Seguridad en VoIP:
Ataques, Amenazas y Riesgos.

Roberto Gutiérrez Gil

VNIVERSITAT DE VALÈNCIA

1. - Índice

1. - Índice 2
2. - Introducción 3
2.1. ¿Qué es VoIP? 3
2.2. Infraestructura básica VoIP 4
2.3. Protocolos y estándares VoIP 6
2.3.1 Introducción a SIP 6
3. - Seguridad de las redes VoIP 10
3.1. Clasificación de los ataques 11
4. - Accesos desautorizados y Fraudes 12
5. - Explotando la red subyacente 13
6. - Ataques de denegación de servicio 14
7. - Ataques a los dispositivos 15
8. - Descubriendo objetivos 16
8.1. Footprinting 16
8.2. Escaneando 18
8.3. Enumeración 19
9. - Explotando el Nivel de Aplicación 21
9.1. Autenticación en VoIP 21
9.1.1 Autenticación del protocolo SIP 21
9.1.2 Crackeo de contraseñas SIP 22
9.2. Manipulación de la señalización 25
9.2.1 Suplantación de identidad en el registro. 25
9.2.2 Desregistrar Usuarios 28
9.2.3 Desconexión de Usuarios 29
9.2.4 Redirección de llamadas. 29
9.3. Manipulación de la transmisión 30
9.3.1 Eavesdropping 30
9.3.2 Inserción de Audio 31
9.4. Fuzzing 32
9.5. Ataques DoS 33
10. - Ingeniería social 35
10.1. SPIT: Spam over Internet Telephony 35
10.2. Vishing: Voip Phishing 35
11. - Asegurando la red VoIP 36
12. - Referencias 38

2. - Introducción

Desde hace algunos años, gracias a la evolución tecnológica se han desarrollado nuevas tecnologías y nuevos dispositivos que han revolucionado totalmente el campo de las telecomunicaciones. Un ejemplo claro fue el desarrollo de los teléfonos celulares que supusieron un punto de inflexión en el panorama de las comunicaciones. Pero la verdadera revolución ha llegado gracias a la explosión de un fenómeno sin igual: **Internet**.

Poco a poco **Internet** se fue convirtiendo en un gigante donde todos compartían información y permitía algo hasta entonces imposible, la comunicación a través del PC. Pronto apareció la necesidad humana de comunicarnos con la voz, que unido a gran cantidad de avances tecnológicos algunos como el procesado digital de señales y el desarrollo de mecanismos de control, priorización y calidad de servicio en redes datos, hicieron centrar las miradas en el desarrollo de la telefonía utilizando un ordenador y en definitiva utilizando esa gran red de comunicaciones que era **Internet**. Las compañías y vendedores de servicios telefónicos ya se habían percatado de esta incipiente tendencia y de que para ellos, suponía un ahorro de costes sustancial la utilización de las redes IP para la transmisión de voz.

Hoy por hoy millones de personas utilizan un ordenador conectado a Internet, tanto en el trabajo como en su tiempo libre, para comunicarse con cualquier otra persona del mundo intercambiando datos, ficheros, correos electrónicos, a través de mensajería instantánea, y de muchos otros modos. Por lo que sería absurdo pensar que el concepto de Internet desde hace algunos años no esta omnipresente en el panorama de las telecomunicaciones.

2.1. ¿Qué es VoIP?

VoIP es el acrónimo de "Voice Over Internet Protocol", que tal y como el término dice, hace referencia a la emisión de voz en paquetes IP sobre redes de datos como puede ser **Internet**. Llegados a este punto se unen dos mundos que hasta entonces habían convivido separados: la transmisión de voz y la de datos.

La tecnología VoIP trata de transportar la voz, previamente procesada, encapsulándola en paquetes para poder ser transportadas sobre redes de datos sin necesidad de disponer de una infraestructura telefónica convencional. Con lo que se consigue desarrollar una única red homogénea en la que se envía todo tipo de información ya sea voz, video o datos.

Es evidente que la utilización de una única red para la transmisión de voz y datos presenta gran cantidad de ventajas. Para un proveedor de servicio de telefonía y datos , por un lado, obtiene mayores beneficios ya que con una sola línea puede ofrecer más servicios. Y por otro lado le supone un ahorro de gastos tanto de infraestructura como de mantenimiento. Una llamada telefónica requiere una gran red de centralitas conectadas entre si con cableado, fibra óptica, satélites de telecomunicación o cualquier otro medio, que equivale a una enorme inversión para crear y mantener estas infraestructuras. En cambio, una llamada telefónica sobre IP supone comprimir la voz y enviarla en paquetes de datos por una línea en la que pueden viajar diferentes llamadas e incluso diferentes datos, sin necesidad de líneas dedicadas ni desaprovechamiento del ancho de banda.

Por otro lado existen también ciertos inconvenientes para el desarrollo de la telefonía sobre IP que se podrían resumir en los siguientes tres conceptos: **Seguridad**, **Fiabilidad** y **Calidad de Servicio** (QoS). VoIP al basarse sobre el protocolo IP (y en muchos casos usando UDP en la capa de transporte) asume la posibilidad de que los paquetes puedan perderse, otro problema es que no hay una garantía absoluta en el tiempo que tardan en llegar los paquetes al otro extremo de la comunicación aunque se utilicen técnicas de priorización. Estos problemas de calidad de servicio telefónico y dependencia de la red de datos suponen uno de los principales problemas para la difusión total de la telefonía por IP. Pero cierto es que, poco a poco dichos problemas se van solucionando con la evolución de las tecnologías involucradas.

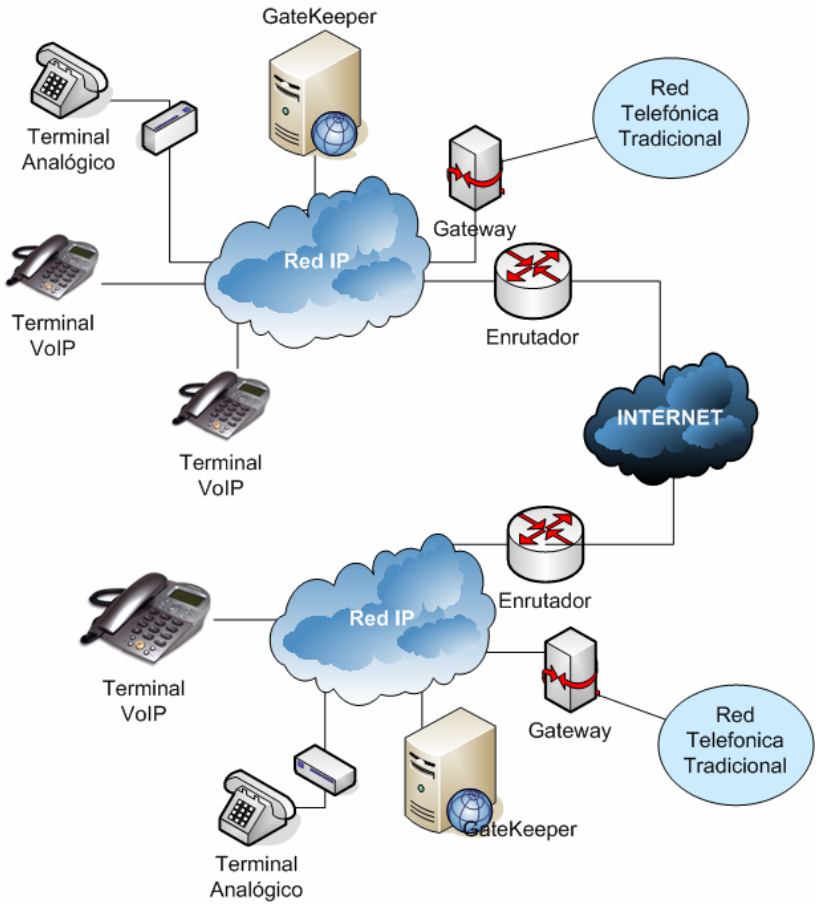
Desde el punto de vista de la seguridad, las llamadas en VoIP se transmiten por Internet o por redes potencialmente inseguras. Lo cual plantea riesgos de privacidad y seguridad que no surgen con un servicio telefónico tradicional. Un ejemplo de ello, es que la infraestructura VoIP se puede ver seriamente degrada por el efecto de algún virus, gusano o por el más que conocido SPAM. VoIP es vulnerable además en muchos otros puntos, ya sea en los protocolos utilizados, en los dispositivos que intervienen, o debilidades en la red por la que se transmite. Durante resto del documento 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.

2.2. Infraestructura básica VoIP

Dentro de la estructura básica de una red VoIP hay que diferenciar tres elementos fundamentales:

- **Terminales:** Son los dispositivos que utilizarán los usuarios para comunicarse. Implementados tanto en hardware como en software realizan las funciones de los teléfonos tradicionales.
- **Gateways:** De forma transparente se encargan de conectar las redes VoIP con las redes de telefonía tradicional.
- **Gatekeepers:** Son el centro neurálgico de las redes VoIP. Se encargan de realizar tareas de autenticación de usuarios, control de admisión, control de ancho de banda, encaminamiento, servicios de facturación y temporización, etc.

En la siguiente imagen podemos ver una estructura de red básica entre lo que serían dos delegaciones de una misma empresa conectadas telefónicamente a través de Internet.



El esquema anterior es un ejemplo sencillo y general de lo que sería una red VoIP, es evidente que coexistirán muchos más servicios y servidores y que la arquitectura será muy dependiente de los protocolos utilizados:

Tipos de arquitectura	Protocolos
Intelligent Endpoint	H.323, SIP
Device Control (Master/Slave)	SCCP (Skinny), MGCP, Megaco, H.248
Peer to Peer:	P2PSIP
Hybrid / Mixed:	H.325, IAX2, Skype

2.3. Protocolos y estándares VoIP

Como ya he comentado brevemente VoIP engloba gran cantidad de protocolos y junto con hecho de que la telefonía IP debe de ofrecer prácticamente los mismos servicios que la telefonía tradicional el número de protocolos , estándares y servidores que pueden ser objetivo de un ataque se dispara. Durante el resto del documento solo se hablará de quizás dos de los protocolos más importantes en VoIP: **H.323** y **SIP**. En menor medida se comentarán otros protocolos como RTP y RTCP.

El **H.323** es una recomendación de la ITU que define los protocolos para la comunicación multimedia a través de redes de paquetes. Nacido originariamente para dar soporte audiovisual en las redes de área local a evolucionado rápidamente para dar soporte y convertirse en un estándar de VoIP. H.323 no es un solo protocolo sino un conjunto que cubren los distintos aspectos de la comunicación como son el direccionamiento, la señalización, la compresión, transmisión de voz y el control de la transmisión. H.323 fue además el encargado adoptar el estándar de **RTP** (Protocolo de Transporte en tiempo Real) para transportar audio y vídeo sobre redes IP.

Otro protocolo ampliamente utilizado en telefonía IP es el protocolo **SIP** (Session initation protocol) en el que se profundizará a continuación.

2.3.1 Introducción a SIP

SIP es un protocolo simple de señalización y control utilizado para telefonía y videoconferencia sobre las redes IP . Fue creado por el **IETF MMUSIC Working Group** y su estructura está basada en otros protocolos como STMP y HTTP con los que guarda cierta similitud. SIP es un protocolo abierto y ampliamente soportado que no depende de ningún fabricante. Su simplicidad, escalabilidad y facilidad para integrarse con otros protocolos y aplicaciones lo han convertido en un estándar de la telefonía IP.

SIP es un protocolo de señalización por lo que solo maneja el establecimiento, control y terminación de las sesiones de comunicación. Normalmente una vez se ha establecido la llamada se produce el intercambio de paquetes RTP que transportan realmente el contenido de la voz. Encapsula también otros protocolos como SDP utilizado par la negociación de las capacidades de los participantes, tipo de codificación, etc.

No hace falta señalar que SIP es un protocolo de aplicación y funcionará tanto sobre UDP como TCP.

Dentro de una red SIP vamos a encontrar los siguientes dos componentes: **Agentes de Usuario (UA) y servidores**. Entre los *User Agent ,* a su vez, podemos encontrar los **agentes de usuario clientes (UAC)** que son los que inician las peticiones de llamada y los **agentes de usuario servidor(UAS)** que reciben las peticiones del UAC.

En una infraestructura SIP vamos a encontramos básicamente cuatro tipos de servidores:

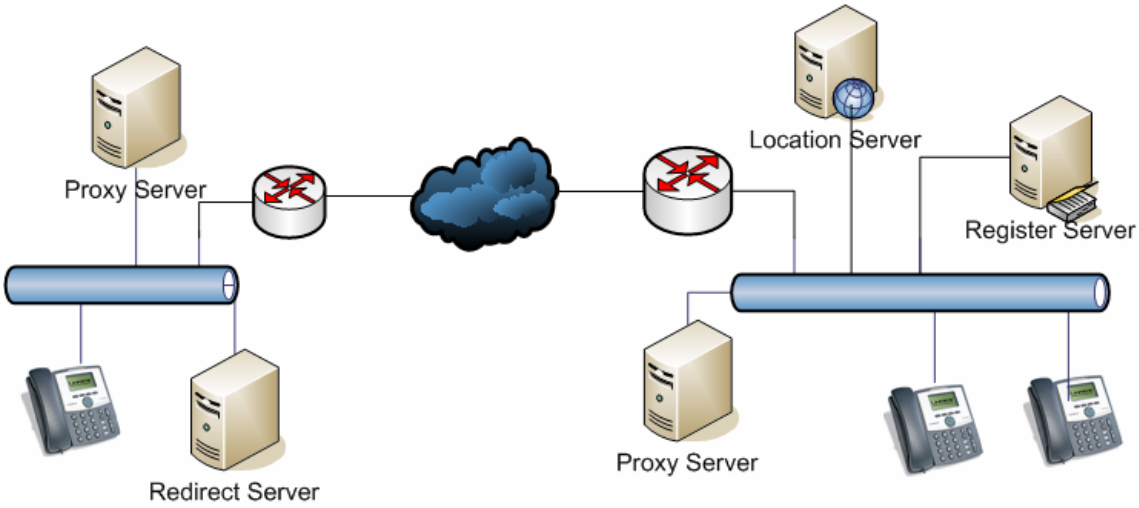
- **Servidor Proxy SIP**: Realiza las funciones intermediador entre le UAC y el UAS. Una vez le llega una petición de inicio de llamada de UAC decide a que servidor debería ser enviada y entonces retransmite la petición, que en algunos casos pude llegar a atravesar varios proxys SIP antes de llegar a su destino.

- **Servidor de Redirección:** Es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

- **Servidor de Registro:** es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.

- **Servidor de Localización:** Facilita información al Proxy o Redirect sobre la ubicación del destinatario de una llamada.

.



En la infraestructura SIP los clientes son identificados por direcciones definidas como URL's muy similares a las direcciones de correo: **user@host** ó **user@dominio** . Ejemplo: **roberto@uv.es**.

En la siguiente tabla podemos apreciar un resumen de los mensajes SIP:

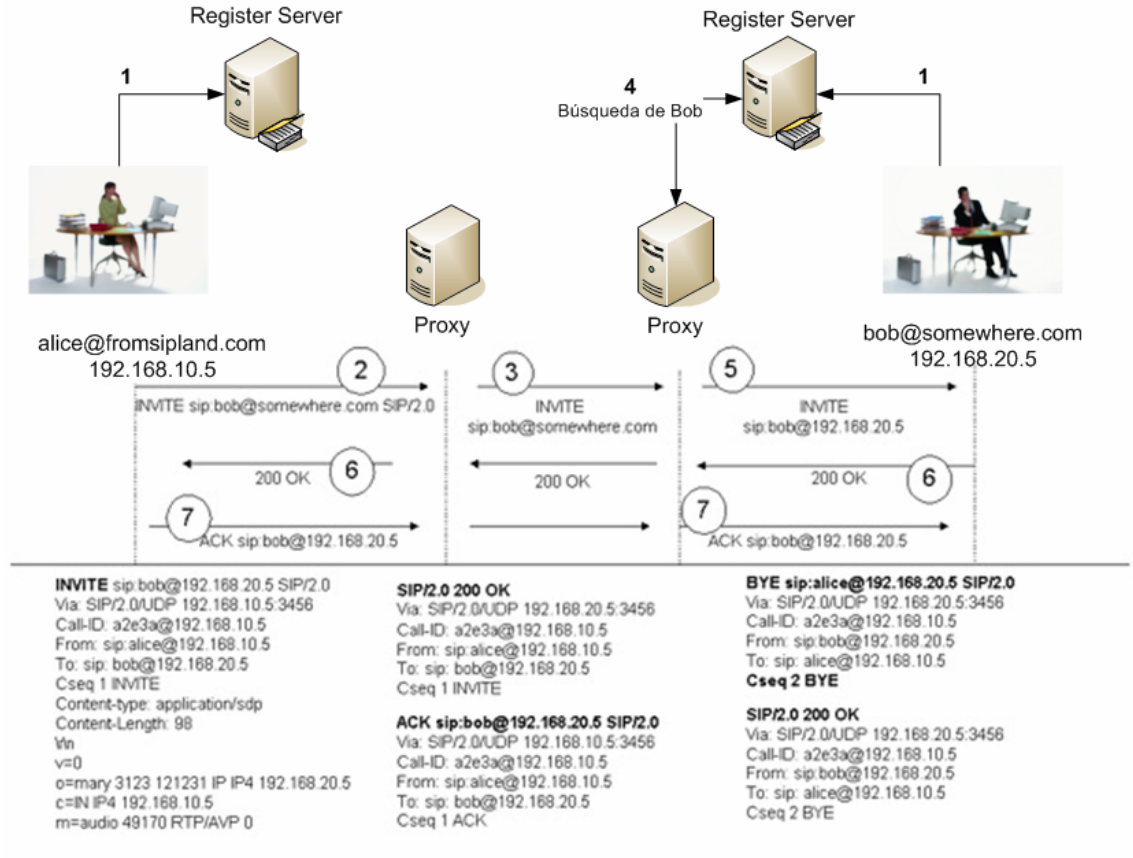
Mensaje	Explicación
INVITE	Permite invitar un usuario o servicio para participar en una sesión o para modificar parámetros en una sesión ya existente.
ACK	Confirma el establecimiento de una sesión.
OPTION	Solicita información sobre las capacidades de un servidor
BYE	Indica la terminación de una sesión
CANCEL	Cancela una petición pendiente de llamada.
REGISTER	Registrar al User Agent.

Del mismo modo tenemos un listado de los códigos de respuesta a las peticiones SIP:

Código	Significado
1xx	Mensajes provisionales.
2xx	Respuestas de éxito.
3xx	Respuestas de redirección
4xx	Respuestas de fallo de método
5xx	Respuestas de fallos de servidor
6xx	Respuestas de fallos globales

Para más información sobre las peticiones y códigos de respuesta consultar el RFC 254.

En el siguiente diagrama muestra un ejemplo de establecimiento de llamada con el protocolo SIP



Antes de iniciarse el proceso de comunicación los dos usuarios, en este caso alice y bob se deben registrar en el servidor de registro (Paso 1). Cuando *alice* quiere contactar con *bob* realiza una petición **INVITE** hacia el Proxy Server que será el encargado de enrrutar el mensaje. El Proxy Server reenvía la petición al destinatario *bob*, previamente consultando en el Servidor de localización la dirección de *bob*. Cuando *bob* descuelga se retransmite un mensaje **200 OK** al emisor de la llamada. Y una vez se han enviado los mensajes **ACK** la llamada queda establecida.

Desde el punto de vista de la seguridad el protocolo SIP conlleva otra clase de riesgos. Como veremos más adelante será susceptible de ataques de secuestro de registro, inundación de mensajes INVITE, desconexión, etc.

Cabe destacar que la sesión SIP llega a utilizar al menos 3 puertos, de los cuales solo uno de ellos es estático, haciéndolo complicado manejar desde el punto de vista de la seguridad ya que, por ejemplo, complica las políticas de cortafuegos.

En el caso de H.323 usa de 7 a 11 puertos, de los cuales solo dos son estáticos. Y el resto se selecciona de forma aleatoria en el rango de puertos por encima del 1024, haciendo casi imposible la aplicación de una política de cortafuegos.

En la siguiente tabla se detalla una referencia de los protocolos y los puertos por defecto que utilizan:

Protocolo	Puertos
Session Initiation Protocol (SIP)	TCP/UDP 5060,5061
Session Description Protocol (SDP	Encapsulación SIP
Media Gateway Control Protocol (MGCP)	UDP 2427,2727
Skinny Client Control Protocol (SCCP/Skinny)	TCP 2000,2001
Real-time Transfer Control Protocol (RTCP)	RTP+1
Real-time Transfer Protocol (RTP)	Dynamic
Secure Real-time Transfer Protocol (SRTP)	Dynamic
Inter-Asterisk eXchange v.2 (IAX2)	UDP 4356

3. - Seguridad de las redes VoIP

A medida que crece su popularidad aumentan las preocupaciones por la seguridad de las comunicaciones y la telefonía IP. VoIP es una tecnología que ha de apoyarse necesariamente muchas otras capas y protocolos ya existentes de las redes de datos. Por eso en cierto modo la telefonía IP va a heredar ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes de VoIP problemas clásicos de seguridad que afectan al mundo de las redes de datos. Por supuesto, existen también multitud de ataques específicos de VoIP como veremos más adelante.

Como vemos la seguridad de VoIP se construye sobre muchas otras capas tradicionales de seguridad de la información.

En la siguiente tabla se detallan algunos de los puntos débiles y ataques que afectan a cada una de las capas. Aunque posteriormente se analizaran muchos de ellos en profundidad algunos ataques que pueden afectar directamente o indirectamente a la telefonía VoIP no serán explicados al ser problemas comunes a cualquier otra red de datos o al alejarse demasiado de la temática del documento.

Capa	Ataques y vulnerabilidades
Políticas y Procedimientos	Contraseñas débiles. Ej: Contraseña del VoiceMail Mala política de privilegios Accesos permisivos a datos comprometidos.
Seguridad Física	Acceso físico a dispositivos sensibles. Ej: Acceso físico al un gatekeeper. Reinicio de máquinas. Denegaciones de servicio.
Seguridad de Red	DDoS ICMP unreacheable SYN floods Gran variedad de floods

Seguridad en los Servicios	SQL injections Denegación en DHCP DoS
Seguridad en el S.O.	Buffer overflows Gusanos y virus Malas configuraciones.
Seguridad en las Aplicaciones y protocolos de VoIP	Fraudes SPIT (SPAM) Vishing (Phising) Fuzzing Floods (INVITE,REGISTER,etc..) Secuestro de sesiones (Hijacking) Interceptación (Eavesdroping) Redirección de llamadas (CALL redirection) Reproducción de llamadas (CALL replay)

Se pude apreciar algunos de estos ataques tendrán como objetivo el robo de información confidencial y algunos otros degradar la calidad de servicio o anularla por completo (DoS). Para el atacante puede ser interesante no solo el contenido de una conversación (que puede llegar a ser altamente confidencial) sino también la información y los datos de la propia llamada, que utilizados de forma maliciosa permitirán al atacante realizar registros de las llamadas entrantes o salientes, configurar y redirigir llamadas, grabar datos, utilizar información para bombardear con SPAM, interceptar y secuestrar llamadas, reproducir conversaciones, llevar a cabo robo de identidad e incluso realizar llamadas gratuitas a casi cualquier lugar del mundo. Los dispositivos de la red, los servidores, sus sistemas operativos, los protocolos con los que trabajan y prácticamente todo elemento que integre la infraestructura VoIP podrá ser susceptible de sufrir un ataque.

3.1. Clasificación de los ataques

Durante los siguientes apartados 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.

Las amenazas de las redes de telefonía IP las podemos clasificar en las siguientes categorías:

- **Accesos desautorizados y fraudes.**
- **Ataques de denegación de servicio**
- **Ataques a los dispositivos**
- **Vulnerabilidades de la red subyacente.**
- **Enumeración y descubrimiento.**
- **Ataques a nivel de aplicación.**

4. - Accesos desautorizados y Fraudes

Los sistemas VoIP incluyen múltiples sistemas para el control de la llamada, administración, facturación y otras funciones telefónicas. Cada unos de estos sistemas debe contener datos que, si son comprometidos, pueden ser utilizados para realizar fraudes. El costo de usar fraudulentamente esos datos VoIP a nivel empresarial pueden ser devastadores. El acceso a los datos telefónicos (de facturación, registros, datos de cuentas, etc) pueden ser usados con fines fraudulentos.

Una de las mas importantes amenazas de las redes VoIP, son los fraudes consecuencia de un acceso desautorizado a una red legal VoIP (por ejemplo haber obtenido anteriormente obtener datos de cuentas). Una vez se ha obtenido el acceso, usuario desautorizados realizan llamadas de larga distancia, en muchos casos incluso internacionales. Principalmente ocurren en entornos empresariales. El control y el registro estricto de las llamadas puede paliar el problema

A modo de curiosidad cabe señalar que las técnicas utilizadas por estos individuos son descendientes de las que utilizaban los famosos "*phreakers*" en las antiguas líneas telefónicas.

5. - Explotando la red subyacente

Paradójicamente una de las principales debilidades de la tecnología VoIP es apoyarse sobre una red potencialmente insegura como son las redes IP. Gran cantidad de ataques hacia las infraestructuras IP van a afectar irremediablemente a la telefonía Ataques de denegación de servicio, inundación de paquetes o cualquier otro tipo de ataque que intente limitar la disponibilidad de la red suponen un gran problema para la telefonía IP tal y como hemos visto anteriormente. Además VoIP será vulnerable a ataques a bajo nivel como el secuestro de sesiones, interceptación, fragmentación IP, paquetes IP malformados y spoofing.

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.

El ***eavesdropping*** en VoIP presenta pequeñas diferencias frente la interceptación de datos en las redes tradicionales. En VoIP vamos a diferenciar básicamente dos partes dentro de la comunicación: **la señalización y el flujo de datos**. Los cuales utilizarán protocolos diferentes. En la señalización nos centraremos durante todo el documento en el protocolo SIP mientras que en el flujo de datos normalmente se utilizará el protocolo RTP sobre UDP.

El impacto de esta técnica es más que evidente, interceptando comunicaciones es posible obtener toda clase información sensible y altamente confidencial. Y aunque en principio se trata de un técnica puramente pasiva, razón por la cual hace difícil su detección, es posible intervenir también de forma activa en la comunicación insertando nuevos datos (que en el caso de VoIP se trataría de audio) redireccionar o impedir que los datos lleguen a su destino.

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 de tu 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 "**Main in the Midle**" 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.

Hay que señalar también la creciente utilización de **redes inalámbricas** supone en muchos casos un vía más a explotar por parte del intruso. Redes Wifi mal configuradas junto con una infraestructura de red insegura puede facilitar e trabajo del intruso a la hora de acceder a la red VoIP para lanzar sus ataques.

6. - Ataques de denegación de servicio

Los ataques de denegación de servicio son intentos malintencionados de degradar seriamente el rendimiento de la red o un sistema incluso llegando al punto de impedir la utilización del mismo por parte de usuarios legítimos. Algunas técnicas se basan en el envío de paquetes especialmente construidos para explotar alguna vulnerabilidad en el software o en el hardware del sistema, saturación de los flujos de datos y de la red o sobrecarga de procesos en los dispositivos.

Llegan a ser especialmente dañinos los llamados DDoS o ataques de denegación distribuidos. Son ataques DoS simples pero realizados desde múltiples computadores de forma coordinada. Las redes y sistemas VoIP son especialmente vulnerables a los DDoS por diversas razones:

La primera y quizás más importante es la dependencia y la necesidad de garantías en la calidad de servicio, que hacen que las redes IP donde se mantengan llamadas telefónicas tengan una tolerancia mucho menor a problemas de rendimiento.

Otra razón es que en una red VoIP existen multitud de dispositivos con funciones muy específicas por lo que ataques contra casi cualquier dispositivo de la red pueden afectar seriamente los servicios de telefonía IP. Muchos de estos dispositivos son muy susceptibles de no manejar, priorizar o enrrutar el tráfico de forma fiable si presentan un consumo de CPU alto. Por lo que muchos de los ataques de DoS se centran en atacar los dispositivos de red y/o inundar la red de tráfico inútil para degradar su funcionamiento y que los paquetes pertenecientes a comunicaciones telefónicas se pierdan o retrasen.

La relación de VoIP y los ataques distribuidos de DoS viene reflejada en el siguiente párrafo:

Recientemente investigadores de la Universidad de Cambrige y del Massachussets Institute of Technology (MIT) han determinado que las aplicaciones de voz sobre IP como puede ser Skype pueden ser una herramienta ideal para dar cobertura y lanzar ataques de denegación de servicio distribuidos. El descubrimiento de algún fallo en la aplicación o en su protocolo podría dejar al descubierto miles de ordenadores que serían potencialmente secuestrados por los atacantes para realizar un ataque mayor contra algún servicio de Internet.

Las aplicaciones y los dispositivos de telefonía IP suelen trabajan sobre ciertos puertos específicos, bombardear dichos puertos con tráfico innecesario pero aparentemente "real" puede causar una denegación de servicio y que usuarios legítimos no puedan hacer uso del sistema. Modificaciones y ataques al servidor DNS pueden afectar de manera directa al servicio de voz. El robo o suplantación de identidad (del destinatario de la llamada o de algún otro dispositivo VoIP) generalmente deriva en una denegación de servicio. El acceso SNMP a los dispositivos, además de ofrecer una gran cantidad de información permite potencialmente al atacante afectar al servicio de Voz sobre IP. En redes VoIP basadas en el protocolo SIP, es posible enviar mensajes CANCEL, GOODBYE o ICMP Port Unreacheable, con el objetivo de desconectar ciertos usuarios de sus respectivas llamadas o evitar que se produzcan no permitiendo la correcta configuración inicial de la llamada (señalización).

Hay que destacar también que algunas situaciones VoIP será vulnerable a ataques de fragmentación IP o envío de resets TCP, que conllevarán la prematura finalización de la llamada.

7. - Ataques a los dispositivos

Muchos de los ataques realizador hoy en día por hackers y crackers hacia las redes de datos tienen como objetivo principal el hardware y el software de los dispositivos. Por lo tanto, en redes VoIP, los gateways, call managers, Proxy servers sin olvidar los teléfonos IP serán potencialmente objetivos a explotar por parte de un intruso.

Hay que tener en cuenta que los dispositivos VoIP son tan vulnerables como lo es el sistema operativo o el firmware que ejecutan. Son muy frecuentes los ataques de *fuzzing* con paquetes malformados que provocan cuelgues o reboots en los dispositivos cuando procesan dicho paquete. Otros ataques de denegación de servicio llamados "*flooders*" tienen como objetivo los servicios y puertos abiertos de los dispositivos VoIP.

Otro aspecto que hace muchas veces de los dispositivos un punto débil dentro de la red son configuraciones incorrectas. A menudo los dispositivos VoIP trabajan con sus configuraciones por defecto y presentan gran variedad de puertos abiertos. Los servicios por defecto corren en dichos puertos y pueden ser vulnerables a ataques de DoS, desbordamientos de buffer o cualquier otro ataque que pueden resultar en el compromiso del dispositivo VoIP.

El intruso a la hora de penetrar en la red tendrá en cuenta estos aspectos e intentará explotarlos. Buscará puertos por defecto y servicios innecesarios, comprobará passwords comunes o los que usa por defecto el dispositivo, etc. En el apartado de Descubrimiento de objetivos se explicaran más detalladamente las técnicas utilizadas en este aspecto.

No hay que olvidares de los dispositivos VoIP que utiliza el usuario directamente.: los teléfonos. A pesar de ser dispositivos más pequeños obviamente son igual de vulnerables que cualquier otro servidor de la red, y el resultado de comprometer uno de ellos puede llegar a ser igual de negativo.

A modo de ejemplo se detalla una vulnerabilidad de que afectó al teléfono IP **Linksys SPA-921 v1.0** y que provocaba una denegación de servicio en el mismo.

Modelo: Linksys SPA-921
Version: 1.0.0
Tipo vulnerabilidad: DoS
Fecha: Octubre 2006
Explicación:

1) La petición de una URL larga al servidor http del dispositivo provoca que el teléfono se reinicie.

2) Un nombre de usuario o un password demasiado largo en la autenticación http provoca que el teléfono se reinicie.

Modo de explotarlo: Trivial

8. - Descubriendo objetivos

Una vez que el hacker ha seleccionado una red como su próximo objetivo, sus primeros pasos consistirán en obtener la mayor información posible de su victima. Cuando el intruso tenga información suficiente evaluará sus siguientes pasos eligiendo el método de ataque más adecuado para alcanzar su objetivo. Normalmente el método de obtención de información se realiza con técnicas de menos a más nivel de intrusión. De este modo en las primeras etapas el atacante realizará un **footprinting** u obtención de toda la información pública posible del objetivo. Más adelante una de las acciones más comunes consiste en obtener la mayor información posible de las máquinas y servicios conectados en la red atacada. Después de tener un listado de servicios y direcciones IP consistente, tratará de buscar agujeros de seguridad, vulnerabilidades y obtener la mayor información sensible de esos servicios (enumeración) para poder explotarlos y conseguir una vía de entrada.

Un ejemplo de ataque de enumeración, podría ser utilizar la fuerza bruta contra servidores VoIP para obtener una lista de extensiones telefónicas válidas. Información que seria extremadamente útil para lanzar otros ataques como inundaciones INVITE o secuestro de registro.

Durante este apartado se explicaran algunas técnicas de enumeración y descubrimiento de objetos así como la obtención de información sensible que atacante podría utilizar a su favor.

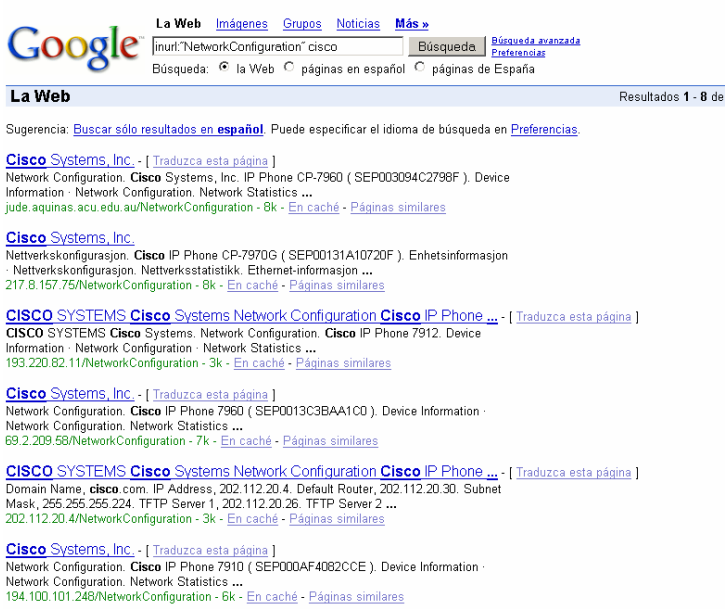
8.1. Footprinting

Se conoce como footprinting el proceso de acumulación de información de un entorno de red especifico, usualmente con el propósito de buscar formas de introducirse en el entorno.

La herramienta básica para esta etapa del reconocimiento será el todopoderoso Google. Las búsquedas se centrarán entorno a la web de la empresa y en su dominio. Se intentarán encontrar perfiles o direcciones de contacto, correos y teléfonos. Estos datos ofrecerán información al hacker para poder realizar ataques de suplantación de identidad y/o ingeniería social. El contacto del servicio técnico también puede resultar útil para extraer algún tipo de información. Otro tipo de información interesante pueden ser las ofertas de trabajo o los perfiles de personal que busca la empresa. Pueden dar información acerca de la estructura de la organización y de la tecnología que emplea.

La mayoría de dispositivos VoIP corren algún servicio web de administración remota. Es posible encontrarlos con google:

inurl:"NetworkConfiguration" cisco



Algunas otras búsquedas interesantes se resumen en la siguiente tabla:

Asterisk Management Portal	*intitle:asterisk.management.portal web-access*
Cisco Phones:	*inurl:"NetworkConfiguration" cisco*
Cisco CallManager:	*inurl:"ccmuser/logon.asp"*
D-Link Phones:	*intitle:"D-Link DPH" "web login setting"*
Grandstream Phones:	*intitle:"Grandstream Device Configuration" password*
Linksys (Sipura) Phones:	*intitle:" SPA Configuration"*
Polycom Soundpoint Phones	*intitle:"SoundPoint IP Configuration"*
Snom Phones:	*"(e.g. 0114930398330)" snom*

Otras técnicas se centran en intentar localizar a través de google extensiones, para después realizar llamadas a los voicemail y estudiar la grabación. El objetivo es obtener el fabricante del servidor, que seguramente sea el mismo para el resto de dispositivos VoIP de la red.

8.2. Escaneando

A partir de la dirección de red de la victima, se pretende obtener un listado de direcciones IP y servicios activos en la red. La mejor forma es escaneando la red con las herramientas adecuadas. Quizás el mejor escáner de puertos existente hoy por hoy sea **NMAP** (http://insecure.org/namp) que ofrece muchas más posibilidades que un simple escáner de puertos.

Entre todas las funcionalidades de nmap existe una que destacaremos especialmente. Y es la identificación del sistema operativo de la máquina escaneada a partir de información que obtiene nmap, como los puertos abiertos que presenta, tipos de servicios, y huellas identificativas de la pila TCP/IP.

En el caso concreto que nos ocupa, nmap tiene la mejor base de datos de huellas para identificar dispositivos VoIP. Veamos un ejemplo de cómo lo hace:

```
nmap -O -P0 192.168.1.1-254
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-02-20 01:03 CST
Interesting ports on 192.168.1.21:
(The 1671 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0F:34:11:80:45 (Cisco Systems)
Device type: VoIP phone
Running: Cisco embedded
OS details: Cisco IP phone (POS3-04-3-00, PC030301)
Interesting ports on 192.168.1.23:
(The 1671 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:15:62:86:BA:3E (Cisco Systems)
Device type: VoIP phone|VoIP adapter
Running: Cisco embedded
OS details: Cisco VoIP Phone 7905/7912 or ATA 186 Analog Telephone Adapter
Interesting ports on 192.168.1.24:
(The 1671 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0E:08:DA:DA:17 (Sipura Technology)
Device type: VoIP adapter
Running: Sipura embedded
OS details: Sipura SPA-841/1000/2000/3000 POTS<->VoIP gateway
```

Vemos resaltado en negrita los detalles del S.O. Una vez ha escaneado los puertos de la máquina y ha obtenido información suficiente, es capaz de identificar de una forma suficiente fiable (al menos mejor que ninguna otra herramienta) el sistema del que se trata.

A la hora de escáner la red objetivo para identificar sistemas VoIP se debería tener en cuenta que los dispositivos SIP usualmente responden a los puertos 5060-5061 tanto en udp como en tcp. En cambio los dispositivos de Cisco que utilicen el protocolo SCCP abrían los puertos 2000-2001 tcp.

8.3. Enumeración

La enumeración es una técnica que tiene por objetivo obtener información sensible que el intruso podría utilizar para basar sus ataques posteriores.

La primera información a obtener es el tipo de servicio que esta corriendo en un determinado puerto, esta identificación ya la realiza correctamente herramientas como **nmap**, pero se podrían hacer manualmente conectado al puerto .En el siguiente ejemplo conectamos a un servidor SIP utilizando la herramienta **netcat** bien conocida como la navaja suiza:

```
[root@attacker]# nc 192.168.1.104 5060
  OPTIONS sip:test@192.168.1.104 SIP/2.0
  Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb
  To: alice <sip:test@192.168.1.104>
  Content-Length: 0


  SIP/2.0 404 Not Found
  Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb;received=192.168.1.103
  To: alice <sip:test@192.168.1.104>;tag=b27e1a1d33761e85846fc98f5f3a7e58.0503
  Server: Sip EXpress router (0.9.6 (i386/linux))
  Content-Length: 0
  Warning: 392 192.168.1.104:5060 "Noisy feedback tells:  pid=29801 req_src_ip=192.168.1.120
       req_src_port=32773 in_uri=sip:test@192.168.1.104 out_uri=sip:test@192.168.1.104 via_cnt==1"
```

Al conectar al puerto especificado manualmente se envía una petición OPTIONS genérica al servidor, para poder estudiar su respuesta. En ella podemos observar que nos muestra información clara sobre el tipo de dispositivo que se trata.

Algunas otras herramientas a automatizan este proceso son:

- **Smap:** Permite identificar dispositivos SIP.
- **Sivus:** Un escáner de vulnerabilidades para SIP. Permite entre otra cosa generar peticiones SIP.
- **Nessus:** Uno de los mejores escáneres de vulnerabilidades. Permite además identificar los servicios y sistemas.
- **VoIPAudit:** Otro escáner VoIP y de vulnerabilidades.

Para poder realizar la mayoría de ataques, el intruso deberá conocer nombres de usuario y extensiones telefónicas correctas. Existen diversos métodos para recavar ese tipo de información:

Una de las técnicas es utilizando las operaciones de registros de usuario. Cuando un usuario pretende registrarse envía una petición REGISTER al servidor de registro y este le responde con un **200 OK** si todo va bien o con un mensaje 4xx si ha habido algún error, el usuario no existe o no tiene los credenciales de autenticación adecuados. Dependiendo del software las respuesta del servidor de registro contra una petición de REGISTER de un usuario existe y no existente puede ser diferente en el sentido de que, si un usuario existe puede que conteste con un mensaje 401 ya que le falte autenticarse pero si el usuario no existe responderá directamente con un mensaje **403 Forbidden**. Esta diferencia en la respuesta puede ser utilizada para enumerar y obtener un listado de usuarios válidos de la red VoIP.

Un método similar al anterior consiste en utilizar mensajes INVITE para enumerar posibles usuarios de la red. Algunos servidores responderán con un mensaje 401 cuando se intenta llamar a un usuario inexistente. El gran problema de este método es que cuando se

acierte y se encuentre un usuario correcto, se estará realizando una llamada y el teléfono del usuario en cuestión sonará y quedará registrada la llamada.

Quizás el método más silencioso para enumerar usuarios es el que utiliza peticiones OPTION. Las peticiones OPTION se utilizan para determinar por ejemplo que codecs soporta un determinado UA. El servidor contestará con un **200 OK** si el usuario existe y un **404 Not Found** si no reconoce el usuario.

Algunas de las herramientas que automatizan todo este proceso, utilizando diccionarios o fuerza bruta con mensajes REGISTER, INVITE o OPTION son: **Sipsak** y **Sipscan**.

Dentro de la plataforma VoIP coexisten gran cantidad de servicios que se podrían aprovechar para obtener información. Algunos de ellos son el DHCP y DNS pero se estudiarán algunas técnicas contra el servicio TFTP y el protocolo SNMP.

La mayoría de dispositivos telefónicos utilizan el protocolo TFTP para manejar sus ficheros de configuración. Normalmente cada vez que un dispositivo VoIP se conecta intenta obtener su configuración del servidor TFTP. El problema es que el servicio TFTP es un servicio altamente inseguro problema que se agrava con el hecho de que en la configuración de los dispositivos se podrá encontrar todo tipo de información valiosa: extensiones, usuarios, passwords, estructura de la red, servidores, etc. Por lo que los servidores TFTP de configuración se convierten en un objetivo claro para comprometer la red VoIP.

La premisa en TFTP es que si se puede averiguar el nombre del fichero de configuración, lo puedes descargar. Muchos dispositivos utilizan nombre por defecto públicamente conocidos, por lo tanto si se identifica el dispositivo puede resultar trivial obtener su configuración del servidor TFTP. Por ejemplo, los dispositivos CISCO el nombre del archivo de configuración mantiene relación con su dirección MAC.

Evidentemente el primer paso debería ser localizar el servidor TFTP en la red. Podemos utilizar un escáner como **nmap** buscando direcciones con el puerto 69 UDP abierto.

Una vez localizado el servidor TFTP, el intruso intentará descargare los ficheros de configuración y como ya ha quedado demostrado la única dificultad que se le presenta es adivinar el nombre de los ficheros. Existen herramientas como **tftpbrute (**que utilizan listados de palabras y diccionarios para atacar el servidor TFTP y descargarse ficheros de configuración. También es posible realizar todo el trabajo manualmente, ya que existen diversas listas que relacionan modelo/fabricante con el nombre por defecto de su archivo de configuración.

El protocolo **SNMP** (Simple Network Management Protocol) que se presenta activo en muchos de los dispositivos VoIP, es otro de los protocolos vulnerables de los que se puede obtener gran cantidad de información.

Los pasos serían los siguientes:

1) Buscar dispositivos con soporte SNMP. Usualmente tendrán el puerto 162 UDP. Se pueden utilizar herramientas como **NMAP** o **SolarWindos SNMPSweep**.
2) Sino se conoce el OID del dispositivo utilizar la **SolarWind MIB** para encontrarlo.
3) Con la herramienta **snmpwalk** y el OID del dispositivo es posible listar la mayoría de aspectos de su configuración.

9. - Explotando el Nivel de Aplicación

El nivel de aplicación de la red IP es quizás uno de los más vulnerables, debido en parte a que VoIP engloba gran cantidad de protocolos y estándares añadiendo cada uno ellos su propio riesgo de segundad. Un ejemplo claro de ellos es el protocolo SIP, muy discutido desde el punto de vista de la seguridad. Entre los ataques específicos contra el nivel de aplicación de VoIP encontramos ataques de secuestro de sesión, desconexiones ilegales, inundación de peticiones, generación de paquetes malformados, falsificación de llamadas y algunos otros que se explicaran a continuación utilizando el protocolo SIP como base.

9.1. Autenticación en VoIP

En toda comunicación, servicio o transmisión de dato existe la necesidad de demostrar que los clientes son quien dicen ser. En VoIP la autenticación requiere que los dos dispositivos que se van a comunicar se autentiquen uno al otro antes de que se produzca cualquier intercambio de información. Esta autenticación mutua esta basada en algún tipo de secreto compartido que es conocido a priori por los dos.

9.1.1 Autenticación del protocolo SIP

El protocolo SIP utiliza la autenticación **digest** para comprobar la identidad de sus clientes. La autenticación **digest** fue originalmente diseñada para el protocolo HTTP, y se trata de un mecanismo bastante simple, basado en hashes que evita que se envíe la contraseña de los usuarios en texto claro.

Cuando el servidor quiere autenticar un usuario genera un desafío digest que envía al usuario. Un ejemplo de desafío podría ser:

```
Digest realm="iptel.org", qop="auth,auth-int",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093", opaque="", algorithm=MD5
```

Destacar que ***nonce*** es la cadena que genera como desafío utilizando el algoritmo MD5 de algún otro dato.

Después de recibir el desafía el UA pedirá al usuario el nombre y la contraseña (si no están presentes en la configuración del dispositivo) y a partir de ellos y del desafío enviado por el servidor generará una respuesta digest como la siguiente:

```
Digest username="jan", realm="iptel.org",
  nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093", uri="sip:iptel.org",
  qop=auth, nc=00000001, cnonce="0a4f113b",
  response="6629fae49393a05397450978507c4ef1", opaque=""
```

De una forma similar el campo **respones** contendrá la respuesta generada por el UA. Cabe destacar el significado del **uri** que indica la dirección sip a la que se quiere acceder y el **cnonce** que es una cadena utilizada por el cliente y el servidor que ofrece cierta protección de integridad al mensaje.

Cuando recibe la respuesta del cliente, el servidor realiza exactamente los mismos pasos. Generando una respuesta digest a partir del desafío y del password del usuario que tiene almacenado en su configuración. Si el hash generado coincide con la respuesta del cliente, el usuario acaba de autenticarse demostrando ser quien dice ser.

Cuando el servidor SIP recibe alguna petición SIP, comprueba si en el mensaje se encuentran las credenciales que autentiquen al usuario, en caso contrario, generará un mensaje de error **401 Unauthorized** al cliente incluyen el desafió digest para iniciar el proceso de autenticación.

El siguiente ejemplo muestra un mensaje REGISTER que contiene las credenciales digest.

```
REGISTER sip:iptel.org SIP/2.0.
Via: SIP/2.0/UDP 195.37.78.121:5060.
From: sip:jan@iptel.org.
To: sip:jan@iptel.org.
Call-ID: 003094c3-bcfea44f-40bdf830-2a557714@195.37.78.121.
CSeq: 102 REGISTER.
User-Agent: CSCO/4.
Contact: <sip:jan@195.37.78.121:5060>.
Authorization: Digest username="jan",realm="iptel.org",
    uri="sip:iptel.org",response="dab81127b9a7169ed57aa4a6ca146184",
    nonce="3f9fc0f9619dd1a712b27723398303ea436e839a",algorithm=md5.
Content-Length: 0.
Expires: 10.
```

9.1.2 Crackeo de contraseñas SIP

Una vez entendido el proceso de autenticación se van a mostrar los métodos y las herramientas para romper esa autenticación y crackear los hashes digest con el fin de obtener el password de un usuario y poder utilizar la identidad de la víctima de forma maliciosa.

Entre las herramientas encontramos **SIPCrack** , que como su nombre indica, crackea las contraseñas del protocolo SIP en Linux. Contiene dos programas **sipdump** para esnifar los hashes de la autenticación y **sipcrack** para crackear los logins capturados.

Se puede descargar de las siguientes direcciones: página oficial http://www.codito.de o PacketStorm http://packetstormsecurity.org.

En caso de encontrarnos una vez más en redes conmutadas puede que sea necesario el uso de herramientas como **ettercap** para realizar la técnica de **man in the middle** y poder esnifar el tráfico necesario.

El programa **sipdump** actúa a modo de sniffer, analizando el tráfico y extrayendo autenticaciones SIP que encuentre.

```
# ./sipdump -i eth0 -d captura.dump
SIPdump 0.1 ( MaJoMu | www.remote-exploit.org )

* Using dev 'eth0' for sniffing
* Starting to sniff with filter 'tcp or udp'
```

sipdump puede también analizar una captura realizada de algún otro sniffer como **tcpdump**. Localiza los paquetes SIP dentro de la captura, los decodifica y extrae los logins que encuentre.

```
# ./sipdump -f capturaSIP.pcap -d fichdump
SIPdump 0.1       ( MaJoMu | www.remote-exploit.org )

* Using tcpdump data file 'capturaSIP.pcap' for sniffing
* Starting to sniff with filter 'tcp or udp'
* Adding 192.168.0.35:50451 <-> 192.168.0.1:50195 to monitor list...id
0
* New traffic on monitored connection 0 (192.168.0.35 -> 192.168.0.1)
* Found challenge response (192.168.0.35:50451 <-> 192.168.0.1:50195)
* Wrote sniffed login 192.168.0.35 -> 192.168.0.1 (User: '200') to
dump file
* Exiting, sniffed 1 logins
*  Adding 192.168.1.35:50451 <-> 192.168.1.100:50195 to monitor
list...id 0
*  New traffic on monitored connection 0 (192.168.1.35 ->
192.168.1.100)
*  Found challenge response (192.168.1.35:50451 <->
192.168.1.100:50195)
*  Wrote sniffed login 192.168.1.35 -> 192.168.1.100 (User: '100') to
dump file
```

Una vez tenemos el hash de la contraseña del usuario, se pueden crackear de dos modos diferentes: Por fuerza bruta y utilizando diccionario. La forma de ejecutar sipcrack es la siguiente:

```
# ./sipcrack -w /usr/share/dict/spanish -d captura.dump

SIPcrack 0.1 ( MaJoMu | www.remote-exploit.org )
--
* Reading and parsing dump file...
* Found Accounts:
Num Server                Client            User Algorithm        Hash
/ Password
  1 192.168.1.100         192.168.1.35 100  MD5
140c0b72f294abd9f4e13eea081a0307

* Select which entry to crack (1 - 1): 1
* Generating static MD5 hash...495ff79e6c8f0378a7c029289a444573
* Starting bruteforce against user '100' (MD5 Hash:
'140c0b72f294abd9f4e13eea081a0307')
* Loaded wordlist: '/usr/share/dict/spanish'
* Tried 47492 passwords in 1 seconds
* Found password: 'hola'
* Updating 'captura.dump'...done
```

Como es normal, el éxito de este ataque dependerá de lo bueno y preciso que sea el diccionario que utilicemos.

Los ataques de fuerza bruta se encargan de probar todas las palabras generadas por todas las combinaciones posibles de cierto grupo de caracteres. Para ello vamos a utilizar uno de los crackeadores más famosos de la historia: **John the Ripeer**, el cual podemos descargarlo de la pagian oficial: http://www.openwall.com/john

John presenta diferentes opciones y formas de configurarse para conseguir el resultado y rendimiento optimo que no trataremos en este documento. Con el **john the ripper** generaremos un diccionario con todas las posibles combinaciones de cierto grupo de caracteres que le indiquemos.

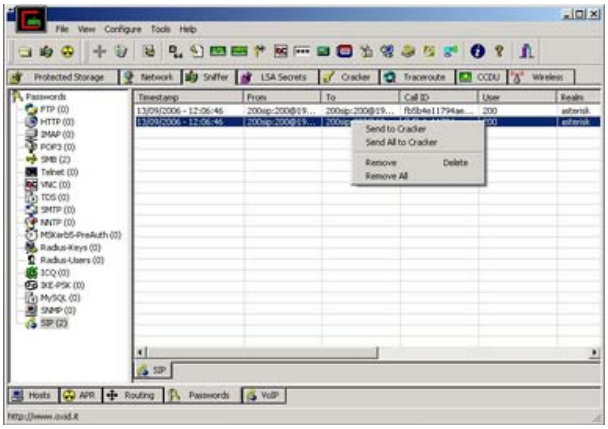
En el ejemplo solo letras y por defecto de hasta 5 caracteres:

```
# john --incremental=alpha --stdout > fichero.txt
words: 11881376 time: 0:00:00:03 w/s: 3960458 current: uxjqv
```

Ahora para cracker la contraseña utilizamos de nuevo **sipcracker** con el fichero generado por el **john**.

```
# ./sipcrack -w fichero.txt -d captura.dump
SIPcrack 0.1 ( MaJoMu | www.remote-exploit.org )
-------------------------------------------------------------------------
-----------------------------------------
* Reading and parsing dump file...
* Found Accounts:
Num       Server                  Client              User
Algorithm       Hash / Password
1         192.168.1.100           192.168.1.35        101         MD5
d666ff953dff9b05a54d0457ab671c78
2         192.168.1.100           192.168.1.35        200
PLAIN           hola
3         192.168.1.100           192.168.1.35        200
PLAIN           hola
4         192.168.1.100           192.168.1.35        101         MD5
da08487896afd6920a077661bfd3997d
* Select which entry to crack (1 - 4): 4
* Generating static MD5 hash...495ff79e6c8f0378a7c029289a444573
* Starting bruteforce against user '101' (MD5 Hash:
'da08487896afd6920a077661bfd3997d')
* Loaded wordlist: 'fichero.txt'
* Tried 5585 passwords in 0 seconds
* Found password: 'asdfg'
* Updating 'captura.dump'...done
```

Otra herramienta que sin duda merece la pena comentar para el crackeo de contraseñas es **Cain**. Una vez más permite realizar todo el proceso de captura de tráfico, envenenamiento ARP, decodificación de protocolos y crackeo de hash por diccionario y fuerza bruta.



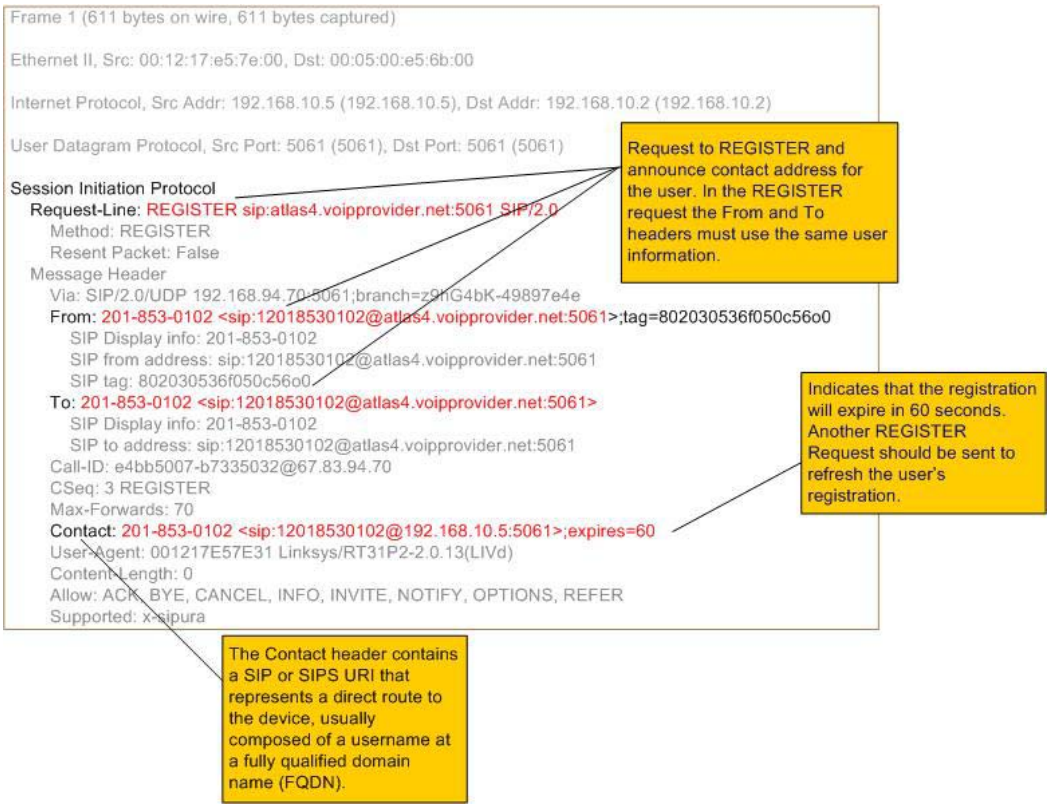
9.2. Manipulación de la señalización

A continuación se detallan algunos de los ataques que se pueden conseguir capturando y manipulando los mensajes de señalización previos al establecimiento de la llamada.

9.2.1 Suplantación de identidad en el registro.

El registro de usuarios es la primera comunicación que se estable en el entorno VoIP entre el usuario y el servidor de registro. Necesariamente esta comunicación debe de realizarse de forma segura, ya que en caso contrario no hay garantías de que el usuario registrado sea quien dice ser durante todo el resto de la sesión. A través de los mensajes REGISTER, los agentes de usuario SIP informan al servidor de su localización actual de manera que el servidor sepa dónde tiene que enviar peticiones posteriores. Si un servidor no autentica las peticiones REQUEST cualquiera puede registrar cualquier contacto para cualquier usuario, y por lo tanto secuestrar su identidad y sus llamadas.

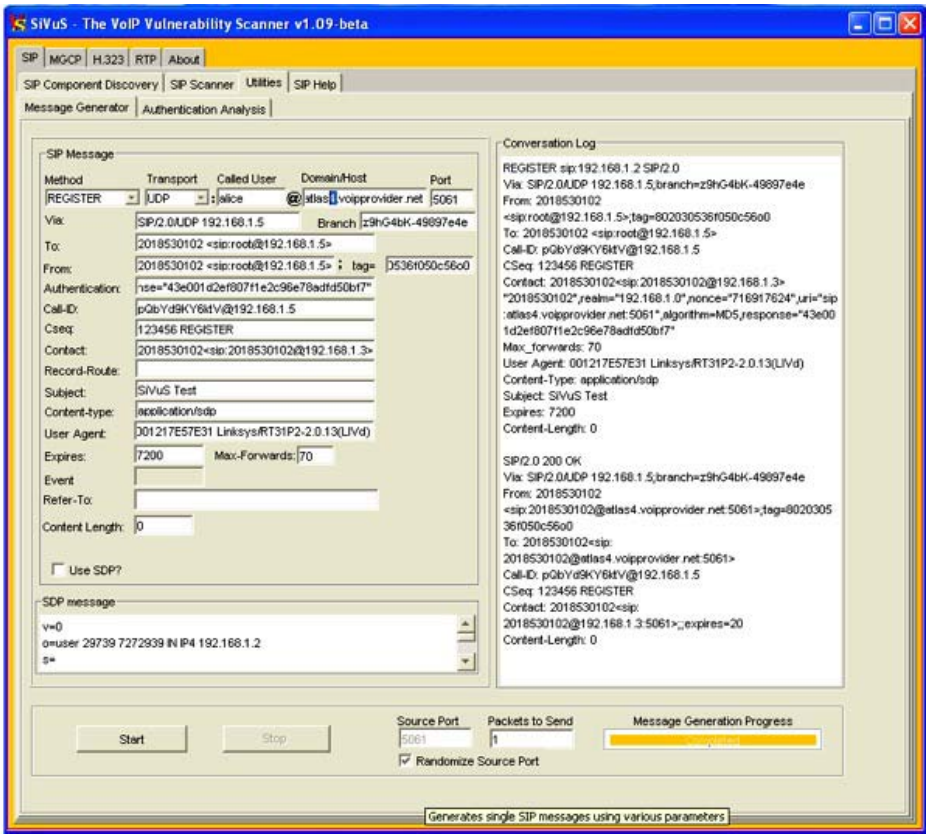
Cuando un Proxy recibe la petición para procesar la llamada (INVITE), el servidor realiza una búsqueda para identificar donde puede ser encontrado el destinatario . En la figura podemos observar un mensaje de respuestas del servidor de registro a una petición de búsqueda de un Proxy Server.



El mensaje REGISTER contiene el campo en la cabecera ***Contact:*** que indica la dirección IP del hardware o software VoIP del usuario destino. En el caso del ejemplo, el usuario

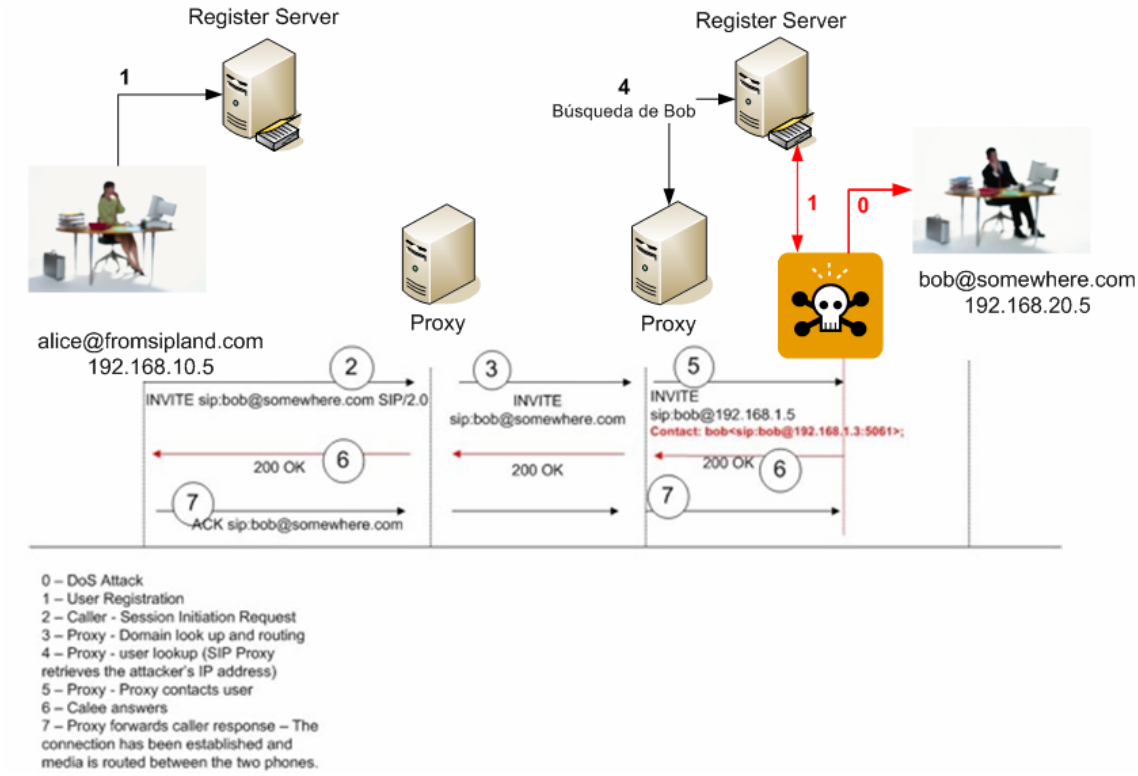
puede ser localizado en el número de teléfono 201-853-0102 o a través de la IP 192.168.94.70. El Proxy redirige la petición INVITE hacia esta dirección IP.

En la figura siguiente se muestra una versión modificada de una petición REGISTER que es enviada por el atacante. En esta petición, todo los parámetros de la cabecera son iguales excepto por el campo ***contact*** que se ha modificado para escribir la IP del atacante. Para generar la petición se ha utilizado la herramienta SiVus :



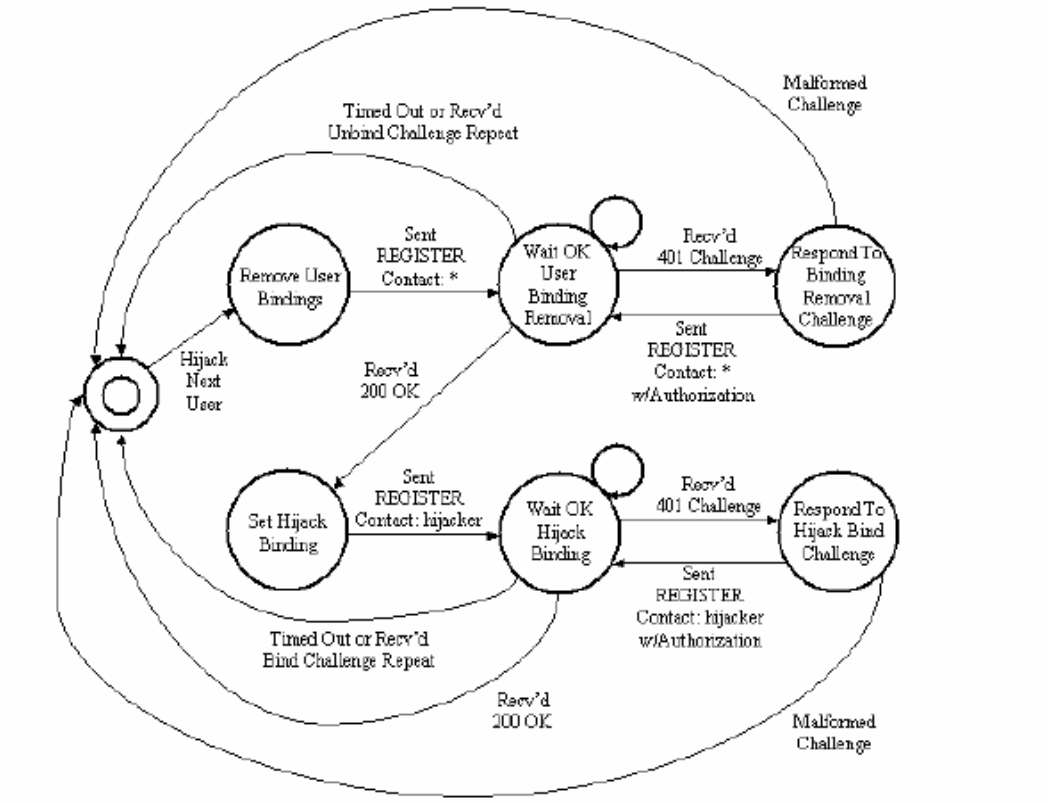
El ataque funciona de la siguiente manera:

1. Deshabilitando el registro legítimo del usuario. (Se explicará en el siguiente apartado).
2. Enviando el mensaje REGISTER con la IP del atacante.
3. En el servidor de registro queda registrado el usuario ***bob*** pero con la dirección IP del hacker.
4. Cuando recibe la llamada, el servidor Proxy consulta la dirección del destinatario ***bob***, pero obtendrá la dirección IP del atacante.
5. El ataque ha tendido éxito. El intruso ha suplantado la identidad de ***bob*** y mientras mantenga el registro todas las llamadas dirigidas a bob llegara a su teléfono IP.



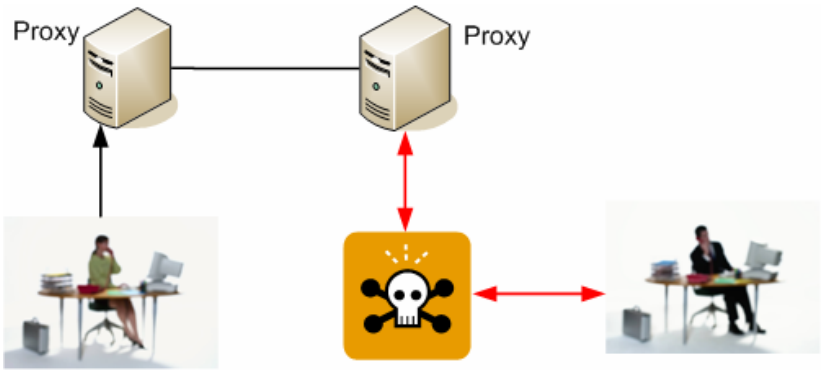
Este ataque es posible llevarlo a cabo por el hecho de que lo mensajes de señalización se envían en texto plano, lo que permite al intruso capturarlos, modificarlo y retransmitirlo como él quiera.

En el siguiente grafo se resume todo el proceso:



En el gráfico vemos que es posible que el servidor requiera autenticación, aspecto que no plantea ninguna problema si previamente el intruso a esnifado y crackeado la contraseña del usuario tal y como se explicaba en el apartado de Autenticación SIP.

A partir de la técnica de secuestro de registro se puede realizar alguna variante del ataque. En el caso anterior evitábamos que el destinatario legítimo recibiera la llamada, pero en algunos casos se puede conseguir realizar un ataque de **Main in the middle** a nivel de red. De esta forma el destinatario legítimo recibirá la llamada y el atacante actuara a modo de servidor Proxy. Se trataría entonces de un ejemplo claro de **eavesdroping**.



Además de la potente herramienta **SiVus** existen un conjunto de tres herramientas para manipular los aspectos del registro de usuarios en SIP:

Registration Hijacker: http://www.hackingexposedvoip.com/tools/reghijacker.tar.gz
Registration Eraser: http://www.hackingexposedvoip.com/tools/erase_registrations.tar.gz
Registration Adder: http://www.hackingexposedvoip.com/tools/add_registrations.tar.gz

9.2.2 Desregistrar Usuarios

El desregistro de usuarios legítimos es una necesidad para conseguir suplantar su identidad como hemos visto en el ejemplo anterior. Básicamente el intruso podrá conseguirlo de las siguientes formas:

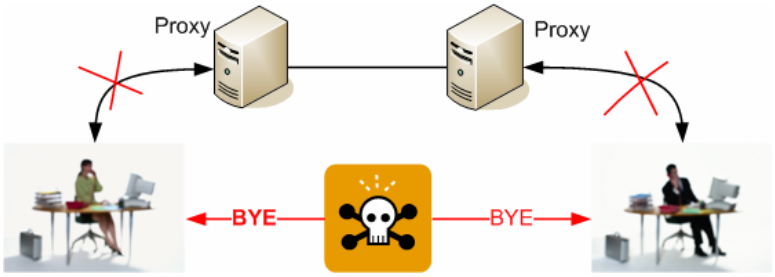
- Realizando un **ataque de DoS** al usuario.
- Generando una **condición de carrera** en la que el atacante envía repetidamente peticiones REGISTER en un corto espacio de tiempo con el objetivo de superponerse a la petición de registro legítima del usuario.
- **Desregistrando el usuario** con mensajes REGISTER.

El intruso puede ser capaz de desregistrar fácilmente un usuario, enviando al servidor de registro una petición REGISTER (simulando ser la victima) con el siguiente campo ***"Contact: *"*** y valor del atributo ***"Expires"*** a cero. Esta petición eliminará cualquier otro registro de la dirección del usuario (especificada en el campo ***"To"*** de la cabecera).

El atacante deberá realizar este envío periódicamente para evitar el re-registro del usuario legítimo o en su defecto provocarle una ataque DoS para evitar que vuelva a registrarse al menos por el tiempo que necesite para realizar el secuestro de la llamada.

9.2.3 Desconexión de Usuarios

El hecho de que muchos de los protocolos se utilizan sin encriptación alguna y de que los mensajes no se autentican de forma adecuada, es trivial para un intruso desconectar a los usuarios de sus llamadas enviando mensajes BYE con la identidad falsificada simulando ser el usuario del otro lado de la línea.



Se puede realizar un ataque similar utilizando mensajes CANCEL, pero solo afectan cuando se esta estableciendo la llamada, es decir, antes de que el destinatario descuelgue el teléfono.

Otro tipo de ataques consistirían en utilizar mensajes ICMP-"port unreachalbe", menajes RESET del protocolo SCCP, o HANGUP para AIX.

Algunas herramientas útiles para automatizar este tipo de ataques son:

Teardown – Injector de mensajes SIP.
http://www.hackingexposedvoip.com/tools/teardown.tar.gz
sip-kill – Inyecta mensajes BYE válidos en una sesión existente:
http://skora.net/uploads/media/sip-kill
sip-proxykill – Técnica similar pero el objetivo son los servidores proxys.
http://skora.net/uploads/media/sip-proxykill

9.2.4 Redirección de llamadas.

La redirección de llamadas suele ser otro de los ataques comunes en las redes VoIP. Existen diferentes métodos que van desde comprometer los servidores o el call manager de la red para que redirijan las llamadas donde el intruso quiera, hasta las técnicas ya mostradas de suplantación de identidad en el registro, man in the middle, etc.
Otra posibilidad es utilizar una herramienta como **RedirectPoison** que escucha la señalización SIP hasta encontrar una petición INVITE y responder rápidamente con un mensaje SIP de redirección, causando que el sistema envié un nuevo INVITE a la localización especificado por el atacante.

Otro modo de redirección el flujo de datos se consigue con las herramientas: **sip-redirectrtp** y **rtpproxy.** Se basan en utilizar mensajes la cabecera SDP para cambiar la ruta de los paquete RTP y dirigirlas a un **rtproxy** que a su vez serán reenviados donde el intruso quiera.

9.3. Manipulación de la transmisión

9.3.1 Eavesdropping

La técnica de la interceptación de la comunicación o **eavesdropping** ya ha sido explicada por lo que en este caso veremos un ejemplo práctico de cómo capturar la señalización y el flujo de una llamada para después poder reproducir el contenido de la misma.

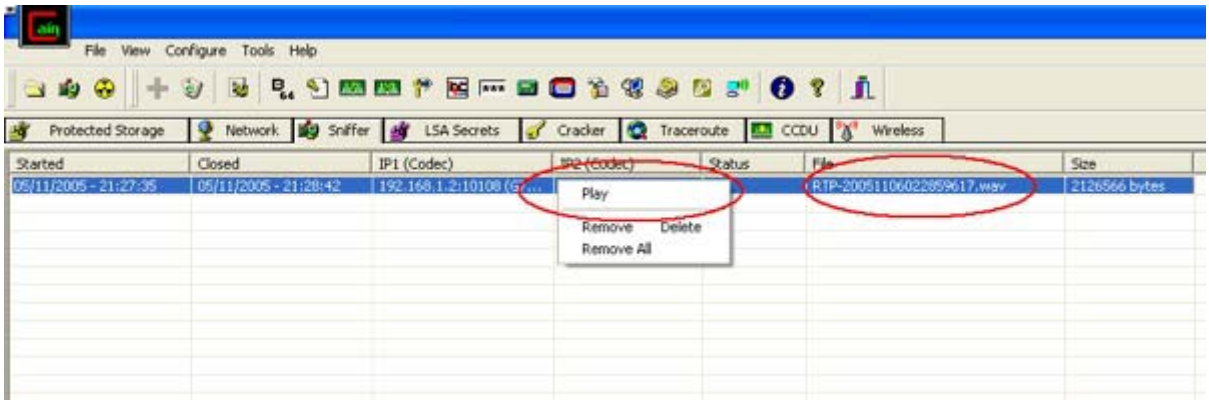
Lo pasos para capturar y decodificar los paquetes de voz interceptados son realmente sencillos. En el primer ejemplo utilizaremos un sniffer como **ethereal**. En algunos casos para poder esnifar el tráfico en redes conmutadas pueden ser necesarias técnicas como el envenenamiento ARP, que básicamente consiste en realizar un **Man in the middle** utilizando tramas ARP spoofeadas. Herramientas como **ettercap** y **arpspoof** pueden ser útiles en este caso.

- **Capturar y decodificar los paquetes RTP.** Esnifar el tráfico de la comunicación con el **ethereal**, este sniffer permite además interpretar los paquetes UDP indicándole que son del protocolo RTP.

- **Seleccionar la opción "Analizar Sesión".** Permite seleccionar un flujo de datos y analizarlo ya no como paquetes individuales sino común flujo continuo de datos.

- **Salvar a un fichero de audio**, para reproducirlo posteriormente. Ethereal permite analizar los datos RTP y salvarlos como un fichero de audio.

Se puede automatizar aun más el proceso si se utiliza la fabulosa herramienta **Cain**. Que además de ser un buen sniffer puede realizar infinidad de funciones y ataques. En el ejemplo que nos ocupa, con el propio **Cain**, podremos esnifa la comunicación VoIP, utiliza el envenenamiento ARP si fuera necesario, y además permita decodificar y reproducir los datos de voz capturados, todo en un mismo programa.



A continuación se describen algunas otras herramientas que merece la pena reseñar:

- **Oreka:** Es un sniffer de VoIP que captura conversaciones y registros y que soporta los protocolos más utilizados: Bidirectional SIP, SCCP de Cisco, Bidirectional Raw RTP. Tiene una licencia GPL y está disponible tanto para sistemas Windows como GNU/Linux.

- **Orktrack y Orkweb:**Orktrack y Orkweb proporcionan una interfaz web para la administración de los registros guardados con orkaudio.

- **Voipong:** Voipong es una herramienta que detecta todas las llamadas de VoIP que se producen en una red. Además codifica dichas conversaciones a ficheros de audio, si se utiliza un códec G711 los convertirá en formato WAV. Soporta SIP, H323, Cisco's Skinny Client Protocol, RTP y RTCP.

- **Angst :** Angst es un snifer que puede funcionar en modo pasivo y activo utilizando diversas técnicas para sniffer dentro de redes conmutadas.

- **Vomit:** Convierte las conversaciones de teléfonos Ciso a un fichero wav.

9.3.2 Inserción de Audio.

En las llamadas VoIP la transmisión del flujo de datos se realiza por razones de sencillez y eficiencia sobre el protocolo UDP. Desgraciadamente UDP es un protocolo que no da garantías en la entrega de sus mensajes y no mantiene ningún tipo de información de estado o conexión. Por lo que a priori la inserción de paquetes UDP extraños dentro de un flujo legítimo puede llegar a ser trivial.

Encapsulado en UDP se encuentra el protocolo RTP que transporta verdaderamente los datos de voz. RTP tampoco lleva un control exhaustivo sobre el flujo de datos relegando las funciones de recuento de paquetes y calidad de servicio al protocolo RTCP (Real time control protocol). El único método que tiene RTP para controlar tramas perdidas y reordenar las que le llega es el campo numero de secuencia de la cabecera.

En esta situación ¿Qué ocurriría si a un dispositivo le llegan dos tramas UDP con el mismo número de secuencia (y diferentes datos)? ¿Descartaría la última que llega por estar repetida?¿Y si la última es la trama legítima? En caso contrario ¿Sobrescribirían los datos de la segunda a la primera al reordenar y reensamblar?. Es evidente que la forma de manejar estas situaciones dependerán mucho del dispositivo o de la implementación del software pero en cualquiera de los dos casos el atacante podría realizar ataques de inserción de paquetes dentro de un flujo RTP consiguiendo insertar de forma exitosa audio en una conversación telefónica. Incluso se ha comprobado que contra algunos dispositivos es suficiente bombardear con paquetes UDP para que esto se inserten en la conversación.

Algunas herramientas con las que poder realizar este tipo de ataque son:

- **RTP InsertSound** : Es capaz de inserta un archivo wav en una conversación activa que este esnifando.
- **RTP MixSound**: Muy parecida a la anterior pero mezcla el sonido insertado con el real de la conversación.

9.4. Fuzzing

Los ataques de **fuzzing** o también conocidos como testeo funcional del protocolo, es una de los mejores métodos para encontrar errores y agujeros de seguridad. Consiste en crear paquetes o peticiones especialmente malformadas para ir más allá de las especificaciones del protocolo. El objetivo es comprobar como manejan los dispositivos, las aplicaciones o el propio sistema operativo que implementa el protocolo, estas situaciones anómalas que desgraciadamente no se han tenido en cuenta en la implementación y casi siempre terminan en un error, denegación de servicio o en alguna vulnerabilidad más grave.

Gracias a la técnica de **fuzzing** se han llegado a encontrar gran cantidad de ataques de DoS y buffer overflows en los productos que implementan los protocolos SIP y H,.323.

Un ejemplo sencillo podría ser el siguiente:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP 10.1.1.1:5060;branch=77ef4c2312983.1
Via: SIP/2.0/UDP 10.1.3.3:5060
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@10.1.3.3
CSeq: 314159 INVITE
Contact: <sip:alice@10.1.3.3>
Content-Type: application/sdp
Contact-Length: 142
(Carga SDP no mostrada)

INVITE sip:bob@biloxi.com SIP/2.0
Via:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaa
Via: SIP/2.0/UDP 10.1.3.3:5060
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@10.1.3.3
CSeq: 314159 INVITE
Contact: <sip:alice@10.1.3.3>
Content-Type: application/sdp
Contact-Length: 142
```

Como vemos el objetivo es provocar un desbordamiento de buffer y la consiguiente denegación de servicio en el dispositivo que procese la petición.

Podemos encontrar una gran herramienta llamada PROTOS que se encarga de automatizar este tipo de ataques contra diversos protocolos como SIP, HTTP y SNMP . En su página oficial encontraremos también mucha documentación valiosa:

http://www.ee.oulu.fi/research/ouspg/protos/index.html

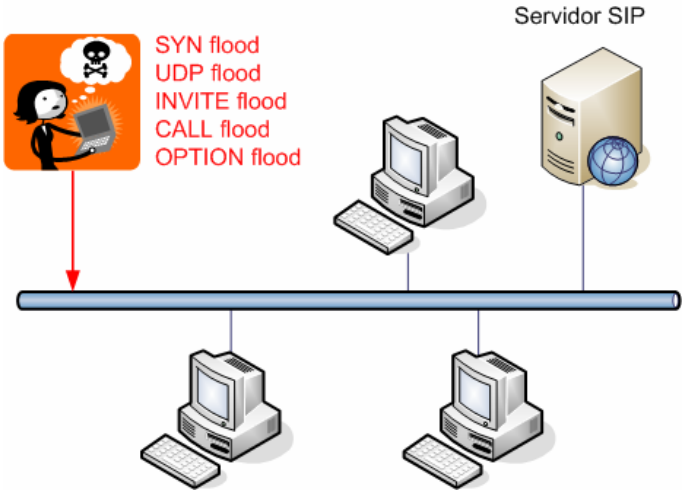
Otras herramientas son:

- **Ohrwurm** - Fuzzer para RTP .
  http://mazzoo.de/blog/2006/08/25#ohrwurm
- **Fuzzy Packet** - Otro fuzzser para RTP
  http://libresource.inria.fr/projects/VoIP_Security/fuzzypacket
- **Asteroid** – Genera peticiones SIP malformadas (INVITE, CANCEL, BYE, etc.)
  http://www.infiltrated.net/asteroid/

9.5. Ataques DoS

Los ataques de denegación de servicio fueron explicados en el apartado anterior, por lo que me limitare a mostrar algunos ejemplos prácticos.

Las redes VoIP siguen siendo vulnerables a los tradicionales ataques de DoS como pueden ser los SYN flood, UDP flood etc. Las aplicaciones VoIP escuchan en ciertos puertos determinados, es posible atacar esos servicios causando un ataque DoS.



Existen gran cantidad de flooders disponibles en la red, podemos descargar y testear el **UDP flooder** de las siguiente dirección :

http://www.hackingexposedvoip.com/tools/udpflood.tar.gz

O en cambio se puede utilizar algún generador de paquetes convencional como **Scapy**:

http://www.secdev.org/projects/scapy/

VoIP presenta cierta dependencia del protocolo DNS por la necesidad de resolver los nombres de dominio. Un ataque a los servidores DNS de la red podría derivar en una denegación de servicio de la red VoIP. Una herramienta interesante para testear el servicio de resolución de nombres es **DNS Auditing tool** que se encuentra disponible en la dirección web : http://www.packetfactory.net/projects/dnsa

Existen también ataques específicos de protocolos como SIP. El caso más común es intentar atacar a las capacidades de los servidores hasta conseguir que dejen de prestar el servicio.

En el siguiente ejemplo podemos ver como una inundación de peticiones INVITE a toda la red VoIP, falseando la identidad de llamante, provocaría que los teléfonos que no estén en uso comenzaran a sonar y si la inundación continua terminaría por colapsar las líneas y los servidores.

Otros ataques de inundación similares se pueden reproducir también con mensajes REGISTER,OPTIONS y CALL.

Algunas herramientas interesantes son **INVITE Flooder** y **RTP Flooder** .

Otro tipo de ataques son los llamados de "smurf" o de amplificación, consiste en identificar los procesos de red que responden con paquetes mucho mayores a los de la petición. De este modo, si el atacante falsifica la dirección origen, emitiendo paquetes pequeños e datos, las respuestas a esas peticiones serán mucho mayores en cuanto a tamaño y le llegaran a la víctima, con el único objetivo de realizar una denegación de servicio.

En general existen gran cantidad métodos diversos para sobrecargar la red y los servidores con el fin de conseguir una denegación de servicio. Problema que se agrava con el hecho que en una infraestructura IP pueden coexistirán gran cantidad de protocolos (**SIP, CMMS, H.225, H.245, RAS, MGCP, TGCP, NC, H.284, Megaco, SKINNY, SCCP, Q.931+, SIGTRAN, ISTOP, SS7, RUDP, RADIUS, COPS, RTP, RTCP**) y dispositivos cada uno de ellos vulnerables de una forma diferente.

10. - Ingeniería social

10.1. SPIT: Spam over Internet Telephony

El SPAM es uno de los problemas más graves en las comunicaciones hoy en día, y la telefonía IP tampoco se escapa. Recibe el nombre de SPIT (Spam over Internet Telephony).
A pesar que hoy por hoy no es una práctica demasiado extendida y no se han registrados demasiados casos, las redes VoIP son inherentemente vulnerables al envío de "mensajes de voz basura". Siendo el impacto en la red VoIP mucho mayor que el SPAM tradicional.
Se prevé que esta tendencia de realizar llamadas y llenar los voicemail de los usuarios con mensajes pregrabados crecerá durante los próximos años a medida que se generalice el uso de telefonía por IP.

10.2. Vishing: Voip Phishing

Al igual que ocurría con el SPAM las amenazas de phishing suponen un gran problema para el correo electrónico. Las denuncias por robo de información confidencial de forma fraudulenta están a la orden del día y exactamente las mismas técnicas son aplicables a la plataforma VoIP. Gracias a la telefonía IP un intruso puede realizar llamadas desde cualquier lugar del mundo al teléfono IP un empleado de la empresa y con técnicas de ingeniería social y mostrando la identidad falsa o suplantando otra conocida por la victima, obtener información confidencial, datos personales, números de cuenta o cualquier otro tipo de información. Las opciones son prácticamente ilimitadas y al igual que el SPIT es posible que el número de incidentes de este tipo se disparen en los próximos años.

11. - Asegurando la red VoIP

Durante todo el trabajo mi intención ha sido dar a conocer la mayoría de problemas de seguridad que pueden llegar a sufrir las redes de telefonía IP y explicar las técnicas y los ataques que intruso utilizaría para atacar entornos VoIP reales. Para redactar una guía de creación de infraestructuras VoIP seguras sería necesario un nuevo trabajo mucho más extenso que el actual, por lo que me limitaré he señalar qué controles de seguridad deben ser imprescindibles en el entorno VoIP y explicar las medidas necesarias para paliar la mayoría de riesgos y ataques comentados en apartados anteriores.

La primera regla de oro: **Mantener los sistemas actualizados y parcheados**. Es totalmente imprescindible, y ya no solo en infraestructura VoIP, que el administrador de la red esté al corriente de los nuevo parches y actualizaciones y los aplique en sus sistemas.

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

Es conveniente 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, un 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 comunicación de los datos pueden ser segura incorporando algún tipo de cifrado. Los teléfonos VoIP pueden cifrar el audio con el protocolo SRTP. **Secure RTP** es un 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.

Intentar proteger y limitar el acceso a la red VoIP en la medida de lo posible, sobre todo desde el exterior.

Limitar los volúmenes de datos y ráfagas de paquetes en puntos estratégicos de la red para evitar gran cantidad de ataques DoS.

Y finalmente algunos consejos para protegerse de ataques de enumeración:

- Corregir los protocolos que contestan diferente modo si el usuario existe o no.
- Configurar correctamente los servicios para que no muestren más información de la necesaria.
- No usar nombres por defecto par archivos de configuración
- No usar TFTP, FTP aunque tampoco sea seguro. LA mejor solución es usar un canal cifrado.
- Desactivar puertos de administración http y snmp.
- Cambiar el password por defecto de todos los lugares.

12. - Referencias

Hacking VoIP Exposed
http://www.hackingvoip.com/

Practical VoIP security
Thomas Porter
http://www.amazon.com/Practical-VoIP-Security-Thomas-Porter/dp/1597490601

A Brief Overview of VoIP Security
By John McCarron
http://www.infosecwriters.com/text_resources/pdf/Voip_JMccarron.pdf

Voice over IP security
By Chris Roberts
http://www.ccip.govt.nz/ccip-publications/ccip-reports/voice_over_ip_security.pdf

VoIP Hacks
By Theodore Wallingford
http://www.oreilly.com/catalog/voiphks/

VoIP Vulnerabilities – Registration Hijacking
By Mark Collier
http://download.securelogix.com/library/Registration_hijacking_060105.pdf

Basic Vulnerability Issues for SIP Security
By Mark Collier
http://download.securelogix.com/library/SIP_Security030105.pdf

SIP Stack Fingerprinting and Stack Difference Attacks
By Hendrik Scholz
http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Scholz.pdf

VoIP Security Issues
By Hendrik Scholz
http://www.wormulon.net/files/pub/Syscan_06_-_VoIP_Security_Issues.pdf

Security in VoIP-Telephony Systems
Johann Thalhammer
http://www.iaik.tugraz.at/teaching/11_diplomarbeiten/archive/thalhammer.pdf

VoIP Security
By Ken Camp
http://www.ipadventures.com/docs/VoIPSecurity.pdf

VoIP: The Evolving Solution and the Evolving Threat
ISS
http://www.iss.net/documents/whitepapers/ISS_VoIP_White_paper.pdf

Enterprise VoIP Security Best Practices
Jupiter Networks Inc.
http://www.juniper.net/solutions/literature/white_papers/200179.pdf

VoIP Security and Privacy Threat Taxonomy
Voipsa
http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

Hacking VoIP Phones: 802.11b/g Wireless & Wired
Shawn Merdinger
http://www.io.com/~shawnmer/voipsecexp/noconname_2006_Merdinger.pdf

Voice Over IP - Security and SPIT
By Rainer Baumann, Stephane, Cavin Stefan Schmid
http://rainer.baumann.info/public/voip.pdf

VoIP-Attacks By Druid
http://druid.caughq.org/presentations/VoIP-Attacks.pdf

Registration Hijacking
http://www.securityfocus.com/infocus/1862/1

Eavesdroping
http://www.securityfocus.com/infocus/1862/2

Eavesdroping
http://blog.txipinet.com/index.php/2006/10/11/40-seguridad-en-voip-iii-captura-de-conversaciones-o-eavesdropping

Cracking SIP I
http://blog.txipinet.com/index.php/2006/10/11/38-seguridad-en-voip-i-cracking-de-contrasenas-sip-en-gnu-linux

Cracking SIP II
http://blog.txipinet.com/index.php/2006/10/11/39-seguridad-en-voip-ii-cracking-de-contrasenas-sip-en-ms-windows

Articulos varios
http://voipsa.org/Resources/articles.php