 35
2.2.1 Sistemas de encriptación 35
2.2.2 Latencia debido a la encriptación / desencriptacion. 38
2.2.3 Programación y la ausencia de QoS en el motor criptográfico. 38
2.2.4 IPSec 39
2.2.5 Papel de IPSec en VoIP 45
2.2.6 Dificultades surgidas de VoIPSec. 45
2.3 Incompatibilidades NAT/IPSec. 46
2.4 Redes Privadas Virtuales (VPN). 47
2.4.1 Túneles VPN Local 49
2.4.2 VPN y Firewalls. 49
2.5 Tamaño de los paquetes Expandidos. 49
CAPITULO 3: Aspectos a considerar sobre la Seguridad en el Despliegue de VoIP en Cuba. *50*
3.1 Soluciones a los problemas de Seguridad en VoIP. 50
3.2 Soluciones a los temas de VoIPSec 57
3.2.1 Encriptación en los puntos finales. 57
3.2.2 Protocolo en Tiempo Real Seguro (SRTP) 57
3.2.3 Gestión de claves para SRTP-MIKEY. 58
3.2.4 Mejores esquemas de Programación. 60
3.2.5 Compresión del Tamaño de los Paquetes. 61
3.2.6 Soluciones a incompatibilidades NAT/IPSec 61
3.3 Normas generales para el establecimiento de VoIP. 62
Conclusiones y Recomendaciones. 66
Referencias Bibliográficas.
Glosario de Términos.

Introducción

El mundo de las telecomunicaciones avanza rápidamente en la introducción de la telefonía IP, tecnología basada en la digitalización de la voz y su transmisión insertada en distintos tipos de paquetes.

Poderosas razones impulsan al cambio de paradigma de conmutación de circuitos hacia la conmutación de paquetes [4], entre estas tenemos, el vertiginoso crecimiento del trafico de datos, que en muchos países a sobrepasado el trafico de voz, originado por la profusa utilización de aplicaciones relacionadas con Internet, como son el correo electrónico, chat, comercio electrónico, tele educación, telemedicina, entre otras [16]. Esto indudablemente reduce los costos del equipamiento de las redes de datos y conlleva al desarrollo de un único tipo de red, capaz de soportar diferentes tipos de medios (voz, video, datos de aplicaciones) lo que conduce a la disminución de los costos de operación [3].

La Voz sobre IP (VoIP) está transformando la industria de las telecomunicaciones. Ofrece oportunidades múltiples tales como honorarios más inferiores de la llamada, convergencia de la voz y de las redes de datos, simplificación del despliegue y mayor integración de las múltiples aplicaciones multimedia. Sin embargo, a pesar de que todas estas oportunidades tecnológicas y económicas, VoIP también introduce nuevos retos. Entre ellos, garantizar la seguridad es quizás el más complejo.

En la actualidad muchos operadores de telecomunicaciones explotan la Telefonía IP, debido a las ventajas económicas, operativas y de servicio aportadas por esta tecnología para la conducción de la voz y otros medios, lo que nos lleva a la necesidad del estudio en el entorno cubano y de la forma en que se implementará esta tecnología; en nuestro caso basados en estudios realizados anteriormente y que contemplan las distintas variantes a seguir en la transformación de la red, así como los lineamientos en la implementación de la Telefonía IP en ETECSA, nos proponemos estudiar con mayor profundidad lo relacionado con la seguridad informática en las redes que soportaran la VoIP, debido a la naturaleza de estas redes y la necesidad de que sean capaces de resistir cualquier ataque.

En Cuba, donde ya se dan los primeros pasos en la migración y para lo cual debemos estar preparados, debemos considerar que se requieren de esfuerzos en el análisis de puntos críticos relacionados con la seguridad en su introducción, investigando las posibles soluciones a vulnerabilidades, para evitar que falle la VoIP.

El presente trabajo permitirá evaluar las distintas variantes sobre seguridad a seguir en la implementación de la nueva red, así como proporcionar importantes lineamientos para la implementación de la seguridad en redes de VoIP en ETECSA, en vista de la experiencia de proveedores lideres y de operadores internacionales que la implementan en sus redes de diversas maneras, por lo que deberá dar respuesta a las siguientes interrogantes:

¿Qué problemas de Seguridad afectan la VoIP según reconocen los operadores de telecomunicaciones y otras empresas emergentes en este campo?

¿Disponemos de los fundamentos teóricos y de la experiencia acumulada en el plano internacional para la implementación de seguridad en el despliegue de la Voz sobre IP?

¿Cuáles serían las vulnerabilidades de la Seguridad predecibles en el despliegue de la VoIP en las redes de telecomunicaciones de Cuba?

¿Qué soluciones se pudieran implementar en nuestras redes de telecomunicaciones utilizadas para VoIP con el objetivo de minimizar las afectaciones a los problemas de Seguridad?

Para responder las interrogantes anteriores el trabajo debe cumplir los siguientes objetivos:

Objetivo general.

Proponer consideraciones relacionadas con la seguridad informática en las redes que soportarán la VoIP, donde se presenten propuestas de soluciones a aquellos problemas previsibles durante la etapa de introducción de la misma en Cuba.

Objetivos Específicos:

- Conocer y analizar los problemas de seguridad que afectan la VoIP, obtenidos en la bibliografía disponible.
- Mostrar las posibles vulnerabilidades que pudieran presentar la implementación de VoIP en nuestras redes de Telecomunicaciones.
- Describir las distintas alternativas que importantes operadores de telecomunicaciones han adoptado para dar protección a su red.
- Consultas a los departamentos de planeamiento estratégico de la Empresa de Telecomunicaciones de Cuba.
- Consultas a un tercero con experiencias prácticas en la introducción de VoIP.
- Proponer, a partir de las experiencias obtenidas de los puntos anteriores, las soluciones a las posibles vulnerabilidades identificadas, que en materia de seguridad informática faciliten la introducción de la Telefonía IP en la Red de Telecomunicaciones de Cuba.

Evaluación del Impacto Económico social.

El trabajo tiene impacto Técnico-Económico, al proponer las líneas generales relacionadas con la seguridad informática en la implementación de la telefonía IP, al nivel de un operador profesional como lo es ETECSA, en el supuesto de que estas proporcionarán las siguientes ventajas:

- Mostrará cuales son las vulnerabilidades fundamentales de este despliegue tecnológico, que en materia de seguridad han surgido, así como las distintas soluciones aplicadas para su prevención.
- Facilitará lineamientos relacionados con la seguridad informática en la telefonía IP, que serán de ayuda en el diseño de la nueva red.

El impacto social, esta dado por la posibilidad de contribuir a la seguridad de la red que brindará servicios a un numero creciente de abonados, proporcionando la elevación de la densidad telefónica del país y la informatización de la sociedad, lo cual también significa ser menos vulnerables a ataques, que pudieran causar problemas en el servicio a los clientes actuales y futuros.

El trabajo se ha concebido para que sea utilizado en la introducción de la telefonía IP en ETECSA, lo que garantiza su aplicación técnica. También puede arrojar resultados docentes, si se tiene en cuenta, que aborda aspectos metodológicos de la implementación de seguridad en una red que soporte VoIP.

Metodología del trabajo.

Se realizo una profunda búsqueda en la bibliografía primaria existente, utilizando textos fundamentales (artículos y tesis recientes y completas sobre el tema). Se realizaron intensivas búsquedas automatizadas en fuentes electrónicas, como es el caso de Internet, teniendo en cuenta el dinamismo de estos temas. No obstante es importante señalar que en este medio son casi nulas las informaciones técnicas de los Operadores de Telecomunicaciones establecidos.

Fueron consultados otros materiales de gran importancia, como las Recomendaciones de la Unión Internacional de Telecomunicaciones (UIT), las Request For Comments (RFC), que constantemente evolucionan con el desarrollo de Internet, propiciando el interfuncionamiento de las redes y tecnologías como la Telefonía IP.

Se realizaron consultas a importantes especialistas de ETECSA, que trabajan en el Planeamiento Estratégico, valorando con estos, la visión de la empresa con relación al camino a seguir para la introducción de la Telefonía IP. De la misma forma se debatió el tema de las redes de datos existentes en el país, con especialistas que explotan estas tecnologías, poniendo énfasis en la posibilidad que tiene el equipamiento adquirido en Cuba, de proporcionar seguridad en redes IP. Se visito el Centro de Gestión de la Unidad de Negocios Datos de ETECSA.

El trabajo lo conforman tres capítulos, el primero de ellos, pretende justificar las razones por las cuales se requiere la aplicación de seguridad en las redes VoIP, se analizan las generalidades del manejo de los datos en un sistema VoIP. De la misma forma se plantean los aspectos de seguridad que conciernen a los distintos protocolos de VoIP. Se sintetizan las vulnerabilidades y ataques que están presentes en redes de conmutación de paquetes de voz, principalmente aquellas que pudieran tener mayor impacto. Se analizan los principales temas de calidad de servicio (QoS) asociados con VoIP que pudieran afectarse por la implementación de las soluciones de seguridad.

En el capitulo II, se identifican las afectaciones a la VoIP provocadas por las soluciones de seguridad aplicadas y se exponen los protocolos y elementos de seguridad a considerar en el planeamiento de estas redes.

Las propuestas de soluciones a los problemas de seguridad en redes VoIP, las distintas soluciones a temas de VoIPSec y soluciones de incompatibilidad entre elementos y protocolos son tratados en el capitulo 3, en este último segmento se muestran normas generales para el establecimiento de la VoIP, tomando en cuenta consideraciones practicas emitidas por el National Institute of Standards and Technology (NIST) [27].

CAPITULO 1: Situación de la Seguridad en las Redes de VoIP.

La transmisión de voz sobre redes IP (VoIP) es una de las tendencias emergentes más importantes en el mundo de las Telecomunicaciones. Como toda nueva tecnología, introduce riesgos de seguridad. Su arquitectura, muy diferente a la de la telefonía basada en conmutación de circuitos, genera problemas de seguridad significativos. La promesa de costos más bajos y mayor flexibilidad, no deben entenderse sin la cuidadosa consideración de los problemas de seguridad introducidos.

El presente Capitulo, centra su atención en las distintas vulnerabilidades que acechan una red VoIP. Se constata como, a pesar de que con la creación de la red de VoIP surgen nuevas amenazas, los riesgos y amenazas que enfrentaban las redes IP, son también un problema para la futura red. Se analiza como la aplicación de varias medidas de seguridad puede causar un marcado deterioro de la QoS. También aborda los aspectos de seguridad de los principales protocolos de VoIP.

1.1 Visión general de VoIP.

Muchos lectores que tienen una buena noción del Internet y de la tecnología de comunicaciones de datos pueden tener una idea sobre la transmisión de voz en tiempo real en un entorno de conmutación de paquetes. Una de las principales causas de confusión para los que tienen poco conocimiento de VoIP es la suposición de que, debido a que la digitalización de la voz viaja en paquetes como otros datos, las arquitecturas y las herramientas de las redes existentes pueden ser usadas sin cambio alguno para la transmisión de voz. VoIP añade varias complicaciones para la tecnología de red existente y estos problemas son complicados por las consideraciones de seguridad.

Los sistemas VoIP asumen una amplia variedad de formas. El término voz sobre IP es asociado con el equipo que proporciona la habilidad para marcar números de teléfono y comunicarse con partes en el otro extremo de una conexión, que tenga cualquier otro sistema VoIP o un teléfono analógico tradicional.

La demanda para los servicios de VoIP ha dado como resultado un amplio conjunto de productos, entre los que se incluyen los teléfonos tradicionales, unidad de conferencia, unidades móviles, computadoras personales (PC) o softphone, entre otros. En adición al equipo del usuario final, los sistemas VoIP incluyen otros componentes, como procesadores de llamada (gestores de llamadas), pasarelas de medios, enrutadores, firewalls y protocolos. La mayor parte de estos componentes tienen homólogos utilizados en las redes de datos, pero las demandas en la ejecución de VoIP requieren que el software y el hardware de una red común, deben ser complementados con componentes VoIP especiales. La naturaleza única de los servicios de VoIP tiene un impacto significativo en las consideraciones de seguridad para dichas redes.

Para establecer una llamada en VoIP, el usuario debe entrar el número a discar, el cual puede ser realmente un número telefónico discado sobre un teclado o un Identificador de Recursos Individuales (URI, siglas en inglés). Posteriormente, ocurre un complejo intercambio de series de paquetes basados en un protocolo de señalización de VoIP determinado.

Como se conoce las computadoras en la red se enlazan por su dirección IP, no con los números o URIs introducidas por los usuarios, para lo cual se requiere el trabajo de protocolos que encuentran la dirección IP que corresponde al número telefónico de la parte llamada.

El primer paso para lograr la comunicación VoIP es convertir la señal de voz analógica a digital, usando un convertidor análogo - digital. Puesto que la voz digitalizada requiere de un gran número de bits, un algoritmo de compresión puede ser usado para reducir el volumen de los datos para ser transmitidos. Después las muestras de voz son insertadas dentro de paquetes de datos para ser llevados sobre Internet. Para el transporte de estos paquetes se utiliza el protocolo RTP (Protocolo de Transporte en Tiempo Real). Los paquetes RTP son a su vez encapsulados en la carga útil de datagramas UDP (User Datagram Protocol), los cuales son procesados en los nodos de las redes ordinarias. En el otro extremo se realiza el proceso inverso, lográndose de esa forma la comunicación.

Con la introducción de VoIP, la necesidad de la seguridad es complicada porque ahora debemos proteger datos y voz. En un sistema telefónico convencional, interceptar conversaciones requiere el acceso físico a la línea telefónica o algún compromiso con el operador de pizarras privada (PBX), si es el caso.

Actualmente, sólo en las organizaciones que manejan información muy sensibles de seguridad, se encripta el tráfico de voz sobre líneas de teléfono tradicionales. Lo mismo no puede ser dicho para conexiones basadas en Internet. Por ejemplo, cuando se ordena mercancía por teléfono, la mayoría de las personas leerán sus números de tarjeta de crédito para la persona en el otro extremo. Los números son transmitidos sin encriptación al vendedor de servicios. En cambio, el riesgo de la transmisión no encriptada de datos a través de Internet es más significativo. Los paquetes enviados desde un usuario de una computadora domestica a un minorista en línea pueden pasar por 15-20 sistemas que no están bajo el control del Proveedor de Servicio de Internet del usuario (ISP) o el minorista. Debido a que los dígitos son transmitidos usando un estándar para transmitir dígitos fuera de banda como mensajes especiales, cualquiera con acceso a estos sistemas puede instalar un software que examine paquetes para información de tarjetas de crédito. Por esta razón, los minoristas en línea usan software de encriptación, para proteger la información y el número de tarjeta de crédito de un usuario. Puede concluirse, que si se transmite voz sobre el Protocolo de Internet (IP) y específicamente a través de Internet, similares medidas de seguridad deben aplicarse.

La arquitectura de Internet actual no proporciona la misma seguridad física en los sistemas alámbricos como las líneas de teléfono. La clave para asegurar VoIP es usar los mecanismos de seguridad semejante a aquellos desplegados en las redes de datos (firewalls, encriptación, etc.) para imitar los niveles de seguridad actuales disfrutado por los usuarios de la RTPC.

1.2 Aspectos de seguridad en los distintos protocolos de VoIP.

La mayoría de los proveedores de servicio reconocen que las redes de VoIP de extremo a extremo constituirán la tecnología soporte de las Telecomunicaciones del futuro, sin embargo, para que esto sea efectivamente cierto, se deben considerar requerimientos claves que aseguran la equivalencia con la RTPC actual, especialmente en cuanto a la calidad ya alcanzada por la antigua red. Entre estos requerimientos se encuentra la selección del protocolo(s) de señalización.

Para una solución de VoIP numerosos protocolos de señalización han sido desarrollados, entre los que se encuentran:

- Protocolos de control de dispositivos, tales como MEGACO/H.248, MGCP (Media Gateway Control Protocol), etc.
- Protocolos de señalización de accesos a los servicios, tales como SIP (Protocolo de Inicialización de Sesión), H.323, etc.
- Protocolos de señalización de servicios en la red, tales como SIP, SIP-T (SIP para Telefonos), BICC (Bearer Independent Call Control), etc.

La selección del protocolo a utilizar en la red del Proveedor de Servicios, depende del conjunto de estos que serán ofrecidos y del equipamiento disponible para proveer estos servicios.

1.2.1 MEGACO/H.248

El IETF (Internet Engineering Task Force) comenzó a trabajar en MEGACO como protocolo de compromiso entre MGCP y MDCP. UIT-T (Unión Internacional de Telecomunicaciones) adoptó la versión 0.1 de MEGACO en abril de 1999 como la especificación inicial para H.GCP (Serie H, GCP - Protocolo de Control de Pasarela), luego H.248. En junio de 1999, el Grupo de Trabajo MEGACO de IETF y la UIT-T divulgaron un único documento que describía un protocolo estándar (MEGACO/H.248) para la interconexión entre los Controladores de Pasarelas de Medios (MGCs) y las Pasarelas de Medios (MGs). Se prevé que gane la aceptación de la industria como el estándar oficial para las arquitecturas de pasarelas descompuestas.

MEGACO (RFC 3525) recomienda mecanismos de seguridad que pueden estar en mecanismos de transporte subyacentes, tales como IPsec (Internet Protocol Security) [22]. H.248 va a un paso adelante al requerir que las implementaciones del protocolo H.248 implementen IPsec si el sistema operativo subyacente y la red de transporte soportan IPsec. Se requieren implementaciones del protocolo usando IPv4 para poner en práctica el esquema AH (Authentication Header) interno. H.248 plantea que la implementación utilizando el encabezado AH proporcionará un conjunto mínimo de algoritmos para el chequeo de integridad usando llaves manuales (en correspondencia con la RFC 2402) [22].

El esquema de AH interino es la utilización de una cabecera AH opcional, que se define en la cabecera del protocolo H.248. El esquema interino del AH interino no proporciona protección contra la escucha clandestina y los ataques repetitivos.

Para MEGACO, la gestión de clave manual se asume y repite la protección, definida por IPsec, puede no ser utilizada en este escenario (el número de secuencia en AH se puede desbordar al utilizar la gestión de clave manual), puesto que la reintroducción no es posible. Además, H.248 plantea que las implementaciones que emplean el encabezado ESP (Carga de Seguridad Encapsulada) proporcionará un conjunto mínimo de algoritmos para el chequeo y cifrado de la integridad (que cumplen con la RFC 2402). Por otra parte, las implementaciones deben utilizar IKE (RFC 2409) para permitir opciones de llaves más robustas. Las implementaciones que utilizan IKE (Internet Key Exchange) deben soportar la autentificación con las firmas RSA (sistema de criptografía de clave pública) y la encriptación de llave pública RSA.

1.2.2 Protocolo SIP

SIP es un protocolo especificado por IETF para iniciar una sesión de comunicación de dos vías. También, SIP es un protocolo del nivel de aplicación, es decir, se desacopla de la capa del protocolo por el que se transporta.

Este puede ser transportado por TCP (Transmission Control Protocol), UDP o SCTP (Stream Control Transmission Protocol). UDP se puede utilizar para disminuir el encabezamiento adicional y para aumentar velocidad y eficiencia. TCP puede ser utilizado si SSL/TLS se incorpora para los servicios de seguridad.

El protocolo de transmisión de control de la trama SCTP ofrece resistencia creciente a los ataques del DoS (Denied of Service) a través de un método de intercambio de 4 vías, es multi-home, o sea cada punto extremo SCTP puede ser conocido por múltiples direcciones IP, siendo el enrutamiento para una dirección independiente de todas las otras, si una ruta se hace no alcanzable, otra será utilizada. Además permite opcionalmente bundling (múltiples mensajes de usuarios) en un único paquete SCTP.

Los servicios de seguridad adicionales se pueden utilizar con SCTP vía RFC 3436 (TLS sobre SCTP) o 3554 (SCTP sobre IPSec). Diferente de H.323, solo se utiliza un puerto en SIP (en H.323 se puede también utilizar un camino que utilice un solo puerto para el caso de llamadas enrutadas directamente). El valor por defecto de este puerto es 5060.

La codificación en texto de SIP hace más fácil de analizar utilizando herramientas estándar. No obstante, algunos nuevos requerimientos son puestos en el firewall en una red de VoIP basada en SIP. Primero, los firewalls deben tener estado (stateful) y monitorear el trafico SIP para determinar que puertos RTP deben ser abiertos y hacerlos disponibles a cualquier dirección. Esta responsabilidad es similar a la tarea de los firewalls en una red basada en H.323, excepto que el establecimiento de la llamada y las cabeceras que analizan es mucho más simple. Otro tema de VoIP basado en SIP, encontramos los firewalls asociado al tráfico de RTP y a llamadas entrantes. Como con H.323, el problema grande para SIP son los NATs.

NAT inhibe los mecanismos de inscripción y comunicación del SIP y requiere soluciones innovadoras para resolver estos temas. Los problemas existen porque en una red basada en SIP, el proxy del SIP está normalmente fuera del dispositivo NAT. Hay tres escenarios principales para utilizar un proxy del SIP:

- El proxy está dentro de la LAN (Local Area Network) corporativa y el trabajador remoto se conecta desde el exterior.
- El proxy está en el lado de la empresa telefónica y los clientes afuera, por ejemplo, compañías pequeñas que se conectan con este proxy para el servicio de VoIP.
- Se conectan dos dominios administrativos, ambos tienen su propio proxy.

De manera que el problema es el intercambio de comunicación entre un servidor proxy que se alcanza con direcciones IP globales y una máquina que se le ha asignado una dirección de red privada. Rosenberg y Schulzrinne [32] clasifican tres diversos conjuntos de problemas que el tráfico del SIP tiene en su configuración: originar solicitudes, recibir peticiones y la manipulación RTP. Se conocen las incompatibilidades de RTP con NAT y se verán temas NAT presentes en el proceso de conformación de la llamada en sí mismo.

Para inicializar una sesión detrás del NAT, un llamante puede simplemente enviar un mensaje INVITE como siempre. El número de puerto saliente (5060) será preservado por el NAT, pero la comunicación de respuesta podría ser afectada. Si SIP se implementa sobre UDP (la llamada SIP es independiente del protocolo) el Servidor Proxy debe enviar la respuesta UDP a la dirección y puerto desde donde arribó la solicitud [32]. Una solución más simple es utilizar la práctica estándar de enrutamiento de comunicación SIP sobre TCP. Con TCP, la respuesta del llamador vendrá encima el mismo canal que la original INVITE y así NAT no será un problema.

Ahora se observarán en profundidad, los problemas específicos de SIP con las llamadas entrantes. Rosenberg & Schulzrinne [32] perfilan el problema desde el proceso de registro mismo. Cuando un usuario hace contacto con el registrador, este proporciona su dirección IP como su dirección accesible y esta se salva en el Servidor de Localización. Sin embargo, esta es su dirección IP Privada. Sin embargo, el servidor proxy se relaciona solamente con direccionamientos IP globales, así que cuando un mensaje viene hacia adentro para username@domain.com, este intentará encaminar esta llamada a la dirección registrada, pero en el dominio público. Por ejemplo, si username@domain.com es registrado en una dirección IP interna de 10.7.34.189, entonces el servidor proxy intenta remitir el tráfico a esta dirección, pero en el dominio público. Si esta dirección es inalcanzable para el servidor proxy, la conexión será rechazada. La solución a esto es una manipulación delicada de las direcciones IP y una expansión de las responsabilidades del servidor proxy SIP.

1.2.3 Protocolo H.323

H.323 es una especificación de ITU para la comunicación de audio y video a través de redes de paquetes. H.323 es actualmente un estándar general, que abarca varios protocolos, incluyendo H.225, H.245, H.235 y otros.

Una red H.323 se compone de varios puntos finales (terminales), de una pasarela y posiblemente de un gatekeeper, de una Unidad de control de Multipunto (MCU). El gatekeeper es el componente principal en los sistemas H.323. Proporciona resolución de direcciones y control del ancho de banda. La pasarela sirve como puente entre la red H.323 y el mundo exterior donde (posiblemente) los dispositivos no utilicen H.323. Esto incluye redes SIP y redes tradicionales PSTN.

El proceso de establecimiento de una llamada VoIP basado en H.323 es complejo. Este tiene diversos protocolos asociados con formularios de comunicación con las más complejas formas de comunicación, incluyendo H.332 (grandes conferencias), H.450.1, H.450.2 y H.450.3 (servicios suplementarios), H.235 (seguridad) y H.246 (interoperabilidad con los servicios de conmutación de circuito) [30]. La autentificación se puede también realizar en cada punto en el proceso de establecimiento de la llamada utilizando claves simétricas o con un secreto compartido a priori [34]. El uso de estos protocolos y/o medidas de seguridad agrega complejidad al proceso del establecimiento de llamadas en H.323. Esta complejidad es superior en la incompatibilidad de H.323 con los firewalls y NATs.

Los firewalls plantean dificultades para las redes de VoIP que utilizan H.323. A excepción del "Q.931-like" H.225, todo el tráfico H.323 se encamina a través de puertos dinámicos. Para el comienzo rápido de H.323 y el H.245 en modo túnel sólo un canal se utiliza (Señalización de Llamadas H.225), generalmente utilizando el puerto 1720. Si se realiza comunicación adicional RAS (Remote Access Service) H.225 con el gatekeeper (UDP), esta se hace a través del puerto 1719. Es decir, cada canal sucesivo en el protocolo se encamina a través de un puerto dinámicamente determinado por su predecesor. Este método provisional de asegurar los canales no se presta a una configuración estática del firewall.

Esto es particularmente cierto en el caso de los firewalls con estados que no pueden comprender el tráfico H.323. Estos filtros de paquetes simples no pueden correlacionar las transmisiones UDP y las respuestas. Esto hace necesario crear agujeros en el firewalls para permitir que el tráfico H.323 atraviese el puente de seguridad en cualquiera de los puertos efímeros que pueda utilizar. Esta práctica introduciría debilidades serias de la seguridad porque para tal implementación necesitaría dejar 10000 puertos UDP y varios puertos TCP específicos para H.323 completamente abiertos.

De manera, que existe la necesidad de un firewall que entienda VoIP y específicamente H.323. En este caso, el firewall, puede leer los mensajes H.323 y abrir dinámicamente los puertos correctos para cada canal, cuando el protocolo se mueve en su proceso de establecimiento de llamadas. El firewall debe ser parte de una arquitectura de seguridad especialmente en escenarios donde las medidas de seguridad provistas por el protocolo se aplican (ejemplo en la integridad del mensaje). Salvo esto, algún tipo de servidor proxy o un el middlebox tendría que ser utilizado. Varias soluciones a este problema se presentan en el capítulo 2.

Incluso con un firewall que entienda VoIP, el análisis del tráfico H.323 no es una cuestión trivial. El tráfico H.323 se codifica en un formato binario basado en ASN.1. Este no utiliza los desplazamientos fijos para la información del direccionamiento y diversas instancias de una aplicación pueden negociar diversas opciones, resultando diferentes desplazamientos de byte para la misma información [36]. Este nivel de complejidad no permite que las herramientas simples de análisis decodifiquen el tráfico; necesitandose generadores de código especiales [30]. Tal tecnología no está disponible en firewalls de filtrado de paquetes tradicionales o aún en firewalls de estado simples. Aunque este análisis se puede hacer usando las pasarelas modernas que entienden VoIP, el complejo y necesario análisis para discernir el contenido de los paquetes codificados ASN.1 introduce tiempo de espera adicional en un sistema sensible a la velocidad, el cual se satura con retardos.

NAT es también un problema para los sistemas de VoIP que utilizan el protocolo de establecimiento de llamada de H.323. NAT complica las comunicaciones H.323 porque la dirección IP interna y el puerto especificado en las cabeceras H.323 y los mensajes, no son las direcciones/número de puertos reales utilizados externamente por un terminal remoto. Esto rompe el procedimiento del "próximo establecimiento" usado por cada protocolo en H.323 (ejemplo: H.225 establece H.245). No sólo el firewall tiene que comprender esto, sino que es esencial que la aplicación de VoIP que recibe estas comunicaciones H.323 reciba correctamente el direccionamiento y los números de puertos traducidos. Así, si H.323 va a atravesar una pasarela NAT, el NAT debe poder reconfigurar de nuevo los direccionamientos en el flujo de control. El NAT, no sólo necesita leer el tráfico H.323, sino que debe ser también modificado para enviar el direccionamiento y los números de puertos correctos a cada uno de los puntos extremos.

1.3.- Vulnerabilidades y ataques en Redes VoIP.

Las vulnerabilidades son todos los defectos o debilidades que presenta un determinado sistema en su diseño, implementación operación y manejo, los que pueden ser explotados para violar la política de seguridad del sistema [34] y en especial en las redes IP y VoIP. Los ataques pueden estar motivados por diversos objetivos, incluyendo fraude, extorsión, robo de información confidencial, venganza, acceso no autorizado a un sistema, anulación de un servicio o simplemente el desafío de penetrar un sistema. Estos pueden ser realizados tanto por usuarios autentificados (empleados internos o colaboradores externos con acceso a sistemas dentro de la red de la empresa) como por atacantes externos a la ubicación física de la organización, accediendo remotamente.

Este punto detalla algunos de los ataques potenciales en un entorno VoIP, incluyendo teléfonos y conmutadores VoIP. La discusión de los ataques se incluye porque las variedades de estos, enfrentados por una organización determinan las prioridades al asegurar su equipamiento de comunicaciones. No todos los ataques están presentes en todas las organizaciones. Una firma comercial puede estar interesada primariamente con el fraude de tarifa, mientras que una agencia gubernamental necesita prevenir el descubrimiento de la información sensitiva debido a privacidad o intereses de seguridad nacional.

Los Riesgos de seguridad de información pueden categorizarse dentro de los tres tipos siguientes: confidencialidad, integridad, y disponibilidad. Los riesgos adicionales relativos a los conmutadores son el fraude y riesgo de daños físico del conmutador, redes físicas o extensiones telefónicas.

El funcionamiento exitoso de las redes de paquetes está en función de un gran número de parámetros configurables, como son: direcciones IP y dirección MAC (física) de los terminales de voz, direcciones de enrutadores, firewall y software especifico VoIP tales como gestores de llamadas y otros programas usados para establecer y enrutar llamadas. Muchos de estos parámetros de redes son establecidos dinámicamente cada vez que un componente de la red es reiniciado o cuando un teléfono VoIP es reiniciado o añadido a la red. Debido a que existen muchos lugares en una red con parámetros configurables dinámicamente, los intrusos tienen una gran cantidad de puntos potencialmente vulnerables al ataque.

Las redes de VoIP no están exentas de los ataques que conciernen a una red IP común, es por eso que se hace necesario un estudio de las principales categorías de ataques que acechan dicha red [18]. Seguidamente veremos algunos de los ataques que acechan a los sistemas de comunicaciones:

• **Rechazo de servicio o denegación de servicio (DoS):** Cualquier ataque que tenga como objetivo obstaculizar un servicio, se incluye en esta categoría. Frecuentemente se aprovechan de una debilidad conocida para hacer fallar a un sistema o subsistema. Por ejemplo, el ping de la muerte se aprovecha de un descuido común en la instalación de las pilas del Protocolo de Internet (IP), por el cual un paquete mayor de lo normal puede hace caer al subsistema de redes. Otro enfoque común consiste simplemente en inundar un sistema (normalmente un servidor) de forma que no se puedan tratar las peticiones normales de servicio.

• **"Piratería" o ataques de intrusos:** Esta categoría engloba los ataques hechos por un intruso mediante el acceso a un área o conjunto de recursos que está pensado para ser inaccesible. Ejemplos clásicos son un sitio Web que se destruye o datos confidenciales que se roban mediante acceso ilegal.

• **Virus y gusanos:** Funcionan introduciendo código malicioso y engañando al usuario desprevenido que lo ejecuta. Una vez lanzados, los virus pueden tomar el control de una máquina, esparcir, destruir o cambiar la información, intentar propagarlos, o también permanecer dormidos durante un periodo de tiempo.

• **Escucha clandestina:** Un atacante oye (u observa) la información en tránsito. La escucha telefónica es un ataque clásico de escucha de conversaciones telefónicas.

• **Ataques activos:** Como la escucha clandestina, afectan a la información en tránsito que se visualiza pero, en vez de observar o recoger información pasivamente, los datos se interceptan, alteran y retransmiten (la línea de la comunicación se rompe y se reencamina a través del atacante).

• **Ataques de usurpación:** En estos ataques, una persona (o máquina) se hace pasar por otra para obtener acceso a un recurso.

• **Ataques de repetición:** Frecuentemente los ataques se basan en enviar o reenviar paquetes, o flujos de paquetes, que ya han sido aceptados por el receptor. Por ejemplo, si un mensaje se envía a un banco con instrucciones de añadir 5000 dólares en una cuenta bancaria, entonces podría ser interesante para el propietario de la cuenta interceptar y repetir el mensaje varias veces.

• **Alteración de paquetes:** En vez de usurpar una identidad, un atacante puede manipular una conexión válida para adaptarse a sus necesidades. Por ejemplo, si se envía un correo electrónico diciendo claramente que "Al Sr. X no le está permitido el acceso al edificio Y", con alterar "edificio Y" por "edificio Z" se le permite al Sr. X acceso ilegal al edificio Y.

• **Ingeniería social:** Aunque no está relacionado con la criptografía, la ingeniería social se aprovecha del punto más débil de la mayoría de los sistemas de seguridad: ¡las personas que los usan y los mantienen!

Hay infinidad de variaciones y combinaciones de estos tipos de ataques, todas las cuales amenazan a nuestros datos y a nuestros sistemas de información. Afortunadamente, existe un arsenal razonable de herramientas para combatir estas amenazas, las cuales se estudiaran mas adelante.

Las vulnerabilidades descritas a continuación son genéricas y pudieran no ser aplicadas a todos los sistemas, pero investigaciones hechas por NIST y otras organizaciones han encontrado estas vulnerabilidades en sistemas VoIP. Esta lista no es exhaustiva; los sistemas pueden tener debilidades de seguridad que no son incluidas en la lista. Para cada vulnerabilidad potencial, una recomendación es incluida para eliminar o reducir el riesgo.

1.3.1 Confidencialidad y privacidad.

La confidencialidad se refiere a la necesidad de mantener la información segura y privada. Para usuarios de computadoras domésticas, esta categoría incluye memorando confidenciales, información financiera, e información de seguridad tales como contraseñas. En un conmutador de telecomunicaciones, la escucha no autorizada de una conversación es una preocupación clara, pero la confidencialidad de la información en el conmutador debe ser protegida para defenderse contra fraude de tarifa, intercepción de voz y datos, y ataques de denegación de servicio. Las direcciones IP de la red, el tipo de sistema operativo, la extensión de teléfonos, mapeadas a determinada direcciones IP, y los protocolos de comunicación utilizados, son ejemplos de información que si bien aislados no son elementos críticos, si facilitan la tarea de los atacadores.

Con teléfonos convencionales, la escucha generalmente requiere acceso físico a la línea, o penetración en un conmutador. Los intentos de acceso físico aumentan el riesgo del intruso a ser descubierto. Las PBXs (Private Branch Exchange) convencionales tienen menos puntos de acceso físico que los sistemas de VoIP. En VoIP, las oportunidades de escuchas a escondidas aumentan dramáticamente, debido a la existencia de muchos nodos en una red de conmutación de paquete.

1.3.1.1 Vulnerabilidad de la contraseña por defecto del conmutador.

Es común para los conmutadores establecer un login/contraseña por defecto (ejemplo admin/admin o root/root.). Esta vulnerabilidad también permite la intervención de la línea telefónica para escuchar conversaciones en la red haciendo espejo de puertos o puenteo de los mismos. Un atacador con acceso a la interfase administrativa del conmutador puede reflejar todos los paquetes de un puerto a otro, permitiendo la intercepción indirecta e imperceptible de todas las comunicaciones. Las fallas en el cambio de las contraseñas por defecto es uno de los errores más comunes cometidos los por usuarios inexpertos. Si es posible, el acceso remoto a la interfaz de usuario gráfica debe ser deshabilitada para impedir la intercepción de sesiones de administración de texto pleno. Algunos dispositivos proporcionan la opción de una conexión directa USB (Universal Serial Bus) en adición a un acceso remoto a través de un interfaz Web. Debe considerarse la posibilidad de deshabilitar puertos espejos de la información en el conmutador.

1.3.1.2 Vulnerabilidad clásica de intervención de la línea telefónica para escuchar llamadas.

La conexión de una herramienta para capturar paquetes o un analizador de protocolo a los segmentos de una red VoIP, facilita la intercepción del tráfico de voz.

Una aceptable política de seguridad física para el entorno de despliegue es un primer paso general para mantener confidencialidad. La deshabilitación de los hubs en los teléfonos IP, así como el desarrollo de un sistema de alarma para alertar al administrador cuando un teléfono IP se ha desconectado serán elementos a considerar en la detección de este tipo de ataque.

1.3.1.3 Corrupción de la caché ARP (Address Resolution Protocol) y desborde ARP.

Debido a que muchos sistemas tienen autenticación pequeña, un intruso puede ser capaz de entrar sobre una computadora en el segmento de red VoIP, y enviar comandos ARP corrompiendo la caché ARP (Address Resolution Protocol). Un ataque ARP Flood en el conmutador debe poner la red vulnerable para la escucha clandestina de conversaciones. La difusión de réplicas ARP es suficiente para corromper muchos cachés ARP.

La corrupción del caché ARP hace posible re-enrutar el tráfico de voz y datos, para su intercepción. Deben utilizarse mecanismos de autenticación, donde quiera que sea posible y limitación de acceso físico al segmento de red de VoIP.

1.3.1.4 Interfaz servidor Web.

Tanto los Conmutadores VoIP como los terminales de voz pueden disponer de interfases servidor Web para administración remota o local. Un atacante puede ser capaz de olfatear los paquetes HTTP (Hypertext Transfer Protocol) en texto pleno para obtener información confidencial. Esto requeriría usar acceso a la red local en la cual reside el servidor. Si es posible, no use un servidor HTTP. Si es necesario para usar un servidor Web para la administración remota, use el protocolo más seguro HTTPS (HTTP sobre SSL o TLS).

1.3.1.5 Vulnerabilidad de la mascara de red Teléfono VoIP.

Un efecto similar a la vulnerabilidad de la caché ARP, puede lograrse asignándole una máscara de subred y una dirección de enrutamiento al teléfono para causar que la mayoría o todos los paquetes que transmite sean enviados a una dirección MAC (Media Access Control) del atacante. Un mecanismo de filtrado en los firewalls puede reducir la probabilidad de estos ataques. El acceso remoto a los teléfonos IP es un riesgo severo.

1.3.1.6 Vulnerabilidad de mapeo de direcciones IP a extensiones.

El descubrimiento de la dirección IP correspondiente a cualquier extensión requiere solamente llamar a esa extensión y obtener una respuesta. Un analizador de protocolo o una herramienta para la captura de paquetes conectada al hub observará directamente los paquetes del objetivo una vez que la llamada es contestada. Conocer la dirección de IP de una extensión particular no es un compromiso en sí mismo, pero lo hace fácil para lograr otros ataques. Por ejemplo, si el atacante es capaz de detectar paquetes en la red local usados por el conmutador será fácil obtener los paquetes enviados y recibidos por un teléfono objetivo. Sin el conocimiento de la dirección de IP del teléfono objetivo, el trabajo del atacador puede ser mucho más difícil, sobre todo debido a que requerirá mucho más tiempo, posiblemente resultando un ataque descubierto.

1.3.2 Problemas de integridad.

La integridad de la información significa que la información permanece inalterada por usuarios no autorizados. Por ejemplo, la mayor parte de los usuarios desean asegurar que los números de cuenta bancaria no puedan ser cambiados por alguien más, o que las contraseñas sean cambiadas solamente por el usuario o un administrador de seguridad autorizado. Los conmutadores de telecomunicación deben proteger la integridad de sus sistemas de datos y configuración. Debido a la riqueza del conjunto de características disponible en los conmutadores, un atacante que pueda comprometer la configuración del sistema puede ejecutar casi cualquier otra tarea. Por ejemplo, una extensión ordinaria pudiera ser reasignada dentro de un grupo de teléfonos que pueden ser escuchados por supervisores o grabar conversaciones para propósito de control de la calidad. El daño o supresión de la información sobre la red IP utilizada por un conmutador VoIP trae como resultado una inmediata denegación de servicio.

El propio sistema de seguridad proporciona las capacidades para el abuso y la mala utilización del mismo. Es decir, la trasgresión del sistema de seguridad no solo permite el mal uso del sistema sino también la eliminación de toda rastreabilidad y la introducción de puertas secretas para intrusos, que serán utilizados por estos en próximas visitas. Por esta razón, el sistema de seguridad debe ser protegido cuidadosamente.

Las amenazas de integridad incluye cualquiera en las que las funciones del sistema o datos pueden ser corrompidos, bien sea accidentalmente, o como un resultado de acciones maliciosas. El mal uso puede involucrar usuarios legítimos (es decir personas de confianza realizando operaciones desautorizadas) o los intrusos.

Un usuario legítimo puede ejecutar una función de operaciones incorrecta, o desautorizada (por ejemplo, por error o sin malicia) y puede causar modificación destructiva, destrucción, supresión o revelación de los datos y software del conmutador. Esta amenaza puede causarse por varios factores incluyendo la posibilidad de que los permisos para el nivel de acceso concedido al usuario sean mayores del que este necesita.

Intrusión: Un intruso puede hacerse pasar como un usuario legítimo y acceder a un puerto de operaciones del conmutador. Existen varias amenazas de intrusión serias. Por ejemplo, el intruso puede usar el nivel de permiso del usuario legítimo y ejecutar funciones de operaciones perjudiciales tal como:

- Revelación de datos confidenciales.
- Causando deterioro de servicio por la modificación del software del conmutador.
- Colisionando el conmutador.
- Eliminación de todos las huellas de la intrusión (por ejemplo, modificando los log de seguridad) de tal modo que ella no pueda detectarse fácilmente.

Estado inseguro: En ciertos momentos el conmutador puede ser vulnerable debido al hecho de que no se encuentra en un estado seguro. Por ejemplo:

- Después que un sistema se reinicie, las características de seguridad viejas pueden haber sido restablecidas a un escenario inseguro y nuevas características pudieran no estar activadas todavía (por ejemplo, todas las contraseñas viejas pueden ser revertidas a la contraseña del sistema por defecto, incluso aunque nuevas contraseñas todavía no sean asignadas). Lo mismo puede ocurrir en el tiempo de recuperación de un desastre.
- En el momento de la instalación el conmutador puede ser vulnerable hasta que las características de seguridad por defecto sean reemplazadas.

1.3.2.1 Ataque de inserción al Servidor DHCP.

Es a menudo posible cambiar la configuración de un teléfono objetivo explotando la respuesta rápida de DHCP (Dynamic Host Configuration Protocol) cuando los teléfonos IP son inicializados. Tan pronto como el teléfono IP pide una respuesta DHCP, un servidor DHCP malo puede iniciar una respuesta con los campos de datos que contienen información falsa.

Esta agresión posibilita los ataques hombre en el medio (man in the middle) en las pasarelas de medios IP y teléfonos IP. Muchos métodos existen con la potencialidad de reiniciar el teléfono remotamente por ejemplo “ingeniería social”, ping flood, MAC Spoofing.

Si es posible, se deben utilizar direcciones IP estáticas para los teléfonos IP. Esto eliminará la necesidad de usar un servidor DHCP. Además, utilizando un sistema de detección de intruso se puede filtrar los paquetes fuera del servidor DHCP desde puertos de teléfonos IP, permitiendo este tráfico solamente desde el servidor legítimo.

1.3.2.2 Ataque de inserción servidor TFTP.

Es posible cambiar la configuración de un teléfono objetivo explotando la respuesta rápida del TFTP (Trivial File Transfer Protocol) cuando el teléfono IP se esté restableciendo. Un servidor TFTP mal intencionado puede suministrar información espuria antes de que el servidor legítimo sea capaz de responder a una solicitud. Este ataque le permite a un atacante cambiar la configuración de un teléfono de IP. Usando un estado basado en un sistema de detección de intruso puede filtrar los paquetes fuera del servidor DHCP desde puertos de teléfonos IP, permitiendo este tráfico sólo desde el servidor legítimo. Las organizaciones que están interesadas en implementar sistemas VoIP deben buscar instrumentos de teléfonos IP que puedan descargar archivos binarios firmados.

1.3.3 Accesibilidad y Denegación de Servicio.

La disponibilidad se refiere a la idea que la información y los servicios estén disponibles en el momento que se necesiten. La disponibilidad es el riesgo más obvio para un conmutador. Los ataques explotan vulnerabilidades en el software del conmutador o protocolos que pueden llevar al deterioro o incluso a una denegación de servicio o funcionalidad del conmutador. Por ejemplo: si un acceso desautorizado puede ser establecido en cualquier rama del canal de comunicación (tal como un enlace CCS o un enlace TCP/IP), ello puede ser posible para inundar la conexión con mensajes falsos causando el severo deterioro (posiblemente denegación) del servicio. Un sistema voz sobre IP puede tener vulnerabilidades adicionales con las conexiones a Internet. Debido a que los IDS (Sistemas de Detección de Intrusos fallan al interceptar un porciento significativo de ataques basados en Internet, los atacantes pudieran ser capaces de sacar de servicio sistemas VoIP explotando debilidades en protocolos de Internet y servicios.

Cualquier red puede ser vulnerable a los ataques de denegación de servicio, simplemente sobrecargando la capacidad del sistema. Con VoIP el problema puede ser especialmente severo, debido a su sensibilidad a pérdidas de paquete o demora.

1.3.3.1 Ataque de agotamiento de recursos CPU sin ninguna información de cuenta.

Un atacante con acceso terminal remoto hacia el servidor puede ser capaz de forzar el sistema para reiniciarlo proveyendo el número máximo de caracteres para los buffers de las contraseñas y login, varias veces en sucesiones. Adicionalmente, los teléfonos IP pueden reiniciarse como resultado de este ataque.

Además de producir una parada al sistema, el reinicio no puede restaurar cambios no comprometido o en algunos casos, pueden restaurar contraseñas por defecto, que pueden introducir vulnerabilidades de intrusión. El despliegue de un firewall deshabilitando conexiones desde entidades de redes desconocidas es el primer paso para resolver este

problema. Sin embargo, existe la oportunidad para un atacante de falsificar su dirección MAC e IP, evadiendo la protección del firewall.

1.3.3.2 Vulnerabilidad de la contraseña por defecto.

Es común para conmutadores tener un login / contraseña fijo. Similarmente, los teléfonos VoIP a menudo tienen secuencia de teclados por defecto que pueden ser usadas para desbloquear y modificar la información de la red.

Esta vulnerabilidad pudiera permitir que un atacante pueda controlar la topología de la red remotamente, posibilitando no solamente la completa denegación de servicio a la red, sino también un ataque "port mirroring" hacia el lugar donde se localiza el atacante, proporcionándole la habilidad para interceptar cualquier otra conversación que tiene lugar en el mismo conmutador. Además, el conmutador puede tener una interfase servidor Web, proporcionándole a un atacante la habilidad para desestabilizar la red sin el conocimiento avanzado de operaciones de conmutación y comandos. En la mayor parte de los sistemas, los teléfonos descargan sus datos de configuración en el arranque utilizando TFTP o protocolos similares. La configuración especifica las direcciones IP para nodos gestores de llamada, de modo que un atacante puede sustituir otra dirección IP que apunta a un gestor de llamada que permita escuchar a escondidas o análisis de tráfico. Cambiar la contraseña por defecto es crucial. Además, la interfaz usuario gráfica debe ser deshabilitada para impedir la intercepción de sesiones de administración de texto en claro.

1.3.3.3 Defecto en el software utilizado.

Como otros tipos de software, los sistemas VoIP también presentan vulnerabilidades debido al desbordamiento de los buffer y la impropia manipulación de la cabecera de los paquetes. Estos defectos típicamente ocurren porque el software no está validando correctamente la información crítica. Por ejemplo, un número entero corto puede ser usado como un índice de tabla sin comprobar si el parámetro pasado a la función excede de 32,767, resultando en acceso de memoria no valido o una colisión del sistema.

Los defectos en el software utilizable típicamente resulta en dos tipos de vulnerabilidades: denegación de servicio o revelación de parámetros críticos del sistema. La denegación de servicio a menudo puede ponerse en práctica remotamente, pasando paquete con cabeceras construidas especialmente que causan que el software falle. En algunos casos el sistema puede ser colisionado, produciendo un dump de memoria en la cual un intruso puede encontrar las direcciones IP de nodos críticos del sistema, contraseñas u otra información relevante de seguridad. Además, el desbordamiento del buffer que permite la introducción de código malicioso ha sido encontrado en el software VoIP, como en otras aplicaciones.

Estos problemas requieren acción del vendedor de software y distribución de parches a administradores. Los intrusos monitorean anuncios de vulnerabilidades, conociendo que muchas organizaciones requieren días o semanas para actualizar su software. El chequeo regular de las actualizaciones de software y parches es esencial para reducir estas vulnerabilidades.

La manipulación de parches automatizados puede ayudar a la reducción de la ventana de oportunidades para intrusos para explotar una vulnerabilidad de software conocida.

1.3.3.4 Vulnerabilidad de cierre forzoso de cuenta.

Un atacador será capaz de proporcionar varios intentos de login incorrecto en el prompt de telnet hasta que la cuenta sea cerrada. (Este problema es común a la mayor parte de los sistemas protegidos por contraseña, porque impide a los atacadores repetir intentos login hasta que la contraseña correcta sea encontrada probando todas las posibles combinaciones.)

La cuenta es incapaz de conectar la máquina durante el tiempo de cierre forzoso establecido. Si el acceso remoto no es disponible, este problema puede ser resuelto con control de acceso físico.

1.4 Calidad de servicio (QoS) y seguridad en VoIP.

La QoS es fundamental en la operación de una red VoIP. A pesar de todo el dinero que pueden ahorrar los usuarios y la elegancia de red que VoIP proporciona, si no pueden dar al menos la misma calidad de establecimiento, operación de conmutación y calidad de la voz como una red de teléfono tradicional, entonces proporcionará poco valor añadido. La ejecución de varias medidas de seguridad puede degradar la QoS. Estas complicaciones varían desde la demora o el bloqueo en la conformación de la llamada por el firewalls a la latencia producida por la codificación y la variación de demora (jitter). Los asuntos de QoS son medulares a la seguridad de VoIP. Si QoS estaba asegurado, entonces la mayor parte de mismas medidas de seguridad corrientes implementadas en las redes de datos de hoy, pueden ser usadas en las redes de VoIP. Pero debido a la naturaleza de criticidad de tiempo que VoIP requiere y su baja tolerancia a la interrupción y pérdida de paquetes, muchas medidas de seguridad puestas en práctica en las redes de datos tradicionales no son exactamente aplicables en su forma actual a VoIP. Los principales problemas originados a la QoS debido a las soluciones de seguridad son presentados en el Capítulo 2.

Los principales aspectos de QoS asociados con VoIP que afectan la seguridad son presentados seguidamente:

Latencia

En VoIP se refiere al tiempo que se toma una transmisión de voz para transitar desde la fuente al destino. Idealmente, se desea mantener la latencia tan baja como sea posible pero existe un extremo inferior práctico en la demora de VoIP.

La UIT en su Recomendación G.114, establece una demora que no supere los 150 ms para tráfico en una sola dirección. Esto se corresponde con la latencia actual experimentada en una llamada doméstica dentro de los Estados Unidos a través de la RTPC. Para llamadas internacionales, una demora de hasta 400 ms, se ha considerado tolerable.

Las llamadas de VoIP deben lograr un salto de 150 ms para emular con la QoS que proveen los teléfonos actuales. Esto deja muy poco margen para el error en la entrega de paquetes. Lo anterior, pone límite a la seguridad que puede ser añadida a una red de VoIP. La codificación de los datos de voz puede tomar entre 1 y 30 ms y el viaje de los datos de la

voz puede estar sobre los 100 ms, aunque realmente puede ser mucho menor . Asumiendo el peor caso (tiempo de transferencia igual a 100 ms), sólo quedarán disponibles de 20 a 50 ms, para tratamiento de las colas en los enrutadores y para tiempos adicionales provocados por mecanismos de seguridad.

La demora no es confinada a los extremos del sistema. Cada salto a lo largo de la red introduce un nuevo retardo de cola y posiblemente una demora de proceso si es un punto de control de seguridad (un firewall o un punto de codificación/decodificación). Además, los paquetes más grandes tienden a causar congestión de ancho de banda e incremento de la latencia. Considerando estos aspectos, VoIP tiende a trabajar mejor con paquetes pequeños en una red lógicamente concebida para mantener la latencia a un mínimo.

Jitter

Se refiere a la demora no uniforme de los paquetes. Ello es causado por situaciones de poco ancho de banda en VoIP y puede ser excepcionalmente perjudicial a la QoS. Las variaciones en las demoras pueden ser más perjudiciales a la QoS que las mismas demoras reales. El Jitter puede causar que al arribo de los paquetes, estos sean procesados fuera de secuencia. Como RTP se basa en UDP, los paquetes fuera de orden no son reensamblados a nivel del protocolo. Sin embargo, RTP permite a las aplicaciones realizar la reorganización utilizando el número de secuencia numérica y los campos de marcas de tiempo. Los gastos generales al volver a reunir estos paquetes no son triviales, especialmente cuando tenemos tiempos tan ajustados en VoIP.

La prescripción general para controlar el jitter en los puntos finales VoIP es el uso de un buffer, pero este tiene que entregar sus paquetes de voz al menos cada 150 ms (normalmente mucho antes que el tiempo de demora de transporte) así las variaciones en la demora pueden limitarse. La implementación del buffer esta definido por la incertidumbre de si un paquete desaparecido está simplemente retardado por un tiempo largo y anómalo o está perdido en realidad.

El jitter también puede ser controlado a lo largo de la red de VoIP utilizando enrutadores, firewalls y otros elementos de red que soportan QoS. Estos elementos procesan y pasan el tráfico VoIP con mayor prioridad que los paquetes de datos. Sin embargo, no todo los componentes de red son diseñados pensando en la QoS.

Otro método para reducir la variación de la demora es modelar el tráfico de la red para disminuir el jitter haciendo un uso eficiente del ancho de banda. Esta limitación está en conflicto con algunas medidas de seguridad en VoIP, principalmente con IPsec, cuyas necesidades de proceso pueden aumentar la latencia, limitando así el ancho de banda efectivo y contribuyendo a la ocurrencia de jitter. El ancho de banda efectivo es comprometido cuando los paquetes son expandidos con nuevos encabezados. En el tráfico IP normal, este problema es insignificante puesto que el cambio del tamaño del paquete es muy pequeño comparado con el tamaño total del paquete. Debido a que VoIP utiliza paquetes muy pequeños, incluso un aumento mínimo es importante porque se incrementa a través de todos los paquetes.

La ventana de entrega para un paquete de VoIP es muy pequeña, de este modo, la variación aceptable en la demora del paquete es incluso menor. Así, el cuidado extremo se debe dar, en el aseguramiento de que las demoras en las entrega de los paquetes, causadas por los dispositivos de seguridad se mantengan uniformes a través de la secuencia del tráfico. La implementación de dispositivos que soportan QoS y mejoran la eficiencia del ancho de banda con la compresión de las cabeceras, permiten demoras más uniformes en una red VoIP con seguridad.

Pérdida de paquetes.

VoIP es excepcionalmente intolerante a la perdida de paquetes. Esto puede ser resultado de latencia excesiva, donde un grupo de paquetes llega tarde y deba desecharse en favor de los nuevos. Ello también puede ser resultado del jitter, es decir, cuando un paquete llega después de que sus paquetes circundantes se hayan limpiado del buffer, haciendo inútil el paquete recibido. El tema de la pérdida de paquetes específicos de VoIP existe además de las pérdidas de paquetes asociados con las redes de datos. En estos casos los paquetes nunca son entregados. Como se ha visto, VoIP utiliza para el transporte de la voz a RTP, que a su vez utiliza el protocolo de transporte no confiable UDP y de este modo no se garantiza la entrega de los paquetes.

Las limitaciones en tiempo no permiten la utilización de un protocolo confiable como TCP en la entrega de medios. Un paquete puede ser reportado perdido, retransmitido y recibido, pero en VoIP las limitaciones de tiempo para la QoS serían excedidas, por lo que no es posible la retransmisión de los mismos. Sin embargo, en VoIP ayuda el hecho, de que los paquetes son muy pequeños, conteniendo una carga útil de sólo 10 - 50 bytes, esto equivale a un tiempo de transmisión de aproximadamente entre 12.5 - 62.5 ms. La pérdida de tan pequeña cantidad de información de voz, no es discernible por un usuario de VoIP humano. No obstante, un problema es que estas pérdidas no se producen de forma aislada. La congestión provocada por la utilización del ancho de banda y otras causas de pérdida de paquetes tienden a afectar todos los paquetes que son entregados alrededor del mismo tiempo. Así aunque la pérdida de un paquete es bastante insignificante, probabilisticamente la pérdida de un paquete significa la pérdida de varios paquetes, lo que degrada severamente la QoS en una red de VoIP.

En una comparación de calidad de VoIP contra la RTPC, un estudio de la Asociación de Industrias de las Telecomunicaciones (TIA) [30], muestra claramente que un porcentaje bastante pequeño de paquetes perdidos provoca que la QoS de la red VoIP, caiga por debajo del nivel que los usuarios han estado disfrutando en sus líneas de teléfonos tradicionales. Cada codec (Coder/Decoder) estudiado por TIA ha experimentado una caída en la satisfacción de los usuarios, cuando la latencia cruza los 150 ms. Sin embargo, aún con menos de 150 ms de latencia, una pérdida de paquete del 5 % del tráfico de VoIP codificado con G.711 (norma internacional para codificar audio telefónico en una trama de 64 kbps) puede hacer caer los niveles de calidad por debajo de los niveles de QoS de la RTPC.

Si las codificaciones se realizan con G.723.1 (compresión de la voz a muy baja razón de bits) o con G.729A (compresión de voz sobre un flujo de 8kbps), pérdidas de 1 y 2 %, respectivamente, son suficientes para situar la calidad en redes de VoIP por debajo de la calidad percibida por un usuario de una red telefónica normal. Con pérdidas de 3 y 4 %, respectivamente, el funcionamiento de estas redes trajo como resultado que la mayoría de los usuarios estuvieran descontentos. Estos resultados corroboraron los informes de un estudio en 1998 en UCal-Berkeley que determinó "tolerable las razones de pérdidas entre el 1 - 3 % y que la calidad se vuelve intolerable cuando más del 3 % de los paquetes de voz se pierden" [7]. Ambos estudios encontraron que mayores proporciones de compresión de carga útil resultaran en una sensibilidad más alta a la pérdida de paquetes.

A pesar de la impracticabilidad de usar un protocolo de entrega tal como TCP, existen ciertos remedios para el problema de pérdida de paquete. Uno no puede garantizar que todos los paquetes sean entregados, pero si el ancho de banda está disponible, enviando información redundante puede anular probabilisticamente la oportunidad de pérdida. Tal ancho de banda no está accesible y la información redundante tendrá que ser procesada, introduciendo incluso mayor latencia al sistema e irónicamente, produciendo posiblemente hasta mayor pérdida de paquetes. Nuevos codecs tales como el Internet de Baja Razón de Bit (iLBC) están siendo también desarrollados para ofrecer calidad de voz y una complejidad computacional como la de G.729A, mientras incrementa la tolerancia a las pérdidas de paquetes.

Ancho de banda y ancho de banda efectivo

En cualquier red, la primera preocupación es si la misma está disponible para el uso, lo cual incluye sus nodos y enlaces entre estos. También debe considerarse la disponibilidad de firewalls, las CPU (Unidad Central de Proceso) y los terminales. No obstante, en este punto la atención se centrará en la disponibilidad de ancho de banda del sistema VoIP.

Como en las redes de datos, la congestión del ancho de banda puede causar perdida de paquetes y otros problemas de QoS en un ordenador principal. Así, la reserva y asignación de un adecuado ancho de banda es esencial para mantener la calidad de la VoIP. La congestión de la red causa una cola de paquetes, lo que crea una latencia en el sistema de VoIP. Un ancho de banda inferior puede también contribuir al jitter, puesto que los paquetes serán entregados en un gran esfuerzo cuando se abra una oportuna ventana en el tráfico.

Los métodos para reducir el ancho de banda utilizado en VoIP incluyen la compresión de encabezado RTP y Detección de Actividad de Voz (VAD). La compresión RTP resume el tráfico de la secuencia de los media, así menos ancho de banda es utilizado. Sin embargo, un esquema ineficaz de la compresión puede causar latencia o degradación de la voz, causando un descenso total de la QoS. VAD previene la transmisión de los paquetes de voz vacíos (es decir cuando un cliente no está hablando, su dispositivo no envía simple ruido blanco). Sin embargo, por definición VAD contribuirá a la inestabilidad en el sistema (jitter) causando la generación irregular de paquetes.

Desde que la voz y las secuencias de datos están compartiendo el mismo ancho de banda finito y las secuencias de datos tienden a contener paquetes mucho más grandes que los de VoIP, las cantidades importantes de datos puede congestionar la red y evitar que el tráfico de la voz alcance su destino en una manera oportuna. Por esta razón, la mayoría de los nuevos dispositivos de hardware desplegados en redes utilizan QoS para VoIP. Estos dispositivos, tales como enrutadores y firewalls, hacen uso de protocolos IP para tipos de servicio (ToS) para enviar el tráfico de los bits de VoIP antes que el tráfico de datos urgentes. Los teléfonos de VoIP a menudo también incluyen las características de QoS [20].

No sólo el ancho de banda disponible del sistema es afectado por la introducción de las medidas de seguridad, sino en adicción el ancho de banda efectivo del sistema de VoIP puede despreciarse significativamente. El ancho de banda efectivo es definido por Barbieri y otros, [8] como "el porcentaje de ancho de banda porta datos reales con respecto a la anchura de banda total utilizado" La introducción de IPsec o de otros formas de cifrado da lugar a una cabecera mucho más grande de proporción de la carga útil para cada paquete y ésta reduce el ancho de banda efectivo como el mismo número de paquetes (pero de tamaño más grande) que se utiliza para transportar la misma cantidad de datos. Las consecuencias de esta reducción incluyen disminución del rendimiento de procesamiento y crecimiento de la demora.

Necesidad de velocidad

El clave para superar temas de QoS como la latencia y la congestión de ancho de banda es la velocidad. Por la definición, un rendimiento de procesamiento más rápido significa tiempo de espera reducido y reducción probabilística de las oportunidades de congestión severa de ancho de banda.

Entre los principales elementos que introducen demora y contribuyen notablemente en la congestión se encuentran el paso a través de firewalls y NATs, así como el cifrado y descifrado del tráfico. Tradicionalmente, éstos son dos de las maneras más efectivas para que los administradores aseguren sus redes. La inserción de firewalls tradicionales y productos de cifrado en una red de VoIP no es factible, particularmente cuando VoIP se integra a redes de datos existentes. En lugar, estas soluciones para redes de datos se deben adaptar al soporte de seguridad del nuevo mundo de la VoIP.

Fallos de corriente y sistemas de respaldo.

Los teléfonos convencionales son alimentados desde la central de conmutación por la propia línea telefónica. La mayoría de las oficinas utilizan sistemas PBX que utilizan sistemas de alimentación de respaldo de modo que continúen operando durante fallos en la alimentación. De la misma manera, son requeridos sistemas de respaldo para mantener vitales los sistemas VoIP en caso de emergencia.

Una organización que proporciona sistemas de alimentación continuos para su red de datos y computadoras de escritorio puede que ya tenga la infraestructura de alimentación necesitada para continuar las funciones de la comunicación durante interrupciones de la alimentación. Sólo debe garantizarse la suficiente potencia de respaldo disponible para el conmutador VoIP de la oficina.

Los costos deben incluir corriente eléctrica para mantener la carga de la batería de la UPS, mantenimiento periódico para los sistemas de reserva y para el reemplazamiento de la batería de la UPS. Si la potencia de emergencia/respaldo se requiere por más de algunas horas, entonces se necesitarán generadores eléctricos, para lo cual deberán ser considerados los costos en combustibles y en el almacenamiento del mismo.

La calidad de servicio, implicaciones para la seguridad

Los requisitos de funcionamiento estricto de VoIP tienen implicaciones importantes para la seguridad, particularmente los problemas de Denegación del Servicio (DoS) [21]. Los ataques específicos de VoIP (es decir, inundaciones de mensajes SIP) pueden dar lugar a ataques DoS para muchos dispositivos VoIP. Por ejemplo, en los puntos finales los teléfonos SIP pueden congelarse cuando intentan procesar una alta razón de tráfico del paquetes de los servidores SIP proxy, también pueden experimentar fallos y discrepancias intermitentes de registro con un ataque de señalización específico de VoIP inferior a 1 Mbps. Generalmente, la razón de paquetes del ataque puede tener más impacto que el ancho de banda; es decir, un alto régimen de paquetes puede dar lugar a una negación del servicio aun si el ancho de banda consumido es bajo.

En el capítulo siguiente se explora la definición del conflicto entre las demandas de velocidad para lograr mantener la QoS y el retraso asociado con estas tradicionales medidas de seguridad.

CAPITULO 2: Afectaciones a la VoIP provocadas por las soluciones de seguridad.

Las redes de paquetes dependen para su funcionamiento exitoso de un gran número de parámetros configurables, entre ellos las direcciones IP Y MAC (física) de los terminales de voz, direcciones de enrutadores y firewalls y software especifico de VoIP tales como componentes de procesamiento de llamadas y otros programas utilizados para establecer y enrutar llamadas. Muchos de estos parámetros de la red se establecen dinámicamente cada vez que los componentes de la red son reiniciados o cuando un teléfono VoIP se reinicia o se conecta a la red. Debido a que hay muchos lugares en una red con parámetros configurables dinámicamente, los intrusos tienen una gran cantidad de puntos potencialmente vulnerables para atacar.

En este capitulo se analizaran la existencia de afectaciones en una red VoIP provocadas por dispositivos y herramientas de seguridad, lo que conduce a la degradación de la calidad de la voz y a un compromiso entre seguridad y calidad de voz y enfatiza la necesidad de la velocidad. También se plantean soluciones a estos problemas de forma que se preserve la QoS y no se degrade la seguridad de la red.

2.1 Firewalls y NATs

Firewalls y NATs plantean un reto formidable para los implementadores de VoIP. Sin embargo, existen soluciones a estos problemas, si uno está dispuesto a pagar el precio. Las soluciones de uso general que se pueden integrar en una configuración de red estándar que contiene un Firewall y/o un NAT son presentadas aquí.

Mucho de los estandares de trabajo hasta el momento se ha hecho en el IETF para SIP, aunque también la UIT ha tomado recientemente los temas de firewall y NAT traversal para H.323 en el grupo de estudio 16. Es importante observar que tres importantes protocolos de VoIP (SIP, H.323, y MEGACO/H.248) todos tienen problemas similares con los firewalls y los NATs. Aunque el uso de NATs se puede reducir con la adopción de IPv6, ellos seguirán siendo un componente común en las redes por los años venideros e IPv6 no aliviará la necesidad de firewalls, así que los sistemas de VoIP deben ocuparse de las complejidades de los Firewalls y NATs.

2.1.1 Firewalls.

Un Firewall es un sistema o grupo de sistemas que refuerzan la política de control de acceso entre dos redes. Para su implementación es necesario tener en cuenta dos aspectos muy importantes: seguridad y accesibilidad, siendo más o menos restrictivo en función de las necesidades. Un aspecto importante desde el punto de vista de la seguridad, es que la comunicación con la consola de gestión del firewall debe viajar de forma encriptada.

La ubicación central que presentan los firewalls en la red es muy beneficiosa para el despliegue de políticas de seguridad. Es el último cuello de botella para el tráfico en la red, por lo que todo el tráfico que entra o sale de la LAN tiene que atravesar el firewall. Esta situación es de gran utilidad para una red VoIP ya que permite simplificar direcciones de seguridad, consolidando las medidas de seguridad en la entrada del firewall, en vez de exigirle a todos los puntos finales que mantengan una política de seguridad al día.

Clasificación de los Firewalls.

De acuerdo al funcionamiento, existen tres tipos de firewalls.

Firewalls sin estado (Stateless):

Funcionan mediante listas de control de acceso, que especifican el tráfico que puede pasar a través del filtro de acuerdo a los valores existentes en las cabeceras TCP, UDP e IP: direcciones IP y puertos UDP y TCP.

Una de sus características es que presentan una gestión muy compleja debido al elevado número de reglas que deben especificarse, ya que la orientación de su diseño se basa en el análisis individual de cada paquete que pasa por la red.

El control de las conexiones es sencillo, ya que por ejemplo, si se especifica una regla que permita tráfico de las conexiones establecidas, por ejemplo en las ACLs del IOS de Cisco, sólo se comprobará que el paquete tiene activo el bit ACK.

Se adaptan a protocolos dinámicos como puede ser FTP, en los que los puertos por los que se realizan ciertas comunicaciones se determinan en el transcurso de la conexión, no están predefinidos inicialmente.

Por otro lado, no pueden manejar de forma segura protocolos basados en UDP, ya que no se disponen en el momento de su configuración de los puertos UDP aleatorios elegidos por los clientes internos de la red, por lo que para habilitar la comunicación es necesario abrir todos los puertos mayores al 1023.

Proxy de aplicación:

Se encargan de reenviar las peticiones de red (mediante llamadas socket) haciendo de intermediario, pero sin aplicar ningún filtro a los datos, un ejemplo de este tipo de Firewall son los traductores de protocolos genéricos, como SOCKs.

Por otro lado, los Proxy de aplicación específicos, disponen de información propia de la aplicación, por lo que son capaces de aplicar restricciones muy particulares, por ejemplo en el caso del protocolo HTTP no permitir la obtención de Aplets Java o en el caso de FTP, permitir enviar ficheros (put) pero no recibirlos (get).

Debido a este conocimiento detallado de la aplicación, se trata de sistemas más seguros, siempre que se disponga de un filtro específico asociado a la aplicación o protocolo que se desea filtrar. En caso contrario suponen una desventaja, ya que en el caso de nuevas aplicaciones no se dispondrá de este, por lo que se deberá aplicar un Proxy genérico.

Realizan un análisis a muy bajo nivel, tienen funciones de contabilidad y auditoria muy detalladas, pero por el contrario el rendimiento es menor debido a su complejidad.

Filtros con estado (Stateful filters):

Estos filtros trabajan con las conexiones o secciones, no con los paquetes individualmente y son inteligentes desde el punto de vista de que controlan cada paquete asociado a cada conexión que transcurre a través de ellos, siendo conscientes de los pasos posibles a realizar por la aplicación o el protocolo.

La configuración es más sencilla, ya que debido al conocimiento intrínseco, en el firewall, con especificar el tráfico deseado, se configurarán automáticamente los caminos necesarios para el tráfico de retorno. Por esto, es capaz de trabajar con protocolos dinámicos como el FTP.

Este tipo de firewall proporciona una seguridad y un rendimiento muy bueno. Como desventaja es posible señalar la dificultad que tienen para analizar los contenidos de las aplicaciones, centrándose más en los protocolos como TCP y UDP.

2.1.2 Necesidades de Firewalls específicos VoIP.

En redes VoIP se despliegan a menudo firewalls específicos para ese tipo de red, los cuales tienen la responsabilidad adicional de permitir que fluyan los datos entre los segmentos de voz y datos. Ésta es una función crucial para una red que contenga teléfonos IP conectados a PC, los cuales se encuentran en la red de los datos, pero necesitan enviar mensajes de voz. Todo el tráfico de voz que viaja a través de estos dispositivos debe ser abiertamente permitido sino está presente ningún firewall debido a que RTP utiliza puertos UDP dinámicos. Dejar abierto tantos puertos UDP, origina brechas en la seguridad. De modo que se recomienda que todos los teléfonos basados en PC se ubiquen detrás de un firewall con estado, el cuál actuará de intermediario en el tráfico de VoIP.

Sin tal mecanismo, un ataque UDP DoS puede comprometer a la red, debido a la cantidad de puertos abiertos. Éste es uno de los ejemplos de cómo los firewalls se usan para proporcionar una segmentación lógica de la red, proporcionando una barrera entre los segmentos de voz y datos. Algunos de los puntos importantes de colisión entre el tráfico de voz y el de datos, donde es necesario utilizar firewalls son:

- Cuando los teléfonos IP conectados a una PC (datos) requieren acceso al segmento (voz) para el establecimiento de llamadas, envío de mensajes, etc.
- Los Teléfonos IP y gestores de llamadas (voz) acceden al correo de voz (datos).
- Los usuarios (datos) acceden al servidor proxy (voz).
- El servidor proxy (voz) accede a recursos de la red (datos).
- El Tráfico de teléfonos IP (voz) hacia el gestor de procesamiento de llamadas (voz) o servidor proxy (voz) deben pasar a través del firewall debido a que tales contactos utilizan el segmento de datos como un intermediario.

2.1.3 Traductores de Direcciones de Red (NAT).

El NAT es una poderosa herramienta que se puede usar para ocultar direcciones de red interna y permite que varios terminales dentro de una LAN compartan la misma dirección IP (externa). Para el propósito de este documento, NAT se refiere a la traducción de direcciones de red y NAPT (Network Address Port Translation), tiene en cuenta además la traducción de puertos. En los NAT, las cabeceras IP de salida se cambian de direcciones LAN privadas a las direcciones IP globales del enrutador. En NAPT las cabeceras TCP/UDP son convertidas. Esto permite que varias computadoras compartan simultáneamente la dirección global IP del enrutador. Las máquinas que no necesitan entrar a Internet, se les puede asignar direcciones locales en la red sin producir conflictos o sin tener que asignarles una dirección IP. Debido a la carencia de direcciones IP en muchas regiones, esta es una funcionalidad extremadamente útil.

Los NATs también contribuyen indirectamente a la seguridad de una LAN, haciendo las direcciones IP internas menos accesibles desde Internet. De este modo, todos los ataques en contra de la red se deben enfocar al mismo enrutador NAT. Como los Firewalls esto suministra seguridad porque solo un punto de acceso debe protegerse y el enrutador será generalmente más seguro que una PC directamente conectada a la red (menos probabilidad de puertos abiertos, programas maliciosos, etc.). La abstracción de la LAN de la red a través de un NAT también simplifica la administración de red. Por ejemplo si se decide cambiar su ISP, solo la configuración del enrutador externo se necesitaría cambiar. La red interna y el esquema de direccionamiento se pueden dejar sin tocar.

A continuación se describen los tipos de NAT.

Cono completo NAT

Un cono completo NAT es uno donde todas las peticiones desde la misma dirección IP interna y su puerto se proyectan a los mismos puertos y dirección IP externa. Además, cualquier host externo puede enviar un paquete al host interno, enviando un paquete a la dirección externa proyectada.

Cono restringido NAT.

Un cono restringido NAT es aquel donde todas las peticiones de la misma dirección IP interna y el puerto se proyectan a la misma dirección IP externa y su puerto. A diferencia del cono completo NAT un host externo (con dirección IPx) puede enviar un paquete al host interno solo si el host interno había previamente enviado un paquete a la dirección IPx.

Cono restringido de puerto NAT.

Un cono restringido de puerto NAT es como un cono restringido NAT, pero la restricción incluye los números de puertos. Específicamente, un host externo puede enviar un paquete, con dirección IPx de origen y puerto de P de origen, al host interno sólo si el host interno previamente había enviado un paquete a la dirección IPx y puerto P. Se usa para facilitar la compartición de las direcciones IP externas.

NAT simétrico.

Un NAT simétrico es uno donde todas las solicitudes desde la misma dirección IP interna y puerto, a una dirección IP destino y puerto específico son "mapeadas" a la misma dirección IP externa y puerto. Si el mismo host envía un paquete con la misma dirección origen y puerto, pero a un destino diferente, entonces se utiliza un mapeo" diferente. Además, solo el host externo que recibe un paquete puede enviar de regreso un paquete UDP al host interno.

Todos los beneficios del NAT tienen su precio. Los NATs "violan la semántica fundamental de las direcciones IP, que constituyen puntos alcanzables globalmente para las comunicaciones" [27]. Este diseño tiene implicaciones significativas para VoIP. Por una parte un intento de hacer una llamada a la red se convierte muy complejo cuando un NAT se introduce. La situación es análoga a una red de teléfono donde varios teléfonos tienen el mismo número, como en una casa con teléfonos múltiples en una línea (observe figura 2.1). Hay varias consecuencias también asociadas a la transmisión de los mismos medios a través de un NAT, incluyendo una incompatibilidad con IPSec (Ver epígrafe 2.3).

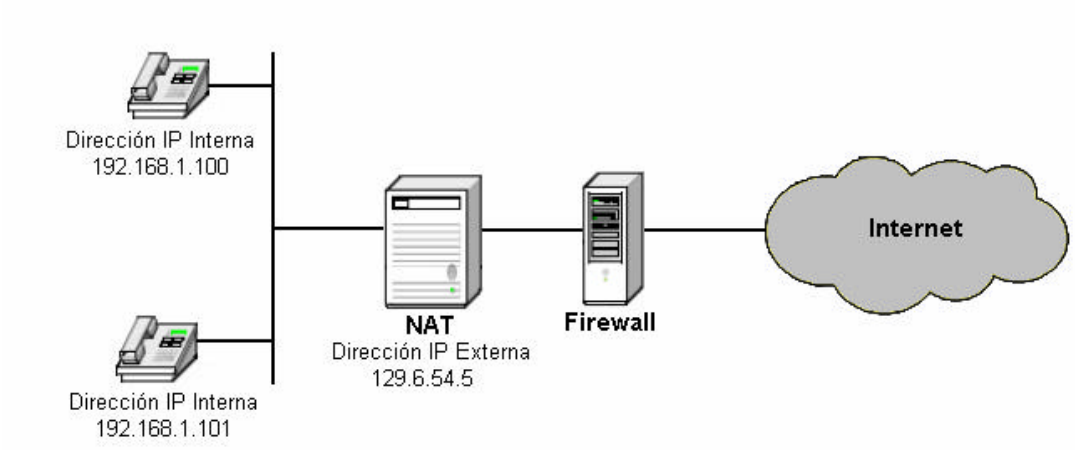

Figura 2.1. Teléfonos IP detrás de un NAT y un firewall.

Conceptualmente, la solución mas fácil a estas incompatibilidades es eliminando o suprimiendo enteramente los NATs, pero estos tienen sus beneficios y aún cuando IPv6 y su espacio de direcciones expandidas se implementasen, de manera que suficientes direcciones IP estuvieran disponibles para que todos dispongan de su propia y única dirección IP, todavía habría necesidad para los NATs.

Algunos ISP usan un esquema donde a los usuarios se les asignen direcciones IP estáticas, una por usuario. Es improbable que un ISP pudiera examinar completamente su sistema y se cambie a una asignación IP dinámica (por ejemplo con DHCP) porque una riqueza de direcciones nuevas está disponible en IPv6. Esto socavaría su red completa y la conduciría a vulnerabilidades y oportunidades para que usuarios maliciosos roben acceso a Internet. Pero muchos usuarios querrán todavía conectar múltiples máquinas a la red usando una dirección IP única, de este modo el uso de los NATs continuará. Hay muchos escenarios análogos a este donde los NATs son las soluciones más baratas, fáciles y eficientes.

NAT también introduce complicaciones de diseño mayores en el control de tráfico de los medios en VoIP. Ante todo, la práctica estándar de NAT de asignar nuevos números de puertos al azar rompe la conexión par de RTP y RTCP y sus números de puertos. La traducción de direcciones y puertos IP por NAT es también problemática para la recepción de paquetes VoIP. Si el enrutador NAT no procesa aproximadamente el tráfico, las nuevas direcciones / puertos no tendrán correspondencia a aquellas negociadas en el proceso de programación de llamadas. En este escenario, las pasarelas VoIP no pueden entregar correctamente los paquetes RTP.

El problema se agrava si los dos participantes de la llamada están detrás de NATs. Varias soluciones están disponibles para los usuarios con control administrativo en la seguridad de sus redes y el dinero para modernizar su hardware firewall/NAT. Para los usuarios sin control de la arquitectura de su red, existe una solución propuesta, que se detalla en el epígrafe 3.2.6. Sin embargo, esta solución se rompe cuando los dos usuarios están detrás de NAT y no se ha implementado exitosamente hasta la fecha.

El uso de NATs añade otra complicación posible a la señalización de llamadas VoIP debido a la naturaleza finita de las uniones de NAT. En un NAT, una dirección IP pública es destinada a una privada por un cierto período de tiempo (t). Esta entrada lograda se borra si ningún tráfico fue observado en los NAT por t segundos o la conexión se interrumpió explícitamente. Un mensaje SIP Invite que activan las uniones de la dirección privada a la pública y establece información de estado cuando atraviesa NAT o el Firewall. Este estado debe finalmente borrarse. Cuando se usa TCP, el cierre de la conexión TCP es usualmente un buen indicador de la terminación de la aplicación. Sin embargo, cuando SIP corre sobre UDP, semejante indicación es pérdida. Además de esto, como un periodo de silencio durante una conversación debe ser más largo que t segundos, al no recibir tráfico para t segundos no podría ser suficiente como una indicación de terminación de sesión. Como resultado, es posible que alguna información de estado se destruya antes de la transacción y/o la llamada realmente se complete.

2.1.4 Mecanismos para solucionar los problemas de NAT.

Especialmente para protocolos de comunicación en tiempo real como H.323 y SIP, NAT causa problema debido a que estos protocolos incluyen direcciones IP en sus mensajes. Para la protección de la integridad el dispositivo NAT tiene que ser un host intermedio fiable para calcular de nuevo la suma de chequeo de la integridad. Desde un punto de vista de seguridad extremo a extremo no es recomendable. Por lo tanto a continuación se describen varios mecanismos para tratar en formas diferentes el problema de los NAT.

Traversal simple de UDP a través de NATs.

Como se define en RFC 3489 [22], el transversal simple de protocolo de datagrama de usuario (UDP) a través de traductores de direcciones de red (STUN) es un protocolo de poco peso que permite aplicaciones para descubrir la presencia y los tipos de NAT y Firewall, entre estos y el Internet público. Proporciona también la habilidad de aplicaciones para determinar direcciones del protocolo de Internet público, destinado para ellos por el NAT (unión de

direcciones). STUN trabaja con muchos NATs existentes y no requiere ningún cambio en ellos. STUN no trabaja con el NAT simétrico, porque el mapeo de direcciones de puertos, es dependiente del destino. El servidor STUN entrega el mapeo de las direcciones IP de los puertos para la conexión al propio servidor de STUN, que es diferente del mapeo para el cliente destino [26].

Traversal usando repetidor NAT (TURN).

El protocolo TURN está diseñado para resolver el problema traversal de medios por el NAT simétrico. El mencionado protocolo permite que un elemento ubicado detrás de un NAT o un Firewall reciba datos entrantes sobre las conexiones de TCP o UDP para complementar las limitaciones de STUN. TURN se basa en un servidor que es insertado en el camino de la señalización y los medios. Este servidor TURN es localizado en los clientes DMZ (Zona DesMilitarizada) o en la red del proveedor de servicios. El cliente SIP de TURN habilitado envía un paquete exploratorio al servidor TURN, el que responde con la dirección IP pública y puertos usados por el NAT para esta sesión. Esta información es usada en los mensajes de establecimiento de llamadas de SIP y para flujos de medios subsiguientes.

La ventaja de este acercamiento es que no existe ningún cambio en la dirección destino vista por el NAT y de esa manera, el NAT simétrico puede ser usado. Es importante destacar que el servidor TURN actuará como un repetidor de datos, recibiendo datos en la dirección que les asigno a los clientes y luego reenviándoselos.

Muchos proveedores de servicios prevén ser capaz de manipular la información de QoS y suministrar seguridad mejorada en los puntos de entrada a la red. TURN no soporta este requerimiento, porque los detalles de la sesión de SIP no son dados a conocer al servidor TURN por el protocolo TURN.

A diferencia de un servidor STUN, un servidor TURN proporciona los recursos (ancho de banda y puertos) a los clientes que se conectan con él. Por lo tanto, solamente los clientes autorizados pueden acceder a este servidor. TURN asume la existencia de un secreto compartido de larga vida entre el cliente y el servidor del mencionado protocolo para lograr la autenticación de las solicitudes de TURN.

El cliente usa el secreto compartido para autenticarse a sí mismo en una solicitud de secreto compartido, enviado sobre TLS. La respuesta del secreto compartido proporciona por una vez al cliente un nombre de usuario y contraseña. Esta contraseña es entonces utilizada para autenticar el mensaje Allocate enviado por el cliente al servidor de TURN para preguntar por una dirección IP pública y puerto. Para datos entrantes, el servidor TURN entonces almacena las direcciones remotas y los puertos de donde vienen los datos y envía los datos al cliente. Este servidor es responsable de garantizar que los paquetes enviados a la dirección IP pública se enruten al servidor TURN.

Establecimiento de conectividad interactiva (ICE).

ICE describe una metodología para el Traversal NAT y para el protocolo de SIP. ICE no es un protocolo, es una armadura que trabaja en conjunto con diferentes técnicas, tales como STUN y TURN, el cual habilita el cliente para investigar su entorno a fin de adquirir de cómo comunicarse con el mundo exterior.

ICE para lograr sus conexiones se apoya en uno o más servidores STUN y TURN externos y extensiones SIP. Los clientes de ICE intercambiaran información de accesibilidad y negociaran para encontrar uno o más caminos de conexión entre ellos. Si establecen que existe más de un posible camino de conexión, ellos intentarán escoger la conexión de mejor calidad basada en mediciones de latencia y jitter. Si el cliente de ICE inicialmente intenta llamar a un cliente no ICE, entonces el proceso de establecimiento de llamada puede ser revertido a una llamada SIP convencional requiriendo Traversal NAT para ser resueltos por otros medios.

Universal Plug and Play (UPnP).

Otra solución diseñada originalmente para el mercado doméstico es el Universal Plug and Play. En este escenario, el NAT es mejorado para soportar el protocolo UPnP y el cliente puede interrogar el NAT directamente en cuanto a su dirección IP externa y número de puerto. Sin embargo, UPnP no escala cuando se produce una cascada de NATs y existen problemas de seguridad potencialmente serios con esta solución, incluyendo vulnerabilidad a los ataques de denegación de servicio [27].

La arquitectura de UPnP no sólo es dirigida a VoIP, sino que está diseñada para permitir la configuración simple de redes pequeñas por personas expertas. UPnP permite aplicaciones a clientes para hallar y configurar los componentes de una red, incluyendo los NAT y los firewalls, que son equipados con software de UPnP. Las aplicaciones de VoIP necesitan hallar y usar direcciones IP externa y puertos que el NAT escoge para la señalización y flujos de medios. Una vez que esta información es conocida, el cliente de VoIP (un SoftPhone o un teléfono SIP Standalone) puede poner esta información dentro de la señalización de VoIP para establecer la llamada. Esto asegura que la llamada se establece usando direcciones públicas y puertos y asegura la conectividad extremo a extremo.

2.1.5 Consideraciones de la programación de llamadas con los NAT y los Firewall.

Los usuarios de VoIP no toleran el estado latente excesivo en el proceso de programación de llamada, el cual corresponde al levantar el auricular y marcar en un sistema tradicional. Los usuarios se enojan con un proceso de programación que requiera más de unos pocos segundos.

Muchos factores afectan el tiempo de programación de una llamada VoIP. A nivel de red, esto incluye la topología de la red y la ubicación de ambos extremos, así como la presencia de un Firewall o NAT.

En el nivel de aplicación, el grado o falta de autenticidad y otras medidas en la seguridad de los datos, así como la selección del protocolo usado para establecer la llamada, pueden modificar dramáticamente el tiempo necesario para preparar una conexión VoIP.

Pasarelas de medios a nivel de aplicación (ALG).

Las ALG son las soluciones comerciales típicas para los problemas de cruce con Firewall / NAT . Un ALG es un software incrustado en un Firewall o NAT, que permite la configuración dinámica basada en una información específica de aplicación. Un Firewall con un ALG VoIP puede analizar y comprender H.323 o SIP y abrir o cerrar dinámicamente los puertos necesarios.

Cuando se emplea NAT, el ALG necesita abrir totalmente los paquetes VoIP y reconfigurar la información de la cabecera allí dentro para que se corresponda con las direcciones IP internas correctas en la red privada o en la red pública para el tráfico saliente. Esto incluye la modificación de las cabeceras y cuerpos de los mensajes (ejemplo SDP) en H.323 y SIP. El problema NAT se alivia cuando el ALG reemplaza las direcciones de red privada con la dirección del mismo ALG.

Este trabaja no solo cambiando la dirección IP, si no también mapea el tráfico RTP dentro de los puertos que ALG puede leer desde y hacia la máquina interna correcta. La necesidad de puertos consecutivos para RTP y RTCP pueden causar un problema aquí porque todo el tráfico VoIP en la red (y tráfico de datos también) es enrutado a través de ALG, así como el volumen de llamadas se incrementa, encontrar suficientes puertos consecutivos se pueden convertir en un problema. De este modo, ambos terminales pueden tener puertos adecuados para convocar una conversación y las deficiencias del Firewall pueden causar que la llamada se rechace como ocupada por el mismo ALG.

El modo de funcionamiento, la manipulación de los paquetes VoIP introducen latencia en el sistema y puede contribuir a jitter cuando un alto volumen de llamadas se experimenta. En dependencia de la arquitectura del firewall, esto también puede poner lento el rendimiento en el firewall, así contribuyendo a una cogestión de red general. Un firewall con soporte ALG pude ser costoso y necesita ser actualizado o reemplazado cada vez que los estándares para VoIP cambian. También, la adición de la inteligencia de aplicación al firewall puede introducir inestabilidades en el mismo. Algunos firewall se han encontrado que son vulnerables a un ataque en los cuales un alto porcentaje de establecimientos de llamadas puede ser enviado, reduciendo las tablas de conexión del firewall. Esta sesión media abierta de VoIP puede que no dure en el firewall por más de 24 horas. Todavía con todas estas cosas en contra, un ALG permanece muy seguro y simple y permite la coexistencia de VoIP, Firewall y NAT.

Soluciones Middlebox.

Una desventaja de los ALGs es que ellos están incrustados en el mismo firewall, y de ese modo la latencia y la disminución del rendimiento de todo el tráfico que viaja a través del firewall se agrega y complica por el volumen de llamadas VoIP. La solución al estilo middlebox intenta aliviar este problema ubicando un dispositivo adicional fuera del firewall que realiza muchas de las funciones asociadas con un ALG. El dispositivo donde se coloca la inteligencia de aplicación puede ser un sistema "in-path" tal como un gatekeeper H.323 o un proxy SIP que se encuentra en la trayectoria de control de la sesión y se considera un sistema confiable que analiza el trafico VoIP y las instrucciones del firewall para abrir y cerrar los puertos, basado en las necesidades de la señalizaciones VoIP a través de un protocolo de

comunicación intermedia (midcom). Un escenario de comunicaciones "middlebox" con la utilización de SIP, se muestra en la Figura 2.2.

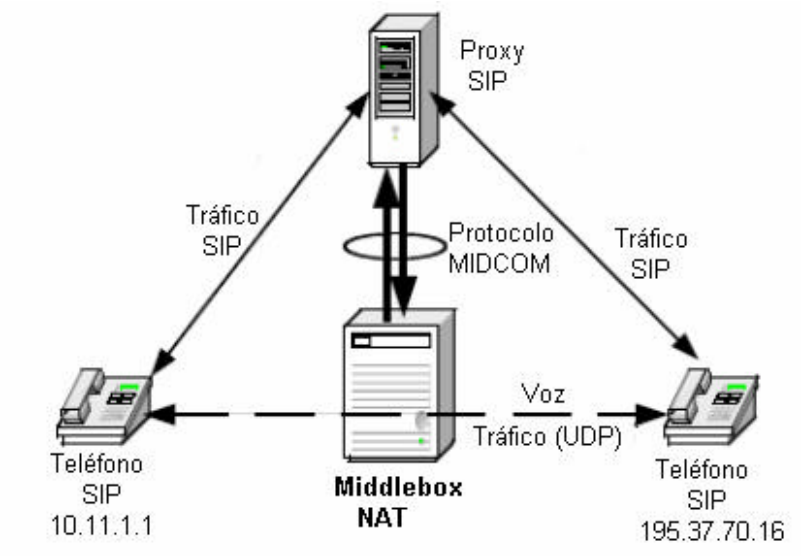

Figura 2.2. Escenario de Comunicación Middlebox.

El protocolo de comunicación intermedia no se ha terminado aún por el IETF.

La extracción de la inspección con estado y la manipulación de los paquetes de señalización del NATs y los firewalls (middleboxes) mejora la escalabilidad y a la larga, reducirá el costo de actualización de la red, debido a no tener que cambiar el firewall cada vez que cambien los protocolos. También existe una mejoría de funcionamiento que viene dado porque se le extraen al procesador dos tareas altamente intensivas (el análisis de VoIP y el filtrado de paquetes) en dos dominios separados de influencia.

Debe considerarse que el "middlebox" necesita protección contra atacantes. Si un intruso tomara el control de un agente midcom pudiera abrir cualquier puerto en el firewall y ganar acceso a la red privada. De modo que si un dispositivo de aplicación conciente (tal como un Proxy SIP) se sitúa fuera del firewall, un segundo firewall debe ser utilizado para proteger el dispositivo.

Controladores de fronteras de sesión.

Mientras que las pasarelas a nivel de aplicación pueden conllevar a preocupación desde el punto de vista de la escalabilidad, las soluciones "middleboxes" no han encontrado salida en los estándares y en productos comerciales tan rápido como se esperaba. En la ausencia de una solución universalmente aceptada a los problemas asociados con el paso a través de los firewall/NAT, los desarrolladores de productos han sacado una solución al mercado que se conoce como Controlador de Sesión, o Controlador de Frontera de Sesión (siglas en inglés SBC). Los SBCs son aplicaciones dedicadas que ofrecen uno o más de los siguientes servicios para un perímetro VoIP: Paso a través de firewall/NAT,

Control de Admisión de Llamada, monitoreo de los Acuerdos de Nivel de Servicio, soporte para una intercepción legal y protocolos de interfuncionamiento.

El análisis por terceras partes de esas soluciones no está ampliamente disponible todavía, pero a corto plazo, se espera que la demanda de estos productos crezca.

2.1.6 Efectos de los Firewall y los NATs sobre QoS.

Los Firewalls y los NATs pueden degradar la QoS en un sistema VoIP introduciendo demora y jitter, los NATs también pueden actuar como un cuello de botella en la red porque todo el tráfico es enrutado a través de un nodo simple. A continuación describiremos detalladamente estos problemas.

La VoIP es altamente sensible a la demora, de este modo un firewall necesita asegurar el tráfico de los datos, pero no puede incurrir en largos periodos de tiempo, incluso aquellos que pasan inadvertidos con el tráfico de datos simple. El problema no solo radica en lo rápido que pueda ser un firewall para interactuar con el tráfico de la red, sino en la velocidad que posea su procesador para encargarse de los paquetes VoIP. Dos aspectos de VoIP pueden causar un comportamiento degradado en la CPU del firewall.

Primero, el proceso de establecimiento de llamadas se tiene que realizar usando H.323 o SIP. Sin tener en cuenta el protocolo usado, los firewalls necesitan escarbar más profundo en estos paquetes para determinar su validez. Una inundación de paquetes de peticiones de llamadas, como resultado de un incremento en el volumen de llamadas o un ataque malicioso, puede intensificar este efecto. La presencia de un NAT agrava este problema porque la carga útil del paquete debe entonces cambiarse a nivel de aplicación para corresponderse con el origen traducido de NAT o las direcciones de destino y sus puertos. Todo este trabajo sobrecarga al procesador del firewall, el cual tiene que llevar a cabo todas estas tareas en un mínimo de tiempo, especialmente si son utilizadas las medidas de seguridad del protocolo, tal como la integridad del mensaje

El otro aspecto de VoIP que puede poner en tensión a la CPU del firewall es el abundante número de paquetes RTP que componen una conversación VoIP. Los firewalls raramente se preocupan por el tamaño de un paquete, pero puesto que cada paquete debe ser inspeccionado, una excesiva cantidad de estos pueden recargarlo. Por ejemplo, un firewall puede resistir 100 Mbit/seg (basado en una suposición de grandes paquetes) pero puede ser sobrecargado por un flujo de pequeños paquetes de 50 byte mucho antes de que su velocidad alcance los 100 Mbit/seg. Para evitar problemas de funcionamiento como los anteriores se diseñan firewalls que tienen en cuenta la QoS/VoIP.

No importa cuan rápida sea la conexión de la red, la CPU del firewall es un cuello de botella para todos los paquetes de red no encriptados. De este modo, una solución a este problema es usar VPN (Redes Privadas Virtuales) para todo el tráfico VoIP.

2.2 Encriptación e IPSec.

Hasta ahora nos hemos enfocado primariamente en la seguridad de la red, protegiendo puntos finales, pasarelas, y otros componentes, de ataques maliciosos. Firewalls, pasarelas, y otros dispositivos semejantes pueden ayudar a protegerse de intrusos que deseen comprometer una red, pero estos no son defensa contra el ataque de un hacker interno.

Otra capa de defensa es necesaria a nivel de protocolo para proteger los propios datos. En VoIP, como en redes de datos, esto puede ser logrado por encriptación de paquetes a nivel de IP usando IPSec. Por este camino, si cualquiera en la red, autorizado o no, intercepta tráfico VoIP no deseado para ellos (por ejemplo por la vía de un sniffer), estos paquetes serán indescifrables.

La suite de protocolos IPSec de seguridad y algoritmos de encriptación es el método estándar para asegurar paquetes contra un visualizador no autorizado sobre una red de datos. Por lo tanto, es lógico y práctico extender IPSec a VoIP, encriptando la señal y los paquetes VoIP en un extremo y descriptandola sólo cuando sea necesitada por su receptor. Pero la naturaleza de los protocolos de señalización y la propia red VoIP impide el uso de tal esquema simple, como ello llegue a ser necesario para enutadores, proxys, etc. para leer los paquetes VoIP.

También, varios factores, incluyendo la expansión del tamaño de los paquetes, cifrando la demora y una ausencia de urgencia de QoS en el mismo motor criptográfico puede causar una cantidad excesiva de demora en la entrega de paquetes VoIP. Esta conduce a un degrado en la calidad de voz, así una vez más existe un trueque entre seguridad y calidad de voz y necesidad de mayor velocidad. Afortunadamente, las dificultades no son insuperables. Experimentos patrocinados por NIST [27] ha mostrado que IPSec puede ser incorporado dentro de una red SIP con aproximadamente una demora adicional de tres segundos en el tiempo de establecimiento de la llamada, una demora aceptable para muchas aplicaciones. En los próximos epígrafes se explica los problemas involucrados con un buen resultado incorporando la encriptación de IPSec en servicios VoIP.

2.2.1 Sistemas de encriptación.

Desde que el hombre ha necesitado comunicarse con los demás ha tenido la necesidad de que algunos de sus mensajes solo fueran conocidos por las personas a quien estaban destinados. La necesidad de poder enviar mensajes de forma que solo fueran entendidos por los destinatarios hizo que se crearan sistemas de encriptado, de forma que un mensaje después de un proceso de transformación, lo que llamamos encriptado, solo pudiera ser leído siguiendo un proceso de desencriptado.

Los métodos de seguridad más populares utilizan la encriptación, el cual es el proceso de codificar la información de tal manera, que solo la persona (u ordenador) con una clave determinada, puede decodificarla y hacer uso de dicha información. La encriptación en ordenadores, está basada en la ciencia de la criptología, que ha sido usada a través de la historia con frecuencia. Antes de la era digital, los que más hacían uso de la criptología, eran los gobiernos, particularmente para propósitos militares. La existencia de mensajes codificados han sido verificados desde los tiempos

del imperio romano. Hoy en día, la mayoría de los sistemas de criptografía son aplicables a ordenadores, simplemente porque la complejidad de los algoritmos es demasiada para ser calculada por seres humanos.

Muchos de los sistemas de encriptación pertenecen a dos categorías:

- Encriptación de clave simétrica.
- Encriptación de clave pública.

Clave simétrica.

En este tipo de encriptación, cada ordenador tiene una clave secreta (como si fuera una llave) que puede utilizar para encriptar un paquete de información antes de ser enviada sobre la red a otro ordenador. Las claves simétricas requieren que sepas los ordenadores que van a estar hablando entre si para poder instalar la clave en cada uno de ellos.

Podemos entender una clave simétrica, como un código secreto que deben saber los ordenadores que se están comunicando para poder decodificar la información a su llegada. Como ejemplo sencillo, imagina que envías un mensaje a otra persona pero sustituyes ciertas letras por signos como asteriscos o interrogaciones. La persona que recibe el mensaje sabe de antemano que letras en particular han sido sustituidas con esos signos por lo que volviendo a ponerlas en su sitio, podrá leer el mensaje. Para los demás, la información no tendrá ningún sentido.

Clave pública.

Este método usa una combinación de una clave privada y una clave pública. La clave privada solo la sabe tu ordenador, mientras que la clave pública es entregada por tu ordenador a cualquier otro ordenador que quiere realizar una comunicación con el. Para decodificar un mensaje encriptado, un ordenador debe hacer uso de la clave pública, entregada por el ordenador original y su propia clave privada.

Una clave pública de encriptación muy popular es PGP (Pretty good Privacy) que permite encriptar casi todo.

Para implementar la encriptación de clave pública a gran escala, como puede ser un servidor Web, se necesita realizar otra aproximación. Aquí es donde entran los certificados digitales. La autoridad certificada actúa como un intermediario en el que ambos ordenadores confían. Confirma que cada ordenador es en realidad quién dice que es y entonces provee las claves públicas de un ordenador a otro.

Clave pública: SSL.

Una implementación de la encriptación de clave pública es SSL (Secure Sockets Layer). Originalmente desarrollada por Netscape, SSL es un protocolo de seguridad para Internet usado por navegadores y servidores Web para transmitir información sensitiva. Este se ha convertido en parte de un protocolo de seguridad general llamado TLS (Transport Layer Security).

En tu navegador, puedes saber si estás usando un protocolo de seguridad, como TLS por ejemplo, de varias formas. Podrás ver que en la barra de direcciones, las primeras letras “http”, serán reemplazadas con “https” y podrás ver un pequeño cerrojo en la barra de estado en la parte inferior del navegador.

La encriptación de clave pública conlleva mucha computación, por lo que muchos sistemas usan una combinación de clave pública y simetría. Cuando dos ordenadores inician una sesión segura, un ordenador crea una clave simétrica y la envía al otro ordenador usando encriptación de clave pública. Los dos ordenadores pueden entonces comunicarse entre ellos usando una encriptación de clave simétrica. Una vez que la sesión ha finalizado, cada ordenador descarta la clave simétrica usada para esa sesión. Cualquier sesión adicional requiere que una nueva clave simétrica sea creada por lo que el proceso es repetido.

Algoritmos de encriptación “hashing”.

La clave en una encriptación de clave pública está basada en un valor llamado hash. Este valor es computado a partir de un número usando un algoritmo llamado hashing. En esencia, este valor es una modificación del valor original. Lo más importante de un valor hash es que es casi imposible conocer el valor original sin saber los datos que se utilizaron para crear el valor hash.

Autenticación.

Este proceso, es otro método para mantener una comunicación segura entre ordenadores. La autenticación es usada para verificar que la información viene de una fuente de confianza. Básicamente, si la información es autentica, sabes quién la ha creado y que no ha sido alterada. La encriptación y la autenticación, trabajan mano a mano para desarrollar un entorno seguro.

Hay varias maneras para autenticar a una persona o información en un ordenador:

- **Contraseñas:** El uso de un nombre de usuario y una contraseña provee el modo más común de autenticación. Esta información se introduce al arrancar el ordenador o acceder a una aplicación. Se hace una comprobación contra un fichero seguro para confirmar que coinciden, y si es así, se permite el acceso.
- **Tarjetas de acceso:** Estas tarjetas pueden ser sencillas como si de una tarjeta de crédito se tratara, poseyendo una banda magnética con la información de autenticación. Las hay más sofisticadas en las que se incluye un chip digital con esta información.
- **Firma digital:** Básicamente, es una manera de asegurar que un elemento electrónico (e-mail, archivo de texto, etc.) es autentico. Una de las formas más conocidas es DSS (Digital Signature Standard) la cual está basada en un tipo de encriptación de clave pública la cual usa DSA (Digital Signature Algorithm). El algoritmo DSA consiste en una clave privada, solo conocida por el que envía el documento (el firmante), y una clave pública. Si algo es cambiado

en el documento después de haber puesto la firma digital, cambia el valor contra lo que la firma digital hace la comparación, invalidando la firma.

Recientemente, otros métodos de autenticación se están haciendo populares en varios medios que deben mantenerse seguros, como son el escaneo por huellas, escaneo de retina, autenticación facial o identificación de voz.

2.2.2 Latencia debido a la encriptación/desencriptación.

Los estudios realizados por Barbieri revelan el motor criptográfico como un embotellamiento para tráfico de voz transmitido sobre IPSec [2]. El factor controlador en el funcionamiento degradado producido por la criptografía eran los algoritmos de programación en el propio motor criptográfico, que serán tratados más adelante. Sin embargo, allí todavía era crítica la demora debido a la encriptación y desencriptación existente. Barbieri prepara un experimento controlado para medir el efecto de encriptación y desencriptación en rendimiento [2]. Ellos probaron cuatro algoritmos criptográficos en una íntegramente red VoIP con una conexión a 100Mbps (para anular los problemas de saturación) usando el mismo tráfico en forma simple como un estándar de comparación. Los algoritmos probados eran (en orden creciente de peso computacional) DES, 3DES, NULL (ninguna encriptación) + SHA-1 y 3DES +SHA-1. Los resultados mostraron que los algoritmos de poco peso computacional lograron mejor rendimiento que los de más peso. Las diferencias entre cada uno de los algoritmos representan la relativa demora asociadas con el tiempo computacional para cada algoritmo. El rango en el rendimiento es significativo, con una diferencia de aproximadamente 500 paquetes por segundo entre DES y 3DES + SHA-1 para un alto volumen de tráfico.

La latencia debido a la encriptación/desencriptación es un problema para cualquier protocolo criptográfico, debido a que la mayor parte de la latencia está fundamentalmente en el tiempo de computación requerido para la encriptación. La utilización de paquetes pequeños en VoIP a una alta velocidad e intolerancia a la pérdida de paquetes, maximizando el rendimiento es crítica. Sin embargo, esto tiene un precio, porque aunque DES (Data Encryption Standard) es el más rápido de estos algoritmos de encriptación, se rompe fácilmente. Reglas actuales del gobierno de los EE.UU prohíben el uso de DES para la protección de información. De este modo, los diseñadores se enfrentan al conflicto entre seguridad y calidad de voz. Dos soluciones a este problema están utilizando algoritmos de encriptación más rápidos (ver epígrafe 3.2.3) e incorporando QoS dentro del motor de criptográfico (ver epígrafe 3.2.4). La latencia trae menos problema para la gestión y/o los datos de señalización que para el tráfico del canal de voz.

2.2.3 Programación y la ausencia de QoS en el motor criptográfico.

El motor criptográfico es un severo cuello de botella en la red VoIP. El proceso de encriptación tiene un efecto debilitante en la QoS, pero este no es el factor extremo en el retraso. La fuerza fundamental, detrás de la latencia asociada con el motor criptográfico es el algoritmo de programación para paquetes que entran en el proceso de encriptación / descriptación. Mientras que los enrutadores y firewall se aprovechan de la QoS para determinar la prioridad de los paquetes, el motor criptográfico no proporciona soporte para la manipulación manual de los criterios de programación.

En el tráfico de datos común el problema es menor debido a que excesivamente más paquetes pasan a través del enrutador que por el motor criptográfico y el tiempo no es tan fundamental. Pero en VoIP, un número voluminoso de paquetes pequeños deben pasar a través del motor de criptográfico y el enrutador. Considerando los problemas de urgencia del tiempo en VoIP, el algoritmo de programación FIFO (First In, First Out) estándar empleado en los motores criptográficos en la actualidad generan serios problemas en la QoS.

Se ha señalado que el rendimiento del algoritmo de programación criptográfico actual es incrementado con el crecimiento del tamaño de los paquetes, concluyendo que programando un mayor número de paquetes tiene un efecto más degradante en el funcionamiento que la encriptación/desencriptación de menos paquetes (pero más grandes) [2]. VoIP con la utilización de muchos paquetes pequeños, provoca que el motor criptográfico alcance más rápidamente el punto de saturación comprometiendo el rendimiento. Esto lleva al comportamiento asintótico del rendimiento para el tráfico encriptado contra el ascenso continuo del tráfico simple y al incremento en la demora del trafico encriptado observado por Barbieri [2].

Estas violaciones de QoS derivadas del motor criptográfico son empeoradas por la presencia del tráfico de datos en una red VoIP. Este escenario será esperado, debido a que una de las motivaciones en el desarrollo de VoIP es la habilidad de que voz y datos compartan la misma red. Los experimentos de Barbieri muestran que tal combinación de tráfico tiene efectos desastrosos en VoIPSec. Esto es especialmente verdadero si los datos heterogéneos necesitan ser encriptados y desencriptados. Puesto que el motor criptográfico no tiene ninguna funcionalidad para cambiar su propio esquema de prioridad basado en el tipo de tráfico que es presentado, los paquetes VoIP están en función del algoritmo de programación FIFO y son a menudo dejados esperando detrás de paquetes heterogéneos largos, a pesar de la menor urgencia de estos paquete grandes. El patrón no uniforme del tráfico de datos también contribuye al incremento del jitter en VoIP.

La variación en el uso del ancho de banda causada por paquetes heterogéneos inflige descontrol total con los tiempos de demora de los medianamente uniformes paquetes VoIP, provocando su arribo en ráfagas. Si estas ráfagas exceden el mecanismo de tiempo asociado con el Buffer, entonces puede ocurrir la pérdida de paquetes. El desarrollo de "schedulers" criptográficos conscientes VoIP aliviaría este problema.

2.2.4 IPSec.

IPSec es una extensión al protocolo IP, que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4. La arquitectura IPSec se describe en el RFC 2401.

IPSec emplea dos protocolos diferentes (AH y ESP) para asegurar la autenticación, integridad y confidencialidad de la comunicación. Este puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula

completamente dentro de un nuevo datagrama IP que emplea el protocolo IPSec. En modo transporte, IPSec sólo maneja la carga del datagrama IP, insertándose la cabecera IPSec entre la cabecera IP y la cabecera del protocolo de capas superiores (vea Figura 2.3).

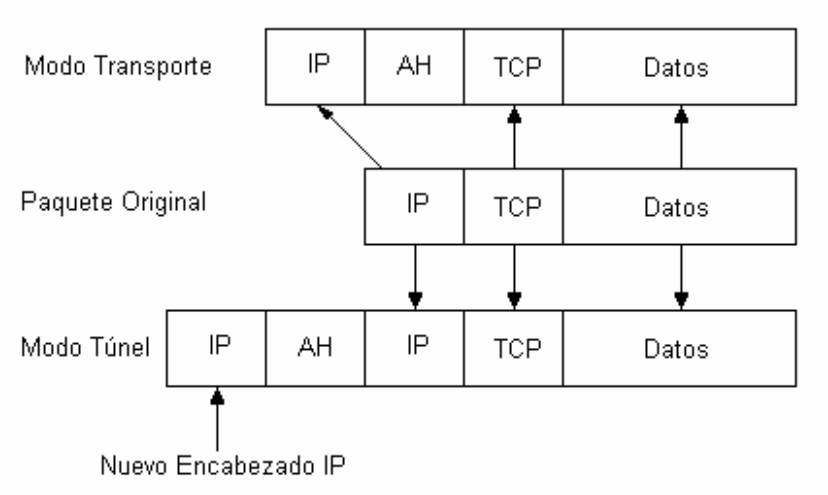

Figura 2.3. IPsec: Modos Túnel y Transporte.

Para proteger la integridad de los datagramas IP, los protocolos IPSec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC, son sus siglas en ingles). Para el cálculo de estos, los protocolos HMAC emplean algoritmos de resumen como MD5 (Message-Digest Algorithm 5) y SHA (Secure Hash Algorithm) para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPSec y el receptor del paquete puede comprobar en el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de los datagramas IP, los protocolos IPSec emplean algoritmos estándar de cifrado simétrico. El estándar IPSec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish.

Para protegerse contra ataques por denegación de servicio, los protocolos IPSec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPSec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en Asociaciones de Seguridad (SA). Las SA, a su vez, se almacenan en Bases de Datos de Asociaciones de Seguridad (SAD).

Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPsec resultante. Estas son las direcciones IP de los participantes de la comunicación IPsec que protegen los paquetes.
- Protocolo IPsec (AH o ESP). A veces, se permite compresión (**IPCOMP**).
- El algoritmo y clave secreta, empleados por el protocolo IPsec.
- Índice de parámetro de seguridad (SPI). Es un número de 32 bits que identifica la asociación de seguridad.

Algunas implementaciones del SAD permiten almacenar más parámetros, como son:

- Modo IPSec (Túnel o T ransporte).
- Tamaño de la ventana deslizante para protegerse de ataques por repetición.
- Tiempo de vida de una SA.

En una SA se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única SA sólo se puede proteger un sentido del tráfico en una comunicación IPSec full duplex. Para proteger ambos sentidos de la comunicación, IPSec necesita de dos asociaciones de seguridad unidireccionales.

Las asociaciones de seguridad sólo especifican cómo se supone que IPSec protegerá el tráfico. Para definir qué tráfico proteger y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la Política de Seguridad (SP), que a su vez se almacena en la Base de Datos de Políticas de Seguridad (SPD).

Una SP suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transporte estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.
- Protocolos y Puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.
- La SA a emplear para proteger los paquetes.

La configuración manual de la asociación de seguridad es proclive a errores y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Uno de los problemas críticos a los que se enfrenta el administrador de sistemas es el intercambio de claves: ¿Cómo intercambiar claves simétricas cuando aún no se ha establecido ningún tipo de cifrado?

Para resolver este problema se desarrolló el protocolo IKE. Este protocolo autentica a los participantes en una primera fase. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad.

Los protocolos IPSec.

Como mencionamos anteriormente la familia de protocolos IPsec está formada por dos protocolos, el **AH** y el **ESP**. Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50. Las siguientes secciones tratarán brevemente sobre sus propiedades:

El protocolo AH

AH protege la integridad del datagrama IP. Para conseguirlo, dicho protocolo calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete, la cual se muestra en figura 2.4.

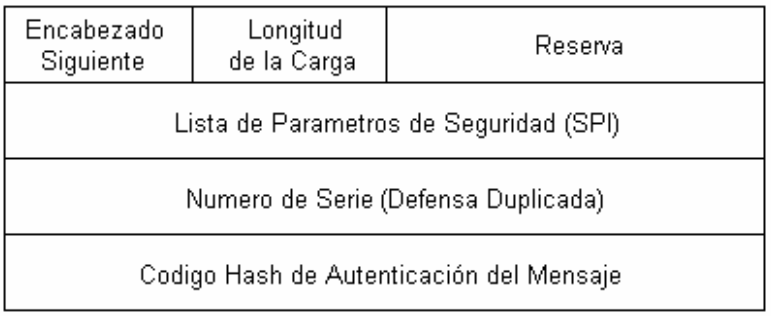

Figura 2.4. La cabecera AH protege la integridad del paquete.

El protocolo AH protege la cabecera IP (incluyendo sus partes inmutables, como son las direcciones IP), por lo que no permite NAT. NAT reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPSec Traversal NAT implementa métodos que evitan esta restricción.

El protocolo ESP.

ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes y se muestra en figura 2.5.

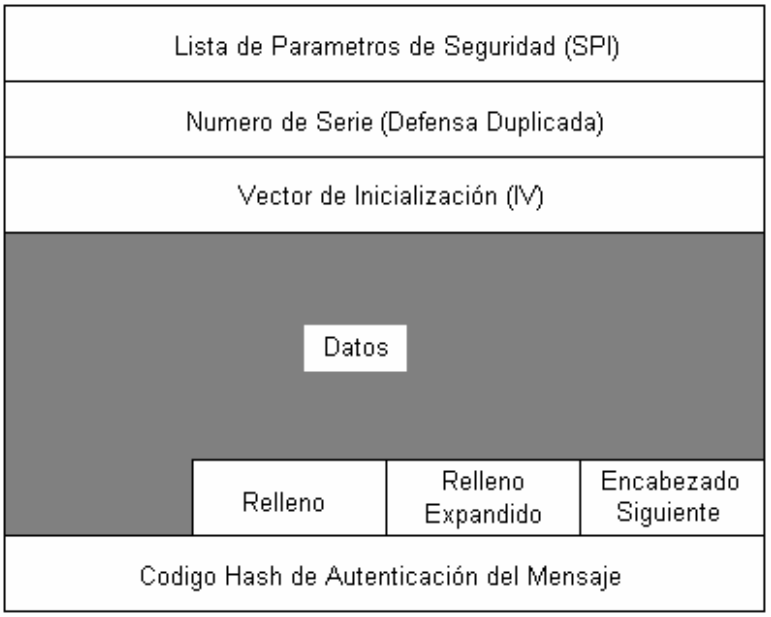

Figura 2.5 Cabecera ESP.

Los primeros 32 bits de la cabecera ESP especifican el SPI. Este SPI especifica qué SA emplear para desencapsular el paquete ESP. Los siguientes 32 bits almacenan el Número de Secuencia. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el Vector de Inicialización (IV) que se emplea para el proceso de cifrado. Los algoritmos de cifrado simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IVs. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPSec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes Siguiente cabecera que especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo.

El uso de NAT, por lo tanto, no rompe el protocolo ESP. Sin embargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPSec. Traversal NAT ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

El protocolo IKE.

IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. El protocolo IKE funciona en dos fases. La primera fase establece una Asociación de Seguridad del Protocolo de Gestión de Claves de Asociaciones de Seguridad en Internet (ISAKMP SA). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPSec.

La autenticación de los participantes en la primera fase suele basarse en Claves Compartidas con Anterioridad (PSK), claves RSA y Certificados X.509 (**racoon** puede realizar esta autenticación incluso mediante Kerberos).

La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y por lo tanto, es susceptible a un ataque de escucha clandestina (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a PSK. Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia SA basándose en la ISAKMP SA. Este a su vez proporciona autenticación para protegerse de ataques de escucha clandestina. Esta segunda fase emplea el modo rápido. Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPsec SAs unidireccionales.

Asociaciones de seguridad de Intercambio de claves de Internet.

El protocolo IKE está diseñado para establecer de manera segura una relación de confianza entre dos equipos, negociar las opciones de seguridad y generar de manera dinámica material de claves criptográficas secretas compartidas. Las SA proporcionarán autenticidad, integridad y opcionalmente, cifrado de los paquetes IP que se envían mediante la asociación de seguridad.

IKE negocia dos tipos de asociaciones de seguridad:

- Una SA de modo principal. La asociación de seguridad IKE que se utiliza para proteger la propia negociación IKE.
- Asociaciones de Seguridad IPSec. Las asociaciones de seguridad que se utilizan para proteger el tráfico de la aplicación.

Se pueden configurar las opciones de directivas IPSec para ambos tipos de asociaciones de seguridad. El servicio IPSec interpreta una directiva IPSec y la amplía a los componentes que necesita para controlar la negociación IKE. La directiva IPSec contiene una definición de un filtro de paquetes. El filtro de paquetes se interpreta de dos formas: una utiliza sólo la dirección y la información de identidad para permitir a IKE establecer una asociación de seguridad de modo principal (la asociación de seguridad IKE); la otra permite a IKE establecer las asociaciones de seguridad IPSec (también conocidas como asociaciones de seguridad de modo rápido).

2.2.5 Papel de IPSec en VoIP.

El predominio y la facilidad de sniffing de paquetes y de otras técnicas utilizadas para la captura de paquetes en una red IP hacen la encriptación una necesidad para VoIP. La seguridad en VoIP comprende la protección de las dos partes que establecen la comunicación. El protocolo IPSec puede ser usado para lograr ambos objetivos mientras es aplicado con ESP usando el método de túnel. Este asegura las identidades de ambos terminales y protege los datos de voz de usuarios prohibidos una vez que los paquetes salgan de la Intranet corporativa. La incorporación de IPSsec dentro de IPv6 tiene la intención de incrementar la disponibilidad de encriptación, aunque existen otras vías para asegurar estos datos a nivel de la aplicación.

VoIP usando IPsec (VoIPSec) ayuda a reducir los ataques hombre en el medio, sniffers de paquetes y muchos tipos de análisis de tráfico de voz. Combinado con las implementaciones de firewall, IPSec hace a VoIP más seguro que una línea de teléfono estándar, donde las personas generalmente asumen que la necesidad de acceso físico para espiar una línea de telefónica es un impedimento suficiente. Es importante destacar, sin embargo, que IPSec no es siempre bueno para ciertas aplicaciones, así algunos protocolos continuarán confiando en sus propias características de seguridad.

2.2.6 Dificultades surgidas desde VoIPSec.

IPSec había sido incluido en IPv6, puesto que es un método de implementación confiable, robusto y extenso para la protección de datos y autenticación del emisor. Sin embargo, existen varios problemas asociados con VoIP que no son aplicables al tráfico de datos normal. Entre los principales están demora, jitter y pérdida de paquetes. Estos problemas son introducidos dentro del ambiente VoIP porque este es una transferencia de medios de comunicación en tiempo real, con solamente 150 ms para enviar cada paquete. En transferencia de datos estándar sobre TCP, si un paquete es perdido, puede ser reenviado por petición. En VoIP, no existe tiempo para hacer esto.

Los paquetes deben llegar a su destino y deben de llegar rápidamente. Por supuesto los paquetes deben también estar seguros durante su viaje, así la introducción de VoIPSec. Sin embargo, el precio de esta seguridad es una decisiva caída en QoS causada por varios factores.

Un estudio realizado en el 2002 por investigadores de la universidad de Milán [2] se centraba en el efecto de VoIPSec en varios problemas de QoS y en el uso de la compresión de cabeceras como una solución a estos problemas. Estudiaron varios codecs, algoritmos de encriptación y patrones de tráfico para acumular una amplia descripción de estos efectos.

También están disponibles algunos resultados empíricos desarrollados por Cisco, como[9]:

Demora.

- Procesamiento - PCM a G.729 a paquete.
- Encriptación - encapsulación ESP + 3ES.
- Serialización - tiempo que toma llevar un paquete fuera del enrutador, cada "salto" generalmente tiene una demora fija:
  - Sobrecabecera IPSec: Alrededor de 40 bytes.(dependiendo de la configuración).
  - Cabecera IP: 20 bytes.
  - Cabeceras UDP+RTP: 20 bytes.
  - Compresión de la cabecera RTP: 3 bytes para IP+UDP+RTP.

Efectos en codecs de 8 Kbps (datos de voz: 20 bytes)

- Texto de voz en claro tienen una sobrecabecera de 3 bytes, que sugiere un ancho de banda requerido de aproximadamente 9 Kbps.
- Encriptación IPSec de voz: sobrecabecera de 80 bytes y requiere de 40 Kbps de ancho de banda.

2.3 Incompatibilidad IPSec y NAT.

Una de las barreras más grandes del despliegue de IPSec es la presencia de un NAT. IPSec autentica las PC; un NAT las oculta. Por lo que los propósitos de ambos están a menudo en desacuerdo. Debido a la confianza en los NATs, en la mayoría de las redes IPv4, hay una dificultad enorme para conseguir que IPSec trabaje correctamente sobre los dispositivos NAT. De hecho, haciendo a voluntad los dos trabajos juntos se puede agilizar la adopción de IPSec.

Lograr con IPSec atravesar un NAT es más difícil de lo que se piensa.

Tres problemas se manifiestan sobre IPSec y NAT:

Violación de la integridad AH. AH almacena la firma digital del paquete antes de que salga del destino. Si ese paquete pasa entonces a través de un NAT (local o alejado), su cabecera IP será modificada. El receptor, cuando calcula su propia versión de la firma del paquete, generará un resultado diverso, porque el NAT modificó el direccionamiento de la fuente. Por lo tanto el receptor desechará el paquete.

Ayudante de IPSec. Muchas de las pequeñas pasarelas/NAT incluyen una característica llamada "ayudante de IPSec" (o "pasaje a través de IPSec"). Diseñado originalmente para el modo del túnel, sus características también actúan en modo transporte. Si los múltiples ordenadores detrás de la pasarela crean asociaciones de seguridad IPSec de destinos fuera de esta, la pasarela transmitirá todo el tráfico entrante IPSec al primer ordenador que creó esta asociación segura. La

función del ayudante de IPSec simplemente recuerda qué ordenador en el interior inició una conversación IPSec y remite todo el tráfico entrante a este, sin modificarlo.

Fragmentación de IKE. Es común que la carga útil de un certificado digital exceda el tamaño de una trama IP. Siempre que una aplicación genere un paquete de datos más grande que una trama IP, IP fragmenta el paquete de modo que cada uno de los fragmentos se ajusten en una simple trama. Mientras que esto está muy bien dentro de una red local, los dispositivos de los bordes de la red (incluyendo muchos NATs) eliminan fragmentos porque los fragmentos malignos preelaborados son una manera popular de evadir algunos firewalls. Los fragmentos que NAT elimina, evitan que IKE trabaje correctamente.

La compatibilidad de IPSec y NAT está distante de ser ideal. Traversal NAT invalida completamente el propósito de AH porque la dirección origen de la máquina detrás del NAT es enmascarada del mundo exterior. De esta manera, no existe forma para autenticar el remitente verdadero de los datos. El mismo razonamiento demuestra la inoperatividad de la autenticación origen en ESP. Esto se ha definido como una característica esencial de VoIPSec, de modo que esto es un serio problema.

Existen muchos otros problemas que se originan cuando el tráfico ESP intenta cruzar un NAT. Si sólo uno de los terminales está detrás de un NAT, la situación es más fácil. Si ambos están detrás de los NATs, la negociación IKE puede ser utilizado para Traversal NAT, con encapsulación UDP de los paquetes IPSec.

2.4 Redes Privadas Virtuales.

La VPN, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet. Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación, para esto las VPN necesitan una serie de requerimientos básicos entre los que encontramos Identificación de Usuario, Codificación de Datos, Administración de claves y Soporte a Protocolos Múltiples.

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto.

Este es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura ¨dial-up¨ (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos módems. Lo común es que sea una red privada virtual.

VPN interna WLAN.

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

VPN punto a punto.

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Este punto es el más común, también llamada tecnología de túnel o tunneling.

Tunneling.

Internet se construyó desde un principio como un medio inseguro. Muchos de los protocolos utilizados hoy en día para transferir datos de una máquina a otra, a través de la red, carecen de algún tipo de cifrado o medio de seguridad que evite que nuestras comunicaciones puedan ser interceptadas y espiadas. Esto supone un grave problema, a fin de evitar que alguien pueda interceptar nuestra comunicación por medio de la técnica de escucha clandestina (man in the middle), como es el caso de la red de redes. Esto es tan simple como utilizar un sniffer, con el cual se podrá recibir y analizar todos los paquetes que circulen por dicha red. Si alguno de esos paquetes pertenece a un protocolo que envía sus comunicaciones en claro y contiene información sensible, dicha información se verá comprometida.

Si por el contrario, ciframos nuestras comunicaciones con un sistema que le permita entenderse sólo entre las dos máquinas que queremos sean partícipes de la comunicación, cualquiera que intercepte desde una tercera máquina nuestros paquetes, no podrá hacer nada con ellos, al no poder descifrar los datos. Una forma de evitar el problema que nos atañe, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, es usar una útil técnica llamada tunneling.

Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser Secure SHell (SSH), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura, el túnel por el cual enviamos nuestros datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos.

2.4.1 Túneles VPN local.

El túnel de IPSec ESP, es un tipo específico de VPN usado para atravesar un dominio público (la Internet) de manera privada. Muchas implementaciones de VoIP han intentado hacer uso de otras técnicas de VPN, incluyendo túneles VPN dentro de una intranet. El uso y beneficios de VPNs en IPSec han sido bastante colosal para algunos afirmando "VoIP es una implementación asesina para VPNs" [12]. Túneles VPN dentro de una LAN corporativa o WAN (Wide Area Network) son generalmente mucho más seguros y rápidos que VPNs IPSec a través de Internet, debido a que los datos nunca cruzan el dominio público, pero ellos no son escalables. Este en tipo de implementación tiene un límite físico en el tamaño de la red privada y como VoIP quiere ser más extenso, no es práctico una implementación para estimar llamadas fuera de la red local como una caja negra. También, no importa como el VPN sea preparado, los mismos tipos de ataques y problemas asociados con VPNs IPSec son aplicables.

2.4.2 Redes Privadas Virtuales y Firewall.

Las VPNs alivian muchos de los asuntos de problemas de los túneles directamente a través de firewall. Por lo tanto, muchos de los problemas específicos de firewall mencionados aquí, se convierten en discusión. Sin embargo, este método poco elegante tiene ciertos inconvenientes. En primer lugar, construyendo un túnel todo el trafico VoIP sobre VPNs prohíbe al firewall analizar los paquetes entrantes y salientes para evitar tráfico malicioso. También, la centralización de seguridad del firewall se pierde virtualmente. Túneles VPN con IPSec pueden ser incompatibles con NAT. Finalmente, un host de nueva QoS y problemas de seguridad se introduce por la integración de IPSec en VoIP.

2.5 Tamaño del paquete expandido.

IPSec también aumenta el tamaño de los paquetes en VoIP, lo cual conduce a más problemas de QoS. Se ha demostrado que el aumento del tamaño de los paquetes incrementa el rendimiento a través del motor criptográfico, pero sacar en conclusión que el aumento del tamaño de los paquetes debido a IPSec conduce a un rendimiento mejor es una falacia. La diferencia es que el aumento en el tamaño de los paquetes pequeños debido a IPSec no es consecuencia de un incremento en la capacidad de la carga útil. El aumento en realidad se debe a un aumento en el tamaño de la cabecera debido a la encriptación y encapsulación de la cabecera vieja IP y la introducción de la nueva cabecera IP más la información de encriptación.

Esto conduce a varias complicaciones cuando IPSec es aplicado a VoIP. En primer lugar, el ancho de banda efectivo es disminuido tanto como un 63 %. Así las conexiones a usuarios simples en áreas de ancho de banda bajas (es decir vía módem) puede hacerse no factible. La diferencia de tamaño puede también causar problemas de demora y Jitter cuando los paquetes son retrasados por la disminución del rendimiento de la red o cuellos de botella en los nodos en la red (tales como enrutadores o firewalls).

CAPITULO 3: Aspectos a considerar sobre la seguridad en el despliegue de VoIP en Cuba.

En este capitulo se muestran las soluciones a los problemas de seguridad planteados en el capitulo 1. También se exponen soluciones a los temas VoIPSec, para lograr el establecimiento de una implementación segura. Se toman en consideración normas generales que son recomendadas por NIST, las cuales permiten dar los primeros pasos en la implementación de seguridad en una Red VoIP. Esto observado bajo la óptica de mantener una relación entre la QoS y la seguridad, punto de gran importancia en la implementación de seguridad en dichas redes.

3.1 Soluciones a los problemas de seguridad en VoIP.

Las soluciones especifican las técnicas y herramientas que se pueden implementar para la defensa frente a los ataques o vulnerabilidades presentados previamente. Saber cómo pueden atacar (y desde dónde), es tan importante como saber con qué soluciones se cuenta para prevenir, detectar y reparar un ataque de red. No se debe olvidar que éstas siempre son una combinación de herramientas que tienen que ver con la tecnología, en la que se centra este estudio y con los recursos humanos (políticas, formación, concienciación, capacitación, tanto de los usuarios como de los administradores de la red).

En el primer capitulo mencionamos algunas amenazas que acechan a los sistemas de comunicaciones. No obstante, con cada amenaza hay partes de tecnología que podemos usar conjuntamente para hacer nuestros sistemas seguros [18]. Si nos fijamos de nuevo en las amenazas, veamos que podemos hacer para contrarrestarlas:

• **Rechazo del servicio o Denegación del servicio (DoS):** No hay una solución integrada para los ataques de rechazo de servicio. No obstante, la industria tiene un mejor conocimiento de sus fallos. En muchos casos, los ¨bugs¨ en la instalación de pilas de protocolos en la red dan lugar a una debilidad explotable. Se están corrigiendo rápidamente mediante parches software.

• **“Piratería” o ataque de intrusos:** Podemos usar firewalls e IDS, complementados por potentes sistemas de autentificación para decidir a quién está permitido hacer qué y a quién se le permite acceder a qué. Cuando estos estén instalados adecuadamente, las principales herramientas de un pirata serán inútiles. La opción de engañar a un firewall para permitir acceso privilegiado se elimina mediante el uso de una potente autentificación y el ámbito de acceso de una conexión no autentificada, se limita mediante reglas de filtrado y análisis de protocolo.

• **Virus y gusanos:** El software de detección de virus ha tenido gran éxito en la erradicación de la mayoría de los virus conocidos, ahora se están equipando los firewall para que detecten virus. Los gusanos se aprovechan de las debilidades de los sistemas de redes; La mayoría de estas debilidades se han corregido (o se están corrigiendo). Además, podemos usar firmas digitales para autentificar el software y para suministrar mejor información sobre la fuente de un programa.

• **Escucha clandestina:** Se puede frustrar utilizando codificación. Siempre que las claves se compartan sólo por aquellos que deberían tener acceso a los datos y que el sistema use buenos principios de seguridad (por ejemplo, usando claves con buenas propiedades, suficientemente aleatorias), entonces estos sistemas tienen un excelente registro de seguimiento.

• **Ataques activos:** Estos ataques son completamente imposibles de efectuar, si se usa una fase de autentificación unida criptográficamente a la sesión de comunicación. Un ejemplo clásico es usar certificados de clave pública para autentificar un intercambio de clave de Diffie-Hellman; después, las claves producidas se utilizan para codificar el resto de la sesión. Un atacante activo no puede jugar a "quedarse en el centro", ya que no se puede autentificar a los participantes de la comunicación. Un riesgo común es no unir la sesión de comunicación a la etapa de autentificación. Esto puede dar lugar a ataques activos de piratería cuando una sesión está a mitad de camino o al menos después de la fase de autentificación.

• **Ataques de usurpación:** La autorización basada en una potente autentificación evitará a la gente engaños de un usuario con privilegios deseados.

• **Alteración de paquetes:** Los paquetes de la red pueden tener sus propias verificaciones de integridad asociadas que evitan efectivamente estos tipos de ataques. Por ejemplo, IPSec tiene un modo que crea un resumen en cada paquete. El destinatario descarta cualquier paquete en el cual falla la verificación.

Los administradores de los sistemas disponen de herramientas para descubrir las vulnerabilidades existentes y para controlar que "todo vaya bien", si los procesos son los normales o si hay movimientos sospechosos en la red o en los sistemas. Por ejemplo, que un usuario esté recurriendo a vías de acceso para las cuales no está autorizado o que alguien intente ingresar en un sistema repetidas veces con claves erróneas que esté probando.

Debe tenerse en cuenta que muchas de las utilidades o técnicas presentadas son a su vez empleadas por los atacantes o ¨hackers¨, pero es este motivo el que las hace realmente útiles desde el punto de vista de la protección, ya que uno de los métodos más efectivos a la hora de proteger el entorno de red se basa en la simulación de un ataque real de intrusión por parte de los administradores (Penetration Test). De esta forma podrá saberse hasta donde puede llegar un intruso que posea ciertas herramientas disponibles libremente en Internet.

A continuación realizaremos un análisis de protecciones y herramientas de seguridad de la familia de protocolos TCP/IP.

Escaneo de puertos.

Al igual que con la mayoría de los ataques cuyo objetivo es obtener información que permita identificar los sistemas y redes a atacar, la detección pasa por la utilización de sistemas IDS. Dado que NMAP (Network Mapper) es una de las herramientas de ataque por excelencia, SNORT supone la competencia por parte de la defensa.

Dicho ataque debe realizarse con cautela, ya que es muy sencillo determinar que se está produciendo, ya que bajo condiciones normales de funcionamiento no se realiza un acceso secuencial a todos los posibles puertos en un rango determinado. Asimismo, existen aplicaciones como PortSentry que pueden tanto detectar el ataque como responder a él, por ejemplo, modificando el módulo de filtrado del sistema atacado para desechar el tráfico provinente del sistema atacante.

Por otro lado, los firewalls suelen incluir un módulo de detección de ataques, aunque no todos tienen la misma prioridad o validez. Por ejemplo, el escaneo basado en SYN puede ser detectado, pero no así el basado en paquetes de FIN. Para poder detectar estos ataques es necesario revisar el resultado de los logs de los firewalls, cuyo tamaño suele ser elevado, por lo que existen herramientas que facilitan estas tareas. También se han creado utilidades que ejecutan sobre productos de filtrado ya existentes, como la utilidad alert.sh preparada para Firewall-1 de Checkpoint.

Desde el punto de vista del escaneo de las vulnerabilidades, la mejor defensa es **disponer de las herramientas empleadas en un ataque, para su descubrimiento y proceder de manera proactiva a solucionar o eliminar la existencia de la vulnerabilidad**, ya sea eliminando el servicio o sustituyéndolo por una versión posterior corregida.

Sniffing, eavesdropping y snooping

La protección básica frente a la extracción mediante sniffers de la información que viaja en los paquetes de datos por la red se basa en la encriptación de la información. A lo largo del texto se analizan diferentes protocolos de comunicaciones que hacen uso de ésta: SSL, S/MIME, SSH, IPSec.

La capacidad intrínseca de los sniffers se encuentra en el propio diseño de las redes de difusión, como por ejemplo ethernet. Una protección frente a esta situación se basa en emplear redes conmutadas en lugar de compartidas, donde los elementos de red, en este caso los conmutadores, segmentan la red para cada uno de los puertos, es decir, que si se dispone de un equipo por puerto (no existen concentradores), un sniffer será capaz solo de visualizar el tráfico destinado al sistema en el que está ubicado. Estos equipos son capaces de crear segmentaciones de la red por grupos de equipos, en base a una distribución lógica en lugar de física, denominadas redes locales virtuales (VLANs). En este caso, el sniffer solo podría visualizar el tráfico destinado a algún equipo de ese grupo o VLAN. Por último, debe considerarse que los conmutadores disponen de la posibilidad de configurar un puerto de monitorización, mediante el cual se volvería a la situación anterior, en la que sería posible visualizar el tráfico de todas las VLANs a través de un punto único.

Encriptación: SSL, PGP, S/MIME

La protección de la información que circula por la red en claro, sólo puede ser protegida frente a las vulnerabilidades asociadas al sniffing, eavesdropping o snooping a través de técnicas de encriptación.

Se comenzará el análisis de esta técnica con el protocolo de seguridad SSL, por ser el más extendido actualmente, principalmente en las comunicaciones encriptadas de conexión a los servidores Web y por ser muy similar a otros

protocolos de encriptación qué se diferencian principalmente en el protocolo de aplicación hacia el que van enfocados, como por ejemplo S/MIME para la transmisión segura de e-mails.

Todos ellos se basan en la aplicación de algoritmos de encriptación asimétricos, mediante la utilización de una clave pública y una privada. Además, pueden verse potenciados por el establecimiento de una infraestructura PKI.

A grandes rasgos y desde un punto de vista práctico, los protocolos que funcionan bajo el mismo principio son:

- SSL: comunicaciones entre navegadores Web y servidores Web, o entre los propios servidores.
- PGP: encriptación de correos electrónicos.
- S/MIME: envío y recepción de mensajes electrónicos.
- SSH: comunicaciones de establecimiento de sesiones (de tipo carácter y gráficas) así como transferencia de ficheros (ver apartado específico).
- IPSec: comunicaciones seguras entre dispositivos de red: clientes, enrutadores, firewalls, etcétera. Permiten el establecimiento de VPNs.

La teoría alrededor de la encriptación es muy extensa, por lo que simplemente se mostrarán las nociones básicas, para analizar más en detalle el propio SSL. Antes de SSL existieron protocolos más específicos orientados a las transacciones Web.

Cuando se habla de encriptación debe siempre tenerse en cuenta los problemas de exportación impuestos por EEUU sobre todas las técnicas, algoritmos, software, etcétera, relacionado con la misma. Por tanto, se habla de "la inseguridad de los programas de seguridad estadounidenses", ya que el objetivo de este gobierno es no permitir el uso externo de algoritmos de encriptación lo suficientemente potentes (normalmente definido por el número de bits de la clave) como para impedirles a ellos el análisis de la información enviada. El máximo nivel permitido hasta hace algunos meses (64 bits en el algoritmo DES) perdió confiabilidad desde que se logró vulnerarlo.

El problema original a la hora de establecer una comunicación encriptada entre dos partes era el intercambio de las claves de una forma segura, ya que al utilizarse inicialmente sistemas de clave privada o simétricos, ambas partes debían compartir la misma clave. Una alternativa a este método, es el uso de sistemas de clave pública o asimétricos, que se basan en la existencia de dos claves, una pública y una privada, ambas complementarias.

Asimismo, dan lugar a la creación del concepto de certificado digital (X.509v3): información de encriptación (clave pública) asociada a un nombre o entidad específica y firmada por un tercero fiable.

En el caso de la Web, los certificados digitales van asociados a una URL (Uniform Resource Locators) concreta y contienen un número de serie, una fecha de expiración, varias extensiones criptográficas y la clave pública del servidor Web. La validez del certificado se obtiene al estar firmado por la clave privada de una Autoridad de Certificación (CA) reconocida oficialmente. Un certificado permite encriptar la información (confidencialidad o privacidad), firmarla

(autenticación) y asegura la integridad de sus contenidos. El protocolo SSL emplea esta técnica para encriptar la información trasmitida entre el cliente y el servidor.

Sistemas de Detección de Intrusos (IDS).

Además de los mencionados parches, una de las herramientas existentes hoy en día que proporciona un mayor control sobre la seguridad son los IDS, también conocidos como NIDS (Network IDS), ya que pretenden contemplar dentro de sus comprobaciones todas y cada una de las vulnerabilidades que se van descubriendo a nivel de TCP/IP y de los servicios de red. Asimismo, ciertos IDS permiten la introducción de nuevos patrones (signatures), de forma que es posible ampliar la base de datos de vulnerabilidades en el momento en que aparecen y no tener que esperar a que el fabricante distribuya una actualización.

Los IDSs suelen conformarse mediante un sistema de gestión centralizado y agentes o monitores remotos que se encargan de analizar el tráfico en los puntos remotos de la red en los que están ubicados. Asimismo, la seguridad de estos sistemas se incrementa al trabajar las interfaces por las que se realiza la monitorización en modo pasivo, es decir, no actúan como destino de ningún tráfico (no disponen de dirección IP), por lo que un atacante no puede detectar su existencia. A su vez, a través del control del tráfico en los enrutadores de los bordes de la red se puede mitigar la obtención de información basada en ICMP (Internet Control Message Protocol), como la franja horaria o la máscara de subred empleada.

Algunos sistemas más avanzados son capaces de modificar de forma dinámica las listas de control de acceso en los enrutadores y firewalls en el momento de detectarse el ataque, con el objetivo de filtrar el tráfico asociado al mismo. Por ejemplo, Cisco Secure IDS emplea esta técnica junto a los enrutadores Cisco y al firewall Cisco PIX.

IP Spoofing.

Mediante la configuración de filtros de conexiones permitidas, especificando a través de qué interfaces, en los dispositivos de interconexión de varias redes (firewalls y screening routers), se pueden controlar las direcciones IP fuente permitidas y por tanto evitar la técnica de IP Spoofing.

Los organismos que realmente pueden evitar el uso de ésta técnica son los propietarios de las redes troncales (backbones) de comunicación, normalmente carriers u operadores de telecomunicaciones, ya que evitan desde su origen que un agresor pueda hacerse pasar por otro usuario. Al actuar de nexo de unión de las diferentes subredes, deben permitir únicamente que el tráfico saliente de cada red al troncal lleve asociada una dirección propia de la red desde la que sale. Así se controla el punto de inicio del IP Spoofing.

DoS y DDoS (Ataque de Denegación de Servicio Distribuido)

La defensa ante los ataques DoS no es directa, ya que se basan en vulnerabilidades inherentes al diseño del protocolo TCP/IP. Pese a eso, existen herramientas de detección de intrusos que son capaces de reconocer las huellas dejadas por las herramientas de DDoS, por ejemplo, al llevarse a cabo la comunicación desde el atacante a la hora de invocar la ejecución de ciertos comandos en remoto. De esta forma se podrá tener constancia de la infección antes de que se lleve a cabo el ataque masivo desde esos sistemas.

Podría ser posible el identificar a los atacantes mediante una combinación de técnicas de auditoria y referencias cruzadas de los ficheros de log, junto a la escucha en los IRCs (Internet Relay Chat) de hacking.

Net Flood.

En este caso la red objetivo no puede hacer nada, ya que aunque se filtre el tráfico, las líneas estarán realmente saturadas con tráfico del atacante, por lo que estarán incapacitadas para cursar tráfico útil.

El método de actuación debería basarse en contactar con el operador que suministra el servicio de conexión a Internet para determinar la fuente del ataque y de ser posible, para que lo filtre en su extremo de la conexión (upstream) de mayor capacidad. Una vez localizada la fuente y siempre que no se haya combinado con la técnica de IP Spoofing, será necesario informar a sus administradores de este hecho, ya que lo más probable es que no sean conscientes de que desde sus sistemas se está desencadenando este ataque.

TCP Syn Flood.

Las versiones actuales de los sistemas operativos, tanto de los sistemas como de los dispositivos de red, contemplan parámetros de configuración para evitar este tipo de ataque.

Connection Flood.

Mediante un sistema de detección eficiente y haciendo uso de filtros de paquetes es posible eliminar este tipo de ataque, siempre eso si, el número de equipos atacantes es reducido, ya que es inviable añadir 1000 reglas al firewall.

Los ataques DDoS reflejan la necesidad de proteger todos los sistemas de una organización, aunque no contengan información valiosa, ya que pueden ser empleados como fuente de origen para la realización de ataques posteriores. Por ejemplo, para detectar este hecho debe tenerse en cuenta que un puerto habitual empleado para el control remoto de un sistema comprometido es el 37337.

La mejor defensa ante este tipo de ataques es seguir las recomendaciones y prácticas de seguridad genéricas: deshabilitar todos los servicios innecesarios, mantener el software actualizado y suscribirse a las listas de correo de seguridad.

Screening Routers.

Los enrutadores de entrada a una red, ya sean propiedad del ISP, conocidos como Customer Premise Equipment (CPE), o de la organización, pueden ser empleados para realizar un filtrado inicial del tráfico IP y se conocen como Screening Routers. Típicamente se basan en tecnologías de filtrado de paquetes (ver los tipos de firewalls existentes), aunque en algunos casos se dispone de implementaciones con estado. Uno de los paradigmas en el filtrado de paquetes se basa en realizarlo lo antes que sea posible, para no desperdiciar capacidad y recursos en manejar paquetes que serán filtrados posteriormente.

Ping of Death.

La solución generada por los fabricantes de las implementaciones se basó en la generación de modificaciones en la pila TCP/IP. En el caso de no disponer de un parche asociado al Sistema Operativo, el ataque puede evitarse filtrando los paquetes ICMP en el firewall de entrada. Una solución aún más detallada es filtrar únicamente los paquetes ICMP fragmentados y no todos, ya que otros protocolos o procedimientos pueden emplear paquetes ICMP para otros propósitos.

Conmutador de Etiqueta Multiprotocolo (MPLS)

El protocolo MPLS permite crear VPNs en las redes IP tradicionales. Este tipo de redes no encriptan los datos, a diferencia de las creadas empleando IPSec. Ambas tecnologías pueden ser empleadas de forma conjunta añadiendo un nivel de seguridad adicional [8].

Infraestructura de Llave Pública (PKI).

La simple generación e instalación de los certificados en los navegadores Web y en el servidor Web, como se explica en el protocolo SSL no es suficiente para confiar en la seguridad y creer que no existen riesgos desde el punto de vista de la seguridad. Tomando de nuevo como ejemplo las comunicaciones Web, pero teniendo en cuenta que esta técnica es aplicable a cualquier protocolo en el que se utilicen certificados digitales, es necesario considerar el procedimiento necesario para comprobar la validez de un certificado (o clave pública) así como para realizar la gestión completa de los mismos: generación, validación y revocación. Toda la gestión global de una arquitectura basada en un sistema de clave pública requiere el establecimiento de una infraestructura PKI.

Tabla ARP

Mediante el envío de paquetes ARP falsos, es posible que un atacante degrade el rendimiento de un sistema (DoS) llenando la caché de rutas de IP con entradas ARP incorrectas. En algunos sistemas, el intervalo de expiración de la tabla ARP no puede ser modificado, pero sí en otros.

Parches de Software de Seguridad.

Muchas de las vulnerabilidades comentadas existen o existieron debido a un error de diseño, programación o implementación de un determinado software, ya sea el propio sistema operativo o una aplicación servidor. Una vez conocida la vulnerabilidad, el fabricante del producto procede a generar y distribuir lo que se conoce como un parche de software de seguridad, es decir, una revisión o nueva versión de los binarios de softwares afectados por la vulnerabilidad, retocados de forma que se elimina el error descubierto. Los anuncios de las diferentes vulnerabilidades, así como la información y el procedimiento para subsanarlas se publican en numerosos portales Web dedicados a la seguridad, así como en las páginas Web de los fabricantes.

Por tanto, si se desea disponer de un entorno lo más seguro posible, es necesario mantener tanto los sistemas como los dispositivos de red actualizados con todos los parches de software de seguridad liberados por el fabricante.

3.2 Soluciones a los problemas VoIPSec.

En el capitulo 2, se mencionaron un número de preocupaciones importantes sobre el papel de IPSec en VoIP. Sin embargo, muchos de estos problemas técnicos son solubles. A pesar de la dificultad asociada a estas soluciones, es bien merecedor el establecimiento de una implementación segura de VoIPSec.

3.2.1 Encriptación en los puntos finales.

Una solución a la demora del tráfico en los enrutadores debido a los problemas de encriptación es manejar la encriptación/desencriptación en los terminales de una red VoIP, de manera que estos deben ser lo suficientemente potentes desde el punto de vista computacional para manejar el mecanismo de encriptación. Pero típicamente los terminales son menos potentes que las pasarelas, las cuales pueden acelerar el hardware a través de múltiples clientes.

Sin embargo, idealmente la encriptación debe mantenerse en cada salto en el tiempo de vida de un paquete VoIP, esto pudiera no ser factible con simples teléfonos IP, con menos posibilidades desde el punto de vista de la potencia computacional del software. En tales casos, puede ser preferible que los datos sean encriptados entre los terminales y el enrutador (o viceversa) pero el tráfico desencriptado en la LAN es ligeramente menos dañado que el tráfico desencriptado a través del Internet. Afortunadamente, el incremento en el poder de procesamiento de nuevos teléfonos está produciendo que esto cada día deje ser un problema. Además, SRTP y MIKEY son protocolos futuros para encriptación de medios y gestores de claves, permitiendo el interfuncionamiento seguro entre clientes basados en H.323 y SIP.

3.2.2 Protocolo de Transporte en tiempo Real Seguro (SRTP).

El protocolo RTP es comúnmente usado para la transmisión de datos audio/video en tiempo real en aplicaciones de Telefonía Internet. Sin protección RTP se considera inseguro, una conversación de teléfono sobre IP puede ser fácilmente escuchada. Además, la manipulación y repetición de los datos en RTP pueden conducir a una pobre calidad

en la voz, debido al atascamiento del flujo audio/video. El Protocolo de Control de Transporte en tiempo Real (RTCP) modifica los datos, incluso pueden conducir a un cambio no autorizado en la QoS negociada e interrumpe el proceso del flujo RTP.

El SRTP es un perfil del RTP, que ofrece no solo confidencialidad, sino también autenticación del mensaje y protección a la repetición para el tráfico RTP y RTCP.

SRTP proporciona una armadura para la encriptación y autenticación de mensajes de flujos RTP y RTCP. SRTP puede lograr un alto rendimiento y una pequeña expansión de paquetes. SRTP es independiente de la especificación de la implementación de la pila RTP y de un estándar de gestión de claves específico, pero Multimedia Internet Keying (MIKEY) se diseñó para trabajar con SRTP.

SRTP proporciona un incremento en la seguridad dada por:

- Confidencialidad para RTP y RTCP por encriptación de sus respectivas payloads (carga útil).
- Integridad a los paquetes enteros RTP y RTCP, conjuntamente con la protección de la repetición.
- La posibilidad para refrescar periódicamente las claves de sesión, la cual limita la cantidad de texto cifrados producida por una clave fija, disponible por un adversario para realizar un cripto análisis.
- Se permite la actualización con nuevos algoritmos criptográficos.
- Seguridad para aplicaciones RTP unicast y multicast.

SRTP ha mejorado su funcionamiento por:

- Bajo costo computacional sostenido por algoritmos predefinidos.
- Bajo costo de ancho de banda y rendimiento alto por límite en la expansión de los paquetes y por una armadura que conserva la eficiencia en la compresión de las cabeceras RTP.
- Huella de identificación pequeña que es un código de tamaño pequeño y memoria de datos para información de claves y listas de repetición.

Las características siguientes también defienden a SRTP.

- Se define como un perfil de RTP, a fin de que pueda integrarse fácilmente dentro de las pilas RTP existentes. Por ejemplo SRTP puede usar relleno RTP porque la porción de encriptación es del tamaño exacto del texto pleno para los algoritmos predefinidos.
- Proporciona independencia del transporte subyacente, redes y capas físicas usadas por RTP, en particular tolerancia alta a la pérdida de paquetes, reordenamiento y robustez para la transmisión de errores de bits en la carga útil encriptada.

- Aligera la carga del gestor de claves debido al hecho que una clave principal simple puede proporcionar material de claves para la protección de la confidencialidad y la integridad, tanto para el flujo SRTP y el correspondiente flujo SRTCP (Secure RTCP). Para requerimientos especiales una clave maestra simple puede proteger varios flujos SRTP.

Debido a que SRTP es definido como un perfil de RTP él puede ser usado con estándares multimedia existentes. Soporte SRTP H.323 es definido dentro del H.235 anexo G, para SIP o más precisamente SDP (Session Description Protocol) mejorado, se haya definido para transportar los datos de gestión de claves necesario para SRTP. De esa manera la combinación de SRTP y MIKEY puede usarse para proporcionar encriptación extremo - extremo, incluso entre diferentes estándares de señalización multimedia como H.323 y SIP.

3.2.3 Gestión de claves para SRTP-MIKEY.

El SRTP usa un juego de parámetros negociados desde el cual las claves de sesión para la protección de la encriptación, autentificación e integridad son combinadas. MIKEY describe un esquema de gestión de claves que direcciona escenarios multimedia en tiempo real (ejemplo: llamadas SIP y sesiones RTSP, flujo, unicast, grupos y multicast) y actualmente está siendo estandarizado dentro del grupo msec (Multicast Security) de IETF. El enfoque yace en el establecimiento de una asociación de seguridad para secciones multimedia seguras, incluyendo gestores de claves y actualización, políticas de seguridad en datos, etcétera, tal que los requisitos en un ambiente heterogéneo se cumplan. MIKEY también apoya la negociación de simples y múltiples secciones crypto. Esto es especialmente útil para el caso donde la gestión de clave se aplica a SRTP, dado que aquí RTP y RTCP pueden ser asegurados independientemente. Los escenarios de despliegue para MIKEY abarcan par a par, simple a muchos y los escenarios de grupos interactivos de tamaños pequeños.

MIKEY apoya la negociación de claves criptográficas y parámetros de seguridad para uno o más protocolos de seguridad. Estos dan como resultado el concepto de sesiones de grupos de criptografía, las cuales describen una colección de sesiones de criptografía que pueden tener clave de encriptación de tráfico común (TEK), generación de clave (TGK) y parámetros de seguridad de sesión.

MIKEY tiene algunas propiedades importantes:

- Puede ser implementado como una biblioteca de software independiente para ser fácilmente integrado en un protocolo de comunicación multimedia. Ofrece independencia de un protocolo de comunicación específico (SIP, H.323, etc.).
- Establecimiento de material de clave mediante el intercambio en dos sentidos, por tanto más adecuada a escenarios multimedia en tiempo real.

- Existen cuatro opciones para distribución de claves:
  - Clave precompartida.
  - Encriptación de clave pública.
  - Intercambio de clave Diffie-Hellman protegido por encriptación de clave pública.
  - Intercambio de clave Diffie-Hellman protegido con clave precompartida y funciones hash con claves (usando una extensión de MIKEY (DHHMAC)).
- Soporte Re- Keying.
- Soporta multidifusión (un transmisor).

3.2.4 Mejores Esquemas de Programación.

La incorporación de AES o algún otro algoritmo de encriptación pueden ayudar a aliviar temporalmente el cuello de botella, pero esta no es una solución escalable debido a que dicho algoritmo no direcciona la causa mayor de desaceleración. Sin existir una forma para que el motor-criptográfico pueda priorizar paquetes, éste será susceptible a ataques de DoS, impidiendo de esa forma el tráfico VoIP urgente en tiempo. Unos pocos paquetes grandes pueden congestionar la cola durante mucho tiempo para hacer que los paquetes VoIP se tarden más de 150 ms, destruyendo la llamada. Idealmente, el motor-criptográfico pudiera implementar la programación de QoS para favorecer los paquetes de voz, pero este no es un escenario realista debido a la velocidad y restricción en la compactación en el motor criptográfico.

Una solución implementada en los últimos enrutadores es programar los paquetes teniendo en cuenta la QoS con anterioridad a la fase de encriptación. Aunque esta heurística resuelve los problemas para todos los paquetes balanceados al entrar en el motor criptográfico en un momento dado, no se dirige a los problemas de los paquetes VoIP que arriban a una cola que ya ha sido saturada con paquetes de datos previamente programados. La prioridad en la QoS puede ser obtenida después del proceso de encriptación asumiendo que los procedimientos de encriptación preservan los bits ToS de la cabecera IP original en la nueva cabecera IPSec. Esta funcionalidad no es garantizada y es dependiente del hardware y software de la red, pero si es implementada permite que la programación de QoS sea utilizada en cada salto que encuentren los paquetes encriptados.

Todavía ni los esquemas de pre-encriptación o post-encriptación realmente implementan QoS o cualquier otro esquema de prioridad para mejorara la programación FIFO del motor de criptoanálisis. Limitaciones de velocidad y de compactación en este dispositivo no permiten que tales algoritmos se apliquen por algún tiempo.

3.2.5 Compresión del tamaño de los paquetes.

Barbieri propuso una nueva solución a los problemas de QoS asociados a VoIPSec como resultado de sus estudios sobre el tráfico VoIPSec, implementando cIPSec (compression IPSec), que es una versión de IPsec que comprime la cabecera interna de un paquete hasta aproximadamente 4 bytes. Esto es posible debido a que muchos de los datos en la cabecera interna de un paquete permanecen constantes o fueron duplicados en la cabecera exterior.

Los resultados de las pruebas iniciales reportadas desde la Universidad de Milán indican que la compresión de las cabeceras IPSec resulta comparable con IP simple en cuanto al uso del ancho de banda. Se lograron resultados considerables en la disminución del jitter, latencia y mejor funcionamiento en el motor criptográfico. El esquema de compresión provocó una mayor carga a la CPU y a las capacidades de memoria de los terminales para lograr la compresión. Se requiere que ambos terminales de una conexión utilicen el mismo algoritmo de compresión.

Sin embargo el estudio fundamentó que el tiempo perdido para la compresión estaba en la fase de encriptación, además que el motor criptográfico es más eficiente con los paquetes comprimidos. Una cosa que ellos no consideraron es la sobrecarga aplicada a la CPU del terminal. Esta puede ser lenta desde el punto de vista computacional (en el caso de un teléfono VoIP simple) o puede estar realizando muchas más funciones que VoIP (en el caso de teléfonos basado en PC). El tiempo real requerido para ejecutar la compresión puede ser mucho mayor que el tiempo ahorrado en el motor criptográfico.

Es importante destacar que el esquema de compresión usado en cIPSec solamente comprime la información de la cabecera del paquete. El asunto de la QoS asociado con los codecs de audio no es aplicable en este escenario porque ningún medio está siendo considerado, sólo las cabeceras IP. Sin embargo las pérdidas de paquetes tienen un efecto perjudicial (por una razón diferente) sobre los paquetes comprimidos en el esquema cIPSec. El esquema de Barbarie necesita mantener información en los terminales del sistema respecto a la sesión actual. Cuando los paquetes se pierden, ellos, no pueden ser reenviados y los terminales necesitan resincronización. Sin embargo, el tiempo ahorrado en el motor criptográfico y la seguridad proporcionada, pudieran bien ser el valor de esta solución.

3.2.6 Soluciones a incompatibilidades NAT/IPSec.

Existen soluciones para el problema de la incompatibilidad IPSec/NAT. Entre ellas se encuentra: Realm-Specific IP (RSIP), IPv6 Tunnel Broker, Capa próxima IP (IPNL) y encapsulación de UDP. A continuación se realizan comentarios de cada una de ellas.

RSIP es un sustituto de NAT y proporciona un túnel libre de obstrucciones entre el host y la pasarela RSIP. RSIP soporta tanto a AH como a ESP, pero su implementación requiere de un examen minucioso de la arquitectura de LAN corriente. Tal vez como resultado de estos problemas, RSIP no se usa ampliamente.

El método IPv6 Tunnel Broker usa un túnel IPv6 como un túnel de IPSec y encapsula un paquete IPv6 en un paquete IPv4. Pero esta solución también requiere de una actualización de la LAN y no trabaja en situaciones donde se usan NATs múltiples.

IPNL introduce una nueva capa dentro de los protocolos de red entre IP y TCP/UDP para resolver el problema, pero IPNL está en competencia con IPv6, que realmente es un estándar mucho más usado.

Probablemente la solución más ampliamente difundida al problema traversal NAT es la encapsulación UDP de IPSec. Esta implementación es apoyada por el IETF y permite que todo el tráfico ESP atraviese el NAT. En modo de túnel, este modelo envuelve el paquete encriptado de IPSec en un paquete UDP con una nueva cabecera IP y una nueva cabecera UDP, normalmente usando el puerto 500. Se eligió este puerto porque es actualmente usado por pares IKE para comunicar, de manera que sobrecargar el puerto no trae consigo nuevos agujeros en el firewall. El campo SPI dentro del paquete UDP encapsulado se fija a cero para diferenciarlo de una comunicación real IK. Esta solución permite que paquetes IPSec atraviesen un NAT en ambas direcciones.

La adopción de este método debe permitir que el tráfico VoIPSec atraviese limpiamente el NAT, aunque se añadan costos el proceso de encapsulación / desencapsulación. La negociación IKE también será requerida para permitir el cruce del NAT. El problema todavía pendiente es que la autenticación basada en IP de los paquetes no puede ser asegurada a través de NAT pero el uso de un secreto compartido (clave simétrica) negociada por IKE puede proporcionar autenticación. Es importante destacar que la autenticación basada en IP es débil comparada con métodos usados por protocolos criptográficos.

3.3 Normas generales para el establecimiento de VoIP.

Debido a la integración de voz y datos en una sola red, el establecimiento de VoIP y una red de datos segura es un proceso complejo, que requiere mayores esfuerzos que aquellos requeridos solamente para redes de datos. En particular, iniciar con estas normas generales que a continuación se relacionan, reconociendo que las consideraciones prácticas, tales como el costo, pueden requerir de ajustes para la entidad.

<u>Desarrolle una arquitectura de red apropiada.</u>

- En la pasarela de voz, que sirve de interfaz con la RTPC, son deshabilitados H.323, SIP y otros protocolos VoIP desde la red de datos. **Utilice una autentificación y control de acceso fuerte en el sistema de pasarela de voz**, como con cualquier otro componente de red crítico. La autentificación fuerte de clientes hacia una pasarela frecuentemente presenta dificultades, particularmente en la administración de las claves. Aquí, mecanismos de control de acceso y el reforzamiento de las políticas pueden ayudar.
- Si el desempeño es un problema, utilice encriptación en el enrutador o en la pasarela, no en los terminales, para proveer IPsec tunneling. Debido a que algunos terminales VoIP, no son computacionalmente suficientemente poderosos para realizar la encriptación, sitúe esta carga en el punto central asegurando que todo el tráfico de VoIP

que emana de la red empresarial sea encriptado. Los teléfonos IP más recientes son capaces de proveer sistemas de encriptación avanzado (AES) realizando esta tarea a un costo razonable.

- Se requiere un mecanismo para permitir el tráfico de VoIP a través de los firewalls. Existen una variedad de soluciones dependientes e independientes de protocolos, incluyendo las ALGs para los protocolos VoIP, los Controladores de Fronteras de Sesión u otras soluciones basadas en estándares cuando se logren completar su madures.
- Es factible la separación lógica de voz y datos en una red. **Subredes diferentes con bloques de direcciones separadas para el tráfico de voz y de datos** (RFC 1918), con servidores DHCP separados, facilitan la detección de intrusos y la protección de los firewalls VoIP.
- Filtros de paquetes con estado (Stateful packect filters) pueden rastrear el estado de las conexiones, negando paquetes que no son parte de una llamada originada propiamente (esto puede no ser práctico cuando la seguridad inherente a protocolos multimedia o cuando la seguridad en las capas más bajas sea aplicada, ejemplo, H.235 anexo D para provisión de integridad o TLS para proteger señalización SIP).
- Utilice IPSec o SSH para toda la gestión remota y accesos de auditoria. Si es práctico, evite la utilización de gestión remota, realice accesos a la PBX IP desde un sistema seguro físicamente.

Asegure que la organización ha examinado y puede manejar aceptablemente y minimiza los riesgos de su información, sistemas operativos y continuidad de operaciones esenciales al desplegar VoIP.

Un especial desafío en el ambiente de la seguridad se crea cuando las nuevas tecnologías se despliegan. Riesgos a menudo no son entendidos totalmente, administradores no están todavía experimentados con las nuevas tecnologías y controles de seguridad y política deben ponerse al día. Por consiguiente, las organizaciones deben cuidadosamente considerar aspectos tales como su nivel de conocimiento y de entrenamiento en la tecnología, la madurez y calidad de sus prácticas de seguridad, controles, política, arquitectura y comprensión de los riesgos de seguridad asociado. Estos problemas deben ser considerados para todos los sistemas, pero es especialmente importante con el despliegue VoIP para los funcionamientos especiales, tal como, los sistemas designados “altos” en la publicación 199 de FIPS (Federal Information Processing Standards) [17].

VoIP puede proporcionar servicios más flexibles a menor costo, pero hay significativos compromisos que deben ser considerados. Puede esperarse que los sistemas VoIP sean más vulnerables que los sistemas de tecnología convencional, en parte porque ellos se conectan a una red de datos y producen debilidades de seguridad adicionales y muchas mas entradas de ataques. La confiabilidad y privacidad puede ser un riesgo mayor en sistemas VoIP a menos que se lleven a cabo controles fuertes y sean mantenidos. Una preocupación adicional es la inestabilidad relativa de la tecnología VoIP comparado con los sistemas de telefonía establecidos. Hoy, los sistemas VoIP todavía están en desarrollo y las normas dominantes no han surgido. Esta inestabilidad está dada porque VoIP utiliza redes de paquete

como un medio de transporte. La red de telefonía pública es ultra confiable, el servicio de Internet generalmente es mucho menos confiable y VoIP no puede funcionar sin las conexiones de Internet, excepto en el caso de usuarios corporativos quienes pueden operar en una red privada. Servicios de teléfonos esenciales, al menos que sean cuidadosamente planeados, organizados y mantenidos, estarán a un mayor riesgo si están basados en VoIP.

Mecanismos de protección apropiados, como son firewalls, deben emplearse. Las entidades deben habilitar, usar y rutinariamente deben probar los rasgos de seguridad que son incluidos en sistemas VoIP.

Debido a las vulnerabilidades inherentes (ejemplo: susceptibilidad para paquetes sniffing) cuando la telefonía opera a través de una red de paquetes, los sistemas VoIP incorporan una serie de rasgos de seguridad y protocolos. La política de seguridad debe de asegurar que estos rasgos sean usados. En particular, los firewalls diseñados para los protocolos de VoIP son un componente esencial de un sistema VoIP seguro.

Debe darse consideración especial a servicios de emergencia de comunicaciones, debido a que el servicio de localización automática no está disponible en VoIP en algunos casos.

A diferencia de las conexiones de la telefonía tradicional, las cuales están adaptadas a una localidad física, la tecnología de conmutación de paquetes VoIP permite a un número particular de usuario estar en cualquier lugar. Esto es conveniente para los usuarios porque las llamadas pueden remitirse automáticamente a su localización. Pero el compromiso complica severamente la prohibición del servicio de emergencias, el cual normalmente prevé la localización del llamador a la oficina de despacho de dicho servicio. Aunque la mayoría de los vendedores de VoIP tienen soluciones para el servicio de emergencia, reguladores gubernamentales y vendedores continúan trabajando en estándares y procedimientos para dichos servicios en un ambiente VoIP. Las organizaciones deben evaluar cuidadosamente aspectos del servicio de emergencia al desplegar VoIP.

Las entidades deben estar conscientes que los controles físicos son especialmente importantes en un ambiente VoIP.

A menos que la red VoIP sea encriptada, cualquiera con acceso físico a la LAN de la oficina podría potencialmente conectarse a la red y entrar en conversaciones telefónicas. Aunque también los teléfonos convencionales se pueden supervisar a través de la línea cuando el acceso físico es obtenido, en la mayoría de las oficinas hay muchos puntos para conectarse con una LAN sin despertar sospechas. Aun cuando la encriptación sea usada, el acceso físico a servidores VoIP y pasarelas puede permitir un ataque al tráfico.

Las entidades, por consiguiente, deben de restringir el acceso a los componentes de la red VoIP para asegurar la seguridad. La seguridad física mide, incluso las barreras, cerraduras, sistemas de control y guardias, los cuales son las primeras líneas de defensa. Dichas entidades deben asegurar que las contra medidas físicas son un plan para minimizar algunos de los riesgos más grandes como la inserción de Sniffer u otros dispositivos supervisores de la red. Por otra parte, hablando de esto, prácticamente significa que la utilización de un Sniffer se puede producir no solo en datos sino en todas las comunicaciones de voz que se interceptan.

Evalué costos para sistemas backup de potencia adicional, los cuales asegurarán el funcionamiento continuo durante fallos de alimentación.

Una valoración cuidadosa debe hacerse para asegurar que la energía este disponible para la conexión de VoIP, así como para cada instrumento de mesa. El costo puede incluir, energía eléctrica para mantener la carga de la batería UPS (Sistema de alimentación ininterrumpido), costo del periodo de mantenimiento para el sistema de generación de potencia de respaldo y el costo del reemplazo de la batería de la UPS. Si la potencia emergente se requiere para más de una hora, se deben de utilizar generadores eléctricos. Los costos para estos incluyen combustible, medios de almacenamiento de combustible y costo para la disposición de combustible de almacenamiento.

Los sistemas softphone, que implementan VoIP usando una computadora personal (PC) ordinaria con un auricular y software especial, no deben usarse cuando la seguridad o privacidad son una preocupación.

Los gusanos, virus y otros software malévolos son extremadamente comunes en PC conectadas a Internet y es muy difícil combatirlos. El conocimiento de las vulnerabilidades en los buscadores web, permite que los atacantes transmitan software malévolos sin el conocimiento de un usuario, aun cuando el usuario no hace nada más que visitar un sitio Web.

Estas vulnerabilidades resultan un riesgo alto en el uso de softphones, para la mayoría de las aplicaciones. En adición, debido a que las PC están necesariamente en la red de datos, usando un softphone, el sistema choca con la necesidad de la separación de las redes de voz y datos.

Conclusiones y Recomendaciones.

VoIP sigue siendo una tecnología aun muy joven, así que es algo especulativo desarrollar un retrato completo de una red VoIP madura, ya que las nuevas tecnologías y los nuevos diseños de protocolo tienen la capacidad de cambiar la VoIP. Aunque hay actualmente diversas configuraciones y protocolos a elegir, eventualmente un estándar dominante surgirá.

Hasta este momento, la seguridad de VoIP ha sido eclipsada fácilmente por la atracción de esta nueva tecnología y las extensas características que promete proporcionar. Esta no ha sido un tema crítico desde que en el pasado, la mayoría del tráfico de VoIP quedó orientado a las redes locales y anchas de empresas de comunicaciones, las cuales son, más o menos aseguradas y protegidas contra la Internet pública. Pero como el uso de VoIP se está dispersando y la telefonía IP se está expandiendo a todos los usuarios finales, los mismos riesgos de la seguridad que han afectado las redes de datos por décadas, se están convirtiendo en riesgos crecientes para la VoIP. Por lo que abrirse a esta nueva tecnología ocasiona un riesgo a la seguridad. Esto es en gran parte debido al hecho de que las redes de nueva generación (NGN) están basadas en VoIP y todos los protocolos IP contienen fallas.

En el trabajo hemos analizado en profundidad las vulnerabilidades que afectan dicha tecnología, así como las posibles soluciones a estas, lo que nos permite basándonos en el contexto de la red cubana realizar las siguientes conclusiones:

- ETECSA debe estudiar los protocolos que están utilizando los principales operadores del mundo en el despliegue de su red VoIP, considerando los requerimientos daves que aseguran la equivalencia con la RTPC actual, especialmente en cuanto a la calidad y seguridad del servicio.
- El país debe crear comisiones de trabajo que rápida y profundamente aborden el estudio de los temas relacionados con la seguridad en la migración de las redes de Telecomunicaciones. De la misma forma debe exigir participación en eventos y organizaciones vinculadas con estos temas.
- ETECSA debe comenzar el análisis para la elección del o los Proveedor(es) de tecnologías de seguridad para VoIP, sobre el(los) que sustentará la migración, ante la complicada situación provocada por el bloqueo económico que vive el país. Un punto muy importante en este sentido será la exigencia de certificaciones de interfuncionamiento con tecnologías de otros fabricantes. El análisis debe comenzar con Proveedores establecidos hoy en el país.
- Utilizar en el despliegue de la VoIP, sus principales protocolos (SIP, H.323 y MEGACO/H.248). Realizando un estudio previo de las opciones tecnológicas disponible en el mercado, pues como mencionamos anteriormente no existe un estándar definido que permita una elección ideal.
- Continuar el proceso de Expansión y Modernización de la Red de Telecomunicaciones de Cuba con soluciones capaces de crear una NGN robusta y segura, que sea capaz de llegar a las instalaciones de los usuarios, facilitando

tanto el servicio de voz paquetizada, como los demás servicios de datos, entre los que prolifera el servicio de Internet. Priorizando la seguridad y la calidad, como los temas principales en las nuevas inversiones.

Este trabajo constituye un marco inicial para el análisis de la seguridad como un punto critico que se debe considerar en la implementación de la VoIP en el país, bien porque no se abordaron en detalles algunos aspectos o porque su complejidad requiere de esfuerzos mayores. Debido a esto se recomienda:

- Recabar más información sobre las experiencias técnicas que en materia de seguridad poseen los más importantes operadores del mundo, obtenidas en el proceso de migración de sus redes, debido a que este es un tema con poca o ninguna presencia publica.
- Poner atención a la gestión de la red, desde el punto de vista de sus elementos. La complejidad de sus servicios y de las formas de proveerlos exigirá una fornida gestión que garantice la detección de cualquier violación en la nueva red.
- Estudiar las soluciones de seguridad que hoy se aplican en las redes IP y la RTPC, para lograr el interfuncionamiento de sus servicios, logrando así una migración segura.
- Disponer de procedimientos y políticas adecuadas que permitan concienciar a los usuarios y administradores de los sistemas informáticos, así como facilitar la aplicación de análisis y controles exhaustivos en la propia red y los elementos que la componen, debido a que con el uso solamente de herramientas de seguridad (firewalls, IPSec, NAT, etc.) no es posible asegurar una red VoIP.
- Mantener una actualización de los avances que se realizan en este campo, así como de los nuevos avisos, vulnerabilidades y tecnologías que salen a la luz. Dicha actualización se pudiera realizar de forma automática, mediante listas de distribución.

Para concluir, reconocemos que proporcionar soluciones de seguridad a la comunicación de VoIP, no es una tarea fácil. Sin embargo, en vista de la fuerza potencialmente versátil de esta tecnología en términos tecnológicos y económicos, la creación y utilización de diversas soluciones son un buen paso de progresión en la dirección correcta para garantizar que los servicios de VoIP proporcionen el mismo nivel de la confianza y confiabilidad que para más que un siglo ahora, a caracterizado el sistema actual RTPC.

Referencias Bibliográficas

1. Arkin, O., Sys-Security Group. (2002, Nov). *Why E.T. Can't Phone Home? Security Risk Factors with IP Telephony based Networks*. Disponible en http:/www.sys-security.com/archive/papers/, accedido el 4/02/07.

2. Barbieri, R., Bruschi, D. & Rosti, E. (2002). *Voice over IPsec: Analysis and Solutions*. Proceedings of the 18th Annual Computer Security Applications Conference. Disponible en http://ieeexplore.ieee.org/, accedido el 10/02/ 07.

3. Beceiro, H. (2001). *Telefonía IP.* Ciudad de La Habana, Cuba: Instituto Superior politécnico José Antonio Echeverría, Departamento de Telemática.

4. Beceiro, H. (2004). *Aspectos Críticos en la Introducción de la Telefonía IP en Cuba.* Santa Clara, Cuba: Universidad Central de Las Villas, Facultad de Ingeniería Eléctrica.

5. Bellovin, S., Cheswick, w. & Rubin, A. (2003). *Firewalls and Internet Security: Repelling the wily Hacker (tercera ed)*. Disponible en http:www.wilyhacker.com/, accedido el 4/02/07.

6. Bourque, L. (2005, April). *VoIP Security Considerations for Enterprises.* Disponible en http://www.enterpriseitplanet.com/security/features/article.php/3497496, accedido el 10/02/07.

7. Chuah, C-N. (2000*). Providing End-to-End QoS for IP based Latency Sensitive Applications* (Technical Report). US: University of California at Berkeley, Dept. of Electrical Engineering and Computer Science. Disponible en http://www.ece.ucdavis.edu/chuah/paper/proposal.pdf, accedido el 4/02/07.

8. Cisco. (2003) *Comparing Multiprotocol Label Switching, IPSec, and a Combined Approach*. Disponible en http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/solmk_wp.pdf accedido el 5/3/07.

9. Cisco Networkers. (2000). *Advanced Topics in Enterprise VPNs and PKI*. Disponible en http://www.cisco.com/networkers/nw00/pres/2403.pdf, accedido el 4/02/07.

10. Claire, R. *Introducción a las Redes Privadas Virtuales. Disponible en* http://www.lugro.org.ar/biblioteca/articulos/introvpn.pdf, accedido el 10/2/07.

11. Collier, M. (2005, September). *The Current State of VoIP Security*. Disponible en http://www.voip-magazine.com/content/view/511/0/, accedido el 10/2/07.

12. Conry-Murray, A. (2002, Nov). *Emerging Technology: Security and Voice over IP – Let's Talk*. Commweb. Disponible en http://sys-security.com/blog/published-materials/articles/, accedido el 15/02/07.

13. Cyber Security Industry Alliance (2005, May). *Cyber Security for IP Telephony.* Disponible en https://www.csialliance.org/resources/pdfs/CSIA_VOIP_May_2005.pdf, accedido el 4/01/07.

14. Dos Santos, G. (2005). *Técnicas criptográficas para la protección de datos*. Disponible en http://dialnet.unirioja.es/servlet/articulo, accedido el 12/3/07.

15. Drew, P. & Gallon, C. (2003, March). *Next-Generation VoIP Network Architecture.* Multiservice Switching Forum (MSF). Disponible en http://www.msforum.org, accedido el 4/01/07.

16. Farnsworth, R. (2004, July). *Enterprise Security – an Enabler of VoIP*. Disponible en http://www.convergedigest.com/blueprint/ttp04/z4cisco1.asp, accedido el 4/01/07.

17. FIPS Pub 199. (2004, febrero). *Standards for Security Categorization of Federal Information and Information Systems.* Disponible en http://csrc.nist.gov/ publications/fips/fips199/FIPS-PUB-199-final.pdf, accedido el 4/01/07.

18. Gamm, B., Howard, B. & Paridaens, O. (2001). *Seguridad de la información: amenazas y mecanismos de protección*. Revista de Telecomunicaciones de Alcatel Dialnet. Disponible en http// dialnet. unirioja.es/servlet/listaarticulos, accedido el 17/12/06.

19. Garretson, C. (2005, July) *VoIP security threats: Fact or fiction?.* Network World. Disponible en http://www.networkworld.com/news/2005/072505-voip-security.html, accedido el 4/01/07.

20. Goode, B. (2002, Sept). *Voice over Internet Protocol (VOIP).* Proceedings of thee IEEE, Vol. 90, NO. 9. Disponible en http://www.cybertelecom.org/voip, accedido el 4/3/07.

21. IBM Internet Security Systems. *Database of Intrusions detected by Network.* Disponible en http://www.iss.net/security_center /advice/Intrusions/default.htm, accedido el 17/3/07.

22. IETF. *RFC Pages*. Disponible en http://www.ietf.org/rfc.html, accedido el 17/12/06.

23. Jaikumar, V. (2004) *VOIP: Don't overlook security*. Computer World. Disponible en http://www.computerworld.com/securitytopics/security/story/ , accedido el 4/3/07.

24. Morrissey, P. (2005, Agosto). *VoIP Security Keeping IP Voice Safe and Sound*. Network Computing. Disponible en http://www.networkcomputing.com/shared/article/168600463, accedido 5/3/07.

25. Newport Networks. (2006). *NAT Traversal for Multimedia over IP Services.* White Paper. Disponible en http://www.newport-etworks.com/whitepapers/nat-traversal1, accedido el 7/4/07.

26. NIST. (2005). *Security considerations for voice over IP systems*. US. Disponible en http:// csrc. nist. gov / publications /nistpubs/ 800-58/sp800-58-final.pdf, accedido el 5/3/07.

27. Osmosis Latina. (2005) .*Seguridad y Encriptación*. Disponible en http://www.osmosislatina.com/aplicaciones/seguridad.htm, accedido el 17/12/06.

28. Percy, K. & Hommer, M. (2003, Jan). *Tips from the trenches on VOIP*. Network World Fusion. Disponible en http://findarticles.com/p/articles/mi_qa3649 /is_200301/ai_n9230872, accedido el 17/12/06.

29. Phifer, L. (2001, Apr). *Slipping IPsec Past NAT*. ISP Planet. Disponible en http://communication-equipment.globalspec.com, accedido el 5/3/07.

30. Radware (2005, Agosto). *VoIP: Security Threats and Solutions*. Disponible en http://www.radware.com/content/document.asp?_v=about&document=6142, accedido el 17/12/06.

31. Rosenberg, J. & Schulzrinne, H. (2001, Mar). *SIP Traversal through Residential and Enterprise NATs and Firewalls*. Internet Draft, Internet Engineering Task Force. Disponible en http://jdrosen.net/sip_entfw.html, accedido el 5/3/07.

32. Schulzrinne, H. & Rosenberg, J. (1998, Julio). *A comparison of SIP and H.323 for Internet telephony*. NOSSDAV, Cambridge, England. Disponible en http://www.cs.columbia.edu/~hgs/papers/Schu9807_Comparison.pdf, accedido el 5/3/07.

33. Shirey, R. (2000, May). *RFC 2828 Internet Security Glossary.* Disponible en http://www.ietf.org/rfc/rfc2828.txt, accedido el 17/12/06.

34. Siles, R. (2002). *Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados.* Tesis. Disponible en http://www.arcert.gov.ar/webs/webdocs.html, accedido el 17/12/06.

35. Sinden, R. (2002). *Comparison of Voice over IP with circuit switching Techniques*. US: Southampton University, Department of electronics and Computer Science. Disponible en http://citeseer.ist.psu.edu/556033.html, accedido el 17/12/06.

36. Spenneberg, R. (2003). *IPSec Como*. Disponible en http://www.ipsec-howto.org/spanish_/t1.html, accedido el 5/03/07.

37. UIT-T. (2003, Octubre). *Recomendación X.805 Arquitectura de Seguridad para sistemas de comunicaciones extremo a extremo*. Disponible en http://www.itu.int/rec/T-REC-X.805/es, accedido el 5/03/07.

38. VOIPSA (Voice Over IP Security Alliance). (2005, October). *VoIP Security and Privacy Threat Taxonomy.* Disponible en http://www.voipsa.org/Activities/VOIPSA-Threat-Taxonomy-0.1.pdf, accedido el 17/12/06.

39. Zimmermann, P., Johnston, A., & Callas, J. (2006, Mar). *ZRTP: Extensions to RTP for Diffie-Hellman Key Agreement for SRTP*. IETF Draft. Disponible en http://www.philzimmermann.com/docs/draft-zimmermann-avt-zrtp-01.html, accedido el 4/01/07.

Glosario de Términos

A

AES	Advanced Encryption System
AH	Cabecera de Autenticación (Authentication Header)
ALG	Pasarelas de medios a Nivel de Aplicación
ARP	Address Resolution Protocol

B

BICC	Bearer Independent Call Control

C

CA	Autoridad de Certificación
CCS	Cálculo de Sistemas Comunicantes)
Codec	Coder/Decoder
cIPSec	Compression IPSec
CPE	Customer Premise Equipment
CPU	Unidad de Procesamiento Central

D

DDoS	Ataque de Denegación de Servicio Distribuido (Distribute Denied of Service)
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone (Zona DesMilitarizada)
DoS	Denied of Service
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard

E

ESP	Encapsulated Security Payload
ETECSA	Empresa de Telecomunicaciones de Cuba SA.

F

FIFO	First In, First Out
FIN	Escaneo que utiliza mapeo inverso para descubrir los puertos cerrados
FIPS	Federal Information Processing Standards

G

GW	Pasarela (Gateway)

H

H.323	Estándar de la ITU para comunicaciones de audio y video a través de redes de paquetes
H.GCP	Protocolo de control de las pasarelas
HMAC	Hash Message Authentication Codes
HTTP	Hypertext Transfer Protocol
Hub	Dispositivo de conexión central en una red que une líneas de comunicaciones en una configuración en estrella

I

ICE	Establecimiento de conectividad interactiva
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
iLBC	Internet de Baja Razón de Bit
Internet	Es un método de interconexión de redes de computadoras implementado en un conjunto de protocolos denominado TCP/IP.
IP	Internet Protocol
IPNL	IP Next Layer
IPSec	Internet Protocol Security
IRC	Internet Relay Chat
ISAKMP SA	Internet Security Association Key Management Protocol Security Association
ISP	Internet Service Provider
IV	Initialization Vector (Vector de Inicialización)

J

JITTER	Variación en el tiempo de arribo de los paquetes

L

LAN	Local Area Network
Latencia	Tiempo que se toma una transmisión de voz para transitar desde la fuente al destino

M

MAC	Media Access Control
MCU	Unidad de control de Multipunto
MD5	Message-Digest Algorithm 5
Midcom	Protocolo de Comunicación Intermedia
MDCP	Media Device Control Protocol
MG	Media Gateway
MGC	Media Gateway Control
MGCP	Media Gateway Control Protocol
MIKEY	Multimedia Internet Keying
MPLS	Multi Protocol Label Switching (Conmutador de Etiqueta Multiprotocolo)
MSEC	Multicast Security

N

NAPT	Network Address Port Translation
NAT	Network Address Translation (Traducción de Direcciones de Red)
NGN	Redes de Próxima Generación (New Generation Network)
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NMAP	Network Mapper
NULL	Valor especial aplicado a un puntero (o referencia)

P

PBX	Private Branch Exchange
PC	Personal Computer
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure (Infraestructura de Llave Publica)
PSK	Pre-Shared keys

Q

QoS	Quality Of Service (Calidad de Servicio)

R

RAS	Remote Access Service
RFC	Request For Comments
RSA	Sistema de Criptografía de Clave Pública
RSIP	Realm -Specific IP
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Protocol
RTPC	Red Telefónica Pública Conmutada (PSTN en Inglés)

S

SA	Security Associations (Asociaciones de Seguridad)
SAD	Security Asocciation Databases
SBC	Controlador de Frontera de Sesión
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SHA	Secure Hash Algorithm (Algoritmo de Hash Seguro)
SIP	Protocolo de Inicialización de Sesión
SIP-T	SIP para Teléfonos
SNORT	Software detector de intrusos basado en red
SP	Security Policy (política de seguridad)
SPD	Security Policy Database
SPI	Security Parameter Index
SRTP	Protocolo de Transporte en tiempo Real Seguro.
SRTCP	Secure RTCP
SSH	Secure SHell
SSL	Secure Sockets Layer
STUN	Simple Traversal of UDP through NATS
SYN	Bit de control dentro del segmento TCP

T

TCP	Transmission Control Protocol
Telefonía IP	Es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP.
TEK	Clave de Encriptación de Tráfico Común
TFTP	Trivial File Transfer Protocol

TGH	Generación de Clave (Generation Key)
TIA	Asociación de Industrias de las Telecomunicaciones
TLS	Transport Layer Security
ToS	Type of Service
TURN	Traversal usando repetidor NAT

U

UDP	User Datagram Protocol
UIT	Unión Internacional de Telecomunicaciones
UPnP	Universal Plug and Play
UPS	Sistema de alimentación ininterrumpido (Uninterruptible Power Supply)
URI	Identificador de Recursos Uniformes
URL	Uniform Resource Locators
USB	Universal Serial Bus

V

VAD	Detección de Actividad de Voz
VLANs	Redes Locales Virtuales
VoIP	Voice over IP
VoIPSec	VoIP usando IPsec
VPN	Virtual Private Network (Redes Privadas Virtuales)

W

WAN	Wide Area Network
WiFi	Wireless Fidelity