ESTADO DEL ARTE DE LA (IN)SEGURIDAD VOIP

JOHN ALEXANDER RICO FRANCO*

Recibido: 12 de junio de 2013 / Aceptado: 25 de julio de 2013

Resumen

La telefonía basada en el protocolo IP (VoIP) es el concepto tecnológico que comprende a todos los mecanismos necesarios para lograr realizar llamadas telefónicas y/o sesiones de videoconferencia a través de redes de datos, permitiendo servicios de telefonía a costos mínimos y de fácil implementación e integración con la red de datos propia de cualquier empresa; y es por estas características que los productos VoIP han tenido una muy rápida y amplia aceptación en todo rango de empresas, uso domestico y otros ambientes que requieren de soluciones de telefonía, pero debido a la concepción de la telefonía como mecanismo seguro de transmisión de información y la visión sesgada de que los mecanismos de seguridad son solo gastos innecesarios o que son procesos engorrosos que disminuyen la facilidad de uso de cualquier tecnología, se pueden llegar a implementar de manera muy insegura o con poca preocupación en este rublo, soluciones VoIP vulnerables y con resultados catastróficos en el manejo de información sensible compartida en conversaciones telefónicas confidenciales.

El presente artículo busca presentar los conceptos y conclusiones que han sido resultado de un proyecto de investigación basado en descubrir y detectar cuales son los grandes inconvenientes que acechan a la tecnología VoIP y encontrar cuales son las soluciones más innovadoras que esta presentando la comunidad de la seguridad de la información a nivel global; para así lograr concientizar a los profesionales de la seguridad y a cualquier actor implicado en una solución VoIP que aparte de los beneficios propios de este tipo de tecnología, esta viene de la mano con vulnerabilidades y problemas de seguridad que hay que tener en cuenta y que son comunes en cualquier tipo de tecnología emergente; pero que a su vez no todo el panorama es sombrío y que existen soluciones de seguridad VoIP que garantizan la integridad, disponibilidad y confidencialidad de la información que circula en forma de voz y/o video en las redes VoIP.

Palabras clave: VoIP, SIP, H323, H.235, RTP, SRTP, gestor de llamadas, terminales VoIP suplantación, espionaje, denegación del servicio (DoS), fuzzing, señalización, seguridad.

Abstract

Voice over Internet Protocol (VoIP) is the technology concept that includes all the necessary mechanisms for making phone calls and video conferencing sessions through

* Ingeniero de Sistemas. Especialista en Seguridad de Redes de la Universidad Católica de Colombia, con más de 5 años de experiencia como consultor independiente en proyectos referentes a temas de seguridad informática, criptografía y realización de pruebas de calidad de software. Catedrático Universitario y Docente Investigador del Grupo de Investigación y Desarrollo de Ingeniería de Sistemas (G.I.D.I.S) de la Corporación Universitaria Republicana.

data networks; allowing telephony services at minimal costs with an easy structure implementation and simple integration with any company data network; and is for these unique features that the VoIP products have a very fast and wide acceptance in whole range of companies, local telephony deployments and other environments that requires telephony solutions, but due to the widespread idea that the phone service is a secure way of transmitting information and the biased view by some employees indicating the security mechanisms are just unnecessary expenses or cumbersome processes that decrease the ease use of any technology may limit some developments of VoIP solutions and the vulnerable VoIP networks can generate catastrophic results in managing of sensitive shared information which is transmitted on confidential telephone conversations.

This article pretend to present the concepts and conclusions which have been the result of a research project based on discovering and detecting the major drawbacks and weaknesses proper the VoIP technology and find out which are the most innovative security solutions that are presenting by the international research community of matters related to information security; and this is for generate awareness among security professionals and any player involved in a VoIP solution that apart from the profits of this technology there are serious security problems and vulnerabilities that must be taken into account and that are common in any type of emerging technology; but dear reader should keep in mind that not all the scene is dark and there are VoIP security solutions that ensure the integrity, availability and confidentiality of the information circulating in the form of voice and / or video in VoIP networks.

Keywords: VoIP, SIP, H323, H.235, RTP, SRTP, Call manager, VoIP terminals, impersonation, wiretapping, denial of service (DoS), fuzzing, data signaling, information security.

Introducción

La percepción sobre la idea de la seguridad informática, ha estado en boga a nivel empresarial en los últimos años y se ha convertido en una necesidad, más que en un compromiso, frente a una tendencia competitiva cada vez mas enfocada al uso de nuevas tecnologías y por ende a mejorar su participación en la Internet; pero esto ha abierto las puertas a un nuevo enemigo, el atacante informático, que busca aprovecharse de la falta de robustez de seguridad de las tecnologías emergentes, de las vulnerabilidades propias de cualquier nuevo proceso de comunicación y de la poca concientización de los usuarios de lo importante que es la información; para así lograr afectar de manera negativa a cualquier empresa a nivel internacional sin mucho esfuerzo o conocimiento técnico. Y si a lo anterior, lo contextualizamos en una época como lo es la actual, en donde todas las grandes organizaciones están extendiendo el uso de redes VoIP (Voice Over Internet Protocol) como mecanismo potenciador de su infraestructura de comunicaciones y también como fuente de reducción de costos. Pero no se está teniendo en cuenta que el ambiente de riesgos asociados a las redes VoIP, se encuentra en constante incremento, ya que los atacantes han descubierto que este ambiente es muy propicio para poder recolectar información empresarial de manera fácil y efectiva.

Así que el fin de este artículo es poder exhibir a cualquier lector interesado, un escrito enfocado a exponer las vulnerabilidades de la redes VoIP; que en la actualidad son una gran fuente de información sensible que un atacante puede adquirir y comprender de manera muy fácil, y también se busca el poder presentar cuales son algunas de las mas nuevas e innovadoras tendencias en seguridad VoIP; las cuales pueden llegar a ser fuente de inspiración de nuevas tecnologías de seguridad o llegar a ser base para proteger la información compartida sobre este tipo de redes en cualquier empresa interesada.

¿Qué es la VoIP?

Para poder iniciar de la mejor manera el estudio sobre la seguridad en la telefonía sobre el protocolo de Internet (VoIP) hay que conocer que es la VoIP; así que se inicia explicando que la tecnología de voz sobre el protocolo IP, se refiere a el concepto tecnológico que engloba las metodologías, tecnologías, protocolos de comunicación y técnicas de transmisión que se utilizan para la distribución de sesiones de video (videoconferencias) y de comunicaciones de voz a través de redes basadas en el protocolo de Internet (IP), esto quiere decir que se envía la señal de voz y/o video en forma digital en paquetes de datos, en lugar de enviarla en forma análoga a través de los circuitos cableados que son exclusivos de la telefonía convencional, como lo son las redes PSTN (Public Switched Telephone Network); así que bajo este concepto hay que tener en claro que los datos de voz y video bajo la tecnología VoIP, viajan en redes de propósito general y que están basadas en paquetes en vez de la típica línea telefónica basada en circuitos.

Una de las ventajas de la tecnología VoIP es que se permite controlar el tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento del servicio telefónico; además es independiente del tipo de red física que lo soporta, permitiendo así la integración con las grandes redes de datos actuales.

En lo referente al concepto de seguridad en redes VoIP, aun es deficiente; debido a que los protocolos y codecs utilizados son parcialmente nuevos y por ende vulnerables, permitiendo así a un agresor poder realizar ataques de denegación de servicio, grabar conversaciones y/o acceder a buzones de voz de manera relativamente fácil; lo cual puede comprometer de manera alarmante la información sensible de una compañía.

Ahora, un aspecto que hay que tener muy presente al momento de analizar que es la VoIP, es que los protocolos VoIP son los que permiten a dos o más dispositivos transmitir y recibir audio y/o video en tiempo real, lo cual es la

base que permite soportar el servicio de llamadas bajo el protocolo IP y que los protocolos mas altamente utilizados al momento de generar soluciones de VoIP son el Protocolo de Inicio de Sesión (SIP – Session Initiation Protocol) y la familia de protocolos H.323; pero existen distintas configuraciones entre protocolos y elementos de red, que pueden ser utilizados en la implementación de una solución VoIP, lo cual genera confusión y permite a cualquier atacante aprovecharse de esta falta de regulación; así que por esto exhibimos cuales son los elementos básicos de una solución VoIP; en lo que refiere a dispositivos de red, son dos los dispositivos fundamentales:

- **Terminales:** Un teléfono VoIP o terminal VoIP es el dispositivo utilizado para iniciar y recibir llamadas; y es el tipo de terminal llamado Softphone el que es más utilizado al momento de implementar una solución VoIP, ya que este es una herramienta VoIP basada en software que permite a cualquier computador de escritorio o teléfono de inteligente poder realizar y/o recibir llamadas VoIP; esta es una solución muy practica y de bajo costo para implementación de terminales VoIP, pero puede ser fácilmente atacada por cualquier usuario mal intencionado, puesto que al ser una herramienta basada en software, puede ser transgredida mediante diferentes técnicas de ataque que se basan en las vulnerabilidades propias de cualquier solución de esta índole.

- **Gestor de llamadas (Call Manager):** Este dispositivo de tipo servidor, es el encargado de identificar y encontrar las diferentes terminales de una infraestructura VoIP al momento de gestionar una llamada telefónica; en pocas palabras este es el encargado de proporcionar las funcionalidades de una central telefónica (PBX) a cualquier solución VoIP y además es el responsable de la autentificación de los usuarios que interactúan con la red VoIP. Este es el dispositivo que más ataques recibe al momento de tratar de comprometer una solución de VoIP, ya que si un atacante logra controlar y/o engañar al gestor de llamadas, puede desde hacerse pasar por un usuario legitimo de la red VoIP hasta escuchar llamadas privadas entre los usuarios de la solución VoIP, pudiendo así comprometer la integridad y confidencialidad de dichas llamadas telefónicas.

Ya habiendo visto cuales son los dos dispositivos de red VoIP básicos, pasamos a ver los protocolos VoIP que más ampliamente son utilizados al momento de generar una solución VoIP.

A. SIP (Session Initiation Protocol - Protocolo de Inicio de Sesión)

El Protocolo de Inicio de Sesión o SIP, fue estandarizado por el Internet Engineering Task Force (IETF) y es el protocolo genérico de cualquier solu-

ción VoIP, ya que es considerado en la actualidad como el estándar para señalización multimedia (video y audio) en redes IP, puesto que este fue diseñado para soportar cualquier clase de sesión de comunicación bidireccional y esto incluye a las llamadas VoIP, tal como se especifica en el RFC 3261[1]. Su funcionamiento es muy básico al ser un protocolo genérico, en si lo que hace este es gestionar todas las solicitudes que son enviadas al servidor SIP (gestor de llamadas) por los distintos clientes SIP (terminales), entonces el servidor SIP procesa dichas solicitudes de comunicación y las responde a los clientes SIP, enviando los respectivos mensajes de respuesta SIP; pero a diferencia de los demás protocolos IP, las implementaciones VoIP deben estar instaladas tanto en el cliente SIP como en el servidor SIP, para que así cualquiera de las dos partes pueda iniciar o finalizar las llamadas IP; este mecanismo de funcionamiento se detalla en la figura 1.

Tal como se puede observar, la arquitectura SIP maneja un diseño muy parecido al modelo transaccional de solicitud/respuesta de HTTP; puesto que en ambos modelos su transacción consta en una solicitud de un cliente o usuario que invoca a un método en particular o función específica del servidor y este responde a el cliente de acuerdo a la respuesta dada por el método o función ejecutada. El protocolo SIP reutiliza la mayora de campos de cabecera y reglas de codificación de HTTP, lo cual hace que su funcionamiento sea fluido en cualquier red basada en protocolo IP, pero lo hace muy sensible a ataques basados tanto en vulnerabilidades del protocolo SIP como en las del protocolo HTTP.

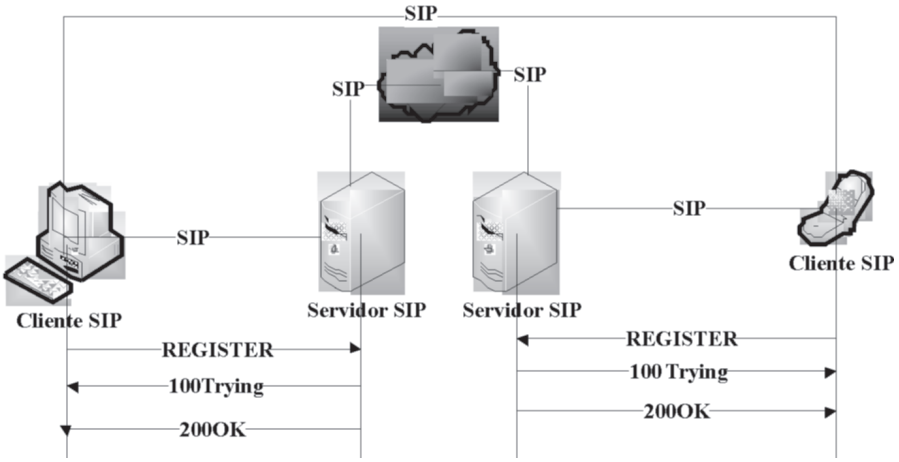

Figura 1. Arquitectura SIP[2]

1 H. SCHULZRINNE, E. SCHOOLER Y J. ROSENBERG; «SIP: Session Initiation Protocol» RFC 3261, 2002.

2 Ibídem.

B. H323

La familia de protocolos H.323 fue presentada por el ITU Telecommunication Standardization Sector (ITU-T) como mecanismo para proveer sesiones de comunicación audio – visual sobre cualquier red basada en paquetes y ha sido ampliamente adoptada por el sector empresarial debido a su fácil integración a las redes de telefonía tradicional PSTN (Public Switched Telephone Network), ya que el protocolo H.323 es un protocolo binario lo cual se acopla perfectamente a la lógica de funcionamiento de las redes PSTN. Los protocolos que son el núcleo de la familia H.323 son los siguientes:

H.225 (RAS): Este protocolo permite el registro, admisión y estatus de la comunicación entre los agentes H.323 (terminales) y el servidor de llamadas H.323 (gestor de llamadas), y es este protocolo encargado de proveer la resolución de direcciones y los servicios de control de admisión a la red VoIP.

H.225: Es el encargado de realizar el proceso de señalización de las llamadas y este es implementado entre los agentes H.323 (terminales).

H.245: Es el protocolo que esta comisionado para el control de la comunicación multimedia, ya que este es el que describe los mensajes y procedimientos que son utilizados para el establecimiento y clausura de canales lógicos de comunicación de audio, video y datos, junto con sus controles e indicadores.

Protocolo de Transmisión en tiempo Real (RTP): Es el protocolo utilizado para enviar y recibir información multimedia (video, voz y texto) entre agentes H.323.

En la figura 3 veremos el funcionamiento a grosso modo del protocolo H.323.

Los abismos de la seguridad generados por la VoIP

La mayoría de los usuarios no técnicos de las redes telefónicas que se basan en el protocolo de Internet; que casi siempre son los que toman las decisiones al momento en invertir en tecnología más por costos que por seguridad o calidad del servicio; manejan un concepto erróneo de una seguridad implícita sobre el manejo de la información que comunica mediante llamadas telefónicas vía VoIP, ya que estos usuarios están seguros de que la información está llegando de manera segura al destinatario que ellos desean y que no existe nadie más «escuchando» dicha comunicación; pero hay que aclarar que esta manta de seguridad fue adquirida por dichos usuarios debi-

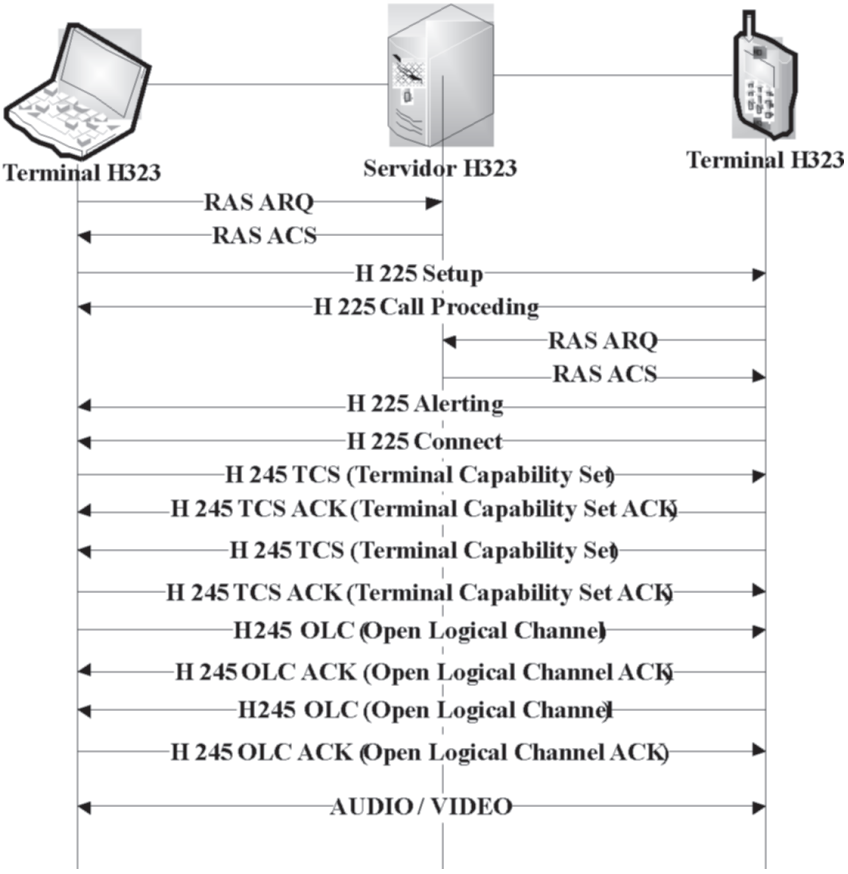

Figura 2. Funcionamiento del protocolo H.323[3]

do a su interacción cotidiana con las redes de telefonía convencional (PSTN - Red Telefónica Conmutada), que si poseen mecanismos seguros como lo son su perímetro y su seguridad física por defecto; pero la estructura propia de la Internet elimina dichas barreras permitiendo que atacantes puedan aprovechándose de la versatilidad (búsqueda de vulnerabilidades) y proliferación (masificación de puntos de ataque) de redes basadas en Internet, permitiendo así la materialización de incidentes de seguridad que pueden afectar seriamente el buen nombre de cualquier compañía y poner en riesgo su competitividad en un mercado (cualquiera que este sea) cada vez más desafiante y complejo.

3 VARIOS; «Packet-Based Multimedia Communications Systems» ITU-T Recommendation H.323, 2003.

Otro aspecto a tener en cuenta al momento de evaluar cuales son los puntos débiles en la seguridad de los ambientes VoIP, es que esta es una tendencia de comunicación parcialmente nueva, y que por ende existen varios protocolos y tecnologías de implementación que aun se encuentran en estado emergente y que por esto pueden generar brechas de seguridad debido a su falta de robustez; y esto sumado a posible negligencia al no adoptar buenas prácticas de seguridad al momento de gestionar una solución VoIP, se puede llegar a generar una red VoIP altamente insegura y que puede llegar a ser bastante nociva a la información sensible que circula por dicha solución.

Pero aunque la seguridad en soluciones de VoIP puede llegar a ser complicada de aplicar, pero no es imposible; lo que hay que tener muy presente y ser consientes, como responsables de la seguridad de la información, es que los agresores informáticos están viendo a las redes VoIP como un nuevo punto de ataque, debido a que un ambiente VoIP desprotegido les puede dar acceso a información sensible de manera rápida y de «fácil» captura en un ambiente de comunicación vulnerable.

Categorías de ataque a sistemas VoIP

Ya habiendo visto cuales son las falencias de seguridad que se pueden presentar al momento de implementar un sistema de comunicaciones telefónicas basado en el protocolo IP; pasaremos a ver cuáles son las alternativas de agresión más ampliamente utilizadas por los atacantes informáticos al momento de comprometer la integridad, disponibilidad y confidencialidad de la información que circula por una red VoIP.

A. Espionaje y análisis de tráfico VoIP

En esta tendencia de ataque a sistemas VoIP, lo que un usuario mal intencionado busca es poder monitorear y en su efecto escuchar las llamadas telefónicas desprotegidas realizadas por dos o más terminales bajo cualquier protocolo VoIP, logrando así socavar la confidencialidad e integridad de la información sensible que se manipula y distribuye por dicho medio.

Las dos técnicas de ataque que son genéricas o meta-ataques utilizados bajo esta tendencia son:

- **Análisis de tráfico VoIP:** Esta técnica busca estudiar como las terminales VoIP se comunican entre sí; mediante la realización de un exhaustivo estudio del comportamiento y estructura de los paquetes VoIP que transitan a través de la solución de telefonía IP que está siendo auditada o atacada,

junto con una investigación de los protocolos VoIP y de red utilizados en la infraestructura de comunicación y las direcciones IP involucradas al momento de realizar las llamadas telefónicas; y es con esta información que el atacante puede estructurar su estrategia de ataque, moldeándola bajo los aspectos específicos de la red VoIP a comprometer .

- **Eavesdropping (Espionaje):** Esta técnica de ataque es la que más afecta a las soluciones de telefonía IP, ya que es en esta donde un atacante pueda escuchar las llamadas realizadas entre dos terminales VoIP; este modelo de ataque es el comúnmente llamado «pinchado» de llamadas, que tan comúnmente escuchamos en el ambiente político colombiano en los últimos tiempos. Esta técnica de ataque se materializa bajo el tipo de ataque llamado Man-in-the-Middle (MitM) donde el atacante que ha logrado tener acceso a la red que soporta a la solución VoIP puede colocarse entre dos terminales VoIP para así lograr escuchar y almacenar en formato de audio las llamadas realizadas entre estas dos terminales y poder apropiarse de cualquier información sensible que haya sido comunicada en dichas llamadas telefónicas.

Otras técnicas de ataque, mas especificas que se pueden apreciar bajo esta clasificación son las siguientes:

Sniffing (Análisis de tráfico) de transferencia de archivos de configuración TFTP

El atacante busca estudiar el trafico UDP (User Datagram Protocol), para descubrir el nombre e información de los archivos de configuración TFTP (Trivial File Transfer Protocol) y asi descargarlos del servidor TFTP para su estudio. Estos archivos contienen datos clave, como lo son passwords y nombres de usuario, que son posteriormente aprovechados por el atacante para realizar nuevos ataques con el uso de credenciales validas y poder ingresar a la solución VoIP como un usuario legítimo.

Escaneo de la red VoIP con pings TCP

En esta técnica, el atacante envía de manera aleatoria peticiones de conexión a diferentes puertos de conexión TCP (Transmission Control Protocol); que son los identificadores de las aplicaciones emisoras y receptoras en cualquier equipo de computo; entonces mediante esta técnica el atacante puede ver el comportamiento de la conexión TCP/IP que soporta a la solución VoIP y así darse una idea de la estructura y del funcionamiento del sistema VoIP que esta maneja.

Escaneo UDP

El atacante envía cabeceras UDP (User Datagram Protocol) vacías a los puertos UDP de la víctima VoIP, y si la victima responde con un paquete UDP, indica que el servicio está activo y así poder aprovecharse posteriormente de sus posibles vulnerabilidades.

Enumeración de usuarios y de extensiones

El atacante se aprovecha del método SIP Register, que es generado por el usuario para el gestor de llamadas VoIP que para este ataque es un servidor SIP, aquí el atacante envía solicitudes de registro a varias extensiones y usuarios de la red VoIP, para así poder listar las extensiones no utilizadas o los usuarios no registrados.

Enumeración de servidores TFTP

La mayora de teléfonos VoIP utilizan un servidor TFTP (Trivial File Transfer Protocol) para descargar el archivo de configuración del teléfono; pero el servidor TFTP no requiere de autentificación para enviar el archivo de configuración y es allí, que si el agresor logra comprometer a el servidor TFTP y envía archivos de configuración corruptos a el teléfono VoIP puede configurarlos de manera insegura o con vulnerabilidades que el atacante podrá aprovechar en futuras arremetidas.

B. Suplantación

Esta clasificación de ataques a sistemas VoIP agrupa a todos los ataques que pueden suplantar la identidad de un usuario, terminal o servicio VoIP autorizado; para que así el atacante pueda realizar redirección de llamadas, acceder a la red VoIP, ya sea a la información sensible que es transmitida por ella, o a elementos físicos de la red VoIP, o a servicios VoIP implementados, o a otros activos VoIP que le interese comprometer.

Este tipo de ataques ocurren debido a la mala estructuración y/o configuración insegura de una red VoIP; puesto que al existir estas falencias no se puede confiar en el identificador de llamadas utilizado por el gestor de llamadas y que es consultado por las terminales VoIP como método de verificación de la identidad del usuario que genera y/o recibe una llamada telefónica, o si la terminal VoIP que está implicada en el proceso de una llamada está realmente autorizada para realizar dicha función; ya que cualquier agresor puede rea-

lizar una suplantación a nivel digital utilizando muestras de voz, que puedan haber sido capturadas en la misma red VoIP, para así poder hacerse pasar por un usuario autorizado o de confianza para el receptor de la llamada y mediante técnicas de modificación de elementos de red, puede hacerse pasar por un equipo o terminal VoIP autorizado.

Algunos ejemplos de ataques basados bajo esta metodología son:

Ataques de Replay

Aquí un atacante utiliza de tonos de llamada (redes PSTN), muestras de voz o paquetes de autentificación VoIP validos que han sido previamente capturados, para así intentar pasar las llamadas realizadas por el atacante como llamadas validas en el sistema y/o engañar al receptor.

Suplantación de Identidad

Este ataque es simplemente lograr que un usuario o terminal VoIP se haga pasar por otro en la red VoIP; la suplantación de identidad como método de ataque en una red VoIP puede llegar a ser muy efectivo al momento de querer tomar información de una víctima que confía en la extensión y de la persona de quien le llega la llamada. Este ataque se logra bajo el concepto de envenenamiento de ARP (Address Resolution Protocol) que es poder relacionar la dirección MAC (Media Access Control Addres) del atacante con una IP real de la red VoIP, logrando así pasar como una terminal VoIP autorizada, y así poder realizar y recibir llamadas en la red VoIP comprometida.

Redirección - Hijacking

En este tipo de ataque se busca que una de las terminales involucradas en una llamada telefónica sea neutralizada y suplantada por una terminal controlada por el atacante, para así poder «secuestrar» la llamada realizada. La suplantación se puede realizar mediante el envenenamiento al servidor DNS (Domain Name System), que en si es engañar al servidor DNS, utilizado en la red que soporta la solución VoIP para que este acepte la veracidad de respuesta de DNS falsas, para así poder direccionar a los equipos VoIP legítimos a terminales controladas por el atacante que se hacen pasar por extensiones autorizadas de la compañía. Este tipo de ataques son utilizados para robar identidades, credenciales y otra información sensible al hacer creer a un usuario legítimo que está hablando con otro usuario de la compañía y que este se encuentra con los privilegios suficientes para poder escuchar y tener acceso a dicha clase de información sensible que el atacante solicita.

C. Interrupción del servicio de telefonía

Cualquier compañía, sin importar su razón social, tiene a su red telefónica como mecanismo principal de comunicación directa con sus clientes, proveedores, empleados y asociados; debido a que la comunicación vía telefónica es mecanismo de intercambio de información que es más ampliamente utilizado y adoptado a nivel mundial. Por lo cual si se presenta cualquier perturbación en el funcionamiento habitual de este servicio, puede afectar de manera negativa y significativa el buen funcionamiento de cualquier organización.

Para nuestro caso, la interrupción del servicio se aplica directamente a todos los ataques que buscan impedir el servicio VoIP, incluyendo sus servicios de acceso y de administración; atacando a cualquier dispositivo de la red que soporta a el servicio VoIP, esto incluye a los servidores VoIP (Gestor de llamadas), las terminales VoIP, routers y demás elementos de red que interactúan o dan soporte a la infraestructura VoIP. Estos ataques pueden ser directos o de manera remota, lo directos son cuando el atacante tiene acceso físico al dispositivo de red y lo corrompe para que deje de funcionar correctamente, este tipo de ataque incluye el corte de suministro de energía a dichos elementos de red, para así poderlos dejar completamente fuera de servicio; y los ataques remotos son los que mediante el envío de paquetes VoIP o de peticiones de conexión de manera indiscriminada y basándose en las vulnerabilidades de los protocolos VoIP, buscan congestionar y por ende bloquear a cualquier dispositivo de la red VoIP o de la red de soporte que utilice la solución de VoIP a comprometer, este tipo de ataques remotos son llamados ataques de DoS (Denegación de Servicio).

Algunos ejemplos de ataques basados bajo esta metodología son:

Ataques DoS distribuidos

Este tipo de ataque Dos (Denial of Service), es donde el atacante logra tener bajo su control a un gran número de equipos de usuarios desprevenidos que son capaces de realizar peticiones de conexión o llamadas VoIP, formando así una red Zombie, con la cual el atacante realizará de manera indiscriminada peticiones a la red VoIP de manera de avalancha aprovechando que cada equipo Zombie puede generar miles de mensajes de conexión o llamadas VoIP a un único dispositivo; buscando así inundar de paquetes VoIP al elemento de red víctima y este termine siendo incapacitado debido a el agotamiento de sus recursos.

Ataques de inundación de UDP

Es el tipo de ataque DoS (Denial of Service) más utilizado por los atacantes, debido a que las direcciones origen de los paquetes UDP (User Datagram Protocol) son fácilmente falsificables y también que la mayoría de dispositivos VoIP actuales soportan al protocolo UDP de manera nativa y por ende transparentemente.

Ataques de inundación de ICMP

En este tipo de ataque a la disponibilidad del servicio VoIP, el atacante busca realizar un ataque DoS, aprovechando que la mayora de firewalls y routers vienen configurados por defecto para dejar circular de manera desapercibida a paquetes ICMP (Internet Control Message Protocol), debido a que por su naturaleza de mensaje de control no son considerados peligrosos sino que son solo de diagnostico; pero un atacante puede tratar de inutilizar a un dispositivo de la red VoIP a comprometerlo mediante el envió indiscriminado dichos paquetes de diagnóstico.

Envío de paquetes malformados (Fuzzing)

Puesto que la mayoría de equipos de red, sean o no VoIP están concebidos y desarrollados para manejar tráfico de red convencional; un atacante puede ver este concepto como una fuente de ataque; ya que estos dispositivos cuando reciben paquetes desconocidos o malformados no saben cómo manipularlos, lo cual esporádicamente lleva al bloqueo del equipo o servidor de red que da soporte a la solución VoIP o directamente a los elementos propios de una red VoIP, logrando asi minar la disponibilidad del servicio VoIP.

Fragmentación de paquetes

El atacante segmenta los paquetes UDP (User Datagram Protocol) y TCP (Transmission Control Protocol), y los envía de manera separada por la red VoIP, buscando así inutilizar a los equipos VoIP o de su infraestructura de red mediante el consumo de recursos, debido a la espera de la llegada del paquete faltante para completar la solicitud de conexión.

Ya habiendo visto grosso modo cuales son las principales técnicas de ataque a servicios de VoIP, pasamos a ver de manera categorizada y clasificada las tendencias de ataque a sistemas VoIP, en el cual podremos observar cuales

son las elecciones de ataque utilizadas por un usuario mal intencionado al momento de querer comprometer un servicio VoIP (ver figura 3).

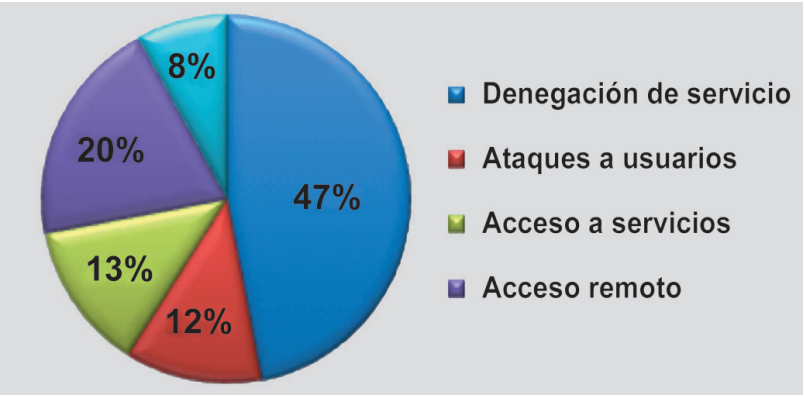

Figura 3. Ataques a redes VoIP.[4]

Como podemos ver la mayoría de ataques a sistemas VoIP buscan generar una interrupción en el servicio de telefonía, buscando así que la disponibilidad del servicio VoIP se vea mermada de manera significativa. Este concepto lo podemos ver claramente reflejado en la siguiente figura (ver figura 4).

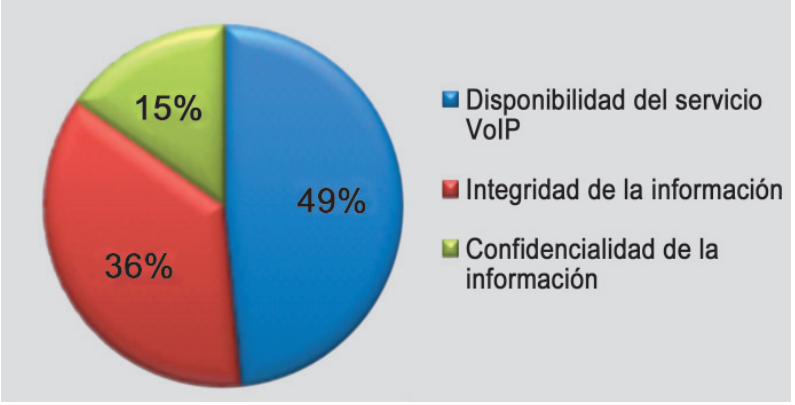

Figura 4. Tendencia de ataques a sistemas VoIP.[5]

4 ANGELOS KEROMYTIS; «Voice over IP Security: A Comprehensive Survey of Vulnerabilities and Academic Research»; Editorial: Springer, 2011.

5 Ibídem.

¿Pero por qué los atacantes deciden afectar la disponibilidad del servicio de VoIP?; con base en esta pregunta se puede analizar y deducir que los atacantes han descubierto que esta característica es la más deseada por los usuarios de las redes VoIP y además que la falta del servicio VoIP genera una gran repercusión y que afecta de manera abismal a los usuarios y/o las empresas que basan su comunicación con sus clientes y demás entes importantes con su red VoIP.

Además hay que tener muy presente que este tipo de ataques son los que tienen una gran facilidad de ejecución para el atacante novato o inexperto en el tema; en cuanto al resto de tipos de ataque a sistemas VoIP, también son de alta peligrosidad, pero su nivel de dificultad al momento de su ejecución es mayor y por ende se requiere de unas condiciones especiales y de un atacante experto o por lo menos familiarizado con la red VoIP a atacar, para tener un índice de éxito favorable.

Mecanismos de seguridad VoIP

Ya habiendo visto cuales son los mecanismos de ataque y de aprovechamiento de las vulnerabilidades de los sistemas VoIP, pasamos a revisar cuales son las tendencias de seguridad en ambientes VoIP.

A. Protección a nivel de señalización

En el momento en que se empieza a pensar sobre la seguridad en redes VoIP, uno de los temas principales a tener en cuenta es la protección de la señalización de los mensajes o paquetes que se intercambian entre los equipos terminales VoIP y los demás elementos de la red VoIP; esto se debe a la gran cantidad de información sensible a nivel de protocolo VoIP que contienen dichos mensajes, como por ejemplo los datos del manejo criptográfico de las llamadas telefónicas, o los mensajes de petición de conexión entre dos terminales VoIP, y junto con la posibilidad de que estos mensajes pueden estar transitando por zonas de la infraestructura de red de soporte de la solución VoIP que son inseguras o con políticas de seguridad cuestionables, pueden darle a un atacante suficiente información para que pueda identificar cual es la estructura, a nivel de protocolo, de la red VoIP que desea comprometer para luego perfilar su estrategia de ataque.

Ya habiendo visto cual es la importancia de la información contenida en los mensajes o paquetes manejados por los dispositivos VoIP, pasaremos a exponer algunas de las medidas de seguridad utilizadas para la protección de información a nivel de señalización que son utilizadas por los dos principales protocolos VoIP:

Mecanismo de protección a nivel de señalización

Protección de la señalización en el protocolo SIP

El protocolo SIP propone en su RFC 3261[6], el uso de varios protocolos de seguridad de señalización, que son ampliamente reconocidos para asegurar la señalización de sus mensajes; entere los cuales se encuentran el IPSec (Internet Protocol Security) donde este protocolo genera un «túnel» de seguridad entre dos entes de la red VoIP, para que así los mensajes que transiten esten protegidos de cualquier ataque. Otra recomendación de seguridad a nivel de señalización en el protocolo SIP es el uso de TLS (Transport Layer Security), que es definido en el RFC 4346[7], donde se implementa una autentificación mutua entre un par de elementos de la red VoIP (terminal y servidor VoIP), este protocolo de seguridad se compone de dos capas, la primera es la llamada TLS Record Protocol o protocolo de registro TLS donde se encarga de mantener la conexión segura entre los dos puntos VoIP asegurados y la segunda capa es el TLS Handshake Protocol o protocolo de negociación TLS donde se gestionan las propiedades de criptografía utilizada en la comunicación entre los entes VoIP, para así poder generar un puente seguro entre ellos para su intercambio de mensajes VoIP. Y por último, otro de los protocolos destacados al momento de aplicar seguridad a nivel de señalización del protocolo SIP es el S/MIME (Secure / Multipurpose Internet Mail Extensions) que es especificado en el RFC 3851[8], el cual provee mecanismos que garantizan la integridad, autentificación y confidencialidad de diferentes mensajes, entre ellos los mensajes utilizados por el protocolo SIP, su funcionamiento a grandes rasgos es que S/MIME firma digitalmente de manera parcial o total al mensaje SIP, logrando así que el receptor del mensaje pueda verificar si el mensaje ha sido manipulado y/o modificado en su tránsito por la red VoIP.

Seguridad a nivel de señalización en el protocolo H.323

El protocolo H.323 maneja un protocolo exclusivo de seguridad, que es el protocolo H.235; este es el que define los procesos de autentificación y de encriptación utilizados al momento de manejo de mensajes entre elementos VoIP que utilizan el protocolo H.225 para establecer la comunicación de mensajes VoIP entre dos elementos de la red VoIP. Una de las grandes ventajas de implementar la seguridad de señalización bajo el protocolo H.235 aparte de la perfecta simbiosis con el protocolo H.323, es el hecho de poder incorporar material criptográfico para la protección de la señalización de mensajes directamente a los mensajes de establecimiento de llamadas.

6 H. SCHULZRINNE, E. SCHOOLER Y J. ROSENBERG; "SIP: Session Initiation Protocol" RFC 3261, 2002.

7 T. DIERKS Y E. RESCORLA; «The Transport Layer Security (TLS) Protocol» RFC 4346, 2006.

8 B. RAMSDELL; «Secure/Multipurpose Internet Mail Extensions (S/MIME)» RFC 3851, 2004.

B. Protección a nivel de multimedia:

La principal preocupación al momento de pensar en la seguridad de soluciones VoIP, es el proteger las conversaciones telefónicas realizadas entre los usuarios de cualquier solución VoIP; ya que si por mas que se aseguren los procesos de señalización de mensajes VoIP pero no se protege la información de los servicios de telefonía y/o de videoconferencia soportados, estaremos perdiendo directamente la información sensible (passwords, nombres de usuario, datos vitales de clientes, entre otra información) contenida en las llamadas telefónicas y/o sesiones de videoconferencia que transitan en la red VoIP.

Es por esto que al momento de generar una solución VoIP segura, se debe pensar en utilizar protocolos de seguridad que protejan tanto a nivel de señalización como a nivel multimedia de manera conjunta, para así generar un único canal de flujo de información VoIP protegido; pero lograr este nivel de protección puede llegar a ser algo confuso para el especialista en seguridad informática, puesto que este tipo de protocolos combinados tienden a ser complejos al momento de diseñar y de implementar en un ambiente VoIP, que solo el simple hecho de implementarlos por separado; y además se debe garantizar que por agregar parámetros de seguridad complejos a la solución VoIP, esta no se vea comprometida en su buen funcionamiento y/o pierda calidad en el servicio, un ejemplo de cómo es la complejidad al momento de generar un ambiente VoIP seguro no debe influir en el funcionamiento optimo del servicio VoIP, es el hecho de que se debe realizar los procesos de encriptación, desencriptación y de autentificación de las llamadas sin agregar tiempos de latencia que comprometan la interacción en tiempo real entre el emisor y el receptor de la llamada telefónica, o el hecho de congestionar a la red VoIP al utilizar ancho de banda extra al momento de ejecutar los servicios de seguridad, ya que lo optimo es que estos se ejecuten de manera transparente al usuario final.

Así que es por estas complejidades de aplicación de seguridad y además del hecho de poder garantizar un proceso de gestión y realización de llamadas telefónicas ágil y similar al servicio prestado por las redes PSTN (Public Switched Telephone Network), que se descuida tanto el concepto de la seguridad en las redes VoIP y pasan estas a ser un campo fértil para ataques por parte de hackers en búsqueda de información sensible y de fácil adquisición.

Pero no todo es negativo al momento de proteger el contenido multimedia (voz y/o video) de un servicio VoIP, ya que existen varios protocolos y me-

canismos de seguridad idóneos para esta materia, pero que son implementados de manera separada con los procesos de protección a nivel de señalización; lo cual permite una menos compleja implementación pero que disminuye de manera sustancial el nivel de protección de los datos que nos puede llegar a generar al utilizar un esquema integrado de protección en ambos flancos.

Entre los protocolos de seguridad VoIP, el más ampliamente utilizado y de mayor integración con el ambiente VoIP, en lo referente a la protección de datos multimedia, es el protocolo SRTP (Secure Real Time Protocol) debido a que cualquier implementación VoIP utiliza al protocolo RTP (Real Time Protocol o Protocolo de Transporte en Tiempo Real) como mecanismo para la transmisión de datos multimedia, esto es debido a que el protocolo RTP realiza comunicaciones multimedia de manera muy superficial, ya que únicamente define de manera básica las características mínimas de la sesión multimedia, para así poder generar una transmisión rápida y sin interrupciones. Asi que debido al amplio uso del protocolo RTP, nace el protocolo SRTP (Secure Real Time Protocol o Protocolo de Transporte en Tiempo Real Seguro), que fue diseñado para poder realizar la transmisión de datos multimedia de manera fluida pero que además agrega componentes de seguridad para garantizar la integridad, autentificación y confidencialidad de las sesiones RTP, como lo son el poder agregar componentes criptográficos y la independencia del transporte de la señal multimedia para así controlar la perdida de paquetes VoIP que puedan ser utilizados de manera no apropiada por terceros mal intencionados.

C. Nuevas tendencias en seguridad VoIP:

En lo que se refiere al futuro en la seguridad en ambientes de trabajo VoIP, la comunidad de investigación y desarrollo de metodologías de seguridad informática, ha presentado varios postulados académicos que presentan metodologías innovadoras, en búsqueda de poder generar soluciones de seguridad robustas que logren mitigar las vulnerabilidades e intentos de ataque por parte de hackers que han descubierto en esta tecnología «emergente», como fuente asequible de información sensible. A continuación se presentaran algunos de las propuestas más interesantes y que implican un aumento sustancial en el nivel de seguridad de una solución VoIP.

El investigador Eric Chen, en su paper llamado «Detecting DoS Attacks on SIP Systems»[9], presenta un mecanismo de detección de ataques de dene-

9 ERIC CHEN; «Detecting DoS Attacks on SIP Systems»; Paper presentado en Proceedings of the 1st IEEE Workshop on VoIP Management and Security (VoIP MaSe); 2006.

gación de servicio (DoS) en ambientes VoIP SIP, que se basa en la medición de las transacciones VoIP realizadas en cada nodo de la solución VoIP, de la cantidad de errores generados en la plataforma VoIP y el nivel de trafico VoIP, para así tener un valor esperado y optimo en cada una de estas variables; y al momento de presentarse anomalías en dichos valores se generaran alertas de un posible ataque de denegación de servicio al administrador de la red VoIP.

Los profesores Vijay Balasubramaniyan, M. Ahamad y Haesun Park, en el documento «CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation»[10], proponen el uso de un mecanismo que se base en los tiempos de duración de las llamadas y en un modelo grafico que represente como es la red social de los consumidores de una solución VoIP; para asi lograr determinar cuál es nivel de reputación de cada uno de dichos usuarios; y basándose en estos datos se lograría determinar cuáles son llamadas legítimas y cuales son simplemente intentos de ataque por parte de un usuario mal intencionado, ya que si se evidencian llamadas de muy corta duración o llamadas de larga duración entre usuarios con una relación social baja puede ser que estas llamadas no sean generadas por las personas dueñas de las extensiones VoIP implicadas.

Los investigadores Alex Talevski, Elizabeth Chang y Tharam Dillon presentaron en formato de paper, el documento «Secure Mobile VoIP»[11]; que es una propuesta de integración de mecanismos de seguridad criptográficos en protocolos VoIP ligeros, para ser implementados en soluciones VoIP en terminales celulares. Este proyecto es un gran avance en búsqueda de generar mecanismos de seguridad que garanticen la confidencialidad en llamadas VoIP generando un canal seguro en un ambiente tan inseguro y amplio como lo es las redes de telefonía celular.

Conclusiones

La tecnología VoIP aun se considera como una tecnología relativamente nueva y de alta adopción, y por ende debe ser tratada como tal en lo que se refiere a su seguridad; teniendo especial cuidado en las vulnerabilidades de

10 V. BALASUBRAMANIYAN, M. AHAMAD Y H. PARK; «CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation»; Proyecto de desarrollo presentado en Proceedings of the 4th Conference on Email and Anti-Spam (CEAS); 2007.

11 A. TALEVSKI, E. CHANG. Y T. DILLON; «Secure Mobile VoIP»; Paper expuesto en Proceedings of the International Conference on Convergence Information Technology; 2007.

sus protocolos y en la arquitectura de las redes de datos que soportan a las soluciones VoIP. Otro concepto a tener en cuenta en lo emergente de la tecnología VoIP, es que los ataques presentados en el anterior artículo, solo pueden ser la punta del iceberg de posibles variaciones o nuevas tendencias de ataque que se puedan aprovechar de la tecnología VoIP, por ende se recomienda al lector, que sea responsable de una solución VoIP estar en constante evaluación de dicha red VoIP, y se invita a todo tipo de usuario VoIP a estar en constante aprendizaje de nuevas técnicas de protección VoIP y de las posibles nuevas vulnerabilidades o riesgos de una solución VoIP, y así poderlos afrontar de mejor manera en un futuro no muy lejano.

Otro concepto a tener en cuenta es que los problemas de seguridad en redes VoIP, no solo se radican en el estado naciente de los protocolos en los que se apoyan para generar los servicios de telefonía y/o teleconferencia; sino que hay que tener muy en cuenta la infraestructura de red que soporta la solución VoIP, por ende hay que purgar cualquier configuración débil o por defecto de los equipos de red que interactúan o soportan a la red VoIP, para así poder minimizar la cantidad de puntos débiles que puedan comprometer de cualquier manera al servicio VoIP a proteger.

Y por último, también se ha podido observar, que cualquier solución de seguridad aplicada en el ambiente VoIP viene de la mano con un costo, que puede ser monetario o de dificultad de implementación, por ende es recomendado que el profesional de la seguridad de la información que se ponga en la tarea de asegurar la información de una red VoIP, balancee de la mejor manera sus necesidades de seguridad frente a los costos que estos conllevan, para así encontrar la solución optima y apropiada de seguridad VoIP.

Referencias

1. H. SCHULZRINNE, E. SCHOOLER y J. ROSENBERG. «*SIP: Session Initiation Protocol*» RFC 3261, 2002.

2. VARIOS. «*Packet-Based Multimedia Communications Systems*» ITU-T Recommendation H. 323, 2003.

3. ANGELOS KEROMYTIS. «*Voice over IP Security: A Comprehensive Survey of Vulnerabilities and Academic Research*»; Editorial: Springer, 2011.

4. T. DIERKS y E. RESCORLA. «*The Transport Layer Security (TLS) Protocol*» RFC 4346, 2006.

5. B. RAMSDELL. «*Secure/Multipurpose Internet Mail Extensions (S/MIME)*» RFC 3851, 2004.

6. ERIC CHEN. «*Detecting DoS Attacks on SIP Systems*»; *Paper presentado en Proceedings of the 1st IEEE Workshop on VoIP Management and Security (VoIP MaSe)*, 2006.

7. V. BALASUBRAMANIYAN, M. AHAMAD y H. PARK. «*CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation*»; Proyecto de desarrollo presentado en *Proceedings of the 4th Conference on Email and Anti-Spam (CEAS)*, 2007.

8. A. TALEVSKI, E. CHANG. y T. DILLON. «*Secure Mobile VoIP*»; *Paper expuesto en Proceedings of the International Conference on Convergence Information Technology*, 2007.

Bibliografía

1. ALAN B. JOHNSTON. «*Understanding Voice over IP Security*»; Editorial: Artech House Publishers, 2006.

2. ANGELOS KEROMYTIS. «*Voice over IP Security: A* Comprehensive Survey of Vulnerabilities and Academic *Research*»; Editorial: Springer, 2011.

3. MARK COLLIER y DAVID ENDLER. «*Hacking* Exposed VoIP: Voice Over IP Security Secrets & *Solutions*»; Editorial: McGraw-Hill, 2006.

4. PETER THERMOS y ARI TAKANEN. «*Securing VoIP* Networks: Threats, Vulnerabilities and *Countermeasures*»; Editorial: Addison-Wesley Professional, 2007.

Infografía

1. D. RICHARD KUHN, THOMAS J. WALSH y STEFFEN FRIES. «*Security Considerations for Voice* Over IP Systems - Recommendations of the National. *Institute of Standards and Technology*»; Documento WEB PDF; [URL: http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf].

2. MARK COLLIER. «*Basic Vulnerability Issues for SIP Security*»; Documento WEB - PDF; [URL: http://download.securelogix.com/library/SIP_Security030 105.pdf].

3. TOSHIO MIYACHI. «*Principles of VoIP Security*»; Documento WEB - PDF; [URL: www.necunifiedsolutions.com/Downloads/WhitePapers/NEC_VoIP_Security BestPractice_Vol_1_WhPpr.pdf].

4. TOSHIO MIYACHI Y TERUHARU SERADA. «*Models of Secure VoIP Systems*»; Documento WEB - PDF; [URL: www.necunifiedsolutions.com/Downloads/WhitePapers/NEC_VoIP_SecurityBestPractice_Vol_2_WhPpr.pdf].