INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN MECATRÓNICA Y TECNOLOGÍAS DE INFORMACIÓN

TECNOLÓGICO DE MONTERREY®

CONTROLES DE SEGURIDAD DE INFORMACIÓN EN TECNOLOGÍA VOIP (VOICE OVER IP)

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:

MAESTRO EN ADMINISTRACIÓN DE LAS TELECOMUNICACIONES

POR:

Fernando Rodríguez Meza

MONTERREY, N.L. JULIO, 2009

INSTITUTO TECNOLÓGICO DE ESTUDIOS SUPERIORES DE MONTERREY

DIVISIÓN DE MECATRÓNICA Y TECNOLOGÍAS INFORMACIÓN

PROGRAMA DE GRA DUADOS EN MECATRÓNICA Y TECNOLOGÍAS DE INFORMACIÓN

Los miembros del comité de tesis recomendamos que la presente tesis del Ing. Fernando Rodríguez Meza sea aceptada como requisito parcial para obtener el grado académico de Maestro en Administración de las Telecomunicaciones.

Comité de tesis:

_____

Dr. Juan Arturo Nolazco Flores
Asesor

_____

Ing. Ricardo Morales González
Asesor

_____

Ing. Pablo D. Díaz López
Sinodal

_____

Ing. Juan Pablo Nigenda Alvarez, MC
Sinodal

_____

Dr. Joaquín Acevedo Mascarúa

Director de Investigación y Posgrado
Escuela de Ingeniería

Julio, 2009

CONTROLES DE SEGURIDAD DE INFORMACIÓN EN TECNOLOGÍA VOIP (VOICE OVER IP)

Por:

FERNANDO RODRIGUEZ MEZA

TESIS

Presentada al Programa de Graduados de Mecatrónica y Tecnologías de Información

Este trabajo es requisito parcial para obtener el grado de Maestro en Administración de las Telecomunicaciones.

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

Monterrey, N.L. JULIO, 2009

Dedicatoria

Esta investigación de tesis está dedicada a la memoria de:

Mi padre…. Apolinar Rodriguez Iturbero †

Mi prima… Miriam Martínez Meza †

Gracias a ti Mamá, hoy he llegado a mi objetivo, Tú me has mostrado como he de luchar diariamente, Ser tu hijo es el mejor regalo que me ha dado la vida.

Gracias a mi esposa Rosario, por compartir las alegrías, tristezas, éxitos y fracasos en estos primeros años de nuestro matrimonio.

A Fernanda por regalarme esa sonrisa que me alienta a seguir siempre adelante.

A ustedes les dedico este logro.

Agradecimientos

A Dios, por darme la oportunidad de hacer mis sueños realidad, por bendecirme con una maravillosa familia, y por estar siempre a mi lado.

A mi esposa por esperar pacientemente a ver realidad este logro.

A mis hermanas Maricela, Yadira, Odalisa, Marilisa, les agradezco todos estos años que han convivido conmigo y me han apoyado en los momentos más difíciles. Ustedes también son parte de mi éxito.

Gracias a toda mi familia, por su cariño y por brindarme su apoyo en todo momento.

A mis asesores Dr. Juan Arturo Nolazco Flores, Ing. Ricardo Morales González que sin sus recomendaciones y apoyo esta tesis no habría sido posible.

A los miembros del Comité por su orientación y tiempo.

¡Muchas gracias!

RESUMEN

Este documento es el resultado de una investigación bibliográfica sobre como lograr controles de seguridad necesarios para asegurar que las llamadas telefónicas basadas en Tecnología IP no tengan problemas de privacidad, confiabilidad, e integridad. La metodología que desarrolle fue entender los principios de VoIP, y analizar las vulnerabilidades potenciales que existen en esta tecnología. Los resultados obtenidos muestran las soluciones posibles para neutralizar los ataques a esta tecnología.

Durante los siguientes capítulos se va a intentar detallar cuales son las amenazas más significativas que afectan a la telefonía sobre redes IP. Como ya se ha comentado la mayoría los riesgos son inherentes de las capas sobre las que se apoya la tecnología VoIP por lo que muchos de los ataques se basarán en técnicas bien conocidas. Se mostraran, también, ciertas vulnerabilidades que afecta específicamente a las redes VoIP y a sus protocolos.

En este trabajo se intentará dar una visión global y explicar los conceptos de seguridad y los ataques más comunes que afectan a las redes de telefonía IP. Dando como resultado controles de seguridad para mitigar estos ataques, vulnerabilidades y amenazas.

Contenido

Dedicatoria

Agradecimientos

Resumen

Tabla de contenido

Lista de figuras

Lista de tablas

Capitulo 1: Introducción 1

Antecedentes 1

Objetivos 1

Justificación 2

Estructura del trabajo 2

Capitulo 2 Revisión de Literatura 4

2.1 Concepto de VoIP 4

2.2 Componentes 5

2.2.1 Terminal 5
2.2.2 Servidores 7
2.2.3 Gateways 7
2.2.4 Conexiones con H.323 10
2.2.5 Conexiones con SIP 10
2.2.6 MGCP 12
2.2.7 Megaco/H248 13

2.3 Amenazas, vulnerabilidades y ataques 14

2.3.1 Tipo De Riesgos 16

2.3.1.1 VoIP Packet Replay Attack 19
2.3.1.2 Data Tunneling 19
2.3.1.2 QoS Modification Attack 20
2.3.1.4 VoIP Packet Injection 20
2.3.1.5 DoS against Supplementary Services 20
2.3.1.6 Control Packet Flood 20

2.3.1.7 Wireless DoS Attack 21
2.3.1.8 Bogus Message DoS 21
2.3.1.9 VoIP Protocol Implementation DoS 21
2.3.1.10 Packet of Death DoS 22
2.3.1.11 IP Phone Flood DoS 22
2.3.1.12 TLS Connection reset 23
2.3.1.13 Rogue VoIP Endpoint Attack 23
2.3.1.14 Registration Hijacking 23
2.3.1.15 Proxy Impersonation 24
2.3.1.16 Toll Fraud 24
2.3.1.17 Message Tampering 24
2.3.1.18 VoIP Protocol Implementation Attacks 25
2.3.1.19 VoIP Social Engineering 26
2.3.1.20 VoIP Call Hijacking 27
2.3.1.21 Network Eavesdropping 27
2.3.1.22 Vishing 28
2.3.1.23 DoS utilizando mensajes SIP CANCEL 28
2.3.1.24 DoS using SIP BYE messages 29
2.3.1.25 DoS using SIP FAILURE (4xx) messages 30
2.3.1.26 Drop of QoS Performance by reusing RTP's SSRC 31
2.3.1.27 RTP packet injection 31
2.3.1.28 Audio codec modification 32
2.3.1.29 Flujo de audio inaudible 32
2.3.1.30 Registration Table Overflow 33
2.3.1.31 Proxy server flooding 33
2.3.1.32 Physical Eeavesdropping 34
2.3.1.33 Cipher Breakage 34
2.3.1.34 Re-INVITE / Session Replay – Mid Session tricks 34
2.3.1.35 (Monitor de llamadas)Call Tracking (1) 35
2.3.1.36 (Monitor de llamadas)Call Tracking (2) 35
2.3.1.37 Call hijacking helped by the registrar server 36
2.3.1.38 Call hijacking helped by the registrar server (2) 36
2.3.1.39 Registration hijacking by forging SIP REGISTER requests 37
2.3.1.40 Registration Hijacking 37
2.3.1.41 Call redirection using 301/302 response messages 38
2.3.1.42 Call redirection attack using 305 response messages 38
2.3.1.43 Request spoofing 39
2.3.1.44 Call masquerading 40
2.3.1.45 Billing fooling 40
2.3.1.46 Theft of service using a legitimate client's credentials 41
2.3.1.47 Spam call 41
2.3.1.48 Instant messaging spam (SPIM) 42
2.3.1.49 Presence spam 42
2.3.1.50 Distributed Deny of Service (DDoS) 43

2.4 Vulnerabilidades 44

Capitulo 3 Análisis de Riesgos 45
3.1 Análisis de riesgos 45
3.2 ¿Dónde es vulnerable VoIP? 46
3.3 Clasificación de ataques 50
3.4 Métricas de seguridad 52
3.5 Protocolos más comunes usados en VoIP 53
3.6 Métricas aplicadas a activos 55
3.6.1 Protocolos 55
3.6.2 Infraestructura de red 57
3.6.3 Sistemas Operativos 58
3.6.4 Servidor IP PBX 59
Capitulo 4 Propuesta de seguridad "Controles de Seguridad" 61
4.1 Mejores prácticas (Seguridad de red) 61
4.1.1 Seguridad física 61
4.1.2 Separación de equipo de voz y datos 62
4.1.3 Mejores Prácticas "de seguridad del cliente" 62
4.1.4 Autentificación 62
4.1.5 Cifrado 63
4.1.6 Seguridad perimetral 63
4.1.6.1 SBC (Session Border Controller) 63
4.1.6.2 STUN / TURN 64

4.2 Seguridad Básica 65
4.2.1 Actualización de software (IPBX, hardphone y softphone) 65
4.2.2 Bloqueo de la configuración (hardphone/softphone) 65

4.3 Separación de equipos de datos y voz 66
4.3.1 Separación en el nivel IP (capa 3) 66

4.3.2 Separación a través de la VLAN (Capa 2) 66
4.3.3 Filtro Inter-VLAN 67
4.3.4 Usando tarjeta de red 802.1q 68
4.3.5 Deshabilitar ó proteger puertos de red adicionales 802.1q 68
4.3.6 Garantizar el acceso a los puertos de switches (ACL,…) 69
4.3.7 Colocación de servicios convergentes dentro de una DMZ 69

4.4 Autenticación 70
4.4.1 HTTP Digest Authentication de mensajes SIP 71
4.4.2 Autentificación mutua 71

4.5 Cifrado 71
4.5.1 Cifrado del flujo de señalización: SIPS,… 72
4.5.2 Cifrado del flujo de datos media: SRTP,… 73
4.5.3 Cifrado con IPSEC (u otra tecnología VPN) 75

4.6 Seguridad Perimetral 76
4.6.1 SBC: Call Admission Control 77
4.6.2 Uso de servidores dedicados para STUN 77
4.6.3 Verificación de la identidad del servidor STUN 77
4.6.4 STUN Cliente: Continuación de escuchar las respuestas después de recibir la primera respuesta 78
4.6.5 Limitar el ancho de banda asignado por persona 78

4.7 Matriz Ataques- Soluciones 79
4.7.1 Controles para mitigar los riesgos 79
4.7 Conclusiones 81
Anexo A
Bibliografía.

Lista de figuras

Figura 1: Familia de protocolo H. 323 5
Figura 2: Diagrama de un equipo terminal 6
Figura 3: Voice over Packet Networks 8
Figura 4: Proceso de llamada con H323 10
Figura 5: Operación SIP Proxy 11
Figura 6: SIP Redirector Server 12
Figura 7: Como MGCP coordina al Media Gateway 13
Figura 8: VoIP vulnerabilities based on protocol layers 45
Figura 9: Componentes vulnerables VoIP 47
Figura 10: Herramientas de testeo de seguridad más comunes 51
Figura 11: Administración efectiva de riesgos 60
Figura 12: Separación de datos 67
Figura 13: Servicios convergentes dentro de una DMZ 70
Figura 14: Encriptación Cliente – Servidor 73
Figura 15: Formato de Voz 74

Lista de tablas

Tabla 1: Descripción de ataque en los niveles de VoIP 16
Tabla 2: Requerimientos de seguridad y amenazas a red VoIP 48
Tabla 3: Ataques a red VoIP 49
Tabla 4: Vulnerabilidades de seguridad en red VoIP 50
Tabla 5: Categorías de riesgos 52
Tabla 6: Frecuencias de categorías 53
Tabla 7: Métricas de amenazas 53
Tabla 8: Protocolos comunes usados en VoIP 54
Tabla 9: Métricas activo protocolo 57
Tabla 10: Infraestructura de red 57
Tabla 11: Sistemas operativos 58
Tabla 12: Servidor IP-PBX 59

Capitulo 1: Introducción

Prefacio

El presente capítulo describe la metodología utilizada para la elaboración de esta tesis. Esto pretende dar un panorama inicial del trabajo y trata de preparar a los lectores a conocer del contenido del trabajo.

1.1 Antecedentes

Los riesgos son inevitables en las primeras etapas de adopción de cualquier tecnología nueva o venidera, principalmente debido a antecedentes limitados o experiencias pasadas. Los riesgos relacionados con la adopción de la tecnología VoIP requieren apropiada consideración a fin de tomar una decisión comercial acertada con anterioridad a su implementación. Es decir, estas tecnologías deben alinearse a los planes comerciales estratégicos de la organización. La aplicación de medidas para minimizar los riesgos de la implementación facilitará la obtención de posibles beneficios. Cada vez más los organismos de control están influenciando los principios de gobierno corporativo. Es decir, obligan a las organizaciones a que consideren ampliamente sus riesgos, en especial aquellos relacionados con la TI.

El aumento de la complejidad técnica al integrar voz y datos en una red, aumenta a su vez la dependencia de la organización en la disponibilidad de la red. Muchas organizaciones no reconocen que con este incremento de la complejidad técnica, aumentan los riesgos de seguridad y disponibilidad de la red, que deben ser adecuadamente evaluados, así como se deben aplicar las medidas necesarias de administración del riesgo.

La seguridad y los riesgos relacionados con la implementación de la tecnología VoIP deben estar presentes en forma contundente en un caso de negocio de adopción de tecnología bien estructurado. En un mercado implacable, las consecuencias de un incidente importante con relación a la seguridad pueden ser substanciales en términos de interrupciones comerciales, pérdida de confianza por parte de los clientes o mayores costos incurridos por fraude o pérdida de oportunidades de negocios.

1.2 Objetivo

El objetivo del presente trabajo es presentar los riesgos, amenazas y vulnerabilidades adheridas a la tecnología VoIP, Con esta tecnología, el tráfico de voz se transforma en datos y por lo tanto se expone a riesgos de confidencialidad, integridad y

disponibilidad. Las aplicaciones de la tecnología VoIP corre el riesgo de cualquier proyecto de TI importante - inadecuada obtención de beneficios, falta de coordinación en los objetivos estratégicos y exceso en los costos. Y para disminuir estos riesgos se necesitan controles de seguridad y en este trabajo mostramos las mejores prácticas de seguridad para la tecnología VoIP.

1.3 Justificación

En un mundo de globalización representado por Internet, las redes actuales son más globales. Como el comercio electrónico, y las aplicaciones de Internet siguen creciendo, y es importantísimo encontrar el equilibrio entre seguir aislado o abrirse a ese mundo, el encumbramiento del comercio móvil y las redes inalámbricas son como el cañón para los muros de un castillo; destrozan el modelo antiguo y demandan la integración sin fisuras de soluciones de seguridad, mas trasparentes y mas flexibles. (Cisco Firewall 2005)

En la actualidad, la falta de medidas de seguridad en las redes es un problema que está en crecimiento y que cada vez es mayor el número de atacantes y cada vez están más organizados. Y para comprobar esto Ernst & Amp, Young (2004) nos muestran de un estudio que se realizo en 1235 organizaciones de distintas industrias (servicios financieros, salud y manufactura), que representan a algunas de las compañías líderes en 51 países, frente a un escenario de incidentes, 77% de las organizaciones destaca que tienen un plan de respuesta y 63% que realiza evaluaciones de vulnerabilidad y penetración en forma regular. Sin embargo, solo 13% considero que su nivel de protección es muy adecuado para defenderse de los ataques externos. Una de las cuestiones que no deja de preocupar a las compañías es el desarrollo de un plan de continuidad del negocio y de un plan de recuperación de desastres: de la encuesta surge que 77% lo tiene desarrollado, pero sólo 58% lo ha probado. Por último, menos de la mitad de los encuestados brindan a sus empleados un entrenamiento constante en seguridad y controles y sólo 24% le otorgo a su departamento de seguridad informática el puntaje más alto en satisfacer las necesidades de la organización.

Para Ruiz (2002) citado en (Blanco 2004) nos dice que la seguridad se está convirtiendo en una prioridad porque la comunicación y la información se han convertido en un factor dominante en el desarrollo económico y social. Las organizaciones desean explotar las posibilidades de las redes de comunicaciones, la seguridad de estos sistemas se está convirtiendo en un requisito previo para el progreso, y que en México, aun hace falta mucho por hacer en cuanto a la cultura de seguridad de información y de telecomunicaciones se refiere.

Señala que sucesos como robo de información, manipulación de datos, se consideran un grave problema ya que al no tener implementados procesos o metodologías de seguridad, las empresas se encuentran expuestas a constantes ataques los cuales pueden ser minimizados a través de modelos de seguridad que puedan adecuarse a las necesidades de las empresas de este país. Ruiz (2002).

1.4 Estructura del trabajo

En este trabajo de tesis se pretende mostrar las dar definición de las amenazas, ataques y vulnerabilidades de la tecnología VoIP, y los elementos necesarios para contrarrestar estas amenazas. También se definirá una matriz de riesgos con la cual a través de ella podremos buscar la solución adecuada al tipo de ataque a esta tecnología.

Capitulo 2: Revisión de Literatura

2.1 Concepto de VoIP

Originalmente la voz y los datos se transmitían a través de sistemas completamente separados. En la comunicación de las organizaciones actuales, el acceso a las redes de datos es tan importante como las comunicaciones telefónicas. Sin embargo en estos días es posible realizar las comunicaciones de voz en las redes internas de las organizaciones utilizando el protocolo IP de Internet (VoIP). De esta forma, la convergencia entre redes ha tenido ya lugar: voz y datos utilizan la misma red, están entremezcladas y forman la base de las soluciones integrales de negocios (Bertels, 2001).

Tradicionalmente los servicios de telefonía y de datos se soportan por redes distintas y basadas en tecnologías completamente diferentes. Para el transporte de voz se ha utilizado hasta ahora las redes telefónicas clásicas, las cuales están basadas en las técnicas de conmutación de circuitos, especialmente desarrolladas para cumplir con las características del tráfico de voz: un tráfico representado inicialmente mediante señales analógicas que más tarde es convertida en una señal digital, que se caracteriza por tener un flujo constante de información (Fernández y Zangger, 2001).

Como menciona Fernández y Zangger (2001), el desarrollo y madurez de las técnicas de transmisión de voz sobre redes de paquetes ha dado lugar a una fuerte tendencia hacia la integración del tráfico de voz en las redes de datos. Aunque a pesar de que en sus inicios se pensaba que la tecnología IP (Internet Protocol) no ofrecería la calidad suficiente y seguridad, actualmente los últimos desarrollos en esta área han cambiado totalmente esa idea, convirtiendo esta tecnología en un estándar de facto para las comunicaciones de datos, voz y otros tráficos de multimedia. Por ello son cada vez más las

empresas que se plantean unificar sus actuales comunicaciones utilizando lo que se ha venido a denominar convergencia de redes (Cable & Wíreless, Cisco System, 2001).

El concepto de VoIP (Voice over IP) es muy simple, se trata de transformar la voz obtenida a paquetes de información y ser manejados y transmitidos por una red IP, y tener la posibilidad de interconectar esta red de datos con la red de telefonía convencional o PSTN. Gracias a esto se pueden tener beneficios como ahorro en los gastos de llamadas de larga distancia y la introducción de nuevas funcionalidades que ofrece la Telefonía IP. (Davison ,2000)

Las redes de Voz sobre protocolo de Internet (VoIP) por sus siglas en inglés son la mayor evolución en telecomunicaciones ello ha acelerado la convergencia de Internet y la redes de telefonía pública (PSTN). Las redes VoIP proveen un atractivo valor de proposición para los proveedores de servicios para migrar por separado los servicios de redes de voz y datos dentro de una red infraestructura convergente.

La telefonía IP tiene una infraestructura que es construida normalmente por diferentes componentes.

2.2 Componentes

2.2.1 Terminal

Una terminal H.323 es un dispositivo de usuario final que facilita las comunicaciones bi-direccionales en tiempo real con otra terminal. Esta puede dar soporte de audio, voz y datos. Una terminal dispone de funciones y capacidades descritas a continuación. (Rodera, 2005)

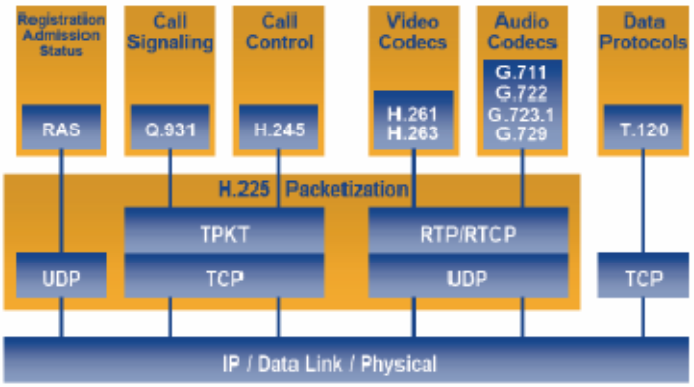

Figura 1, Familia de protocolo H. 323, TippingPoint Technologies (2004)

- La unidad de control del sistema, (H.245 y H.225.0), que proporciona control de llamada, el intercambio de capacidad, el envío de mensajes y la señalización.
- Transmisión de media, que se encarga de recibir los flujos de audio, video, datos, control y mensajes hacia la interfaz de red Codec de Audio, el cual codifica la señal de audio del micrófono para transmisión y decodifica el audio recibido hacia el altavoz. Requiere de G.711µ y G711a y codecs de audio como G722, G723.1, G728 y G729.
- Interfaz de red, debe dar servicio de extremo a extremo fiable para el canal de control H.245, los canales de datos y el canal de señalización de llamada.
- Codec de video, esta función es opcional y su función es codificar y descodificar video de acuerdo con la recomendación H.261 Quarter Comment Intermediate Format (QCIF).
- Canal de datos. Soporta aplicaciones tales como acceso a bases de datos, transferencias de ficheros, etc. (Rodera, 2005)

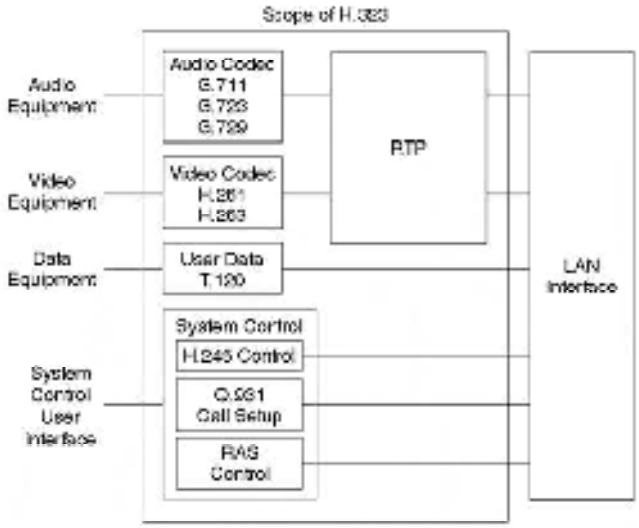

Figura 1.2: Diagrama de un equipo Terminal.

Figura 2, Diagrama de un equipo terminal (Rodera, 2005)

2.2.2 Servidores

Para establecer una llamada de voz sobre IP (VoIP), es necesario las terminales con una dirección IP y un puerto. Las terminales registran su dirección IP, el servidor almacena estas direcciones ò los números de teléfonos asociados, cuando un teléfono liga un numero, el servidor intenta resolver ese número a una dirección IP. Para conseguir obtener esta información el servidor se comunica con otros servidores ò servicios, el servidor de telefonía IP es responsable de la autentificación de los registros.

2.2.3 Gateways

Suelen llamarlos de diferentes maneras, por las comunidades de telecomunicaciones.

- Media gateways MGs
- Interworking functions IWFs
- Frame relay access devices FRADs

La red de VoIP utiliza Media Gateway para realizar las funciones tradicionales del codec conversión de analógico a digital del tráfico de la voz y crear paquetes de voz IP. Proporciona el interfaz necesario para transportar el contenido de la voz sobre la red del IP y es fuente del tráfico portador de VoIP. Típicamente, los Media Gateways convierten cada conversación o llamada en una sola sesión del IP transportada por RTP que funciona sobre User Datagram Protocol (UDP) por sus siglas en inglés.

La figura 3 muestra la operación genérica del procesamiento de voz en un Gateway, que adopta la voz por ejemplo en una T1, se ve en los canales individuales en cada spot de tiempo de la T1 y analiza el contenido de cada slot de tiempo. Lo primero que buscará será la frecuencia del modem, esta será una audio frecuencia de 2.1 Khz. y si no hay tal frecuencia, entonces buscará la presencia de una señal multifrecuencia tono dual (DTMF) (Wright, 2001).

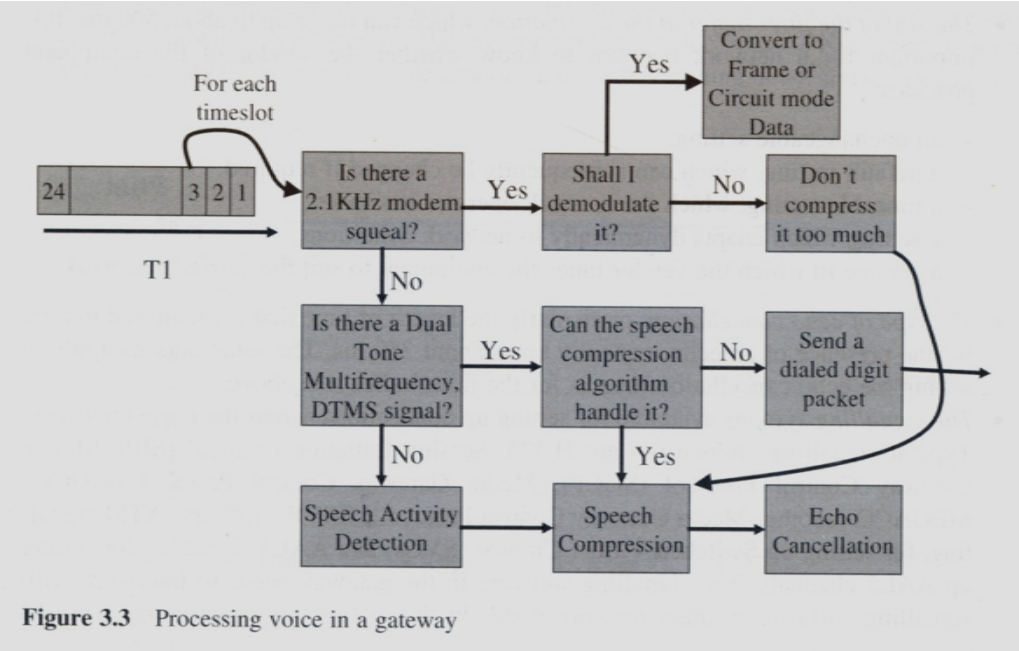

Figura 3, Voice over Packet Networks, 2001.

Si no hay una señal DTMF o frecuencia de modem, Entonces se supone que hay un speech humano sobre este espacio de tiempo. Se remueve el silencio del speech, y se aplica

un algoritmo de compresión de voz y cancelación de eco con el fin de generar paquetes de voz que se envían fuera en el paquete de voz de la red.
Por otro lado si se detecta la frecuencia de modem, hay dos alternativas.

1.- usar un algoritmo de codificación de voz, posiblemente el mismo que se usa para discurso humano, pero no se puede usar un codec que comprima el discurso demasiado, por ejemplo Vocoding. El modem no puede ser codificado por codecs del mismo tipo. Típicamente se usa un algoritmo de compresión que genera 64,32 o 16 Kbps.

2.- Esta opción es para fax tráfico de datos sobre un modem es convertida dentro de un marco de datos. En otras palabras, se demodula el fax o los datos, convirtiéndolos dentro de paquetes de datos y enviados sobre paquetes de red como paquetes de datos. (Wright, 2001)

Proporcionan características opcionales, tales como compresión de voz análoga y/o digital, cancelación de eco, supresión del silencio, y acopio de la estadística. Las características y los servicios de la entrada de los medios pueden incluir alguno ò todo lo siguiente:

- Trunking Gateway que interconectan entre la red del PSTN y una red de VoIP. Tales Gateways manejan típicamente una gran cantidad de circuitos digitales.
- Cajas cable/módem, dispositivos del xDSL, dispositivos wireless banda ancha y otro Gateways residenciales que proporcionan un interfaz análogo tradicional a una red de VoIP.
- Escala-Reducida (empresarial) de VoIP Gateways y otros MG de acceso que proporcionan interfaz análogo o digital tradicional de PBX a una red de VoIP.

La industria utiliza a veces los términos “Gateway” y “Gatekeeper” alternativamente. Esto refleja el hecho de que los avances de la tecnología ahora permiten al mismo dispositivo realizar funciones gatekeeping - control de la admisión de la llamada y “Bandwidth Management” así como la conversión de analógico a digital y la otra tarea de procesamiento de voz tradicionalmente asociada con MD. (Juniper, 2007)

La señalización de los protocolos implementados en una solución VoIP determina las características y funcionalidades disponibles. Así como la forma en que los componentes de VoIP interactúan entre sí. Actualmente, una variedad de protocolos e implementaciones de VoIP con una amplia gama de funciones están en uso.

Los elementos son:

- H323, estándar de la ITU para establecer conexiones VoIP.
- SIP, estándar de Internet Engineering Task Force (IETF) para establecer conexiones VoIP.
- MGCP, Primer protocolo desarrollado por IETF para control de la Señalización entre componentes de VoIP.
- H.248, El protocolo de la IETF y la ITU para el uso de señales de control de la información entre VoIP.

2.2.4 Conexiones con H323.

Opción por parte de ITU para establecer conexiones VoIP, este es un paquete basado en sistema de comunicación multimedia, sus especificaciones definen varias funciones de señalización. Así como formatos relacionados con paquetes de servicios de audio y video.

Las redes H323 contienen tres componentes de solución primaria:

- Servidor de procesamiento de llamadas, Que almacenan y aplican la información sobre topologías de red, ruteo de llamadas a Gateways VoIP y dispositivos de usuario final.
- MG, terminación final e interfase con redes No-H323, tal como PSTN.
- Gatekeepers, funciona como una unidad central para control de admisión, manejo de ancho de banda, y señalización de llamadas.

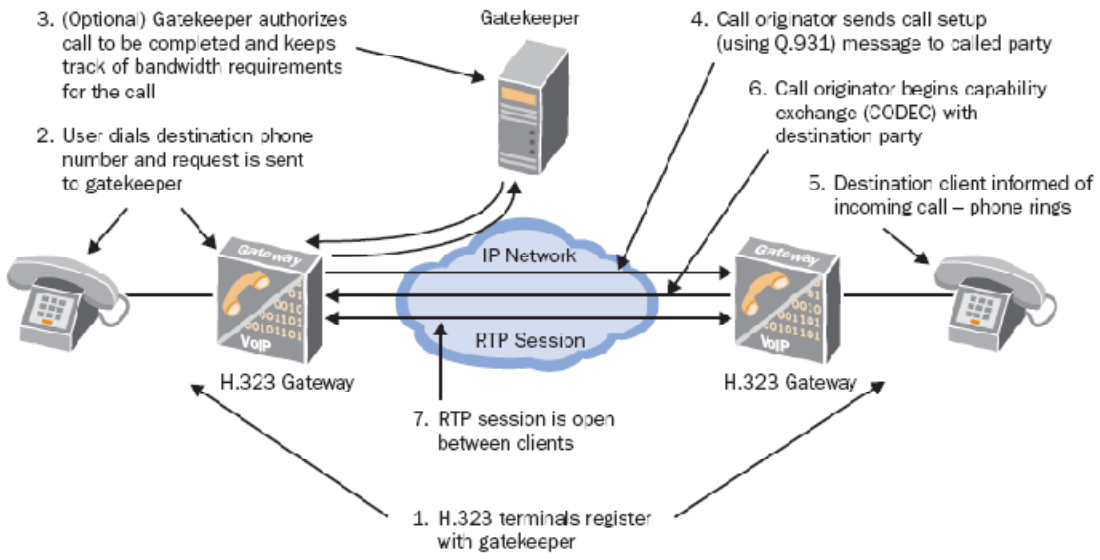

Figure 2: H.323 Call Setup Process

Figura 4, Proceso de llamada con H323, (Juniper, 2007)

2.2.5 Conexiones con SIP

Es un protocolo desarrollado por el IETF MMUSIC Working Group con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual. Durante el año 2000, SIP fue aceptado como el protocolo de señalización de 3GPP y elemento permanente de la arquitectura IMS (*IP Multimedia Subsystem*). SIP es uno de los protocolos de señalización para voz sobre IP, acompañado por H.323.

Las aplicaciones cliente-servidor SIP son compatibles con la movilidad de usuario con dos modos de funcionamiento: Proxy y Redirect. En modo proxy, los clientes SIP envían solicitudes al servidor proxy. Este se encarga de las solicitudes o las remite a otros servidores SIP, ayuda a enrutar las peticiones hacia la localización actual del usuario, autenticar y autorizar usuarios para darles servicio, posibilitar la implementación de políticas de enrutamiento de llamadas, y aportar capacidades añadidas al usuario

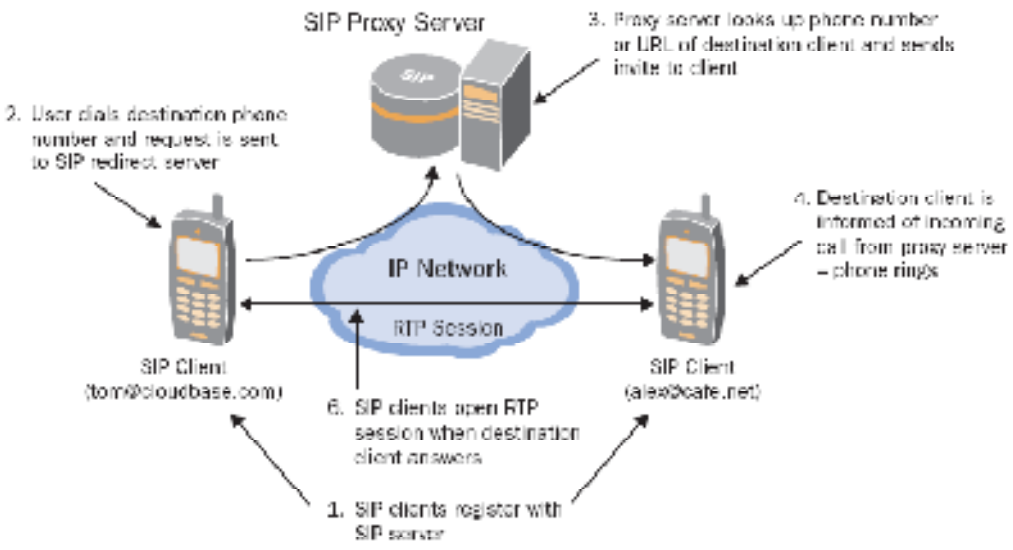

Figura 5. Operación SIP Proxy (Juniper, 2007)

Cuando el servidor SIP opera en modo Redirect, el cliente SIP envía la solicitud a el servidor SIP, entonces mira la dirección destino, El servidor SIP devuelve la dirección de destino para el iniciador de la llamada, que la usa para indicar el destino SIP cliente.

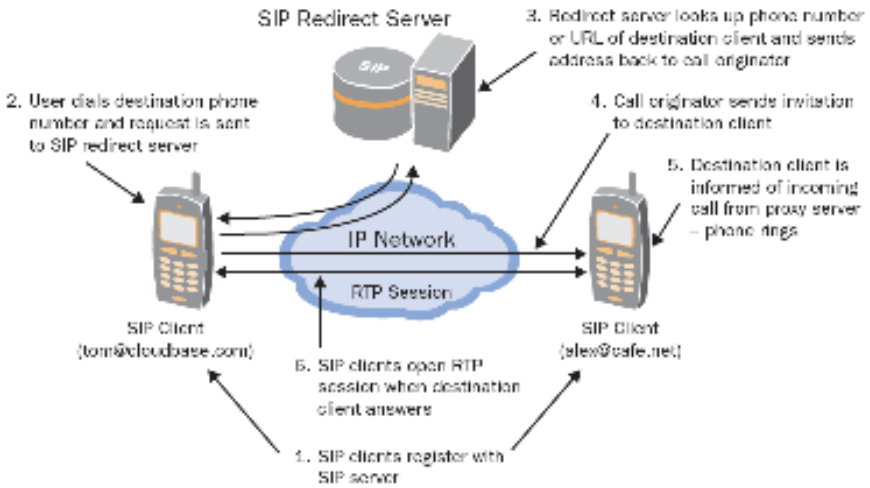

Figura 6, SIP Redirector Server (Juniper, 2007)

SIP (tal como se define en RFC 2345) es la base para el (IMS) IP Multimedia Subsystem. Datos multimedia y protocolo de control que la IETF está desarrollando en relación con el Proyecto Tercera Generación (3GPP). IMS utiliza SIP y otras interfaces estándar entre aplicaciones, capas de red, y los sistemas de back-office para la creación de

un marco flexible que puede ofrecer cualquier tipo de tráfico de voz, datos, vídeo, o multimedia sobre cualquier red de acceso alámbrica o inalámbrica.

ITU y IETF definieron los protocolos de control VoIP diseñados para el intercambio de Control de señalización de información entre los elementos de redes VoIP. El anterior de este protocolo, MGCP, es actualmente apoyado por IETF como un estándar informal. MGCP es un predecesor incompleto de H248. (Juniper, 2007)

2.2.6 MGCP

Fue definido en el RFC 2705 Media Gateway Control Protocol, como un estándar de Internet por el IETF. Este Protocolo divide la funcionalidad en segmentos de un switch de voz tradicional en tres unidades funcionales: Media Gateway, Media Gateway Controller, Signaling Gateway. Esto permite a manejar cada VoIP gateway independientemente como entidad separada.

MGCP es un protocolo de control maestro-esclavo que coordina las acciones del media gateway. Se utiliza para controlar el gateway control a fin de facilitar el acceso a la red PSTN (Public Switched Telephone Network) por sus siglas en ingles, y viceversa. Utilizado para convertir los datos de un formato que se utiliza en PSTN a una que se utiliza en redes IP que se utilizan para el transporte de paquetes de datos

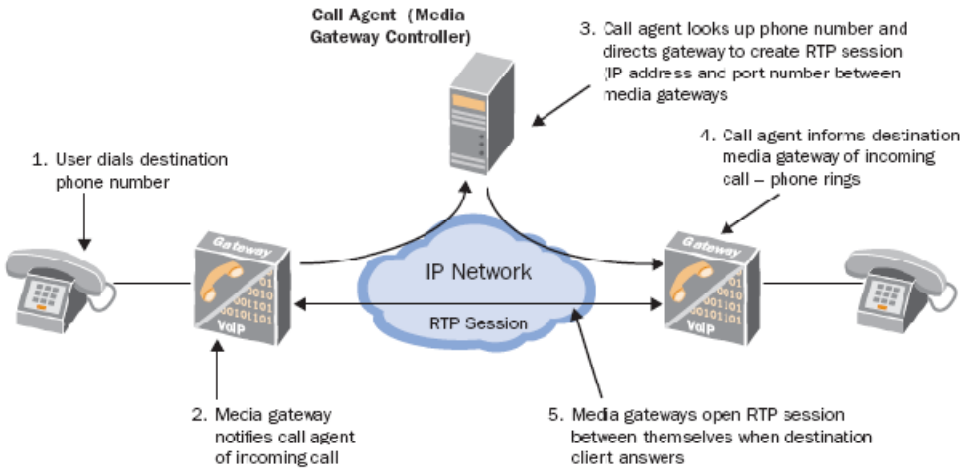

Figura 7, Como MGCP coordina al Media Gateway (Juniper, 2007)

2.2.7 Megaco/H248

Es el resultado de la colaboración entre los estándares de IETF e ITU. Define el mecanismo necesario de llamada para permitir a un controlador Media Gateway el control de puertas de enlace para soporte de llamadas de voz/fax entre redes RTC-IP ó IP-IP. Este protocolo está definido por la IETF RFC 3525.

Antes de la cooperación entre ITU e IETF, existían diversos protocolos que cumplían estas funciones; entre ellos se encontraban MDCP y MGCP.

H.248 es un complemento a los protocolos H.323 y SIP: se utilizará el H.248 para controlar al Media Gateways y el H.323 ó SIP para comunicarse con otro controlador Media Gateway.

2.3 Amenazas, vulnerabilidades y ataques.

La convergencia de voz y datos por el mismo medio de transmisión, Es una de las consecuencias de esta convergencia, en caso de un gran ataque a la red, la infraestructura de las telecomunicaciones de la organización puede estar en peligro. Menciona Porter, (2006) que para asegurar toda la infraestructura de VoIP requiere de la planificación, el análisis, y de un conocimiento detallado acerca de las características específicas de la aplicación que se elija usar.

Una amenaza es el potencial para un evento o circunstancia activa o pasiva que puede causar daño físico o financiero, mientras que el ataque es un evento hostil actual ejecutado usando un script automático dañino como virus o gusano. Rontti (2006). En Cisco System una amenaza lo describen como un acceso no autorizado a una red. Estas

amenazas son persistentes debido a las vulnerabilidades, que son problemas que pueden surgir como resultados de una mala configuración del hardware o software, un diseño pobre de la red, unas carencias tecnológicas heredadas o el descuido del usuario final. Como lo describen en Cisco Firewall (2005).

La seguridad de información almacenada o en tránsito, es de vital importancia para los negocios modernos. Las empresas requieren que dicha información esté disponible y que sea completamente confiable y protegida contra intrusos. Los medios de proporcionar tal aseguramiento a las organizaciones son a través de un estándar de seguridad. El ISO 17799 es el estándar de seguridad más reconocido en el mundo. Hefferan (2003).

Las motivaciones para esos ataques son numerosas y pueden variar desde utilizar los sistemas comprometidos para atacar a otros sistemas, realizar espionaje industrial, e incluso por simples razones maliciosas como perturbar y dañar sistemas. (Keith 2003).

(Keith 2003). Comenta que existen, literalmente docenas de diferentes formas de que un intruso consiga tener acceso a un sistema las más habituales serian:

- Ingeniería social.
- Errores de software.
- Virus y código troyano.
- Configuración pobre del sistema.

Para proteger a los usuarios de estos ataques, Young (2003) hay que integrar adecuadas soluciones para la seguridad del sistema, tales soluciones para todo este tipo males creados por actividades criminales serian las técnicas criptográficas. La autentificación, integridad de mensajes, y la encriptación son muy importantes en la cultivación, improvisación y promoción de la seguridad en Internet. Y que sin tales procedimientos de autentificación un atacante puede tener acceso a la red una y otra vez.

Tradicionalmente, las redes de comunicaciones se pueden clasificar en redes de voz y de datos quienes a su vez se clasifican según la técnica de conmutación que se emplea, es decir pueden ser basadas en conmutación de circuitos, de paquetes o de mensajes. (Huidobro, 2001).

Clasificación de ataques

Estas pruebas se pueden estructurar en niveles:

- Ataque externo sin conocimiento del sistema, localiza el sistema, aprende lo suficiente para poder accederlo.
- Ataque externo con acceso al sistema, puede hacer login y acceder a los servidores de red, a menudo intenta ampliar el nivel de acceso.
- Ataque interno con acceso al sistema, los verificadores o tester son usuarios autorizados con cuentas restringidas, son como usuarios ordinarios, el objetivo es obtener privilegios o información no autorizada. La utilidad del estudio de penetración se basa en la documentación, las conclusiones indican si los defectos son o no endémicos, no proceden del éxito o fallo en la penetración intentada. Areitio Bertolín (2006)

La siguiente lista solo hace referencia a la clasificación de las amenazas más conocidas con el uso de la tecnología VoIP.

- DoS
  Ataques con resultado de la falta de disponibilidad del servicio/sistema para usuarios legítimos.

- Escucha clandestina
  Ataques que pueden escuchar todo el trafico de voz ó datos, este tráfico no sufre cambios solo es observado.

- Manipulación del tráfico.

Los ataques pueden desviar el tráfico hacia el intruso, esta desviación puede ser para redirigir una llamada a una persona ilegítima ó para incluir una persona ilegitima en la conversación.

- Identidad
  Ataques basados en la manipulación de la identidad (usurpación, robo,…)

- Robo de servicio.
  Ataques para utilizar un servicio sin tener que pagar el costo al proveedor.

- Manipulación de comunicación
  Ataques que permiten la comunicación de un intruso para establecer comunicación con un usuario legitimo.

La tabla siguiente describe los niveles generales que puede ser atacada una infraestructura VoIP.

Vulnerabilidad	Descripción
Infraestructura IP	Vulnerabilidades no relacionadas a sistemas No-VoIP pueden dar lugar a compromiso de la infraestructura VoIP.
Sistema operativo	Los dispositivos VoIP heredan las mismas vulnerabilidades como el sistema operativo o firmware de las que se ejecutan.
Configuración	En su configuración por defecto la mayoría de los dispositivos VoIP trae exceso de servicios abiertos, esto servicios por defecto corren sobre puertos abiertos los cuales pueden ser vulnerables a ataques DoS, desbordamientos del buffer o autentificación bypass.
Nivel de aplicación	Tecnologías inmaduras pueden ser atacadas para interrumpir o manipular los servicios.

Tabla 1, Descripción de ataque en los niveles de VoIP, 2006.

Porter, Bassin, Chaffin, & Cross (2006) señalan que hay varias formas de clasificar a las amenazas, en VoIP figuran amenazas concretas usando una clasificación simplificada: Datos, interrupción de servicio, robo de datos y servicios VoIP.

2.3.1 Tipo De Riesgos

La introducción de la Tecnología VoIP significa que el tráfico de voz debe tratarse en el mismo contexto que los datos, a los fines de la seguridad, ya que comparten el mismo medio. El aumento de la complejidad técnica al integrar voz y datos en una red, aumenta a su vez la dependencia de la organización en la disponibilidad de la red. Muchas organizaciones no reconocen que con este incremento de la complejidad técnica, aumentan los riesgos de seguridad y disponibilidad de la red, y que deben ser adecuadamente evaluados, así como se deben aplicar las medidas necesarias de administración del riesgo para estas amenazas y ataques.

A medida que se reemplazan los sistemas PABX por computadoras y equipos de red con sistemas operativos convencionales, las redes se tornarán cada vez más vulnerables a las amenazas comunes, tales como ataques de virus y de negación de servicios (DoS). Las exposiciones que se experimentaron con los sistemas convencionales son más usuales con la tecnología VoIP, ya que el conocimiento sobre redes es mayor. Cada punto de ingreso a la red es un potencial punto de ataque y por lo tanto la administración del riesgo es esencial. Esto lógicamente incluye cada auricular de teléfono habilitado con la tecnología IP u otro dispositivo telefónico de IP.

Los siguientes puntos mostrados son algunos ejemplos adicionales de interceptación de señalización o llamada y Hijacking. Esta clase de amenazas, aunque normalmente más difícil de lograr que DoS, puede resultar significativa pérdida o alteración de los datos. Ataques de DoS, ya sean causados por métodos activos o involuntariamente, a pesar de su importancia en términos de calidad de servicio, se encuentran muy a menudo irritante para los usuarios y administradores. Interceptación y el secuestro de los ataques, por otra parte, son casi siempre activa con los ataques de robo de servicio, información, o monetario como objetivo. Baugher (2004).

Interrupción de Servicio.

VoIP Call Data Flood
VoIP Implementation DoS Exploit
VoIP Protocol DoS Exploit
Network Service DoS Attacks
VoIP Endpoint PIN Change
VoIP Packet Injection
QoS Modification
VoIP Control Packet Flood
TCP/UDP/ICMP Packet Flood
OS/Protocol Implementation DoS Exploit
Wireless DoS Attack
VoIP Application Dos Attacks
VoIP Packet Replay
VoIP Packet Modification
VLAN Modification

Robo de Datos y Servicios.

VoIP Social Engineering
ARP Cache Poisoning
Network Eavesdropping
Address Spoofing
VoIP Control Eavesdropping
VoIP Voicemail Hacks
Rogue VoIP Device Connection
VoIP Call Hijacking
VoIP Application Data Theft
VoIP Call Eavesdropping
VoIP Toll Fraud

El ataque Negación de servicio (DoS) puede afectar algunos servicios basados en redes IP, El impacto de un ataque DoS pueden variar desde la degradación leve del servicio a la pérdida completa de servicio. Hay varias clases de ataques de DoS. Un tipo de ataque en el cual los paquetes pueden simplemente ser inundadas dentro ò en la red objetivo de múltiples fuentes externas es llamado ataque distribuido de denegación de servicio (DDoS). Abdelnur, Cridlig, State and Festor (2006).

La segunda gran categoría de Negación de Servicio (DoS) se produce cuando las condiciones dentro de los dispositivos de la red interna son el blanco de una avalancha de paquetes de manera que fallen, Como en el escenario DdoS descrito anteriormente, se produce la interrupción del servicio de agotamiento de los recursos principalmente los recursos de ancho de banda y CPU. Para Ejemplo, algunos teléfonos IP dejan de funcionar si reciben un paquete UDP más grandes de 65534 bytes en el puerto 5060. Porter, Abdelnur, Cridlig, State and Festor (2006).

Ni controles de integridad ni encriptación puede prevenir estos ataques. Ataques DoS ò DDoS se caracterizan simplemente por el volumen de paquetes enviados hacia el ordenador victima; si esos paquetes están firmados por un servidor, real o contener direcciones IP falsas, o están cifrados con una clave ficticia, ninguno de estos son relevantes para el ataque. Ataques de DoS son difíciles de defender, y debido a que VoIP es sólo otro servicio de la red IP, no es menos susceptible al ataque DoS como cualquier otro servicio de la red IP. Kent (1998). Además, los ataques de DoS son especialmente eficaces contra los servicios como VoIP Y otros servicios en tiempo real, ya que estos servicios son más sensibles a las repercusiones negativas de la red. Los virus y gusanos se

incluyen en esta categoría, ya que a menudo la causa DoS o DDoS debido al aumento de tráfico de la red que se generan como parte de sus esfuerzos para reproducirse y propagarse. Kent (1998).

Sistemas de VoIP deben cumplir con estrictos requisitos de disponibilidad de los servicios. Algunos ejemplos de amenazas DoS puede hacer que el servicio de VoIP sea parcial o totalmente no disponible, Esta lista no es exhaustiva, pero ilustra algunos escenarios de ataque. Porter, Kuhn, T.J. Walsh, and S. Fries (2004).

2.3.1.1 VoIP Packet Replay Attack

Captura y reenvía paquetes VoIP fuera de la secuencia (por ejemplo, RTP SSRC - SSRC es un campo de encabezado de RTP que significa Fuente de sincronización) a puntos finales, añadiendo demora a la llamada en curso y degradando la calidad de la llamada. Kuhn (2004).

2.3.1.2 Data Tunneling

No es exactamente un ataque, sino más bien a través de un túnel de datos crea llamadas de voz, en esencia, una nueva forma de módem no autorizada. Por transporte de las señales de módem a través de una red de paquetes mediante el uso de modulación código de pulso (PCM) codificada por paquetes o residen en la información de cabecera, VoIP puede ser utilizado para apoyar un módem a través de una llamada sobre una red IP. Esta técnica puede utilizarse para eludir o debilitar un modem de escritorio y ocultar la conexión desautorizada datos. Esto es similar en concepto a lo que se llama "IP sobre HTTP" (es decir, "Firewall Enhancement Protocol "RFC 3093), un clásico problema para algunos puertos abiertos sobre un cortafuegos de fuentes internas. M. Gaynor, S. Bradner (2001).

2.3.1.3 QoS Modification Attack

Modificar protocolos de control no específicos de VoIP en campos de información en los paquetes de VoIP y de datos de terminales IP para degradar o negar el servicio de voz. Weatherspoon (2000) Por ejemplo, si un atacante cambiara 802.1Q VLAN tag o paquetes de bits IP ToS, por comprometer la configuración de dispositivos de punto final, el atacante podría perturbar la calidad del servicio de una red de VoIP. Subordinando tráfico de voz a tráfico de datos, por ejemplo, el atacante podría retrasar considerablemente entrega de los paquetes de voz. Porter, (2006).

2.3.1.4 VoIP Packet Injection

Envía paquetes de VoIP forjados a la terminal IP, a los que se inyectan voz, ruido ó lagunas en llamada activa. Por ejemplo, cuando se utiliza RTP sin autenticación de los paquetes RTCP (y sin muestreo SSRC), un atacante puede inyectar paquetes RTCP en un grupo de multidifusión, cada uno con una diferente SSRC, que puede crecer exponencialmente el tamaño del grupo. Porter (2006).

2.3.1.5 DoS against Supplementary Services

Iniciar un ataque DoS contra otros servicios de la red sobre la que depende el servicio de VoIP (por ejemplo, DHCP, DNS, BOOTP). Por ejemplo, en las redes de VoIP, donde se basan las terminales IP, DHCP asigna direcciones, desactiva el servidor DHCP impide puntos finales telefónicos (soft y hard) de la adquisición de la información de direccionamiento y enrutamiento que necesitan para hacer uso del servicio VoIP. Abdelnur, Cridlig, State and Festor (2006).

2.3.1.6 Control Packet Flood

Servidores Flood VoIP o terminales IP con paquetes de llamadas no autenticados (por ejemplo, H.323 GRQ, RRQ, URQ paquetes enviados a UDP/1719). La intención del atacante es agotar el dispositivo, sistema, o los recursos de la red en la medida en que el servicio de VoIP quede inutilizable. Algún puerto abierto en el procesamiento de la

llamadas por mantenimiento o administración o servidores relacionados con VoIP pueden ser objetivos para este ataque DoS. Porter, Abdelnur, Cridlig, State and Festor (2006).

2.3.1.7 Wireless DoS Attack

Iniciar un ataque DoS en Terminales de VoIP inalámbrica enviando tramas 802,11 o 802.1X que causa la desconexión de red (por ejemplo, 802.1X EAP –fallas, ataque WPA MIC, radio espectro interferencias). Weatherspoon (2000) Por ejemplo, un mensaje de integridad de código ataque explota una contramedida en virtud del cual un punto de acceso inalámbrico desvincula estaciones cuando se recibe dos tramas inválidas con 60 segundos, causando la pérdida de conectividad de la red durante 60 segundos. En un entorno de VoIP, una interrupción de 60 segundos de un servicio es bastante extrema. Porter, Abdelnur, Cridlig, State and Festor (2006).

2.3.1.8 Bogus Message DoS

Envía a los servidores VoIP o terminales IP paquetes del protocolo VoIP que causan desconexión en llamadas o condiciones de red ocupada. (Por ejemplo, RTP SSRC colisión, forjado RTCP BYE, forjado CCMS, Botón de empuje falso en Terminales). Estos ataques causan un proceso de mensajes falsos al teléfono y hacen terminar incorrectamente una llamada, o inducir a un error para creer que parte de la línea de llamada está ocupada. Porter (2006).

2.3.1.9 VoIP Protocol Implementation DoS

Enviar a servidores VoIP o terminales IP paquetes no válidos para explotar el protocolo VoIP una implementación de vulnerabilidad del ataque DoS.

2.3.1.10 Packet of Death DoS

Inundación de Servidores VoIP o terminales IP con paquetes o fragmentos al azar de TCP, UDP, ICMP para agotar el rendimiento del CPU, ancho de banda, sesiones TCP, y así sucesivamente. Por ejemplo, un atacante puede iniciar un TCP fuera de la Banda ataque DoS mediante el envío de un gran volumen de paquetes TCP marcado "prioridad de entrega" (TCP bandera de Urgente). En cualquier inundación, el aumento de la transformación de carga interfiere con la capacidad del sistema receptor para procesar tráfico real, en un principio retrasar el procesamiento de tráfico de voz, pero en última instancia, perturbando el servicio completo. Abdelnur, Cridlig, State and Festor (2006).

2.3.1.11 IP Phone Flood DoS

Envía un gran volumen de datos de una llamada hacia una terminal VoIP para agotar el rendimiento del CPU, ancho de banda, las sesiones TCP, Y así sucesivamente. Sistemas de respuesta de voz interactiva, Gateways, servidores de conferencia, y sistemas de mensajes de voz son capaces de generar más datos que una terminal puede manejar y así puede servir de apoyo a las inundaciones de la terminal IP. Porter, Abdelnur, Cridlig, State and Festor (2006).

Cuando el tráfico IP entre remitente y el destinatario pasa a través del dispositivo del atacante, que es trivial para el atacante para olfatear este tráfico utilizando herramientas de libre disposición como Ethereal o tcpdump. Alguna información sin encriptar (incluido el correo electrónico, Nombres de usuario y contraseñas, y el tráfico Web) puede ser interceptada y vista. Como lo describe Hensell (2003) Esta intervención puede tener drásticas consecuencias para el tráfico de VoIP. Herramientas libres tales como vomit y rtpsniff, o herramientas privadas tales como voipcrack, permiten la intercepción y decodificación de tráfico de VoIP. El contenido capturado puede incluir Speech, señalización e información de facturación, multimedia. Conversaciones recorriendo el interior de la red IP pueden ser interceptadas y grabadas con esta técnica. Hensell (2003).

Hay una serie de variaciones de las mencionadas técnicas. En lugar de imitar a su víctima, el atacante puede emular una puerta de enlace. Esto permite al atacante interceptar

numerosos paquetes stream. Sin embargo, la mayoría de las técnicas de redirección ARP se basan en sigilo. El atacante en estos escenarios se espera que no se detectado al hacerse pasar por usuario. Posando como puerta de entrada puede resultar en alerta a los usuarios de la presencia del atacante debido a imprevistos problemas con la red, ya que con frecuencia cambia cuando de forma inesperada los atacantes manipulan los procesos de ARP. Baugher (2004).

2.3.1.12 TLS Connection Reset

Son a menudo utilizados para la seguridad de señalización entre los teléfonos y gateways, solo enviando el tipo adecuado en cierto modo de paquete dañado y la conexión TLS se pondrá a cero, interrumpiendo la señalización de los canales entre el teléfono y el Servidor.

2.3.1.13 Rogue VoIP Endpoint Attack

Un ejemplo sería, una Terminal renegada puede usar una conexión sin protección y auto registrar teléfonos VoIP para obtener acceso en la red. Con contraseña RAS se puede utilizarse para hacerse pasar por un legítimo punto final. Porter (2006).

2.3.1.14 Registration Hijacking

Se produce cuando un atacante Impersonaliza un UA válido para registrar y sustituir la inscripción con su Propio dirección. Este ataque causa que todas las llamadas sean enviadas al atacante. Porter (2006).

2.3.1.15 Proxy Impersonation

Se produce cuando un atacante, manipula un UA SIP o un proxy en la comunicación con un servidor proxy renegado. Rosenberg (2002) Si un Atacante obtiene éxito imitando el Proxy, tendrá acceso a todos los SIP Mensajes. Porter (2006).

2.3.1.16 Toll Fraud

Terminales VoIP legítimas o renegadas se usan en un servidor VoIP para dar lugar a llamadas no autorizadas sobre la red PSTN. Por ejemplo, los controles de acceso insuficiente pueden permitir a los dispositivos renegados puede dejar hacer llamadas mediante el envío de peticiones VoIP a aplicaciones de procesamiento de llamadas. Servidores VoIP pueden ser hackeados en el fin de realizar llamadas gratuitas a destinos fuera de la red. Ingeniería social puede ser usada para obtener prefijos de líneas externas. Porter (2006).

2.3.1.17 Message Tampering

Capturar, modificar, y retrasar paquetes no autentificados VoIP a terminales. Por ejemplo, un Rogue 802,11 AP pueden intercambiar tramas enviados o recibidos por terminales inalámbricos en caso de ausencia de carga útil control de integridad (Por ejemplo, WPA MIC, SRTP) es utilizado. Como alternativa, estos ataques pueden ocurrir mediante el secuestro del registro, suplantación de proxy, o un ataque a cualquier componente de confianza al proceso de mensajes SIP o H.323, como por ejemplo el proxy, Registro de los servidores, media gateways, o firewalls. Estos ataques MITM no-ARP. Weatherspoon (2000).

2.3.1.18 VoIP Protocol Implementation Attacks.

Enviar paquetes inválidos a servidores VoIP o terminales para explotar la implementación CVEs del protocolo VoIP. Tales ataques puede conducir a una escalada de privilegios, la instalación y el funcionamiento de programas maliciosos.

Rosenberg (2002) menciona que los ataques de DoS, ya sean intencionales o no intencionales, son las amenazas más difíciles de defender en VoIP a defender. La conmutación natural de paquetes de las redes de datos permite conexiones múltiples para compartir el mismo medio de transporte. Por tanto, a diferencia de los teléfonos de redes de conmutación de circuitos, una terminal IP pueden recibir y potencialmente participar en varias llamadas a la vez. De esta manera, una terminal puede ser usada para amplificar los ataques. Sobre redes VoIP, los recursos tales como el ancho de banda deben ser asignados eficiente y equitativamente para garantizar el máximo número de llamadas. Esta propiedad puede ser violada por los atacantes quien agresiva y abusivamente obtiene una innecesaria cantidad de recursos. Porter (2006) Alternativamente, el atacante puede simplemente inundar la red con un gran número de paquetes de manera que los recursos no están disponibles para todas las otras llamadas.

Además, los virus y gusanos DoS crean condiciones debido al tráfico de la red generados por estos agentes que conforme se van replicando y buscando otras terminales para infectarlas. Estos agentes son probados para causar estragos incluso con garantizadas redes de datos. Las redes VoIP, por su naturaleza, son exquisitamente sensibles a este tipo de ataques. Kuhn, Walsh, and Fries (2004).

El robo de servicios e información también es también problemático sobre redes VoIP. Estas amenazas son casi siempre debido a los ataques activos. Muchos de estos ataques pueden ser frustrados mediante la aplicación de controles de seguridad adicionales en la capa 2. Esta capa 2 de seguridad incluye características como DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Puertos de Seguridad, y VLAN ACLs. Esta base fundamental para esta clase de ataques es que la identidad de uno o varios de los dispositivos que participar no es legítima. Kuhn, Walsh, and Fries (2004).

Las terminales deben ser autenticadas, y los usuarios finales deben ser validados con el fin de garantizar la legitimidad. Secuestro e interceptación de llamadas gira en torno al concepto de engañar, manipulación débil o inexistente medida de autenticación. Estamos familiarizados con las distintas formas de autenticación, de la contraseña utilizada para acceder al equipo hasta la llave que abre la puerta de frente. Porter (2006) El marco conceptual para la autenticación se compone de tres factores: "algo que usted tiene" (una clave o Token), "algo que usted sabe" (una clave secreta o apretón de manos), o "algo que usted posee"(patrón de las huellas dactilares o del iris). Validar los mecanismos de autenticación de usuarios por uno o una combinación de estos. Algún tipo de acceso no autentificado, en particular a los principales componentes de infraestructura, como el IP PBX o servidor DNS, por ejemplo, pueden dar lugar a consecuencias desagradables para los usuarios y administradores. Kuhn, Walsh, and Fries (2004).

2.3.1.19 VoIP Social Engineering

ARP Cache Poisoning.- ARP es un protocolo fundamental de Ethernet. Tal vez por esta razón, la manipulación de paquetes ARP es un potente mecanismo de ataque y frecuentes en las redes de VoIP. Lamentablemente, varias técnicas y herramientas existen que permiten a cualquier usuario olfatear tráfico en una red conmutada, porque ARP no tiene ninguna disposición para la autenticación de las preguntas o respuestas de la consulta. Entre estas técnicas, la redirección ARP, ARP spoofing, ARP hijacking, ARP cache poisoning son métodos relacionados para interrumpir el proceso normal de ARP. Estos términos son frecuentemente intercambiados y confusos.

ARP redirección puede trabajar bidireccionalmente, y un dispositivo de spoofing puede inmiscuirse en medio de una conversación entre dos dispositivos IP en una red conmutada. Para enrutar los paquetes sobre los dispositivos que realmente debería estar recibiendo los paquetes, esta inserción (Conocido como hombre / Monkey / Moron en medio del ataque) puede que no sea detectado por algún tiempo. Un atacante puede enrutar paquetes a /dev/null (a ninguna parte), resultando un ataque DoS.

Como todos el tráfico IP entre el verdadero remitente y el receptor pasará a través del dispositivo del atacante, Por lo tanto el atacante podrá husmear (Sniff) el tráfico utilizando herramientas libres como Ethereal o tcpdump. Cualquier información sin cifrar (incluidos correo electrónico, nombres de usuario y contraseñas, y el tráfico de Internet) pueden ser interceptados y vistos.

2.3.1.20 VoIP Call Hijacking

Es la inyección, supresión, adición, supresión, sustitución u otra modificación de cualquier parte de cualquier comunicación con la información que altera cualquier parte de su contenido y/o de la identidad, la presencia o estado de cualquiera de sus partes. El secuestro de conversación es un método de ataque que altera el contenido o la información acerca de las partes en la comunicación y se aplica a cualquier parte de cualquiera de las comunicaciones incluidas las de voz, vídeo, texto y / o imágenes de datos, sin embargo ya sean encapsuladas o codificada. (voipsa, 2005)

2.3.1.21 Network Eavesdropping

Uno de los mayores problemas sea quizás la interceptación o eavesdropping. Traducido literalmente como “escuchar secretamente”, es el término con el que se conoce a la captura de información (cifrada o no) por parte de un intruso al que no iba dirigida dicha información. En términos de telefonía IP, estamos hablando de la interceptación de las conversaciones VoIP por parte de individuos que no participan en la conversación.

Las formas de conseguir interceptar una comunicación pueden llegar a ser tan triviales como esnifar el tráfico de la red si los datos no van cifrados. Existen excelentes sniffers como ethereal/wireshark que permitirán capturar todo el tráfico del segmento de la red. Por el contrario, lo normal es que nos encontramos dentro de redes conmutadas por lo que para esnifar el tráfico que no vaya dirigido a nuestro equipo serán necesarias otras técnicas más elaboradas como realizar un “Man in the Middle” utilizando Envenenamiento ARP. Entre las herramientas que podremos utilizar se encuentra el conocido programa

ettercap, Cain & Abel, la suite de herramientas para Linux Dsniff y vomit (Voice over misconfigured Internet telephones) por citar algunos ejemplos.

2.3.1.22 Vishing

Proviene del término Voice Phishing, es decir, se trata de una derivación del phishing con un fin de fraude electrónico pero, en lugar de atacar al usuario a través de un correo electrónico, utiliza una llamada telefónica generada desde la infraestructura tradicional o bien, utilizando voz sobre IP. Martínez (2006).

Menciona Martinez (2006) que este tipo de estafa por Internet utiliza números de teléfono IP como si fuesen los atención al cliente de tarjetas de crédito o servicios financieros. La estafa vishing sigue el mismo procedimiento que el phishing: el usuario recibe un falso e-mail en el que se le advierte de alguna circunstancia relacionada con su cuenta bancaria o tarjeta de crédito donde se incluye un teléfono en lugar de una dirección web al que puede llamar para aclarar dudas o resolver el problema. En esa llamada se solicita cierta información confidencial (técnicas de ingeniería social) para validar que el usuario es el afectado. Si por alguna razón, el usuario no se encuentra, entonces deja un recado hacia un servicio automatizado con líneas 01-800 para que sea atendido.

Martínez (2006) describe que la segunda parte del ataque es a través del 01-800, un call-center apócrifo con el audio tradicional de la institución financiera de atención telefónica, donde de manera automatizada solicitan los datos de cuenta, pin, etc. Lo peor en estos casos, es que el número 01-800 corresponde a un número dado de alta mediante servicios de VoIP que no necesariamente se encuentran en el país, y que en ocasiones dependiendo de la compañía, fueron pagados y se utilizan por máquinas anónimas dentro de la red, por lo que su ubicación es algo compleja desde el punto de vista de perseguir al delincuente.

2.3.1.23 DoS utilizando mensajes SIP CANCEL

Identificador: A.01
Fuente de ataque: LAN/ VPN Utilizando SIP

Meta: SIP
Propósito: Impacto sobre la disponibilidad

Descripción:

Con este ataque es posible cancelar una llamada en una terminal o para cancelar una llamada saliente iniciada por una terminal.

El mensaje CANCEL se utiliza normalmente para cancelar una petición previamente enviado por un terminal. El atacante debe primero escuchar en la red para recuperar un mensaje de denuncia entre la persona que llama y la receptora, por lo general es un mensaje INVITE para hacer un ataque DoS. Después de analizar el mensaje para recuperar suficiente información sobre la llamada, el atacante podría crear un falso mensaje de CANCEL y enviar un INVITE a la llamada para cancelar el mensaje. Por lo cual ninguna de las partes puede realizar la llamada y el propósito del atacante se realiza. Litzistorf, Contreras (2006).

Sin embargo, cabe señalar que el mensaje CANCEL no tiene ningún efecto en una solicitud que el UA (llamado) ya ha aceptado. Sin embargo, en un mensaje INVITE toma algún tiempo para generar una respuesta, por lo que son un blanco fácil para el ataque que se ha descrito anteriormente, ya que el atacante tiene tiempo para analizar el mensaje INVITE y formar el mensaje CANCEL. Reynolds and Ghosal (2006).

Realización:

El atacante debe ser capaz de escuchar en la red para localizar un mensaje inicialización de una conexión SIP. También debe ser capaz de insertar un mensaje CANCEL después de recibir el mensaje INVITE por el objetivo.

2.3.1.24 DoS using SIP BYE messages

Identificador: A.02
Fuente de ataque: LAN/ VPN Utilizando SIP
Meta: SIP
Propósito: impacto sobre la disponibilidad

Descripción:

Este ataque puede cortar una comunicación entre dos terminales existentes. El mensaje de solicitud BYE se utiliza normalmente para poner fin a un período de sesiones establecido por SIP. El atacante debe escuchar en la red para recuperar entre el mensaje de solicitud del emisor y el receptor.

Después de analizar el mensaje para recuperar suficiente información sobre la comunicación, el atacante podría crear un falso mensaje y enviar BYE de UA (emisor), a UA (receptor) a fin de terminar la comunicación. El objetivo del atacante se ha hecho y ambas partes deben hacer una nueva convocatoria. Reynolds and Ghosal (2006).

Realización:

El atacante debe ser capaz de escuchar en la red para localizar un mensaje inicialización de una llamada. También debe ser capaz de insertar un mensaje CANCEL justo después de recibir el mensaje INVITE por el objetivo.

2.3.1.25 DoS using SIP FAILURE (4xx) messages

Identificador: A.03
Fuente de ataque: LAN/ VPN Utilizando SIP
Meta: SIP
Propósito: Impacto sobre la disponibilidad

Descripción:

Este ataque es impedir que una llamada se lleve a cabo. Los mensajes de respuesta SIP Request Failure (4xx) se utilizan normalmente para responder a una solicitud de mensaje SIP cuando algo no ha ocurrido correctamente. Cabe señalar que las respuestas 4XX son definitivas del servidor y el cliente no vuelve a la misma petición.

El atacante debe escuchar en la red para recuperar un mensaje de consulta entre la persona que llama y la que recibe la llamada (un mensaje de respuesta tipo INVITE será el mejor candidato para este tipo de ataque). Después de analizar el mensaje para recuperar suficiente información sobre la comunicación que tiene lugar, este puede configurar un falso mensaje de respuesta 404 (Not Found) ó 410 (Gone) o cualquier otro código (pero los mensajes 404 y 410 son buenos ejemplos) y enviarlo al UA (emisor) antes de que el UA (receptor) tenga oportunidad de responder al mensaje de solicitud inicial de SIP. El objetivo del atacante se habrá logrado y dicha comunicación entre UA (Emisor) puede llegar a pensar que UA (receptor) no existe. Ataques similares pude ser utilizando mensajes tipo 5xx (Server failures) ó 6xx (Global failures) son posibles. Reynolds and Ghosal (2006).

Realización:

El atacante debe ser capaz de escuchar en la red para localizar un mensaje inicialización de una conexión SIP. También debe ser capaz de insertar un mensaje FAILURE justo después de la aparición del mensaje INVITE por el objetivo.

2.3.1.26 Drop of QoS Performance by reusing RTP's SSRC

Identificador: A.04

Fuente de ataque: LAN/ VPN
Meta: RTP
Propósito: Impacto sobre la disponibilidad

Descripción:

Este ataque es el uso de un SSRC (sincronización fuente, fuente de sincronización) existente a fin de causar una pérdida en el rendimiento QoS (calidad de servicio). A continuación, el atacante tendría que crear un paquete RTP utilizando el mismo SSRC para crear colisiones y una pérdida en el rendimiento QoS, ya que el recurso debe detectar la colisión. (RFC 1889, 3261). Litzistorf, Contreras (2006).

Realización:

El atacante debe ser capaz de escuchar en la red para localizar una comunicación y cuál es el SSRC utilizado.

2.3.1.27 RTP packet injection

Identificador: A.05
Fuente de ataque: LAN/ VPN
Meta: servidor de registro
Propósito: Impacto sobre la disponibilidad

Descripción:

Este ataque tiene como objetivo interrumpir la comunicación, el atacante primero debe escuchar el RTP de la llamada de la persona que llama, analizar su contenido y formar un paquete que contiene un encabezado similar RTP, pero con un mayor número de secuencia de tiempo y de forma que el paquete reproducidos por otros paquetes (si es que realmente se reproducen).Por lo tanto, la comunicación será interrumpida y la llamada no se realizará correctamente. (RFC 1889, 3261).

Realización:

El atacante debe ser capaz de escuchar en la red para localizar una comunicación e identificar el *timestamp* de los paquetes RTP. También debe ser capaz de insertar mensajes RTP falsos con *timestamp* cambiados.

2.3.1.28 Audio codec modification

Identificador: A.06

Fuente de ataque: LAN/ VPN.
Meta: RTP / Terminales: soft/hard phones.
Propósito: Impacto sobre la disponibilidad y la integridad de los datos.

Descripción:

Este ataque tiene como objetivo utilizar la falta de control de flujo a los medios de comunicación y cambiar algunos de sus parámetros para crear más tráfico del normal.
El atacante se aprovecha de las vulnerabilidades de SIP sobre el flujo de los datos, y puede ser modificada sin que SIP este consciente de estos cambios. Esto resulta una interrupción de la conversación no (pero debería) detectadas por proxies. Litzistorf, Contreras (2006).

Un cambio en el codec podría resultar en un mayor uso de paquetes y, por lo tanto, utilizar más el ancho de banda y deteriorar las comunicaciones. (RFC 1889).

Realización:

El atacante debe ser capaz de identificar un flujo de medios de comunicación y modificarlo.

2.3.1.29 Flujo de audio inaudible

Identificador: A.07
Fuente de ataque: LAN/ VPN
Meta: RTP / Terminales: soft/hard phones
Propósito: impacto sobre la disponibilidad y la integridad de los datos

Descripción:

En una comunicación legítima entre ambas partes, el atacante envía flujos RTP mal intencionado para superponer el flujo RTP legítimo. Para ello, el atacante debe hacer mapeo en la red para conocer el puerto UDP utilizados por el flujo RTP, así como el codec de audio utilizado. Una vez conocidos estos valores, se puede utilizar diferente software para enviar flujo RTP mal intencionado, por citar algunos son:

- SipCrack (http://remote-exploit.org/index.php/Sipcrack)
- SIPsak (http://sipsak.org)
- Skora.net VoIP Tools (http://skora.net/voip/voip.html

Realización:

El atacante debe ser capaz de controlar el puerto UDP y el codec utilizado por la señalización RTP y hacerla inaudible. (RFC 1889).

2.3.1.30 Registration Table Overflow

Identificador: A.08
Fuente de ataque: LAN/ VPN utilizando SIP
Meta: SIP
Propósito: impacto sobre la disponibilidad.

Descripción:

Este ataque es causar un desbordamiento en la tabla registros para evitar el registro de legítimos usuarios en el servidor. El atacante envía un gran número solicitud de mensajes REGISTER (con Diferentes URI) al servidor de archivos para llenar su tabla de registros y evitar el login de los usuarios legítimos para utilizar el servicio. (RFC 1889).

Realización:

El atacante debe ser capaz de enviar mensajes al servidor de registro.

2.3.1.31 Proxy server flooding

Identificador: A.09
Fuente de ataque: LAN/ VPN
Meta: SIP
Propósito: Impacto sobre la disponibilidad.

Descripción:

Este ataque tiene como objetivo la inundación de los servidores proxy con mensajes INVITE para evitar que los usuarios legítimos realicen llamadas. El atacante envía una gran cantidad de mensajes sobre un proxy, que deben normalmente ser transferidos a los beneficiarios. El problema es que el número de sesiones simultáneas soportadas por el servidor proxy es limitado, los recursos son agotados rápidamente, lo que significa que llamadas realizadas por usuarios legítimos mediante el proxy víctima no puede tener lugar. Jeremy (2003).

Realización:

El atacante debe ser capaz de escuchar en la red para localizar un mensaje inicialización de una conexión SIP. Así como también insertar un mensaje FAILURE justo después de la recepción del mensaje INVITE por el objetivo

2.3.1.32 Physical Eeavesdropping

Identificador: A.10
Fuente de ataque: LAN/ VPN utilizando SIP
Meta: RTP / Terminales: soft/hard phones
Propósito: impacto sobre la privacidad de los datos

Descripción:

Este ataque es para escuchar o grabar una conversación. El atacante obtiene acceso a la red física y las herramientas utilizadas para espiar directamente en el cableado. Puede hacerlo entre el UA y un switch o entre dos comutadores (switches). lo que le permitiría reproducir el contenido de los paquetes. (RFC 1889).

Realización:

El atacante debe tener acceso físico a cables de red para poder escuchar el tráfico.

2.3.1.33 Cipher Breakage

Identificador: A.11
Fuente de ataque: LAN/ VPN utilizando SIP
Meta: RTP / Terminales: soft/hard phones
Propósito: Impacto sobre la privacidad de los datos

Descripción:

Este ataque es conocer el contenido de un paquete descifrado. Escuchar mensajes de señalización SIP para recuperar la clave DES (campo k) posteriormente poder descifrar el contenido de los paquetes de audio codificados con el sistema de cifrado y el contenido de la conversación. (RFC 1889).

Realización:

El atacante debe ser capaz de escuchar en la red y recuperar mensajes de conversaciones cifrados y el SIP que contiene la clave DES. Así como también debe tener un método para tratar de descifrar los mensajes. Litzistorf, Contreras (2006).

2.3.1.34 Re-INVITE / Session Replay – Mid Session tricks

Identificador: A.12
Fuente de ataque: LAN/ VPN
Meta: SIP
Propósito: impacto en la confidencialidad, disponibilidad e integridad de los datos

Descripción:

Este ataque se destina a registrar una llamada o cambiar los ajustes de configuración de una llamada. El atacante debe escuchar en la red y recuperar un mensaje INVITE entre un emisor y receptor. Él puede introducir un mensaje INVITE en la conversación actual para que los parámetros se tomen (por ejemplo, parámetros de enrutamiento) y una tercera parte que se introduzca en la conversación, por ejemplo, para facilitar el registro de la conversación. (RFC 3261). Litzistorf, Contreras (2006).

Realización:

El atacante debe ser capaz de escuchar SIP y de insertar mensajes falsos.

2.3.1.35 (Monitor de llamadas)Call Tracking (1)

Identificador: A.13
Fuente de ataque: LAN/ VPN
Meta: Terminales: soft/hard phones
Propósito: Impacto en la confidencialidad,

Descripción:

Este ataque es para saber quien se está comunicando, ¿cuál es la frecuencia de conexión y la duración de la comunicación? El atacante debe recuperar los mensajes INVITE y BYE, mientras escucha en la red en que momento y por cuanto tiempo dura la comunicación. (RFC 3261).

Realización:

El atacante debe ser capaz de escuchar en la red y recuperar mensajes INVITE y BYE.

2.3.1.36 (Monitor de llamadas)Call Tracking (2)

Identificador: A.14
Fuente de ataque: LAN/VPN, utilizando SIP
Meta: RTP/ Terminales: soft/hard phones
Propósito: Impacto en la confidencialidad

Descripción:

Este ataque está destinado a captar información sensible de interlocutores. El objetivo del ataque es la recuperación de tonos DTMF ((Dual Tone Multi Frequency) entre todo el tráfico de voz. Esto permitirá que el atacante pueda obtener información que va desde información sobre el buzón de voz (número de teléfono, correo de voz, contraseñas) información sobre tarjetas de llamadas o incluso números de tarjetas de crédito. Toda la información que se transmite a través de DTMF puede ser recuperado por este medio. Arkin (2006).

Realización:

El atacante debe ser capaz de escuchar en la red y recuperar los paquetes de comunicación RTP. El objetivo debe ser también el uso de tonos DTMF en algo interesante (contraseñas, etc.)...

2.3.1.37 Call hijacking helped by the registrar server

Identificador: A.15
Fuente de ataque: LAN/VPN
Meta: Servidor de Registro
Propósito: Impacto en la confidencialidad.

Descripción:

Este ataque tiene como objetivo desviar una llamada mediante la alteración de las conexiones del servidor de registro. El atacante tiene en primer lugar conseguir enlaces del servidor del registro en el sistema desde un URI para recuperar la lista de direcciones. A continuación, se combinará con su URI con todos los registros correctos en un registro y el mensaje de solicitud de estas grabaciones dará mayor prioridad utilizando un parámetro <<q>>

Este parámetro indica una relativa preferencia por este campo de contacto en comparación con otras conexiones a esta dirección para registrarse, esto significa que el plan que el atacante ha llevado desde su URI puede utilizarse suplantando la del usuario legítimo. (RFC 3261).

Realización:

El atacante debe ser capaz de enviar y recibir datos desde el servidor de registro. También debe ser capaz de forjar solicitudes REGISTER fraudulentas.

2.3.1.38 Call hijacking helped by the registrar server (2)

Identificador: A.16
Fuente de ataque: LAN/VPN
Meta: Servidor de registro
Propósito: Impacto en la confidencialidad y disponibilidad.

Descripción:

El atacante tiene en primer lugar conseguir enlaces del servidor del registro en el sistema desde un URI para recuperar la lista de direcciones. A continuación, se combinará con su URI de todos los registros de mensajes correctos en un registro que indique su solicitud y registre una baja prioridad con el parámetro<<q>>. Este parámetro indica una

relativa preferencia por este campo de contacto en comparación con otras conexiones a esta dirección para registrarse. Litzistorf, Contreras (2006).

A continuación, el atacante realizar un ataque DoS sobre todos los registros con una mayor prioridad para que el proxy no puede enviar un mensaje y cambia automáticamente a la siguiente entrada, por ejemplo aquellos que tienen una prioridad inferior (como el atacante). (RFC 3261).

Realización:

El atacante debe ser capaz de enviar y recibir datos desde el servidor de registro.

2.3.1.39 Registration hijacking by forging SIP REGISTER requests

Identificador: A.17
Fuente de ataque: LAN/VPN
Meta: SIP / Servidor de registro
Propósito: Impacto en la confidencialidad, disponibilidad e integridad de los datos

Descripción:

Este ataque tiene como objetivo reorientar las llamadas al atacante para sabotear el servidor de registro. El atacante debe escuchar en la red para recuperar un mensaje del tipo REGISTER. Luego, después de analizar este mensaje, puede configurar un mensaje REGISTER y volver a inscribirse en el registro de servidor con una nueva URI para la víctima. Reynolds and Ghosal (2006).

Este resultado tener que redirigir todas las llamadas que se envíen a la nueva URI (por ejemplo, la de el atacante) que permite al atacante plagiar el objetivo y llevar a cabo su plan. Reynolds and Ghosal (2006).

Realización:

El atacante debe ser capaz de escuchar el mensaje REGISTER, analizar y volver el mensaje REGISTER al servidor para registrar y plagiar el objetivo.

2.3.1.40 Registration Hijacking

Identificador: A.18
Fuente de ataque: LAN/VPN
Meta: SIP / Servidor de registro
Propósito: Impacto en la confidencialidad, disponibilidad e integridad de los datos

Descripción:

Este ataque tiene como objetivo reorientar las llamadas al atacante para sabotear el servidor de registro. Al conseguir en la red un mensaje de solicitud REGISTER, el atacante será capaz de modificar y enviar uno nuevo en el intervalo de tiempo definido inicialmente por el *timestamps* especificado en el mensaje REGISTER original, pero con el campo "expires", que contiene el valor "0" para quitar vínculos con el usuario legítimo. Doswald (2006)

Por lo tanto, la víctima ya no puede registrar su teléfono como una dirección de contacto adecuado y todas las llamadas de la víctima van a ser redirigido al atacante. (RFC 3261).

Realización:

El atacante debe ser capaz de escuchar el mensaje REGISTER, analizar y volver el mensaje REGISTER fraudulento al servidor de registro.

2.3.1.41 Call redirection using 301/302 response messages

Identificador: A.19
F**uente:** de ataque: LAN/VPN
Meta: Terminales / Soft / hard phones
Propósito: Impacto en la confidencialidad.

Descripción:

Este ataque tiene por objeto reorientar el tráfico de señalización a cualquier otra parte que sea desconocida. El atacante debe escuchar en la red para recuperar un mensaje INVITE entre el emisor y receptor. Luego, después de analizar la mensaje y recuperar la información suficiente acerca de la comunicación que tendrá lugar, puede configurar un falso mensaje de respuesta de tipo 301 (Moved Permanently) ó 302 (Moved temporarily) y enviarlo al UA (Emisor) antes del UA (Receptor) por lo cual ha tenido tiempo para responder al mensaje original de la solicitud de SIP. Doswald (2006)

Una vez que reciba la respuesta del mensaje anterior UA (emisor), se llevará a cabo un nuevo intento de llamada a la dirección indicada por el atacante. Por lo cual el propósito del atacante será un éxito. Reynolds and Ghosal (2006).

Realización:

El atacante debe ser capaz de escuchar en la red y recuperar un mensaje del tipo INVITE. También debe ser capaz de crear mensajes de respuesta de tipo 301 ó 302; antes de enviar la respuesta legítima.

2.3.1.42 Call redirection attack using 305 response messages

Identificador: A.20
Fuente de ataque: LAN/VPN
Meta: SIP
Propósito: impacto en la confidencialidad, disponibilidad e integridad de los datos

Descripción:

Este ataque tiene por objeto reorientar la señalización del tráfico a fin de modificarla a un servidor proxy corrupto.

Los mensajes de respuestas de redirección (3xx) son enviados por el UA y proporcionar normalmente la nueva ubicación del usuario ó alternativas que cumplan con los servicios de la llamada (como es el caso de código 305, lo que indica que el recurso solicitado se puede acceder a través del proxy que figura en el contacto). (RFC 3261).

El atacante debe escuchar en la red para recuperar un mensaje SIP entre la solicitud del emisor y el receptor. Después de analizar el mensaje y obtener suficiente información, puede configurar un mensaje de respuesta de tipo 305 y enviarlo al remitente del mensaje recuperado. Esta última deberá mandar la señalización del tráfico a través del proxy especificado y recibir automáticamente la respuesta de la misma manera. Doswald (2006)

El objetivo del atacante tendrá éxito porque la señalización del tráfico será redirigido a través de un proxy y luego la posibilidad de modificar el cruce de los paquetes. (RFC 3261).

Realización:

El atacante debe ser capaz de escuchar en la red e identificar un mensaje de señalización de una comunicación. También debe ser capaz de configurar un mensaje de redirección y enviar antes de la respuesta legítima. Por último, debe ser capaz de comportarse como un proxy SIP, para que sea intercambie datos con el cliente y el servidor legítimo. Doswald (2006)

2.3.1.43 Request spoofing

Identificador: A.21
Fuente de ataque: LAN/VPN
Meta: SIP/ terminales: soft/hard phones
Propósito: Impacto en la confidencialidad, disponibilidad e integridad de los datos.

Descripción:

Este ataque tiene como objetivo cambiar la identidad del remitente de un mensaje para hacer creer al destinatario de la llamada que habla de un usuario legítimo, El atacante primero debe escuchar en la red para recuperar un mensaje de solicitud de tipo REGISTER

Cualquier tipo INVITE y modificar determinados campos de contenidos que figuran en la cabecera antes de enviar el mensaje falso de requerimiento. Esto significa que crea que el receptor se dirigió a un usuario específico cuando en realidad intercambio datos (habló) con el atacante. Por lo tanto, la víctima ya no puede registrar su teléfono como una dirección de contacto valido y todas las llamadas a la víctima van a ser redirigidas al atacante. (RFC 3261). Doswald (2006).

Realización:

El atacante debe ser capaz de escuchar los mensajes SIP INVITE ó REGISTER, analizar, modificarlo y volverlas manipuladas

2.3.1.44 Call masquerading

Identificador: A.22
Fuente de ataque: LAN/VPN utilizando SIP
Meta: SIP/terminales: soft/hard phones
Propósito: Impacto en la disponibilidad de los datos

Descripción:

Este ataque es con la intención de ocultar la identidad de la persona que llama a la que va a tomar la llamada. El recurrente oculta su identidad a fin de que el UA llamado no pueda saber quién llama y conteste el teléfono. Esto significa que el usuario puede estar expuesto a anuncios grabados, entre otras cosas. (RFC 3261).

Realización:

El atacante debe ser capaz de llamar a la meta y ocultar su número telefónico.

2.3.1.45 Billing fooling

Identificador: A.23
Fuente de ataque: LAN/VPN
Meta: SIP/ terminales: soft/hard phones
Propósito: Impacto en la integridad de los datos

Descripción:

Este ataque tiene como objetivo realizar llamadas de voz gratuitas. El atacante y su cómplice establecerán un patrón para que los mensajes SIP se oculten dentro de los mensajes RTP / RTCP.
El proxy SIP será incapaz de detectar el tráfico de señalización (SIP), permitiendo que el flujo de datos continúe el tránsito (RTP / RTCP). El CDR (*Call Detail Recording*) no se ejecutará, por lo que ambas partes pueden hacer llamadas telefónicas libres. (RFC 3261).

Realización:

Los atacantes deben ser capaces de modificar los paquetes RTP / RTCP, y tienen que añadir la información de señalización (SIP).

2.3.1.46 Theft of service using a legitimate client's credentials

Identificador: A.24
Fuente de ataque: LAN/VPN
Meta: SIP
Propósito: Impacto en la integridad de los datos

Descripción:

Este ataque tiene como objetivo hacer llamadas gratis utilizando la información un usuario legítimo.

El atacante debe escuchar en la red para recuperar una solicitud de mensaje REGISTER de un UA (emisor), y de ir al servidor de registro. Después de analizar el mensaje recuperado, el atacante envía un mensaje de respuesta de tipo 301 (Moved Permanently) para engañar a los usuarios que el servidor de registro SIP sido trasladado a la nueva dirección como uno de sus servidores.

Por lo tanto el usuario registrado (atacante) con el poder ilegítimo, puede recuperar información del usuario y el uso legítimo. A continuación, el atacante puede suplantar a los legítimos usuarios y hacer llamadas gratuitas ó redireccionar el tráfico hacia un servidor de registro. (RFC 3261).

Realización:

El atacante debe ser capaz de escuchar en la red y recuperar un mensaje del tipo REGISTER entre el objetivo y el servidor de registro. También debe ser capaz de enviar una redirección a la meta antes de la respuesta legítima y remendar el funcionamiento del servidor de registro para recuperar información de los legítimos usuarios

Por último, debe ser capaz de utilizar la información recopilada ilegítimamente para inscribirse en el verdadero servidor de registro y hacer llamadas gratuitas.

2.3.1.47 Spam call

Identificador: A.25
Fuente de ataque: LAN/ VPN, utilizando SIP
Meta: Terminales / soft/hard phones
Propósito: Impacto en la integridad de los datos

Descripción:
Este ataque pretende hostigar con mensajes pregrabados a la persona cuando recoja el auricular, este tipo de spam se define como una serie de pruebas de inicio de sesión (por ejemplo, la solicitud INVITE), tratando de establecer una sesión de comunicación de voz. Cuando la persona que llama cuelga el receptor, el atacante (spam) aprovecha para transmitir su mensaje a través del medio de comunicación en tiempo real. Rosenberg,(2006)

Realización:
El atacante debe ser capaz de llamar a la víctima.

2.3.1.48 Instant messaging spam (SPIM)

Identificador: A.26
Fuente de ataque: LAN/ VPN, utilizando SIP
Meta: Terminales / soft/hard phones
Propósito: Impacto en la integridad de los datos

Descripción:
Este ataque tiene como objetivo generar un gran número de mensajes instantáneos (a menudo comerciales) en las terminales de usuario.

El atacante envía un gran número de mensajes instantáneos no solicitados, que contiene el mensaje que el spammer quiere mostrar. El spam es enviado utilizando la solicitud de mensaje SIP MESSAGE.

Sin embargo, cualquier solicitud de mensaje muestra automáticamente el contenido en la pantalla de la terminal de usuario no permitiéndole trabajar. Por ejemplo, las solicitudes INVITE con grandes cabeceras en Asunto (desde el campo Asunto a veces se muestra al usuario). Rosenberg, (2006)

Realización:

El atacante debe ser capaz de enviar SIP MESSAGES al destino.

2.3.1.49 Presence spam

Identificador: A.27
Fuente de ataque: LAN/ VPN, utilizando SIP
Meta: Terminales / soft/hard phones
Propósito: Impacto en la integridad de los datos

Descripción:

Este ataque está destinado para ser puesto en la lista blanca (lista de amigos) de un usuario a fin de enviar mensajes instantáneos ó iniciar otras formas comunicación. El atacante envía una gran cantidad de mensajes de consulta de presencia (Por ejemplo mensajes de solicitud SUBSCRIBE) con la esperanza de entrar en la lista blanca ó "lista de amigos" de un usuario para enviar mensajes instantáneos o iniciar otras formas de comunicación. Rosenberg, at (2006)

A diferencia de la mensajería instantánea, el spam tiene no tiene presencia de ningún contenido real en el mensaje, juegan solamente con la paciencia del usuarios que, en última instancia, acepta la solicitud y pone el usuario en la lista blanca para dejar de recibir la solicitud.

El ataque también puede hacerse mediante el envío de la solicitud a un gran número de usuarios maximizando las posibilidades de que una persona acepte la solicitud. Rosenberg, at (2006)

Realización:

El atacante debe ser capaz de enviar consultas (Por ejemplo mensajes de solicitud SUBSCRIBE) al destino.

2.3.1.50 Distributed Deny of Service (DDoS)

Identificador: A.28
Fuente de ataque: LAN/ VPN, Internet Externo
Meta: cualquier ordenador de la red (Via cliente STUN)
Propósito: Impacto sobre la disponibilidad.

Descripción:

Este ataque tiene como objetivo lanzar un ataque de denegación de servicio distribuido a través de STUN.

El atacante distribuye a un gran número de clientes una dirección asignada falsa apuntando al objetivo. Esto hará que los clientes STUN piensen que sus direcciones son iguales a las del objetivo. Los clientes entonces darán esta dirección para recibir el tráfico (por ejemplo, mensajes SIP ó H.323). Todo el tráfico se centrará en el objetivo. El ataque puede crear una gran sobrecarga de tráfico en el objetivo, especialmente cuando se usa con los clientes que utilizan STUN para inicializar aplicaciones multimedia. (RFC 3489).

2.4 Vulnerabilidades

Las vulnerabilidades de VoIP abarcan no sólo defectos inherentes dentro de la propia aplicación de VoIP, sino también en los sistemas operativos, aplicaciones y protocolos que VoIP depende. La complejidad de VoIP crea un gran número de vulnerabilidades que afectan las tres clásicas áreas de seguridad de la información: confidencialidad, integridad, y disponibilidad (CIA). McGann, Sicker (2005)

Para efectos de visualizar mejor estas vulnerabilidades se han distribuido sobre las capas de TCP / IP, algunas de estas vulnerabilidades utilizan más de una capa.

La seguridad física es un problema importante en todos los sistemas de información, incluido VoIP. Mencionan McGann, Sicker (2005) Sin embargo, es muy difícil para una herramienta evaluar o supervisar el estado de la seguridad física. VoIP debe considerar los riesgos de la confidencialidad física. Si bien muchos ataques explotan debilidades dentro de una o más capas de red, algunos de ellos son también dependientes de ataques físicos de vectores que existen en interfaces no utilizadas sobre equipos VoIP. Esto incluye Jacks de datos, puertos switch / hub, rango inalámbrico, y interfaces adicionales en el teléfono VoIP.

Menciona McGann, Sicker (2005) que estas interfaces deben permanecer deshabilitadas a menos que sean necesarias para su funcionalidad. Además, medidas de seguridad, como autenticación, filtrado de direcciones, y alarmas para cuando los dispositivos sean desconectados pueden mitigar los riesgos implicados en la seguridad física.

En la siguiente tabla se proporciona una descripción de las vulnerabilidades identificadas en estas capas del protocolo TCP/IP. Esta investigación muestra que muchas de las vulnerabilidades afectan a más de un área de seguridad de la información y, a menudo, incluye debilidades en la confidencialidad, integridad y disponibilidad. Dicha tabla muestra la relación entre las vulnerabilidades individuales y las zonas de seguridad de la red que afectan. McGann, Sicker (2005).

Capa	Vector de ataque	Confiabilidad	Integridad	Disponibilidad
Interface de red	Physical Attacks	X		X
	ARP cache	X	X	X
	ARP flood			X
	MAC Spoofing	X	X	X
Internet	Redirect via IP spoof	X	X	X
	Malformed Packets	X	X	X
Trasporte	TCP / UDP Flood			X
	TCP / UDP Replay	X	X	
Aplicación	TFTP server Insertion		X	
	DHCP server Insertion		X	
	DHCP Starvation			X
	ICMP flood			X
	Registration Hijacking	X	X	X
	MGCP Hijack	X	X	X
	Message Modification	X	X	
	Spoof via header	X	X	X
	Cancel / bye attack			X
	Redirect method	X		X
	Encryption	X	X	X
	Default configuration	X	X	X
	Unnecessary services	X	X	X
	Buffer overflow	X	X	X
	Legacy Network	X	X	X
	DNS Availability			X

Figura 8, VoIP vulnerabilities based on protocol layers (McGann, Sicker 2005)

3.1 Introducción

Una preocupación por la seguridad de la tecnología VoIP es que todas las vulnerabilidades inherentes a las redes IP afectarían también a las redes convergentes de VoIP, presentando nuevos riesgos para una empresa de servicios de voz. Las vulnerabilidades en la infraestructura de red pueden afectar la seguridad y disponibilidad de la red VoIP. Los sistemas VoIP son también vulnerables debido a las debilidades en los sistemas operativos sobre el cual están montados los servidores de VoIP. (ISS, 2005)

Además de estos riesgos de seguridad en sistemas operativos y la red de datos, amenazas concretas de VoIP van aumentando el riesgo en una organización tal como la voz y redes de datos convergentes. Más medidas de seguridad son necesarias para la gestión de este riesgo añadido (ISS, 2005)

Areitio Bertolin (2006) menciona que los defectos de seguridad y vulnerabilidades son fallos de políticas, procedimientos y controles de seguridad que permiten que un sujeto cometa una acción que viola la política de seguridad. El sujeto se denomina atacante y utiliza el fallo para violar la política explotando o forzando la vulnerabilidad. El test de penetración utilizado en auditoria puede probar la presencia de vulnerabilidades, pero no la ausencia de ellas.

Los riesgos en la seguridad no pueden eliminarse o prevenirse completamente; sin embargo una administración y una valoración eficaces de los riesgos pueden minimizar significativamente su existencia. Un nivel aceptable de riesgo es la cantidad de éste que las empresas están dispuestas a asumir. Generalmente, se puede asumir el riesgo si el coste de implementar salvaguardas para reducirlos excede de lejos los beneficios. (Cisco Firewall 2005)

3.2 ¿Dónde es vulnerable VoIP?

Potencialmente, cada componente de un sistema VoIP puede ser vulnerable. Esto incluyen los protocolos, la infraestructura IP (routers, switches), IP / PBXs (private branch exchanges), Servidores VoIP, teléfonos individuales o "soft phones" (PC con auricular). Un cuidadoso diseño y funcionamiento de la red VoIP junto con la implementación de determinadas tecnologías de seguridad garantizarían la calidad, fiabilidad y Seguridad para el tráfico de VoIP. (ISS, 2005)

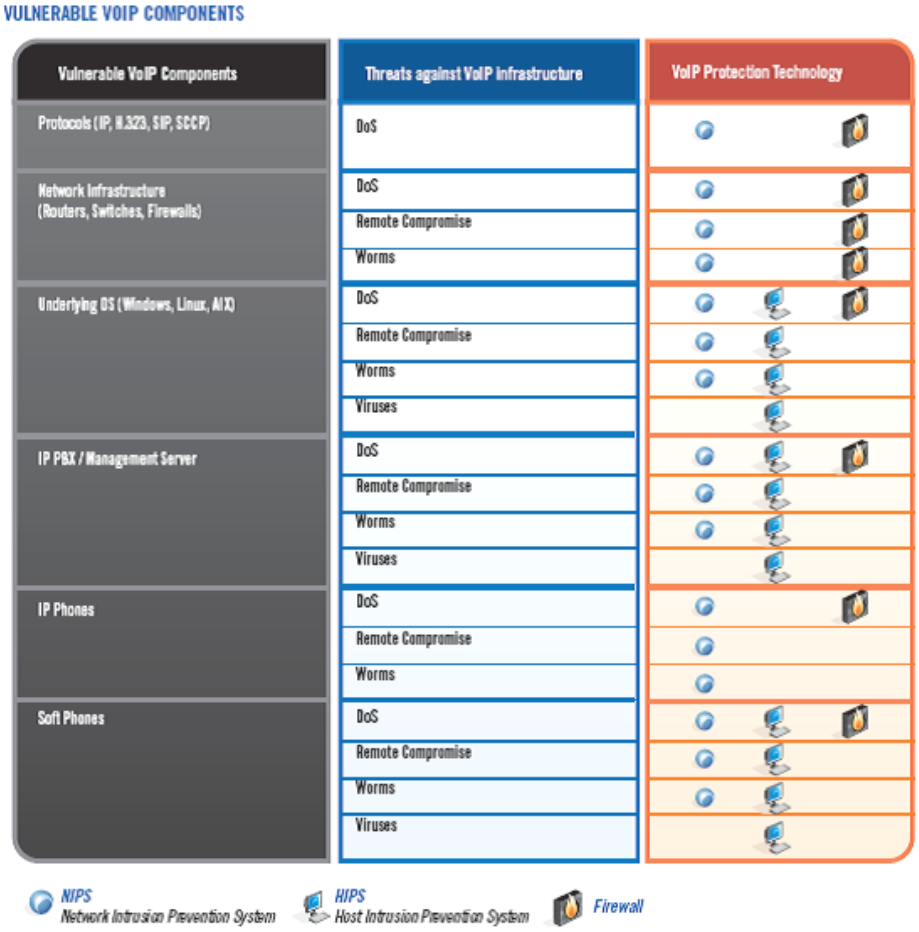

Figura 9, Componentes vulnerables VoIP, ISS (2005)

Rontti (2006), menciona que la confiabilidad de las redes VoIP están amenazadas y algunos ejemplos de ello son el acceso no autorizado, la escucha de las comunicaciones. A su vez la integridad tiende ser amenazada por el fraude telefónico, el uso anónimo del servicio, alteración de datos privados, y por ultimo disponibilidad y la calidad del servicio

son acechadas por la interrupción del servicio de la red VoIP, Como se muestra en la siguiente figura.

Security and Reliability Goals and Requirements			
Confidentiality	Integrity	Availability	Quality of Service
Security Threats in VoIP			
Unauthorized Access	Call Fraud	Service Disruption	
Eavesdropping of communicatios	Anonymous Use		
Leaking Location Data	Trust in Interconnections		
Disclosure of Privacy Data (A)	Alteration of Privacy Data (A)		

Tabla 2, Requerimientos de seguridad y amenazas a red VoIP, Rontti Tero, White paper Codenomicon Ltd

Considerando que diversos "malware" o códigos maliciosos como los gusanos, virus, troyanos, etc. Suelen perturbar todos los requisitos de seguridad, entre otros ataques. Rontti (2006) menciona que los ataques activos requieren cambios a la red, a diferencia de los ataques pasivos que estos no requieren ningún cambio, y que hay "eventos" naturales los cuales pueden ser atacados en contra de los requisitos de seguridad. En la figura 2, se describe la distribución de ataques y eventos a las redes VoIP.

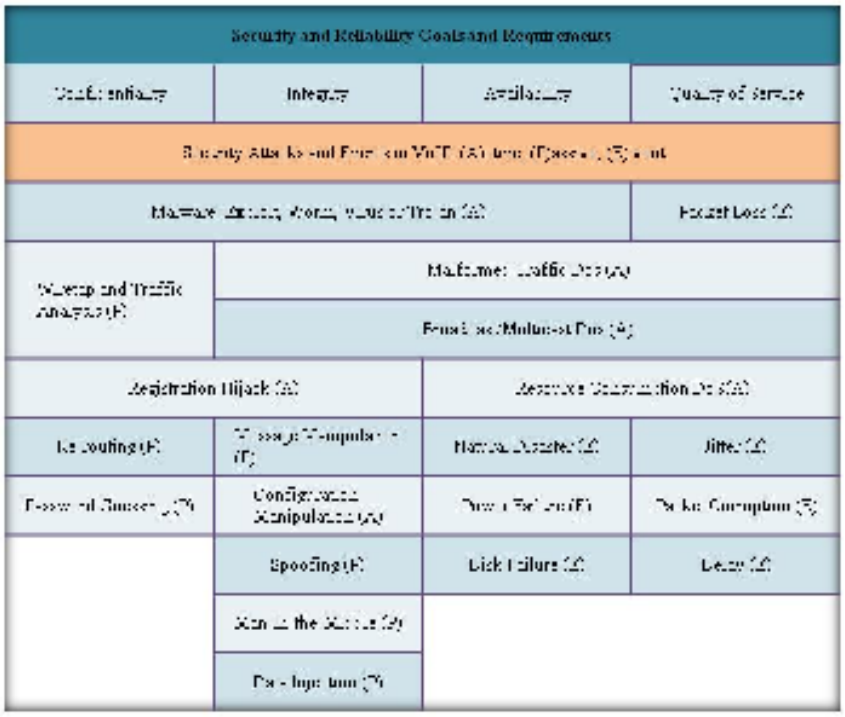

Tabla 3, Ataques a red VoIP, Rontti Tero, White paper Codenomicon Ltd

En las actuales vulnerabilidades que se han presentado a las redes VoIP estas pueden ser divididas como se describió anteriormente en diseño, implementación y defectos de programación, muchos de estos defectos pueden habilitar uno o varios diferentes ataques, por lo cual es importante entender la falla detrás de los riesgos, como lo comenta Rontti (2006). Describiéndolo como se puede visualizar en la figura siguiente.

Security and Reliability Goals and Requirements			
Confidentiality	Integrity	Availability	Quality of Service
Vulnerabilities (flaw or weakness)in VoIP: (D)esign, (I)mplementation, (C)onfiguration			
Insufficient Integrity Checks (D)		Low Bandwidth (C)	
File/Resource Manipulation Flaws (I)		Low Resources (C)	
Insufficient Encryption (D)	Weak Authentication (D/C)	String/Array Manipulation Flaws (I)	Physical Connection Quality (I)
Bad Passwords (C)	Execution Flaws(I)	Heterogeneous Network (D/C)	Packet Collision (I)
		Lacking Fall-back System (D)	

Tabla 4, Vulnerabilidades de seguridad en red VoIP, Rontti Tero, White paper Codenomicon Ltd

Areitio Bertolín (2006) por su lado nos dice que el objetivo es violar la política de seguridad del sitio, intentar violar limitaciones específicas en la seguridad, encontrar algún número de vulnerabilidades dentro de un período de tiempo.

Pruebas de vulnerabilidades / penetración

Estas pruebas o pseudo-ataques se llevan a cabo por un equipo de evaluación y su objetivo es emular un ataque contra uno o más sistemas de computadoras para descubrir la forma de la violación del sistema de los controles de seguridad, esto lo mencionan Porter, Rosela, Bassin (2006) es para obtener información sensible, servicios sin autorización, o para simular daños en el sistema por negar servicio a los usuarios legítimos.

Las pruebas pueden consistir en algo tan simple como un escaneo con aplicaciones como Nmap ó Nessus, estas pueden ser tan detalladas como pruebas en contra de una arquitectura de aplicaciones de negocios. Porter, Rosela, Bassin (2006) Se concluye con éxito cuando:

- Un número definido de fallas se encuentran.
- Un conjunto nivel de penetración de tiempo ha transcurrido.
- La política de seguridad se viola suficientemente.
- El dinero y los recursos se han agotado.

- Un programa en particular o de la transacción se ejecuta.
- Sistemas de gestión de red son subvertido.

Discovery	Scanning	Vulnerability Assessment
Whois	Hping	tcpdump
SamSpade	Nmap	Voipong
WSPingPro	LDAPMiner	Wepcrack
SuperScan	scanrand	Getif
dig	NetStumbler	Nessus
nslookup	Kismet	Retina
ping	Nikto	Brute
traceroute	PSTools	WinFingerprint
TCPTraceroute	WSPingPro	Lophtcrack5
	SQLPing 2	ISS Internet Scanner
	ToneLoc	SnagIT
	Dsniff	@stake Proxy
	SuperScan	Ethereal
		Ettercap
		Amap
		John the Ripper
		Netcat

Figura 10, Herramientas de testeo de seguridad mas comunes, Bassin, Rosela, Porter, PVoIPS.

Mencionan Porter, Rosela, Bassin (2006) que es una de las fases más importantes de las pruebas de penetración, y se da cuando la vulnerabilidad es probada en redes VoIP, así como estas pruebas de vulnerabilidades tienen el potencial para generar suficiente tráfico en la red que la calidad de voz es negativamente afectada.

3.3 Métricas de seguridad

Una medida interna que se puede utilizar para cuantificar una vulnerabilidad es un "métrica de amenazas". Esta métrica se basa en dos parámetros independientes: la percepción de un riesgo (tabla 1) y una frecuencia estimada (tabla 2). A partir de esto se forma una combinación de los dos resultados, y se coloca en una matriz de 3x3.

Esta métrica de amenazas (MA) tiene varios propósitos: En primer lugar, es utilizado para dar prioridad a una vulnerabilidad descubierta. Una MA's alta o severa (tabla 3) requerirá atención inmediata, y también pueden requerir un análisis más profundo.

Porter (2006) describe un ejemplo de ello, si una vulnerabilidad recién descubierta ocupa el puesto de MA con un H1, todos los miembros del equipo de inmediato comprenden que se trata de un problema grave y que requiere una acción inmediata, mientras que una MA de L3 indica una cuestión insignificante.

Categorías de riesgos	
Riesgo alto (H)	Pérdida de información crítica propietaria, perturbación de sistema, o severo daño al ambiente.
Riesgo medio (M)	Pérdida de información propietaria, mayor daño al sistema ó ambiente
Riesgo bajo (L)	Daño menor en sistema o ambiente

Tabla 5, Construcción propia de datos obtenidos de PVS, Bassin, Rosela, Porter, 2006.

Frecuencias de categorías	
Frecuente (1)	Probable de casos más frecuentes
Ocasional (2)	Posibilidad de casos frecuentes
Improbable 3)	Prácticamente imposible

Tabla 6, Construcción propia de datos obtenidos de PVS, Bassin, Rosela, Porter, 2006.

Métrica de Amenazas

	Riesgo alto (H)	Riesgo Medio (M)	Riesgo bajo (L)
Frecuente (1)	H1	M1	L1
Ocasional (2)	H2	M2	L2
Improbable 3)	H3	M3	L3

Tabla 7, Construcción propia de datos obtenidos de PVS, Bassin, Rosela, Porter, 2006.

Después de conocer las métricas de seguridad, se pueden aplicar a:

3.4 Protocolos más comunes usados en VoIP

Protocolo	Aplicación	Madurez	Nivel de riesgo
H. 323	Call Signaling, control Message Formating, Stream Packetization	Medio-alto; Alta interoperabilidad de múltiples proveedores, pero todavía se utilizan extensiones propietarias de la mayoría de los proveedores	Alto, Utiliza hasta 11 puertos en cada período de sesiones; configuraciones de firewall estándar abre todos los de puertos potenciales posibles de aplicaciones, lo que hace redes extremadamente vulnerables.
Protocolo Internet (IP)	El protocolo de capa de red en la suite del Protocolo de Internet, se Usa para comunicar datos a través de una red de conmutación de paquetes	Relativamente alto; IPv6 Mejora sobre IPv4, la versión de IP en todo el mundo, principalmente en el uso de direcciones de 128 bits, en lugar de direcciones de 32 bits.	Alta, Debido a su naturaleza, IP proporciona sólo mejor esfuerzo de entrega, y protocolos de la capa superior deben abordar cuestiones de fiabilidad.
Media Gateway control Protocol (MGCP)	Control y estado de la comunicación de las llamadas entre Softswitch / Media Gateway Controller y Media Gateway	Relativamente bajo; La industria estándar de facto es el informativo RFC 2705, y mantenida por el consorcio Softswitch PacketCable; implementación aplicación de la norma posterior MEGACO/H.248 sigue siendo escasa	Medio; MGCP soporta IPSec para protección de mensajes, y permite a los call agents proveer gateways con “sesion keys” para encriptación de mensajes de audio, para protección contra eavesdropping.
Protocolo de transporte de tiempo real (RTP)	Streaming Media (ejemplo, tonos, anuncios, mensajes	Medio-alto; Primero definido por ITU-T, después	Media; encriptación soportada, pero típicamente

	de voz)	adoptado por IETF, y ahora abarca perfil específico para audio y videoconferencia y seguridad opcional RTP	comprometida con el rendimiento.
Protocolo de inicio de sesión (SIP)	Iniciación, modificación, terminación de sesiones multimedia de usuarios.	Medio; Extensiones propietarias todavía utilizadas por los principales proveedores de sistemas que permiten características no estándar.	Medio; SIP soporta encriptación point-to-point, pero las desventajas administrativas y técnicas persisten, y carece de definición para SIP que requiere enviar a múltiples "endpoints"

Tabla 8, Construcción propia con datos recopilados de varios autores, 2006.

3.5 Métricas aplicadas a activos

3.5.1 Protocolos

En estas tablas siguientes se aplican las métricas a los activos principales de la tecnología VoIP, mostrando el tipo de amenaza y qué tipo de vulnerabilidad afecta a este activo.

Activos	Amenazas	Vulnerabilidades			Riesgo
		Confiabilidad	Integridad	Disponibilidad	
Protocolos	Flooding (TCP/UDP/ICMP Packet Flood)			X	Degrada la calidad de la llamada, Detiene el dispositivo, lo congela, o hace que no responda.
	Flood Amplification (UDP)			X	Amplifica las inundaciones, Invoca la funcionalidad a que responda con más datos de la solicitud.
	Fuzzing	X		X	Muchos Endpoint´s se

					congelan, detienen, colgaran, no responderán, ó de otra manera entraran en una condición DoS. Algunos dispositivos básicos puede comportarse de manera similar. Eficaz método de identificación de bugs de software
	Signaling Manipulation Overview	**X**		**X**	Inyecta señalización maliciosa de mensajes dentro de un canal de señalización, envía nuevas señalizaciones de mensajes a Endpoints o servicios
	Forced Call Teardown			**X**	DoS: una llamada en progreso es forzada a finalizar
	Registration (call) hijacking		**X**	**X**	Las nuevas llamadas para el Endpoint son ruteadas a un dispositivo malicioso en lugar de los dispositivos legítimos.
	Media Hijacking		**X**	**X**	Media Redirección, duplicación, o terminación.
	Caller ID-spoofing	**X**	**X**		Un atacante puede aparecer a la llamada de alguien que no sabe su identidad. Un atacante puede ser erróneamente autenticado.
	Media injection (UDP)			**X**	Modificación, reemplazo, borrado.
	Eavesdropping the Media	**X**	**X**		Las llamadas dejan de ser privadas, el tráfico de datos puede ser observado y grabado.
	ARP Cache Poisoning and ARP Floods			**X**	Al Corromper la cache ARP permite re-enrutar el tráfico para interceptar

					el tráfico de voz y datos de tráfico.
	DoS usando mensajes SIP CANCEL / FAILURE / BYE	**X**		**X**	Corte de la comunicación existente entre dos terminales
	Packet Spoofing and Masquerading	**X**			Robo de identidad
	Replay Attacks		**X**	**X**	Capturar un paquete valido con el cual pueda ser re-enviado dentro de la red buscando como objetivo responder y ofrecer más tráfico para captura, eventualmente proveer suficiente información para pasar al paquete Spoofing y masquerading ó simplemente encontrar un punto de entrada a la red realizar eavesdropping u otro ataque.

Tabla 9, Construcción propia con datos recopilados de varios autores, 2006.

3.5.2 Infraestructura de red

Activos	Amenazas	Vulnerabilidades			Riesgo
		Confiabilidad	Integridad	Disponibilidad	
Network Infrastructure	Configuration Disclosure: Infrastructure	X	X		Revelación de información sensible tales como: nombres de usuario y contraseñas • Call Server, Gateway, servidor de registro, etc • Servicios disponibles VoIP
	Call Redirection and Hijacking	X	X		Perdida de información confidencial y interrupción del servicio
	Malicious Calling			X	Este puede ser perjudicial y costoso, sobre todo cuando las llamadas son re-enviadas por ejemplo a los teléfonos celulares.
	Caller-ID Name Disclosure	X	X		Revelación de información no clasificada potencialmente.
	Eavesdropping the Environment	X			El Dispositivo contesta silenciosamente la llamada -- El audio del dispositivo puede ser espiado.
	Voice mail bombing (Vbombing)				Denegación de servicio, al menos la interrupción del servicio.

Tabla 10, Construcción propia con datos recopilados de varios autores, 2006.

3.5.3 Sistemas Operativos

Activos	Amenazas	Vulnerabilidades			Riesgo
		Confiabilidad	Integridad	Disponibilidad	
Underlying OS (Windows, Linux, Aix)	Buffer over flow	X		X	El programa escribe más información en el espacio del buffer que tiene asignado en la memoria. Esto permite a un atacante sobreescribir los datos que controla la ejecución del programa y tomar el control del programa para ejecutar el código del atacante en lugar del código de proceso.
	Virus	X	X	X	Causa daños en el sistema, consumo de memoria de CPU principal, tiempo de procesador, disminución de performance
	Worms			X	Causa daños en el sistema, consumo de memoria de CPU principal, tiempo de procesador, disminución de performance
	Malas configuraciones	X		X	Permiten ejecutar código o comandos de manera arbitraria, negar servicios (Denial of service) y acceso no autorizado a información crítica.
	Phising	X	X		Espionaje, fraudes en los cobros de las cuentas de teléfono y ataques de negación de servicios.

Tabla 11, Construcción propia con datos recopilados de varios autores, 2006.

3.5.4 Servidor IP PBX

Activos	Amenazas	Vulnerabilidades			Riesgo
		Confiabilidad	Integridad	Disponibilidad	
IP PBX / Management Server	Service Interception and Eavesdropping	X	X		Compromise of PBX hosts and voice gateways; Poor control, detection and management systems; Poor security awareness and practices; and Poor physical security.
	Service fraud and abuse	X		X	System Abuse; Toll fraud; Poor control, detection and management systems; and Poor physical security.

Tabla 12, Construcción propia con datos recopilados de varios autores, 2006.

Por su parte Ransome & Rittinghouse (2005) mencionan en su investigación que hay dos principales razones por las cuales un atacante atacaría un PBX: (1) tener acceso al resto de la red y (2) por razones fraudulentas tales como llamadas libres de larga distancia y teleconferencias, llamadas de sistemas de tarjeta, y el uso del PBX como un derivador para cubrir sus huellas. Como VoIP se hace más popular, PBX son más integrados con las redes IP tradicionales de datos. En general, la mayoría de las empresas están tan preocupadas por los hackers y sus redes de datos. Para delincuentes profesionales, esto es a menudo el vínculo débil perfecto para acceder a la red de datos a través de la centralita no garantizada. Por lo tanto los PBX son vulnerables a los ataques.

KPMG (2007) Menciona que existen una serie de controles de administración, operativos y técnicos que se deben considerar para una buena administración de los riesgos, que se describen en el cuadro que sigue:

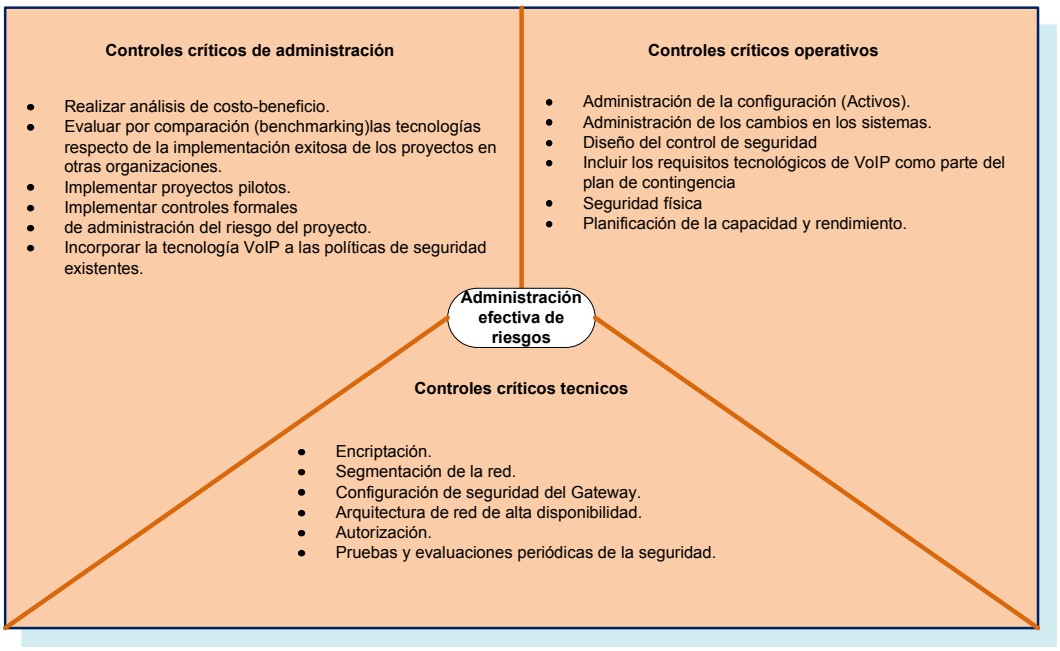

Figura 11, Administración efectiva de riesgos, KPMG, (2007).

Resumen

VoIP transporta paquetes de voz a través de la LAN y pueden exponer a las empresas a las vulnerabilidades de seguridad que ponen en situación de riesgo toda su red. Debido a que la mayoría de los dispositivos de seguridad de red de datos no fueron diseñados para la transmisión de voz, la telefonía IP requiere medidas adicionales para proteger las redes de los ataques.

Muchas organizaciones instalan sistemas de telefonía IP en sitios remotos y fallan en considerar aspectos adicionales de seguridad de la red que deben ser colocados antes de su implementación.

Este descuido puede llevar a costosas consecuencias causadas por graves ataques de red. Y los riesgos de seguridad de VoIP difieren de las que normalmente se encuentran con los sistemas tradicionales PBX. Las empresas no deben asumir que los proveedores han tomado las medidas adecuadas para eliminar las carencias de seguridad en sus productos. Por lo tanto son los usuarios finales quienes deben de soportar la carga de atender sus problemas de seguridad de red y gestionar proactivamente su VoIP. La conciencia de los factores de riesgo descritos en este capítulo ayudara a preparar la seguridad para VoIP y también ayudara a mitigar las posibles brechas de seguridad internas y aumentar la concienciación sobre la seguridad dentro de su organización a reducir significativamente los riesgos de ataques injustificados.

Propuesta de seguridad (Controles de seguridad)

Métodos de seguridad propuestos son basados en los siguientes elementos:

- Separación de voz y datos.
- Autentificación
- Cifrado
- Seguridad perimetral

4.1 Mejores prácticas (Seguridad de red)

La mayoría de las empresas que ponen en marcha una infraestructura de VoIP y eligen una convergencia de red IP (la misma red física de datos y VoIP) por razones económicas y prácticas. Por lo tanto, es claro que la seguridad de la infraestructura de VoIP está estrechamente vinculada a la seguridad de la red IP.

4.1.1 Seguridad física.

La seguridad física es un elemento clave para conseguir una buena seguridad de VoIP. Su aplicación, entre otras cosas, es reducir al mínimo el riesgo de las escuchas clandestinas y el riesgo de denegación de servicios, por ejemplo, desconectar la alimentación de un switch ó un servidor. Acceso a equipos de red (enrutadores, conmutadores,…) servidores VoIP por lo tanto, se limita a sólo las personas autorizadas.

Las soluciones adoptadas para garantizar la seguridad física dependerá del nivel de seguridad necesarias (habitaciones con cerradura, lectores de tarjetas, biometría, guardias...).

Además, la organización debe de adoptar medidas para prohibir a empleados desconectar un cable de red (desde un PC o un hardphone). Es más, un empleado malicioso podría desconectar su hardphone para conectar un ordenador. Y este equipo sería inmediatamente conectado a la VLAN de VoIP; lo que es inaceptable en la vulnerabilidad de la seguridad.

4.1.2 Separación de equipo de voz y datos

La manera más eficaz de mejorar la seguridad de una red de VoIP es separar los equipo VoIP y datos en dos zonas (DATOS + VoIP) de seguridad.

Si el nivel de seguridad requerido es alto y los recursos lo permiten, es recomendable subdividir el área VoIP dependiendo de los tipos de equipo (por ejemplo, zona de servidores VoIP, zona de hardphones, Zona de softphones…).

Esta separación se puede hacer en forma física (dos redes físicamente independiente con switches independientes) o de una manera lógica. La separación lógica es a menudo preferida por razones presupuestarias. En caso de presencia de softphones en la arquitectura, se debe de crear una VLAN para estos dispositivos.

4.1.3 Mejores Prácticas "de seguridad del cliente"

(Notas sobre los softphones.)

Este apartado se refiere a las máquinas con un uso del softphone ya que plantean dos problemas importantes:
En primer lugar, softphones instalados en un Sistema Operativo (SO). Contienen Bugs y se descubren nuevas vulnerabilidades todos los días. Además en los softphones la superficie de ataque es mucho más importante que los hardphones teniendo en cuenta que es la combinación de ataque de la aplicación softphone y del sistema operativo.

Las principales mejores prácticas para su aplicación son:

- Actualización de parches de seguridad para el S.O
- Políticas de Gestión de contraseñas
- Instalación de software antivirus y la actualización regular de su base de datos.

4.1.4 Autentificación

Tras la separación de los equipos de VoIP y Datos, la autenticación es el segundo punto crucial para la seguridad, Varios métodos de autenticación son posibles dependiendo del nivel de seguridad requerido.

El mínimo de la seguridad se logra mediante la aplicación de una autenticación HTTP Recopilación entre teléfonos IP y VoIP servidores. Este método de autenticación es más generalizado. Desgraciadamente, no permite la autenticación mutua y no es muy robusto frente a los ataques fuera de línea de tipo fuerza bruta.

Un mayor nivel de seguridad puede lograrse mediante la aplicación de un protocolo para proporcionar autenticación mutua (autenticación del Teléfono IP por el servidor y el servidor de autenticación por el teléfono IP), tales como

- SIP
- IPSec
- Protocolos propietarios

4.1.5 Cifrado

Este Cifrado (parcial o total) será necesario si la confidencialidad de las conversaciones es requerido. Varias variantes se pueden aplicar:

• Cifrado de flujo de señales (SIPS)
• Cifrado de flujo de medios (SRTP)
• IPSec

Nota: Hay que tener en cuenta que la escucha es posible en una red telefónica convencional (PBX -- PSTN) y el riesgo de escuchar son igualmente importantes en la aplicación de VoIP sin cifrar en la empresa. El cifrado de las comunicaciones de VoIP proporciona un nivel de seguridad (especialmente en términos de confidencialidad) y más hablando de una red telefónica clásica.

4.1.6 Seguridad perimetral.

El perímetro de seguridad se refiere a los equipos en el borde de la red de VoIP y proporciona protección contra ataques externos.

4.1.6.1 SBC (Session Border Controller)

Es un dispositivo que controla los flujos de VoIP colocado en el borde de la red y, opcionalmente, (dependiendo del dispositivo) realiza una serie de funciones de control de llamadas para desahogar la carga sobre la convocatoria de agentes dentro de la red. Muchas personas comparan al SBC VoIP contra un firewall. Sin embargo, las características que ofrecen, aunque muy diferentes en función de las marcas, van mucho más allá del firewall, por ejemplo:

- *Call Admission Control*
- Conversión del codec media
- Configuración de puertos en el servidor de seguridad ó firewall necesarias para las comunicaciones VoIP.
- NAT. *Traversal* / STUN
- ALG (application layer gateway).
- …

Arquitectura interna de un SBC

SBC está compuesto de dos módulos:

1. La función de señalización de SBC (SBC-SIG) controla el acceso de mensajes de señalización de VoIP para el núcleo de la red, y manipula el contenido de estos mensajes.
2. La función de los medios de comunicación de SBC (SBC-MEDIA) controla el acceso de los medios de comunicación los paquetes a la red, ofrece servicios diferenciados y QoS para los diferentes flujos de los medios de comunicación, e impide el robo de servicio.

Estos dos módulos se pueden combinar en una caja (single-box SBC) o estar en dos cajas (dual-box SBC).

La solución (single-box SBC) es más simple de aplicar y se debe preferir en infraestructuras de VoIP de pequeñas y medianas dimensiones. En cambio (dual-box SBC).permite una mayor flexibilidad en su despliegue y puede satisfacer las necesidades. Sin embargo, se requiere de la aplicación de un protocolo como Megaco / MGCP para permitir la comunicación entre el módulo de señalización SBC (llamada agente de llamadas en el RFC de MGCP) y los módulos de SBC Media (llamado medios de comunicación de puerta de enlace en el RFC MGCP).

4.1.6.2 STUN / TURN

STUN *(Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators* es un protocolo que permite a las aplicaciones para descubrir las presencia del firewall + NAT entre ellos y la Internet. También determina qué dirección IP pública se ha asignado por el NAT. Se trata de un protocolo cliente-servidor ó una aplicación, como por ejemplo un softphone puede incluir un cliente STUN que va a enviar peticiones a un servidor STUN. Las respuestas desde el servidor permiten al cliente NAT deducir el tipo de NAT utilizado como la dirección y el número de puerto que se ha asignado.

TURN *(Traversal Using Relay NAT)* es un protocolo que permite a un elemento estar situado detrás de un NAT ó firewall para recibir datos. Su funcionamiento es también cliente-servidor y el cliente (incluido en una aplicación) hace una petición al servidor STUN, que responderá por la dirección que se alcance (funciona como una retransmisión de datos).

4.2 SEGURIDAD BÁSICA.

4.2.1 Actualización de software (IPBX, hardphone y softphone)

Identificador: S.01
Descripción de la solución:

El IPBX los hardphones y softphones contienen todo el software. El código de este software puede contener vulnerabilidades (desbordamiento de búfer,...) y, por tanto, ser vulnerables a diversos ataques. Por lo tanto, es muy importante mantener una versión actualizada del software, incluyendo cuando las vulnerabilidades del software fueron descubiertas. Para ello, se debe:

- Consultar regularmente las páginas web de los fabricantes de hardware / software de los equipos introducidos en la infraestructura de VoIP, ó mejor, estar inscritos en sus boletines que informan automáticamente si un nueva versión / parche está disponible.
- Prueba de parche en el equipo de prueba
- La mejora en los equipos de producción si la prueba anterior esta conclusa. NSA(2006)

4.2.2 Bloqueo de la configuración (hardphone/softphone)

Identificador: S.02
Descripción de la solución:

Una vez que el hardphone / softphone son configurados, es importante que la contraseña de configuración sea bloqueada y resguardada para evitar que un usuario pueda modificar los parámetros de ajustes (deshabilitar la autenticación,...). Además, en la organización se deben adoptar medidas para prohibir a los empleados realizar cambios en la configuración de los equipos de infraestructura VoIP. DISA (2006)

4.3 SEPARACIÓN DE EQUIPOS DE DATOS Y VOZ.

4.3.1 Separación en el nivel IP (capa 3)

Identificador: S.03
Descripción de la solución:

La solución consiste en asignar un rango de direcciones IP (por ejemplo: 192.168.1.x) para redes de datos. En esta red se incluyen las instalaciones que estaban presentes antes de la introducción de la red VoIP: servidores (de archivos, controlador de dominio,…), etc.

Un rango de direcciones IP diferentes (por ejemplo: 192.168.1.x) ser atribuye a equipos de VoIP.

Una vez que esta separación se lleva a cabo, es posible definir ACL de equipos de capa (*switches* L3 / routers /firewalls) a fin de autorizar las comunicaciones entre las direcciones IP permitidas. Además, si los servicios tales como DNS, DHCP ó NTP son necesarios, la red VoIP debe tener sus propios servidores. DISA (2006).

4.3.2 Separación a través de la VLAN (Capa 2)

Identificador: S.04
Descripción de la solución:

La segunda fase de nuestra defensa en profundidad es definir una VLAN DATOS dedicados a los equipos de la red actual, a fin de obtener una red de datos y una VLAN VoIP dedicados en los equipos VoIP. Para obtener una mejor separación, es aconsejable crear en lugar de VLAN VoIP, para cada clase de equipos de VoIP como por ejemplo:

- *Hardphones* ----> VLAN VoIP Hardphones
- *Softphones* ----> VLAN VoIP Softphones
- Servers ----> VLAN VoIP Servers
- …

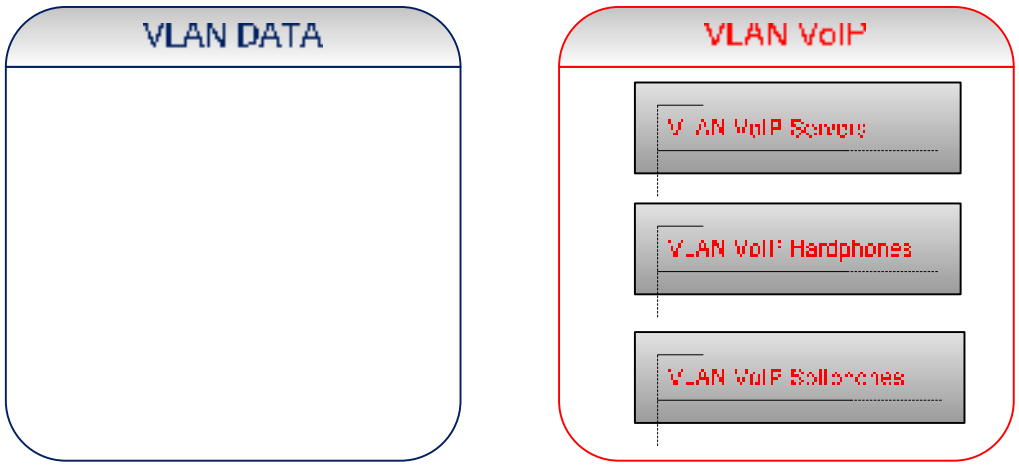

Figura 12, Separación de Datos, BP_VoIP, (2006)

Esto permite crear reglas de filtrado más finas y mejor QoS. Además, si un ataque se produce sobre VLAN VoIP Softphone, no afectará el buen funcionamiento de otros sistemas VLAN VoIP.

Si esto no es posible (por razones de funcionalidad, en particular) para prohibir cualquier comunicación entre VLAN DATOS y VoIP, un filtrado inter-VLAN (a nivel de *switchs* y/o routers) y/o *firewalls* deberán ser establecidos para filtrar estrictamente el tráfico entre las VLAN´s. DISA (2006).

4.3.3 Filtro Inter-VLAN

Identificador: S.05
Descripción de la solución:

Las comunicaciones entre VLAN´s establecidas en S.04 deben ser estrictamente filtradas para permitir sólo el flujo requerido. El filtrado debe ser una lista blanca (sólo el flujo definido es autorizado).

La filtración se puede realizar:

- Definiendo las ACL en los *switches* y/o routers de conexión VLAN
- Colocando un firewall entre las VLAN´s

Las reglas de filtrado deben estar basadas en direcciones IP, números de puertos/protocolos y *flags* TCP/IP de tal manera de crearlas lo más estrictas posible y permitir sólo las comunicaciones necesarias. Por ejemplo, los teléfonos IP no necesitan enviar un flujo de datos (multimedia), (por ejemplo RTP) para Servidores VoIP. Así que en vez de permitir que todas las comunicaciones entre el sistema VLAN VoIP hardphones /

softphones y servidores VLAN VoIP, sólo el tráfico en el protocolo de señalización (SIP, por ejemplo) se debe permitir. NSA (2006).

4.3.4 Usando tarjeta de red 802.1Q

Identificador: S.06
Descripción de la solución:

El principal peligro al instalar un softphone en un equipo, es que al estar este equipo ya conectado a la red de datos, se convierte en un terminal VoIP, esto es contrario a lo propuesto en el identificador S.04.

Hay una solución para mantener la separación de las VLANs. La solución es dotar a los ordenadores con una tarjeta Ethernet que soporta el protocolo 802.1q y configurar el uso de este protocolo.

Estas tarjetas permiten el tráfico de Ethernet para separar el tráfico de datos y el trafico de VoIP (resultante de un softphone) haciendo uso de cada tipo de tráfico en su respectiva VLAN. El S.O, la tarjeta Ethernet y softphone soportan 802.1q. CISA (2006).

4.3.5 Deshabilitar o proteger puertos de red adicionales 802.1q.

Identificador: S.07
Descripción de la solución:

Algunos hardphones poseen uno (ó más) puertos para permitir la conexión un equipo u otros equipos de red. Este puerto adicional está diseñado para utilizarse para conectar varios equipos de red: el hardphone funciona como un Hub. El hardphone y el equipo están por lo tanto, en la misma red/VLAN que es contrario a la mejor solución del identificador S.04.

La solución consiste en desactivar el puerto (s) extra (s) o activar el protocolo 802.1q sobre el hardphone. La separación entre la red / VLAN datos y VoIP puede mantenerse. CISA (2006).

4.3.6 Acceso a los puertos de switches (ACL,…)

Identificador: S.08
Descripción de la solución:

La separación establecida con las soluciones S.03 y S.04 puede verse ser un peligro si individuo tiene la posibilidad de conectar una máquina a un puerto de un conmutador. Para evitar esto, las medidas de seguridad siguientes se pueden poner en marcha (clasificadas por orden creciente de eficacia):

- Los puertos no utilizados deben ser desactivados.
- Los puertos no utilizados deben ser colocados en una VLAN no utilizada.
- Un ACL (colocado en un puerto o en un *switch completo*) deben crearse para permitir el acceso sólo a determinadas direcciones MAC.
- Una autenticación 802.1x deben aplicarse (si los *switches* y Teléfonos IP lo permiten)

La solución basada en ACL es recomendada. DISA, NSA (2006)

4.3.7 Colocación de servicios convergentes dentro de una DMZ.

Identificador: S.09
Descripción de la solución:

Con el fin de no comprometer la separación de VLAN DATOS y VoIP, los servicios convergentes (servicios que requieren acceso a la VLAN datos y VLAN VoIP) deben ser colocados en una zona desmilitarizada (DMZ).
Las reglas del firewall deben ser tan estrictas como sea posible para permitir sólo flujos necesarios. NSA (2006).

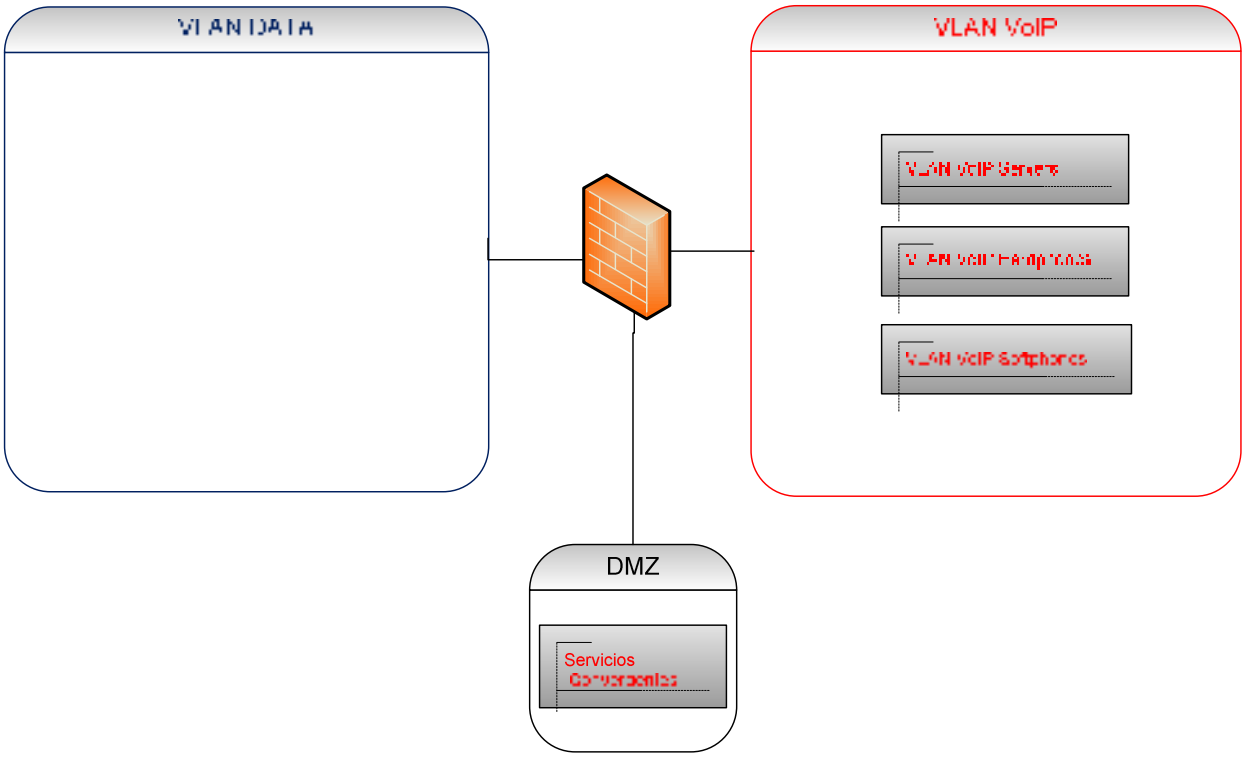

Figura 13, Servicios convergentes dentro de una DMZ, BP_VoIP, (2006)

4.4 AUTENTICACION

4.4.1 HTTP Digest Authentication de mensajes SIP.

Identificador: S.10
Descripción de la solución:

HTTP Digest Authentication permite el servidor para autenticar los mensajes SIP REGISTER y/o INVITE enviadas por un Teléfono IP. Los ataques basados en el robo de la identidad del cliente ya no son posibles (siempre y cuando la política de gestión de contraseñas sea eficaz). NSA (2006).
La aplicación de esta autenticación requiere que se configure HTTP Digest

- En el registro
- En los phones IP

Esta configuración consiste generalmente en:

- Definir el dominio de autentificación.
- Introducir la contraseña (secreto compartido entre el Servidor de registro y el Teléfono IP).

Este método de autenticación es susceptible a ataques *offline* de tipo bruta fuerza, se recomienda definir las políticas que requieren una contraseña compleja y una contraseña de longitud mínima. NSA (2006).

4.4.2 Autentificación mutua

Identificador: S.11
Descripción de la solución:

La autenticación mutua permite a un servidor autenticar al cliente y el cliente autenticar al servidor. Ataques basados en el robo de identidad no son entonces posibles.
Los métodos de autenticación mutua que pueden aplicarse:

- SIPS.
- H.235 para H.323.
- Protocoles propietarios.

El establecimiento de un método de autenticación mutua requiere de la configuración del método elegido:

- En el IPBX.
- En los IP Phones. NSA (2006).

4.5 Cifrado

4.5.1 Cifrado del flujo de señalización: SIPS,…

Identificador: S.12
Descripción de la solución:

El cifrado del flujo de señalización permite garantizar la confidencialidad e integridad de los datos intercambiados. Espiar en esas corrientes son por lo tanto evitable.
Los protocolos pueden ser implementados son:

- SIPS (en reemplazo de SIP)
- protocolos propietarios

Sin embargo, es importante señalar que el cifrado del flujo presentará una sobrecarga. Esta sobrecarga puede llegar a ser importante para los servidores VoIP si el número de llamadas simultáneas es importante. Por lo tanto, es importante probar la carga generada por la aplicación de cifrado a fin de conocer los límites de la infraestructura VoIP para permitir el diseño de equipos de VoIP. NSA (2006).

Con respecto a SIPS

SIPS se basa en el TLS (**Transport Layer Security)**. La integridad de los datos está garantizada a través de MACs (*Message Authentification Code*) basado sobre las funciones de hash MD5 (16 octetos) ó SHA-1 (20 octetos).

Proporciona, además de la encriptación, dependiendo de la configuración:

- La autentificación simple (servidor de autenticación para el Teléfono IP).
- La autentificación mutua entre los servidores y Teléfonos IP.

Autenticación de entidades se basa en el protocolo X.509, y tiene lugar durante la fase de *handshake de* TLS. También es durante esta fase que se negocian algoritmos (*cypher* y MAC) y la generación de la clave simétrica del período de sesiones, para la encriptación de datos.

El siguiente diagrama detalla los principales intercambios en un *handshake de* TLS.

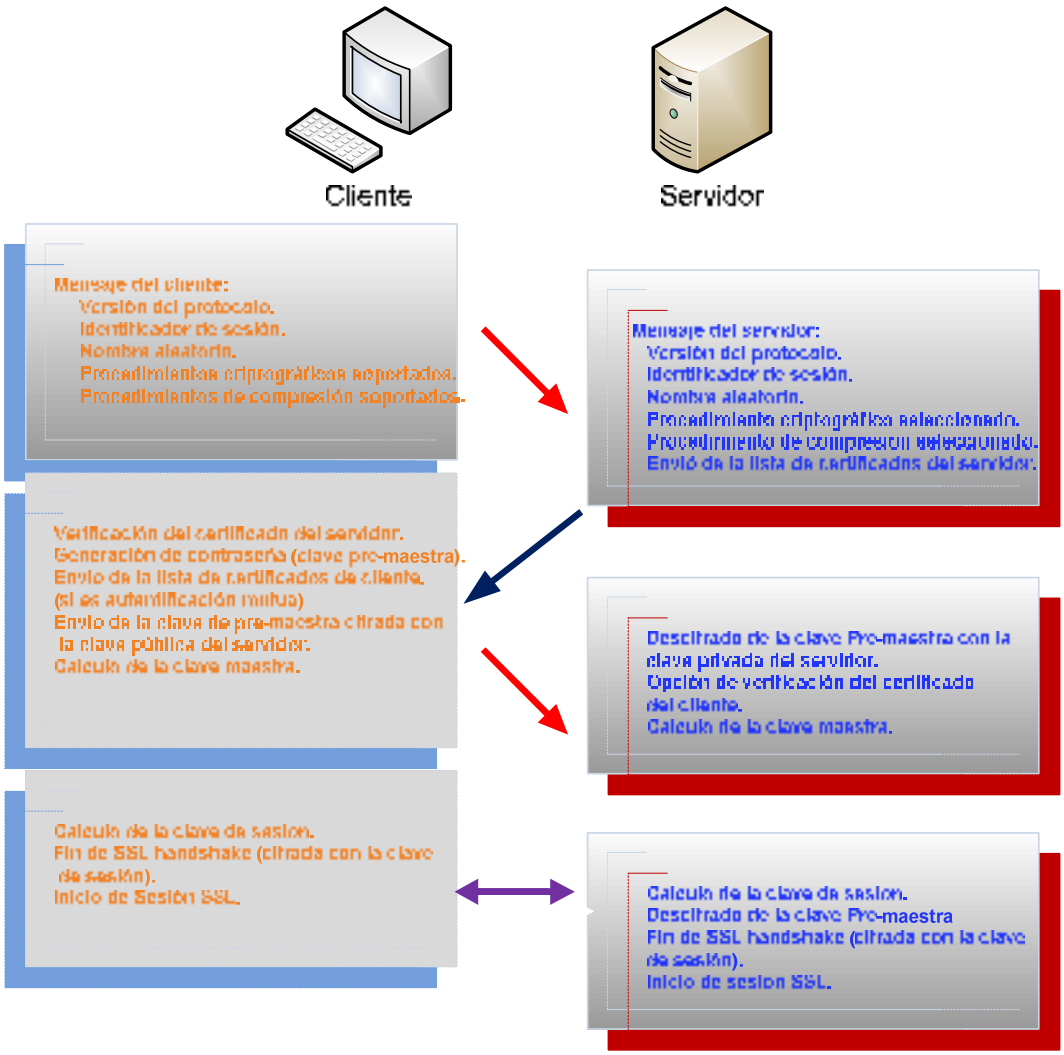

Figura 14, Encriptación cliente - servidor, BP_VoIP, (2006).

4.5.2 Cifrado del flujo de datos media: SRTP…

Identificador: S.13
Descripción de la solución:

El cifrado del flujo de datos multimedia garantiza la confidencialidad y la integridad de los datos intercambiados. Las escuchas clandestinas de este tipo de flujos pueden prevenirse. Además, esto proporciona cifrado de autenticación mutua entre los Teléfonos IP.

Los protocolos que pueden ser implementados son:

- SRTP (en sustitución de RTP)
- H.235 para H.323
- Protocoles propietarios

Es importante señalar que el cifrado de flujo de datos generara una sobrecarga, que puede perjudicar la calidad de la conversación. De hecho, como el audio en tiempo real son muy sensibles a los períodos de tiempo (tiempo de retraso), así como las variaciones de retrasos (jitter). Por lo tanto, debemos comprobar que la sobrecarga generada por el algoritmo del cifrado es tolerable (tolerable, que implica que las sobrecargas no degradan demasiado la calidad de la conversación). NSA (2006).

En cuanto a SIP (y, más específicamente, RTP)

El protocolo SRTP ((*Secured Real-Time Transport* Protocol) es una extensión del protocolo RTP que proporciona confidencialidad, autenticación y protección contra la repetición del tráfico RTP y RTCP. El uso de AES (*Advanced Encryption Standard*) en modo de *stream cipher* garantiza una buena seguridad pero no del aumento del tamaño de la carga encriptada. La etiqueta de autenticación utilizada para comprobar la integridad de los datos añade 10 bytes de cada paquete RTP / RTCP, pero puede ser reducida a 4 bytes, si la transmisión se efectúa en un canal de comunicación lento. Anónimo (2000).

RTP y RTCP pueden garantizar la seguridad de manera criptográfica respectivamente por SRTP y SRTCP (*Secured Real-Time Transport Control Protocol*) pero no causa problemas importantes en la calidad de transmisión. NSA (2006).

Formato de voz un paquete SRTP.

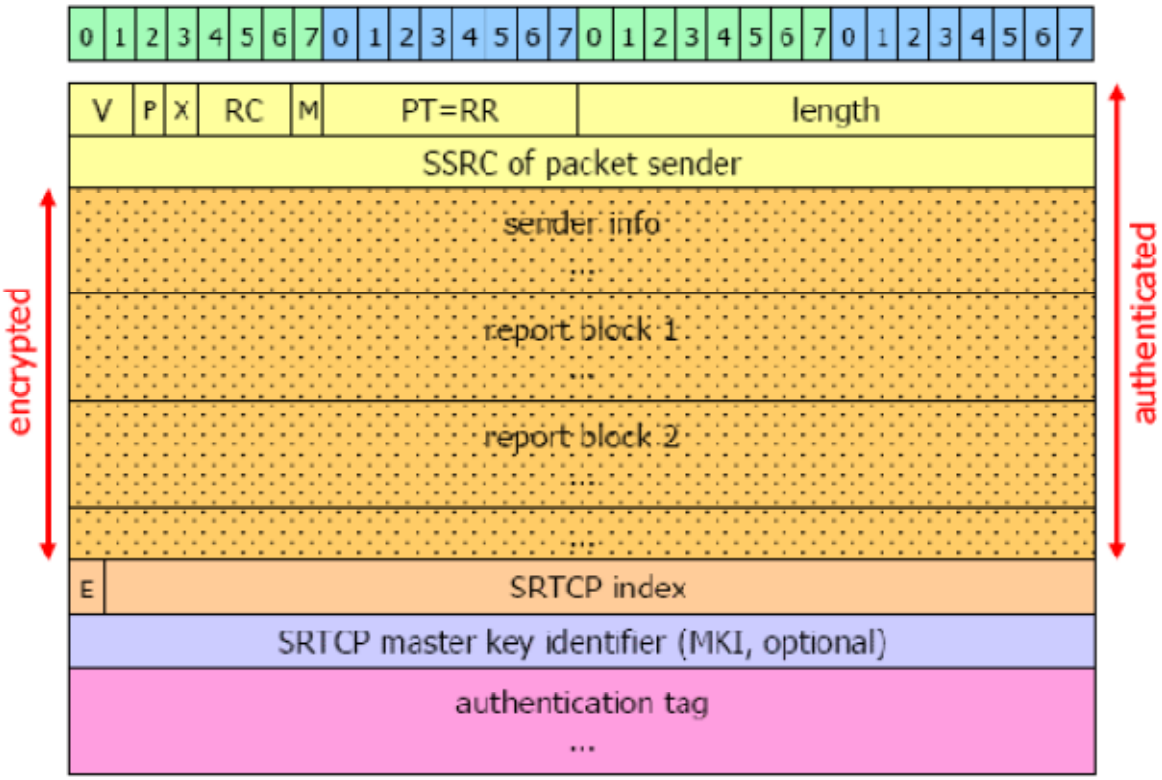

Figura 15, Formato de voz, BP_VoIP, (2006).

Uno puede ver fácilmente que sólo el cuerpo de RTP está codificado. El campo MKI es opcional e identifica la clave primaria a partir de la cual otras sesiones se derivan. El MKI podrá ser utilizado por el receptor para recuperar la clave primaria correcta cuando tenga la necesidad de una renovación la clave se producirá.

La etiqueta de autenticación es un checksum criptográfico (HMAC SHA-1) calculado sobre cabecera y el cuerpo del paquete RTP. Su uso contribuye a proteger los mensajes contra la modificación no autorizada. La duración predeterminada de la etiqueta es de 10 octetos, pero puede reducirse si el canal de transmisión no permite una gran aumentar el tamaño de los paquetes RTP.

La seguridad de paquetes RTCP es similar a la de RTP. La única diferencia es la exigencia de utilizar la autenticación de la etiqueta para evitar que un atacante pueda completar un flujo multimedia RTP mediante el envío de mensajes SIP BYE. NSA (2006).

4.5.3 Cifrado con IPSEC (u otra tecnología VPN)

Identificador: S.14
Descripción de la solución:

El encriptado de flujo con IPSec **(**u otra tecnología VPN**)** permite garantizar la confidencialidad e integridad de los flujos. Autenticación mutua de los protagonistas esta también asegurada.

Los protocolos que pueden ser implementados son:

- IPSec
- Otra tecnología VPN

Es importante señalar que el cifrado de flujos introducirá un *overhead*. Debemos por lo tanto, probar que este *overead* es tolerable antes de implementar una VPN.

Con respecto a SIP (y, más concretamente, SIP protegido por IPSec)

IPSec es un mecanismo general que puede ser utilizado para proteger a los mensajes SIP en el nivel IP. Con SIP, cada *proxy* debe tener acceso de lectura / escritura en la cabecera de los mensajes SIP con el fin de agregar ó quitar cabeceras IVA. Para posibilitar el uso de IPSec ESP ((*Encapsulating Security Payload*) ó AH (Authentification Header), su funcionamiento debe basarse en un Modo Hop-By-Hop.

IPSec se basa en una variedad de mecanismos para proteger el intercambio de datos en la red. Funciona en la capa IP y se ocupa de todos los paquetes IP. Por lo tanto, protege a todas las aplicaciones y puede ser aplicado en todos los dispositivos a través de la red en un punto a punto para ver el enlace. Labouret (2000).

Su objetivo es prevenir el espionaje del flujo de datos y el acceso ilegal a recursos, que ayuda a garantizar la confidencialidad y la autenticidad de los datos intercambiados. También proporciona protección contra *replays-attacks*. Es bueno señalando que permite un alto nivel de protección cuando se utiliza con algoritmos fuertes y en un entorno seguro. Labouret (2000).

Estas características son proporcionadas por los mecanismos criptográficos:

- Message Authentication Code (MAC) = Autenticidad de datos.
- Cifrado de datos = Confiabilidad de datos.
- Número de secuencia = Protección contra replays-attacks.

Estos mecanismos se llevan a cabo con dos extensiones del protocolo IP:

- AH (Authentification Header) que garantiza la autenticidad de Datagramas IP.

- ESP (Encapsulating Security Payload) garantiza la confidencialidad de datos y/o autenticidad.

AH y ESP pueden funcionar con varios algoritmos criptográficos, Sin embargo, la IETF recomienda el uso de **triple DES** (128 bits) para la encriptación y el HMAC-MD5 ó HMAC-SHA1 para la autenticidad. NSA (2006).

4.6 SEGURIDAD PERIMETRAL

4.6.1 SBC: Call Admission Control

Identificador: S.15
Descripción de la solución:

Los ataques de DoS, por definición, implican un número inusualmente elevado de las transacciones de red, gracias al SBC el administrador de la red tiene la capacidad de definir los canales sobre la base de diversos criterios, para limitar el tráfico entrante y/o saliente de una red. De esta forma, el SBC evita la sobrecarga de los *switchs* y poner fuera de servicio determinados equipos y/o la red. Hardwick (2005).

Se recomienda colocar canales en lo siguiente:

- Limitación del tráfico de señalización de VoIP por sesión.
- Limitación del tráfico de señalización de VoIP por usuario registrado (*subscriber*).
- Limitación del tráfico de señalización de VoIP por red.
- Limitación del volumen global de señalización de VoIP.

También se recomienda que los mismos tipos de canales den informes de la señalización de VoIP en general, sino en el tipo de mensaje de señalización VoIP. Hardwick (2005).

4.6.2 Uso de servidores dedicados para STUN

Identificador: S.16
Prevenir ataques: (refiriéndose a su identificación).

Es recomendable que el servidor STUN este ejecutándose con todos los puertos TCP y UDP desactivados excepto los puertos STUN. Esto evitara que los virus ó troyanos infecten los servidores STUN, y así evitar que se vean comprometidos. (Permite evitar el método 1 descrito en los ataques) RFC 3489

4.6.3 Verificación de la identidad del servidor STUN

Identificador: S.17
Descripción de la solución:

STUN contiene un mecanismo de verificación de la integridad de mensajes, pidiendo al cliente STUN hacer la primera solicitud de un secreto compartido al servidor STUN. El servidor STUN responderá dando un nombre de usuario y una contraseña. Luego de que el cliente haga su solicitud, se insertara un campo “Message Integrity” y un nombre de usuario que permita al servidor comprobar la integridad del mensaje. A continuación, las respuestas también contendrán un campo para verificar la integridad de los mensajes.

Por lo tanto, debemos comprobar que este activado y que las solicitudes contengan el campo de "integridad del mensaje", y debidamente y verificarse adecuadamente en cada transacción.RFC 3489

4.6.4 STUN Cliente: Continuación de escuchar las respuestas después de recibir la primera respuesta

Identificador: S.18
Descripción de la solución:

La recepción de una respuesta por parte del servidor STUN, Debe normalmente, terminar las transmisiones de solicitud. Sin embargo, los clientes deben continuar la escucha de las respuestas durante 10 segundos después de la primera respuesta. Si durante esos diez segundos una respuesta que se recibe contiene otra información, es probable que un ataque esté curso.

Por lo tanto, es importante garantizar que los clientes STUN utilizados para hacer esta verificación y advertir al usuario si es necesario. Esta solución no resuelve

directamente el problema, pero advierte al usuario en caso de ataque, que puede adoptar otras disposiciones para bloquear y / o cortar cualquier comunicación.RFC 3489.

4.6.5 Limitar el ancho de banda asignado por persona

Identificador: S.19
Descripción de la solución:

Dado que los servidores STUN implementaron las funciones de turnar las asignaciones de recursos, es probable que sean víctimas de ataques del tipo denegación de servicio (DoS), Todas las solicitudes de asignación son autenticadas, a fin de evitar a un usuario malicioso lanzar un ataque. Sin embargo, un atacante autenticado podría generar múltiples solicitudes de asignación.

Para evitar que un usuario malicioso pueda asignar todos los recursos del servidor, se recomienda que el servidor pueda implementar un modesto límite de ancho de banda para ser asignada por persona.

Sin embargo, este mecanismo no impide a un gran número de usuarios mal intencionado de aplicar un número reducido de recursos. Tales ataques son posibles utilizando botnets, y son difíciles de detectar y prevenir. Rosenberg (2006).

4.7 MATRIZ ATAQUES- SOLUCIONES.

4.7.1 Controles para mitigar riesgos

Concluimos con la siguiente matriz, muestra las amenazas a la seguridad y sus potenciales ataques, Podemos describirla como:

Columnas lado izquierdo = lista de ataques, con su ID y su nombre.

Columnas parta alta = lista de soluciones, clasificadas por tipo (ID y Nombre).

Una cruz en la matriz indica que el ataque fue contrarrestado por la solución.

Para un análisis más detallado:

La matriz se puede leer de dos maneras:

1. verticalmente, ayuda a ver el (los) ataque(s) es (son) contrarrestado(s).
2. Horizontalmente, ayuda a ver la (s) solución(es) apropiada(s).

Leyenda

X La solución neutraliza el ataque.
X La solución cubre algunos de los ataque, sin embargo todavía algunos activos pueden alcanzar algún ataque.
X La solución cubre el ataque, pero es posible que una persona este autenticando datos de un usuario legítimo.
-- Solución compuesta relacionada por una cruz a la izquierda.

Matriz de Mitigación de Riesgos

				Separacion de Red DATOS/VoIP							Autent.		Encriptación			Seguridad Perimetral				
		S. 01 Actualización de software (IPBX, hardphone y softphone)	S. 02 Bloqueo de la configuración (IPBX, hardphone y softphone)	S. 03 Separación Nivel capa 3	S.04 Separación VLAN	S.05 Filtro Inter-VLAN	S.06 Tarjeta de red 802.1q	S.07 Desactivación puertos adicionales	S.08 Garantizar acceso a los puertos de switches (ACL,...)	S.09 DMZ para los servicios convergentes	S.10 HTTP Digest Authentication	S.11 Autentificación mutua	S.12 Encriptación del flujo de señalización (SIPS, ...)	S.13 Encriptación del flujo de multimedia (SRTP, ...)	S.14 Encriptación del flujo de datos(IPSEC,...)	S.15 SBC : Call admission control	S.16 Utilización de servidores dedicados para STUN	S.17 Verificación de la identidad del servidor STUN	S.18 Continuación de escucha de respuestas tras recibir la primera resp	S.19 Limitación de ancho de banda asignado por persona
Denial of Service	A01 DoS SIP CANCEL			X	---	---	---	---	X		X	X	X		X					
	A02 DoS SIP BYE			X	---	---	---	---	X		X	X	X		X					
	A03 DoS SIP FAILURE			X	---	---	---	---	X		X	X	X		X					
	A04 Perdida de Qos utilizando RTP			X	---	---	---	---	X		X	X		X	X					
	A05 RTP packet injection			X	---	---	---	---	X						X					
	A06 Audio códec modification			X	---	---	---	---	X						X					
	A07 Stream Inaudible			X	---	---	---	---	X						X					
	A08 Registration table overflow										X	X	X		X	X				
	A09 Proxy server flooding			X	---	---	---	---	X		X	X	X		X	X				
Escucha Clandestina	A10 Physical eavesdropping			X	---	---	---	---	X				X	X	X					
	A11 Cipher Breakage			X	---	---	---	---	X											
	A12 Re-INVITE / Session replay			X	---	---	---	---	X		X	X	X		X					
	A13 Call Tracking (1)			X	---	---	---	---	X				X		X					
	A14 Call Tracking (2)			X	---	---	---	---	X					X	X					
Hijacking Traffic	A15 Call hijacking helped by the registr			X	---	---	---	---	X		X	X	X		X					
	A16 Call hijacking helped by the registr			X	---	---	---	---	X		X	X	X		X					
	A17 Hijack registration by SIP REGIST			X	---	---	---	---	X		X	X	X		X					
	A18 Hijacking registration			X	---	---	---	---	X		X	X	X		X					
	A19 Call redirection using 301/302 mes			X	---	---	---	---	X				X		X					
	A20 Call redirection using 305 mess			X	---	---	---	---	X				X		X					
ID	A21 Request Spoofing			X	---	---	---	---	X				X		X					
	A22 Call Masquerading										X	X								
Vuln. Serv	A23 Billing Fooling																			
	A24 Thef of service			X	---	---	---	---	X		X	X	X		X					
Spam	A25 Spam Call										X	X	X		X					
	A26 Instant messaging spam (SPIM)										X	X	X		X					
	A27 Presence Spam										X	X	X		X					

4.8 Conclusiones

Este trabajo de Tesis tuvo la intención de mostrar la mayoría de los problemas de seguridad que pueden llegar a sufrir las redes de telefonía IP, Así como explicar las técnicas y ataques que utilizarían intrusos para atacar entornos VoIP. Durante este trabajo realizado nos limitamos exclusivamente a señalar qué controles de seguridad deben ser imprescindibles en el entorno VoIP y explicar las medidas necesarias para contrarrestar estos riesgos y ataques comentados en los capítulos dos y tres de este trabajo.

En la actualidad es inevitable no tener ataques a nuestra infraestructura VoIP, pero siguiendo un buen base line de seguridad podemos lograr disminuir estos riesgos, por lo cual siempre es importante mantener los sistemas actualizados y parcheados. Esto es totalmente imprescindible, y no solo en infraestructura VoIP, sino también el administrador de la red debe de estar corriente de los nuevos parches y actualizaciones para que estos sean aplicados en los sistemas.

Es esencial que VoIP se asiente sobre una infraestructura de red segura, protegidas por cortafuegos bien administrados, ya que la detección de muchos de estos ataques descritos anteriormente se puede realizar instalando sistemas de detección de intrusos (IDS) o de prevención (IPS) en los lugares estratégicos de la red. Estos serán capaces de detectar y prevenir ataques contra los protocolos (fuzzing), ataques contra servicios (exploits y vulnerabilidades), escaneos y ataques DoS. Es evidente que el IDS/IPS requerirá una configuración adecuada para conseguir su fiabilidad. Es muy recomendable la existencia en la red de sistemas antivirus actualizados que la protejan de ataques de virus, gusanos y troyanos.

Confidencialidad, Integridad y Disponibilidad (CIA por sus siglas en ingles): Un simple pero muy aplicable modelo de seguridad los tres principios fundamentales que deben garantizarse en cualquier tipo de sistema. Este principio es aplicable en todo el espectro de seguridad. La confidencialidad se refiere a los mecanismos que aseguren que sólo las

personas autorizadas puedan tener acceso a la información segura. Criptografía y cifrado son ejemplos de los métodos utilizados para asegurar la confidencialidad de los datos. Integridad significa que la información no se modifica a medida que se mueve entre los puntos finales.

Una medida adecuada para lograr seria modificar los protocolos y configurar dispositivos para que utilicen autenticación en todos los mensajes que se intercambia. Además de la autenticación ya explicada anteriormente, existen otros dos aspectos esenciales de la seguridad en VoIP son la autorización y el cifrado. Los dispositivos deben de tener limitado los grupos de elementos o direcciones IP de los que pueden recibir tráfico. Realizando, de este modo, una correcta configuración es posible limitar muchos de los ataques de denegación de servicio.

El cifrado es quizás una de las principales y más necesarias medidas que se deben adoptar en una infraestructura VoIP. El uso de TLS/SSL para establecer canales de comunicación seguros resolverá la mayoría de problemas de eavesdroping, manipulación y reproducción de los mensajes que se intercambian.

Las comunicaciones de los datos pueden ser seguras incorporando algún tipo de cifrado. Los teléfonos VoIP pueden cifrar el audio con el protocolo SRTP. Secure RTP, que es una réplica del RTP pero ofrece confidencialidad, autenticación de mensajes y protección evitando los ataques de interceptación e inserción de audio entre toros. SRTP es ideal para provee telefonía IP porque usando con una compresión de las cabeceras no afecta prácticamente a las Qos.

Es evidente que el canal de señalización también debe de ir completamente cifrado. Utilizar VLAN's para priorizar y proteger el tráfico VoIP separándolo en canales lógico de las redes de datos.

Y recordar que un sistema que en un principio sea muy seguro, con el paso del tiempo disminuirá su nivel de seguridad si no es actualizado con frecuencia.

Bibliografía

- Academia de Networking de Cisco Systems, “Fundamentos de seguridad de las redes”, Editorial Cisco Press, 2005, Pág. 1-25.

- Anonimo Wikipedia, “Advanced Encryption Standard” the free enciclopedia, Version mayo 2006. Consultado 30 enero 2009 en línea: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

- Areitio Bertolín Javier Dr, White paper Universidad de Deusto, “Análisis en torno a la auditoría de seguridad en tecnologías de la información y las comunicaciones” 2006.

- Arkin, Ofir, “VoIP - The Next Generation of Phreaking” Revision 1.1, 2006, consultado 30 de Enero de 2009 en linea: http://blackhat.com/presentations/win-usa-02/arkin-winsec02.ppt

- Baugher, McGrew, "The Secure Real-time Transport Protocol" RFC371 1, March 2004.

- Bertels Robert; “Comunicaciones de voz sobre redes de datos: Convergencia de servicios mediante Telefonía Internet”. Novatica. Mayo-Junio 2001. No. 51. [En línea]. Disponible: http://novatica.ati.es/socios/2001/151/151-47.pdf

- Cable & Wíreless Cisco Systems; “Convergencia IP” boletic, Noviembre-Diciembre 2001, No. 24, [En línea]. Disponible: http://www.astic.es/nr/astic/boletictodos/ boletic24/revista6.pdf.

- Colado Cesar, Franco Alfonso, White paper Germenius, “Metricas de seguridad, una vision actualizada” [en línea] consultado 14 Febrero 2008,

- Commerce, 2004. Consultada Octubre 24, 2007 En línea: http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

- D J Thorne (2001). VoIP -- The Access Dimension. BT Technology Journal, *19*(2), 33. Consultada Octubre 7, 2007, from ABI/INFORM Global database. (Document ID: 349717131).

- D.R. Kuhn, T.J. Walsh, and S. Fries, “Security Considerations for Voice Over IP Systems,” Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800-58, Technology Administration, U.S. Department of
- Davison Jonathan, “Voice over IP: A systematic approach to understanding the basics of Voice over IP”, Ciscopress, 2000, EUA.

- DISA, “IP Telephony & VoIP : Security technical implementation guide” version 2, release 2, Abril 2006, consultado 30 enero 2009 en línea: http://iase.disa.mil/stigs/stig/VoIP-STIG-V2R2.pdf

- Ernst & Young,”Revela escasa importancia otorgada a la seguridad informática”, Prensa La Nación, 2004 [En línea], Consultada 3 de junio 2007. ProQuest document, http://0-proquest.umi.com.millenium.itesm.mx:80/pqdlink?did=750587831&sid=1&Fmt=3&clientId=23693&RQT=309&VName=PQD

- Fernández Cambronero, Zangger Eberhard; “Presentación: voz sobre IP, la revolución de las redes telefónicas”. Novatica, No. 151, 2001. Pág. 3-5. [En línea]. Disponible: http://www.ati.es/novatica/2001/151/nv151sum.html

- H. Abdelnur, V. Cridlig, R. State and O. Festor, “VoIP Security Assessment: Methods and Tools” Paper 1-4244-0144-5/06/ IEEE, 2006

- Hardwick, jon, “Session border controllers Enabling the VoIP revolution”, Febrero 2005, Consultado 30 enero 2009 en línea: http://www.dataconnection.com/network/download/whitepapers/sessionbordercontroller.pdf

- Hefferan, Rossynne. “BS7799 – Information – Security Management”. Institute of scientific & Tecnical Communicators, 2003 [En Línea] www.istc.org.uk/site/bs7799.asp

- http://cve.mitre.org/compatible/vulnerability_management.html

- http://www.germinus.com/sala_prensa/articulos/Metricas%20de%20Seguridad_Una%20vision%20actualizada.pdf

- http://www.uv.es/~montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf

- http://www.voipsa.com/Activities/taxonomy-wiki.php

- Huidobro José Manuel; “Fundamentos de Telecomunicaciones” Paraninfo, España, 2001. Cap. 1, pp. 2-10.

- IETF web site http://www.ietf.org

- J. Rosenberg, C. Jennings, Cisco, J. Peterson, Neustar, “The Session Initiation Protocol (SIP) and Spam draft-rosenberg-sipping-spam-02” Marzo 2006, consultado el 30 enero 2009 en linea: http://tools.ietf.org/id/draft-ietf-sipping-spam-02.txt

- J. Rosenberg, et al., "SIP: Session Initiation Protocol," RFC3261, June 2002.

- Jeremy, George, “Security Considerations SIP.edu Cookbook”, Junio 2003, Consultado 30 De Enero 2009 en linea, http://mit.edu/sip/sip.edu/security.shtml

- Jorge Alberto blanco Cruz, “Modelo de seguridad de información para redes inalámbricas móviles basado en ISO 17799”, TESIS ITESM 2004.

- Keith E. Strassberg, Richard J Gondek, “Firewall”, Editorial Mc Graw Hill, 2003, pag.1-5

- Kent, Atkinson, "Security Architecture for the Internet Protocol, "RFC2401, November 1998.

- L. Hensell, “The new security risk of VoIP,” E-Commerce Times, 2003, Octubre 12, 2007, en línea: http://www.ecommercetimes.com/story/31731.html.

- Labouret, Ghislaine, “IPsec: from fundamentals to the IKE Protocol” Marzo 2000, consultado 30 enero 2009 en línea: http://www.hsc.fr/ressources/presentations/websec2000/index

- M. Gaynor, S. Bradner, “Firewall Enhancement Protocol (FEP)” RFC 3093, 1 Abril 2001.

- Martínez, Claudia, “Vishing Amenaza financiera”, BSecure Noviembre 2006. No. 33 En Linea http://www.bsecure.com.mx/articulo-49-6419-366.html

- NSA, “Security Guidance for Deploying IP Telephony Systems” febrero 2006, Report Number I332-016R-2005, consultado 30 enero 2009 en línea: http://www.nsa.gov/ia/_files/voip/I332-016R-2005.PDF.

- Porter Thomas, Bassin Brian, Chaffin Larry, Cross Michael, “Practical VoIP Security”, Editorial Syngress, 2006.

- Reynolds, Brennen and Ghosal, Dipak, "Secure IP Telephony using Multi-layered Protection", Department of Computer Science University of California 2006, Consultado En Linea: 30 De Enero 2009, http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/3.pdf

- RFC 1889 - RTP: A Transport Protocol for Real-Time Applications

- RFC 3261 - SIP: Session Initiation Protocol

- Rontti Tero, White paper Codenomicon Ltd, "Threats, Vulnerabilities and Attacks in Voice over IP" 2006, [en línea] consultado 9 Febrero 2008, http://www.ouka.fi/wirelesscities/Presentations/codenomicon-rontti2006-06-07.ppt#261,6,VoIP Security Covers All Areas of Security Research.

- Rosenberg J,Huitema C, Microsoft,Mahy R, Plantronics, Wing D, Cisco Systems, "Simple Traversal Underneath Network Address Translators (NAT) (STUN) draft-ietf-behave-rfc3489bis-04" julio 2006, Expira Enero 2007, consultado en linea: http://tools.ietf.org/html/draft-ietf-behave-rfc3489bis-04

- Sabato John , Hash Joan, Graffo Laurie, "Security Metrics Guide for Information Technology Systems" NIST-National Institute of Standards and Technology Computer Security. July, 2003.

- Weatherspoon, Sultan "Overview of IEEE 802.11b Security" Paper Intel Technology Journal Q2, 2000.

- Web site http://csrc.nist.gov/

- Web site www. http://www.deusto.es

- Web site www.codenomicon.com

- White Paper Internet security system, "Multi-layered Security Solutions for VoIP Protection", 2005. [En línea] Consultado 9 Febrero 2008, http://www.xforce.iss.net/documents/whitepapers/ISS_Voip_Protection_White_paper.pdf web site http://www.iss.net/

- White Paper, Mcafee, "McAfee Avert Labs Top 10 Threat Predictions for 2008", 2008. [En línea] Consultado 9 Febrero 2008, http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_avert_predictions_2008.pdf web site http://www.mcafee.com

- Wright, David J, "Voice over Packet Networks", editorial Wiley, 2001, pag. 3-65.

- Young Man Rhee, "Internet Security Cryptographic principles, algorithms, and protocols", editorial Wiley, 2003, pag. 3- 32.