WHITE HACK 2004

28-30 Mayo 2004

Seguridad en Redes Convergentes:

Seguridad en Voz sobre IP (VoIP)

Internet Security Auditors

Daniel Fernández Bleda

CISSP, OPST/OPSA Trainer

Co-Founder

Índice

- ¿Qué es VoIP?
- Protocolos y estándares de VoIP
  - H.323
  - SIP
  - RTP
- Una nueva perspectiva del enemigo
- Vulnerabilidades típicas de VoIP
  - Ataques DoS
  - Escuchas
  - Capturas
  - Reenvíos
- Soluciones
- Entonces, ¿VoIP es seguro?
- Referencias

¿Qué es VoIP?

- Es un nombre con el que se refiere al transporte de comunicaciones telefónicas (Voz, también video) a través de una red de datos (red IP).
- Es una tecnología madura pero todavía en evolución.
- Existen gran cantidad de estándares y los fabricantes los adoptan todos para ofrecer interoperatividad.
- VoIP emplea el protocolo TCP/IP, que no ofrece QoS.
- TCP/IP fue diseñado con el objetivo de enviar datos con la esperanza que estos lleguen a su destino.
- Para conseguir QoS se han desarrollado protocolos de nivel superior.

Protocolos y estándares de VoIP

- **Protocolos de Señalización**: permiten la localización de usuarios, establecimiento y negociación de sesiones y la gestión de los comunicantes - **H.323**, MEGACO, MGCP y **SIP** -.

- **Protocolos de Transporte de Datos (Media)**: permiten digitalizar, codificar y decodificar, empaquetar, enviar, recibir y reordenar las muestras de voz - **RTP**, **RTCP**, SCTP -.

- **Protocolos/Servicios de Soporte**: complementan las funcionalidades, eficiencia y seguridad de los anteriores - DNS, Servidores de Localización, Sistemas de QoS, Protocolos de enrutado, servidores de AAA, etc…-

H.323 (I)

- H.323 es una “suite” de protocolos desarrollada por el *International Telecommunication Union (ITU-T)* para transferir voz y video sobre una red de datos:
  - H.225: call control signaling, registro y admisión
  - H.235: aspectos de seguridad -Autenticación, Integridad, Privacidad y No Repudio
  - H.245: Negociación del uso del canal
  - H.261: Codecs de Video
  - G.723/G.729: Codecs de Audio

- Desde la versión publicada el año 1996 han aparecido versiones 2 (1998), 3 y 4 (2000) para poder competir con el formato desarrollado por el IETF, SIP, dado que H.323 se desarrollo para ser usado en LANs y no en WANs (Internet).

H.323 (II)

- Es el primer protocolo utilizado masivamente en aplicaciones de videoconferencia y VoIP.
- Desde la versión publicada el año 1996 han aparecido versiones 2 (1998), 3 y 4 (2000) para poder competir con el formato desarrollado por el IETF, SIP, dado que H.323 se desarrollo para uso en LANs.
- Programas de videoconferencia (NetMeeting, GNomeMeeting, etc.) y multitud de IP SoftPhones emplean H.323.
- Existe un desarrollo Open Source de la pila H.323, así como software de VoIP libre en www.openh323.org.
- Seguramente SIP haga que pase a ser un protocolo menos usado, pero actualmente, dadas las deficiencias de todos ellos, se ha planteado su continuidad y cohabitación en redes multi-protocolo.

H.323 (III)

Un sistema H.323 se compone de cuatro componentes:

- **Terminal**: Este es el dispositivo del usuario final, soporta tráfico bidireccional de voz, datos y/o video con otro terminal. Un terminal sería un SoftPhone en un PC o un teléfono IP.
- **Gateway**: Son los responsables con otros gateways u otras redes. Si el dispositivo al que se conecta en otra red no soporta H.323, el gateway será el responsable de realizar la conversión entre ambos protocolos. El gateway también será el encargado de realizar la conexión entre la red telefónica y la basada en IP.
- **Multipoint Control Unit**: Ofrece suporte para sistemas de multiconferencia entre diferentes terminales de usuario.
- **Gatekeeper**: Provee de servicios de autenticación para permitir a los usuarios finales registrase en la red de VoIP. Es el encargado de gestionar las políticas de acceso y traslación de direcciones.

Session Initiation Protocol (SIP)

- Es un protocolo desarrollado por el *Internet Engineering Task Force (IETF*) en 1999 con el RFC 2543 y mejorado con el RFC 3261 en 2002.
- Mucho más moderno que H.323 y que facilita la escalabilidad, reutilización e interoperatividad entre componentes de la red VoIP.
- Si H.323 se basa en binario (ASN.1), SIP se basa en texto (ASCII).
- Es muy similar a protocolos como HTTP o SMTP y emplea el modelo petición/respuesta (*request/response*).
- SIP está basado en una serie de mensajes empleados para mantener una máquina de estados (similar a TCP/IP) en cada uno de los extremos de la comunicación.

Componentes de SIP (I)

- User Agent Client (UAC)
  - End Systems
  - Send SIP Requests
- User Agent Server (UAS)
  - Listening for Incoming Requests
  - Execute an “internal logic”/program to determine the appropriate response
- User Agent
  - UAC + UAS

Componentes de SIP (II)

- Redirect Server
  - Redirect “callers” (requests) to another Server
- Proxy Server
  - Relay Call Signaling (“Proxy requests to another server”)
  - Can “fork” requests to multiple targets
  - Able to maintain basic Call-State (or not)
- Registrar
  - Receives registrations requests regarding current user locations
  - Stores the information at a “Location Server”

Tipos de Mensajes SIP

- Los mensajes que definen los RFCs de SIP son estos:

INVITE: Petición de invitación a un usuario para iniciar la llamada.

ACK: Aceptación de inicio del intercambio de mensajes INVITE.

BYE: Finalización (o transferencia) de la llamada entre terminales.

OPTIONS: Petición de información sobre capacidades del terminal.

REGISTER: Registro de información de la localización actual en un servidor SIP de registro.

CANCEL: Petición de fin de búsqueda o llamada de un usuario.

INFO: Petición de información durante una llamada.

PRACK: Aceptación Provisional.

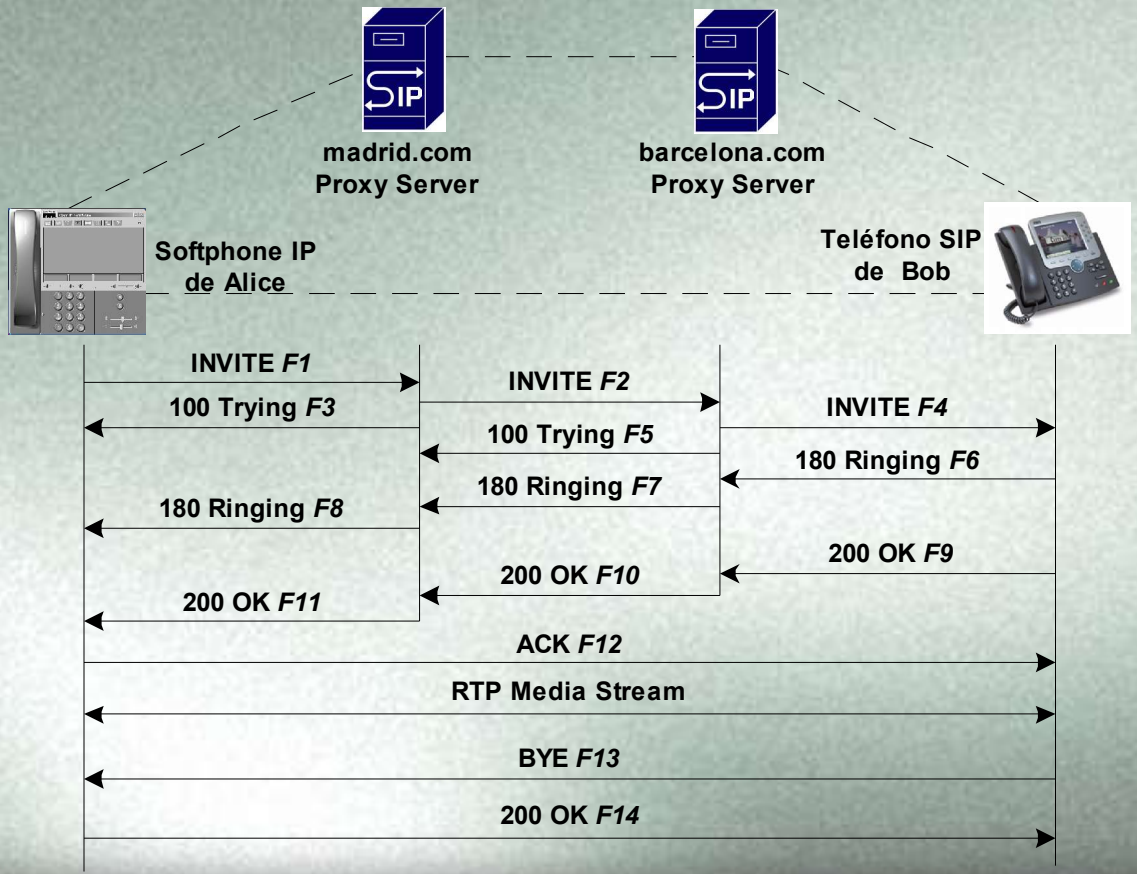
COMET: Pre-condición dada.

SUBSCRIBE: Petición de subscripción a un evento.

NOTIFY: Notificación a los participantes en una llamada.

Funcionamiento básico de SIP

- Este es un ejemplo (RFC3261) que muestra el funcionamiento básico del establecimiento de una sesión (comunicación o llamada) mediante SIP entre dos dispositivos que implementan este protocolo. Este esquema típico recibe el nombre de “trapezoide SIP”.



Un mensaje SIP

Método SIP

INVITE sip:bob@barcelona.com SIP/2.0

La dirección en la que Alice espera recibir las respuestas. Este parámetro indica la ruta que el mensaje de retorno debe seguir.

Via: SIP/2.0/UDP pc33.madrid.com;branch=z9hG4bK776asdhds

Max-Forwards: 70

El nombre y la/s direcciones URI SIP o SIPS a las que se envía el mensaje.

To: Bob <sip:bob@barcelona.com>

From: Alice <sip:alice@madrid.com>;tag=1928301774

Contiene un identificador único para esta llamada.

Call-ID: a84b4c76e66710@pc33.madrid.com

Típico número identificador de secuencia y el nombre del método SIP.

CSeq: 314159 INVITE

SIP o SIPS URI que representa la ruta directa a Alice.

Contact: <sip:alice@pc33.madrid.com>

Content-Type: application/sdp

Content-Length: 142

(La información SDP no se muestra)

Real-Time Transport Protocol (RTP)

- RTP definido por el IETF en el RFC 1889.
- RTP provee de mecanismos a las aplicaciones para el envío de audio y video entre extremos en redes uni- o multicast.
- RTP no ofrece QoS para aplicaciones de tiempo real.
- El protocolo RTP se complementa con un protocolo de control (RTCP) que permite monitorizar el flujo de datos enviados mediante RTP.
- Es el protocolo de transporte utilizado por los dispositivos VoIP.

Una nueva perspectiva del enemigo

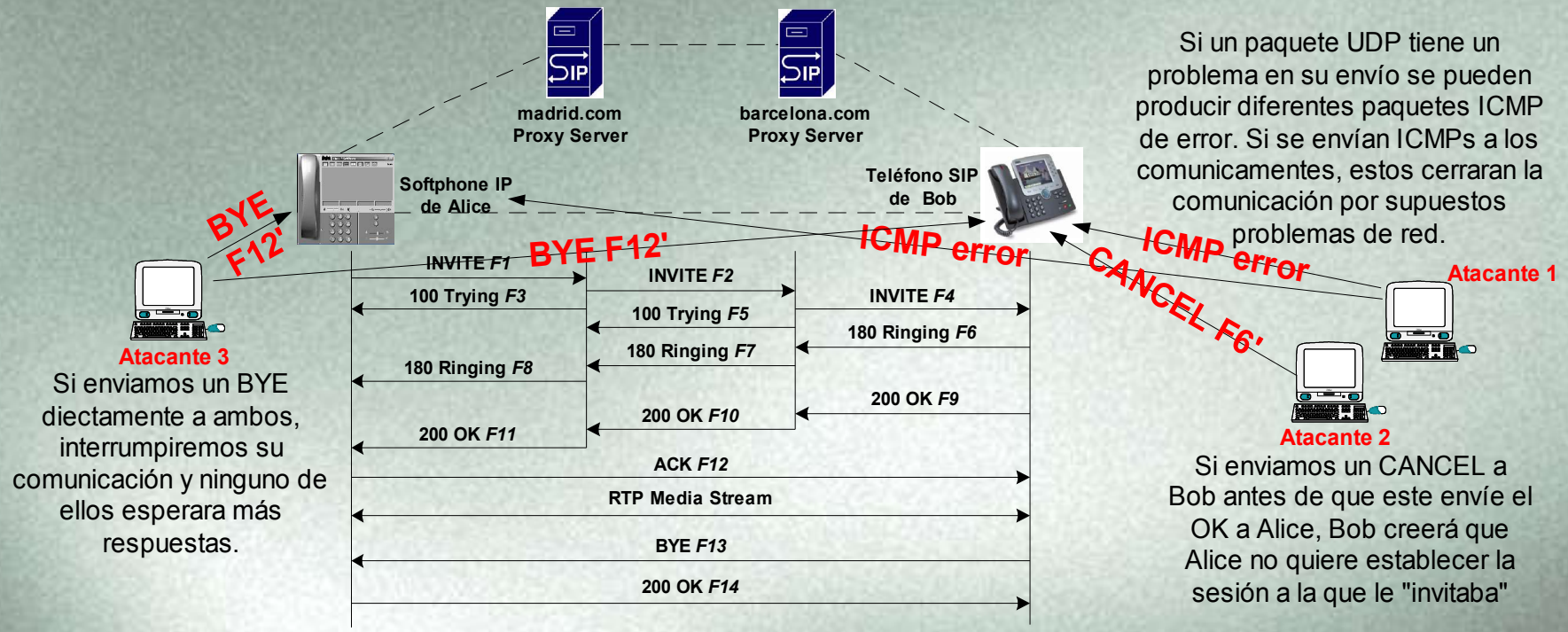
- Con la convergencia **Datos** y **Voz** se produce también la convergencia del atacante: **Hacker** (o Cracker, según preferencias) y **Phreaker**.
- Un **Hacker** ataca los **Sistemas de Información** (**SI**).
- Un **Phreaker** ataca los **Sistemas de Telefónicos** (**ST**).
- Un **Hacker** puede atacar los **SI** a través de los **ST**.
- Un **Phreaker** puede atacar a los **ST** a través de los **SI**.
- Se multiplica el efecto de un ataque de ambos.

Vulnerabilidades típicas de VoIP

- Los tipos más comunes de ataques a los que VoIP es sensible son:
  - **Ataques de Denegación de Servicio** (**DoS**): Mediante el envío de paquetes a los interlocutores, los proxies u otros servidores que gestionan las llamadas y que impiden o interrumpen las conexiones.
  - **Escuchas** (**eavesdropping**): Mediante la captura de los paquetes de gestión de sesión (SIP, H.323, ...) o los de voz que se encapsulan en Real-Time-Protocol (RTP) y su decodificación o los paquetes.
  - **Captura de llamadas (Call hijacking)**: Mediante el envío de paquetes VoIP suplantando alguno de los participantes en las llamadas (packet spoofing).
  - **Reenvío de paquetes (Replay)**: Mediante la retransmisión de paquetes (capturados o generados) de manera que los dispositivos VoIP los procesen de nuevo.
  - **Ataques a la Integridad de los Mensajes**: Mediante la moficación de los mensajes enviados entre usuarios o dispositivos.

Ataques DoS (SIP)

- Existen multitud de condiciones en las que se pueden realizar ataques de Denegación de Servicio a uno de los participantes en las sesiones o a ambos.



Si un paquete UDP tiene un problema en su envío se pueden producir diferentes paquetes ICMP de error. Si se envían ICMPs a los comunicamentes, estos cerraran la comunicación por supuestos problemas de red.

Si enviamos un BYE diectamente a ambos, interrumpiremos su comunicación y ninguno de ellos esperara más respuestas.

Si enviamos un CANCEL a Bob antes de que este envíe el OK a Alice, Bob creerá que Alice no quiere establecer la sesión a la que le "invitaba"

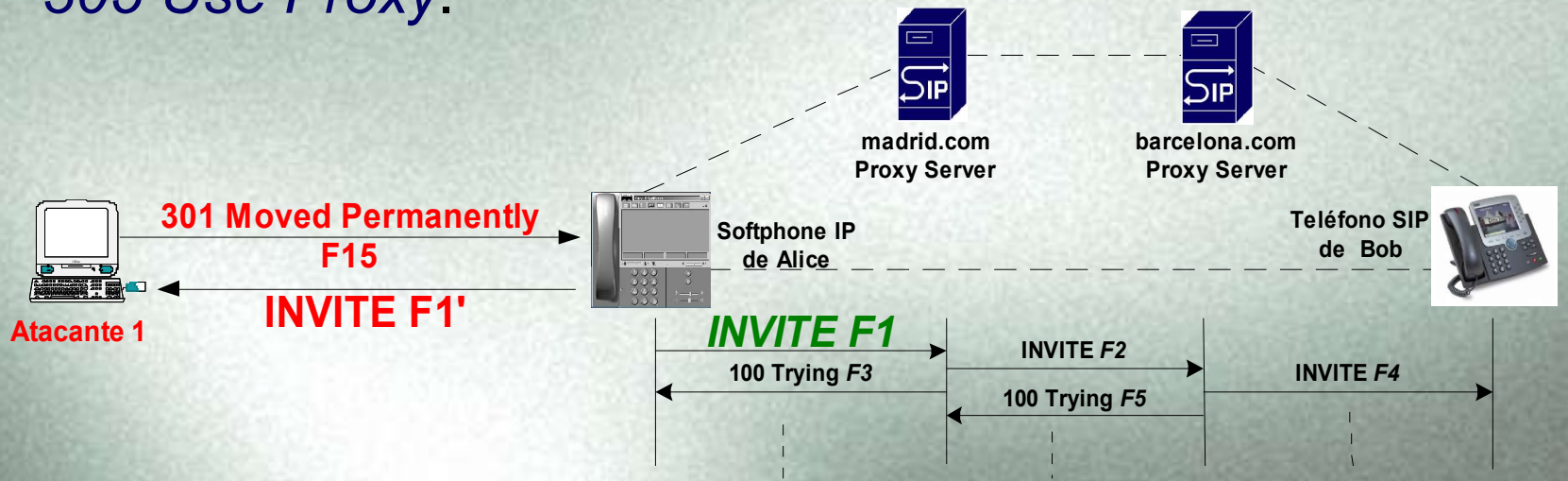
Ataques de Escuchas (Call Tracking)

- Escuchando todo el tráfico SIP de la red se puede hacer un seguimiento de las llamadas y su contenido:
  - Quién llama a quién.
  - Cuando se hacen las llamadas.
  - Cuanto tiempo duran las llamadas.
  - Donde se encuentran las personas que mantienen las conversaciones.
  - Capturando tonos teléfonicos (DTMF) podemos conseguir código a buzones de voz, passwords, códigos, etc.
- Esto también sucede en H.323 (en el protocolo H.225) donde se envían los datos de los comunicantes para el establecimiento de la sesión.

Ataques de Captura (Call Hijacking)

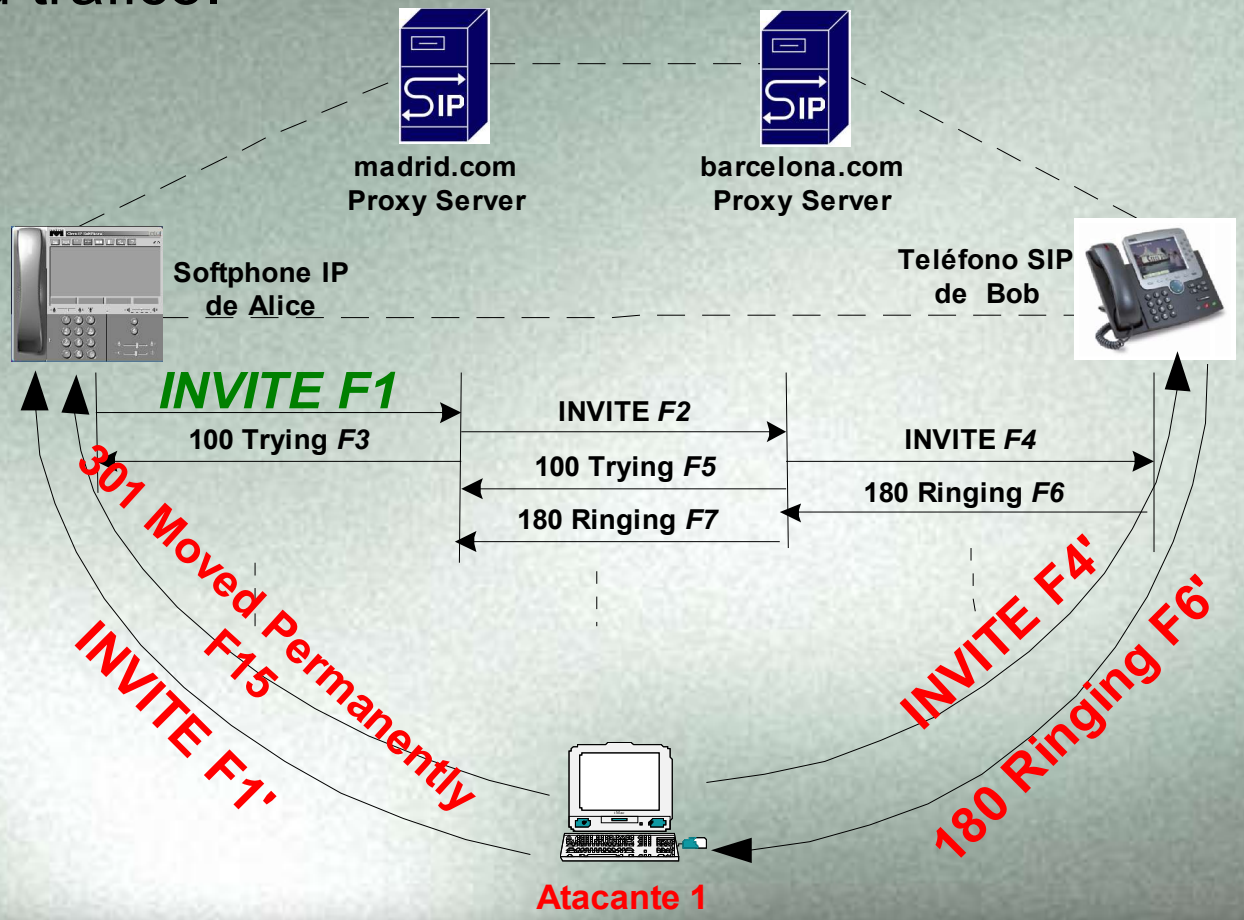
- Mediante mensajes *301 Moved Permanently*:

  Según el RFC 3261: “The user can no longer be found at the address in the Request-URI, and the requesting client SHOULD retry at the new address given by the Contact header field (Section 20.10). The requestor SHOULD update any local directories, address books, and user location caches with this new value and redirect future requests to the address(es) listed.”
- Sucede lo mismo con mensajes *302 Moved Temporarily* y *305 Use Proxy*.



Ataques de Captura/Reenvío (MITM)

- Mediante mensajes *301 Moved Permanently* además podemos hacer creer que Bob a cambiado de lugar, pero seguir enviando los mensajes de Alice a Bob para, haciendo de "proxy transparente" entre ambos, capturar todo su tráfico.



Ataques de Escuchas (RTP)

- Es fácil capturar el tráfico RTP que contiene la voz de los interlocutores que participan en la llamada.
- Los codecs/decodecs de audio están basados en estándares de uso habitual.
- Capturando un conjunto de paquetes RTP continuos podemos extraer el flujo de voz digitalizada, decodificarla y volverla a reproducir.
- Existe una implementación sencilla y eficiente, Open Source que realiza esto en sesiones H.323: VOMIT (Voice Over Misconfigured Internet Telephones).

Soluciones

- VoIP jamás se debe implementar en redes sin la suficiente segmentación lógico y físico.
- Los servidores VoIP (proxies, registrars, etc.) son tan sensibles a sufrir **intrusiones** como el servidor web de la empresa. Es necesario **securizarlos** y **gestionarlos.**
- El uso de VPNs y encriptación fuerte tendrán que ser “opciones por defecto”. SIP soporta S/MIME y PGP, pero debe configurarse y usarse. El inconvenientes es que incrementan los retardos y pueden impedir una comunicación fluida.
- Contar con **especialistas** en Telefonía IP y Seguridad a la hora de la implantación de VoIP.
- Y sobre todo, **auditar** las redes tras cambios y también de forma periódica, y **monitorizar** todos sus componentes y tráfico.

Entonces, ¿VoIP es seguro?

- VoIP es más seguro que una tarima de 1,50 metros en una oficina.
- La red de VoIP será tan segura como lo sea la red de datos.
- Si la red de datos ha sido auditada recientemente y han sido detectados y corregidos sus problemas, VoIP se aprovechará de estas mejoras.
- Si el esfuerzo necesario para obtener la información de una llamada VoIP es mayor que el valor intrínseco de la propia información, VoIP será “suficientemente seguro”.
- La seguridad es un equilibrio, que debe encontrarse.

Referencias

- Internet Engineering Task Force - Request For Comments (RFC):
  http://www.ietf.org/rfc/
- Sys-Security (Presentaciones de Ofir Arkin sobre VoIP):
  http://www.sys-security.com/
- VOMIT (Voice over misconfigured IP Telephones):
  http://vomit.xtdnet.nl/
- CISCO (documentación sobre VoIP y protocolos VoIP):
  http://www.cisco.com/
- SANS Institute (SANS InfoSec Reading Room):
  http://www.sans.org/rr/
- SIP Express Router (GNU SIP proxy):
  http://www.iptel.org/ser/
- SJPhone (SIP/H.323 Softphone para Windows/Linux/PocketPC):
  http://www.sjlabs.com/

WHITE HACK 2004

28-30 Mayo 2004

Seguridad en Redes Convergentes:

Seguridad en Voz sobre IP (VoIP)

Daniel Fernández Bleda

Internet Security Auditors

dfernandez@isecauditors.com

CISSP, OPST/OPSA Trainer

Co-Founder

www.isecauditors.com

Gracias por vuestra asistencia