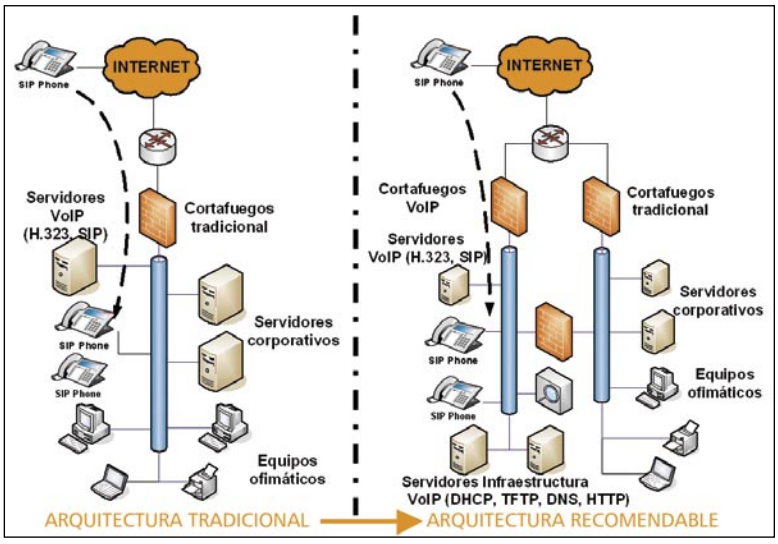
Despliegue con garantías de la tecnología VoIP

Dadas las ventajas de la tecnología VoIP, su despliegue en entornos empresariales está creciendo al tiempo que muchos operadores de telecomunicaciones empiezan a ofrecerla a sus clientes como un servicio de valor añadido. Para hacer un despliegue con garantías es necesario conocer el impacto de ésta en las redes y sistemas IP ya existentes y los problemas inherentes (no sólo de seguridad) de una tecnología que parece definida pero que en realidad está aún en evolución.

Javier Fernández-Sanguino

La tecnología de Voz sobre IP (VoIP) promete causar nuevos quebraderos de cabeza a los responsables de seguridad de las grandes organizaciones y los operadores, como ya ha pasado con algunas tecnologías "de moda", como las redes inalámbricas WiFi o la mensajería instantánea. El despliegue actual de la VoIP es aún reducido; sin embargo, muchos operadores de red están evaluándola o desplegándola para complementar su oferta de servicios de valor añadido asociados a la utilización de tecnologías de banda ancha. Al mismo tiempo, cada vez más organizaciones están considerando el sustituir sus sistemas analógicos de voz por sistemas VoIP.



Propuesta de arquitectura corporativa VoIP

Riesgos de una arquitectura VoIP

Los problemas de seguridad de esta tecnología no son nuevos y se vienen discutiendo desde hace algún tiempo **[1] [2] [3]**. Por resumir, los problemas típicos en un despliegue VoIP están asociados a:

– La confidencialidad: la capacidad de obtener información de las conversaciones realizadas a través de la red VoIP. Esto no incluye sólo la información del contenido de la llamada en sí; en algunos casos, puede incluso ser relevante la información estadística de las llamadas (quién llama a quién y durante cuánto tiempo).

– La integridad: la manipulación de conversaciones en curso a través de la inyección de tráfico, o la manipulación de los elementos de la red VoIP.

– La disponibilidad: la capacidad de interrumpir las comunicaciones VoIP e impedir el uso del servicio.

La capacidad de violar la confidencialidad **[4]** de las llamadas se evidencia porque los protocolos sugieren la utilización de mecanismos de cifrado de transporte (IPsec) en lugar de incorporar el cifrado en el propio protocolo (salvo en el caso de SRTP).

Existen múltiples formas de comprometer la confidencialidad de una comunicación, bien manipulando los dispositivos que forman la red que la transportan para acceder al tráfico cursado, o bien directamente manipulando el puerto físico al que están conectados éstos.

La tecnología de Voz sobre IP (VoIP) promete causar nuevos quebraderos de cabeza a los responsables de seguridad de las grandes organizaciones y los operadores, como ya ha pasado con algunas tecnologías "de moda", como las redes inalámbricas WiFi o la mensajería instantánea.

Los propios dispositivos finales también son susceptibles de ataque. Para identificar a otro dispositivo final VoIP basta con analizar el tráfico cuando se llama a la extensión o número final e identificar la dirección IP destino. Una vez obtenida la dirección IP se puede:

– Reconfigurar el equipo mediante alguno de los múltiples mecanismos de administración disponibles (HTTP, TFTP, SNMP o telnet) para que envíe el tráfico al atacante o, simplemente, para que envíe sus registros de actividad para determinar quién llama o a quién llama el dispositivo.

– Dejarlo sin servicio, para lo que existen múltiples ataques posibles: enviar respuestas DHCP falseadas, inundarle de paquetes, utilizar problemas de implementación de los protocolos, etc.

Estos ataques se pueden combinar. Por ejemplo, se puede forzar el reinicio de un equipo mediante ataques de denegación de servicio para, acto seguido, cambiar la configuración cuando éste arranque enviándole configuraciones manipuladas por TFTP.

La mayoría de los fabricantes de teléfonos IP diseñan sus mecanismos de gestión facilitando estos ataques. Así, los siguientes mecanismos de gestión son vulnerables:

– Servicio de administración vía web habilitado con contraseñas por defecto ('123', 'admin', etc.). Aunque disponga de una contraseña, al no estar cifrado y utilizar autenticación básica en muchos casos podría interceptarse ésta al utilizarse desde otro equipo.

– Mecanismos de descarga de nuevas versiones software que utilizan protocolos (TFTP o HTTP) o de acceso a red (DHCP o DNS) no cifrados y sin autenticación mutua, lo que permite ataques de suplantación e intercepción.

Más graves aún son los errores de implementación de los estándares publicados **[5]** que se observan en los dispositivos y con consecuencias en su seguridad, como demostró el proyecto PROTOS **[6]**, que dio lugar a la alerta del CERT/CC CA-2003-06 **[7]**. Más recientemente han surgido ataques similares.

Un usuario malicioso, haciéndose pasar por un teléfono, puede obtener a través del servidor DHCP información de la infraestructura de la red: servidor de TFTP utilizado para las descargas de configuraciones y software, localización del Gatekeeper, comunidad SNMP de acceso a los equipos y servidores SNMP autorizados, servidor de DNS y zona de DNS, etc. Los datos en particular dependerán de la tecnología que se esté utilizando. Una

vez identificados los distintos elementos de la infraestructura:

– A través del servidor de TFTP es posible obtener información adicional de la red como por ejemplo la dirección IP y puerto de los servidores HTTP utilizados para la descarga de actualizaciones de software (en el caso de existir), los códigos de acceso para marcar llamadas exteriores e internacionales dentro de una organización, etc. La información concreta facilitada de nuevo dependerá del fabricante.

– Accediendo o suplantando el servidor empleado para la descarga de configuraciones o nuevas versiones de software, ya sea TFTP o HTTP, será posible modificar todos los dispositivos que las utilicen.

– Accediendo o suplantando al servidor de DNS es posible redirigir el tráfico si los servicios se identifican por nombre (suplantar al Gatekeeper o al proxy SIP).

– Accediendo al Gatekeeper, proxy SIP o al SoftSwitch será posible obtener información detallada de las llamadas efectuadas e, incluso, obtener sus volcados. En el caso de un operador, el Softswitch dispone de toda la información de los abonados de la red y su facturación y es la puerta a otros servicios de la red (mensajería unificada, conferencia..).

Evidentemente, estos ataques a la infraestructura pueden tener otras consecuencias: la suplantación de personalidad (registro en la infraestructura con una extensión o número distinto del que uno puede utilizar), el fraude en llamadas (si existe interconexión con la red pública y tarificación asociada a esta interconexión) u otros ataques que pueden afectar gravemente a un negocio basado en este servicio.

Elementos de la arquitectura a asegurar

Es imprescindible, por tanto, asegurar los distintos elementos que forman parte de una arquitectura que ofrezca servicio de VoIP para evitar los ataques antes mencionados.

En el caso de los dispositivos finales, asegurando que no es posible configurarlos de forma remota, que se ha modificado la contraseña de acceso por omisión y que utilizan la última versión de *firmware* careciendo, por tanto, de vulnerabilidades conocidas. Si se trata de los elementos básicos de la arquitectura, deben estar correctamente configurados y bastionados para evitar intrusiones en los mismos. Deben, por tanto, revisarse los Gatekeeper, Softwitches o *proxies* SIP, y servidores de DNS, TFTP o HTTP utilizados. No se debe olvidar que muchas veces éstos se basan en sistemas operativos de propósito general[1].

Los dispositivos que gestionan el tráfico de la red deben estar protegidos frente a ataques, restringirse el uso de la administración remota y disponer de filtros para dificultar la suplantación de equipos finales. Finalmente, debe asegurarse que el tráfico del propio servicio no puede ser capturado con facilidad y ha de cifrarse para que no pueda ser reproducido aún en este caso.

CARACTERÍSTICAS	AcmePacket Net Session Director (SD)	Edgewater Networks EdgeProtect 5300 y 6400 SBC	NetRake nCite DE y nCite SE
Funcionalidades:	Seguridad, niveles de calidad (SLA) e interceptación legal de comunicaciones	Seguridad, niveles de calidad (SLA) e interceptación legal de comunicaciones	Seguridad, niveles de calidad (SLA) e interceptación legal de comunicaciones
Referencia	www.acmepacket.com	www.edgewaternetworks.com	www.netrake.com
RENDIMIENTO			
Throughput	5 Gbps	No publicado	No publicado
Latencia	15 microsegundos (datos) 5-10 microsegundos (señalización)	No publicado	Inferior a 31 microsegundos en carga máxima
Máximo número de sesiones concurrentes	32.000 (G. 729)	10.000 (G.711)	21.000 - 42.000 llamadas activas (G.729/20ms framing)
Alta disponibilidad	1+1 activo-pasivo	1+1	1+1 activo-activo

Características de los Gateways Controllers

VoIP está aún en desarrollo con protocolos en constante evolución, por lo que las organizaciones u operadoras que quieran desplegarla (o estén desplegándola ya) deberán pensar en cómo asegurar la confidencialidad de las llamadas con una arquitectura de cifrado sostenible y cómo garantizar la seguridad de los distintos elementos que conforman el servicio integral VoIP.

Problemas de despliegue y soluciones "tradicionales"

Existen varios elementos que afectan a la capacidad de despliegue de la VoIP: la necesidad de introducir nuevos elementos que den soporte a la infraestructura, los problemas de interoperabilidad de los protocolos de VoIP (que utilizan puertos dinámicos) con sistemas de filtrado tradicionales o barreras de NAT, la necesidad de cifrar el tráfico y la necesidad de asegurar una calidad de transporte de tráfico suficiente para garantizar que no exista *jitter* en las conversaciones (provocado por variaciones de retardo o latencia).

La solución tradicional consiste en utilizar los servidores corporativos existentes (de DHCP, DNS, TFTP, HTTP...) en lugar de introducir nuevos elementos, utilizando, muchas veces, la misma red de datos que usan otros equipos (p.ej., ofimáticos). Si es necesario conectar a los equipos a través de Internet se utilizan los dispositivos de filtrado para tratar los protocolos de señalización (SIP, H.323, MGCP), de flujo de media (RTP) y de control de la conversación (RTCP). Algunos cortafuegos existentes (como es el caso de PIX de Cisco, Firewall-1 de Check Point, o Netscreen de Juniper, entre otros) se han adaptado para poder gestionar estos protocolos de forma nativa. Si no se puede actualizar el software o no soporta los protocolos, entonces se deben "abrir" agujeros para garantizar que es posible recibir las llamadas entrantes desde el exterior. Para el cifrado se utilizan las redes privadas virtuales existentes o se introducen terminadores de túneles y, cuando surgen problemas de latencia, se intentan resolver incrementando el ancho de banda disponible.

Sin embargo, esta solución no tiene en cuenta que los sistemas de filtrado o cifrado impactan negativamente sobre la latencia y el retardo (porque tienen que modificar los paquetes o inspeccionarlos), no disponen de control de calidad de servicio y su comportamiento es "peor" para tráfico que está formado por paquetes de tamaño reducido. Las cifras de rendimiento que dan los fabricantes de cortafuegos tradicionales en sus especificaciones técnicas son sobre pruebas basadas en un tráfico más "manejable". Las pruebas realizadas por Germinus sobre sistemas de cortafuegos de alta gama dan un *throughput* en una línea de 100 Mbps saturada para paquetes pequeños (64 bytes) que es un 56% del observado para paquetes de gran tamaño (1518 bytes). Si el ancho de banda utilizado es mayor, entonces empiezan a aparecer pérdidas de tráfico significativas. Algunos estudios realizados sobre terminadores de túneles **[8]** muestran problemas similares con el tráfico VoIP.

[1] Por ejemplo, Cisco utiliza una versión de Windows en su Call Manager mientras que Avaya emplea una versión de GNU/Linux.

En instalaciones reducidas puede que no aparezcan estos problemas pero sí se evidencian cuando la instalación crece y el tráfico es mayor. Llegados a este punto los problemas que surgen no afectan sólo al servicio VoIP (pudiendo hacerlo incluso inviable) sino también a todo el tráfico que circula por estos sistemas, perjudicando a toda la organización. A continuación, y como se muestra en la figura, se discutirán algunas recomendaciones para una arquitectura escalable de servicio VoIP.

Recomendaciones de arquitectura

En primer lugar, es más que recomendable separar la red de voz y datos por lo menos con redes lógicas separadas (distintas VLANes, distinto direccionamiento) e introduciendo filtros para que sólo utilicen la red de tráfico los dispositivos autorizados, evitando así ataques "casuales". Deben introducirse sistemas de filtrado entre redes si es necesario conectar ambas, por ejemplo, para que los teléfonos accedan a un directorio corporativo o para utilizar servicios de mensajería instantánea.

Esta mejora de la seguridad introduce dificultades en su despliegue y hace más compleja la provisión: se necesitan dos puntos de red por puesto (para el teléfono y para el PC) y deben crearse VLANes adicionales. Para solventar esto existen teléfonos VoIP con dos conexiones de red, una se conecta al PC de sobremesa y otra a la red, que segmentan el tráfico en VLANes distintas a través de VLAN *tagging* (802.1q). Esta segmentación también limita la utilización de *softphones* (PCs con software VoIP) para acceder a la red VoIP.

En segundo lugar, para proteger a los teléfonos que deban recibir llamadas entrantes desde Internet se recomienda utilizar tecnologías alternativas a los sistemas tradicionales de cortafuegos y específicas para VoIP. Por ejemplo, puede ser mejor usar *Border Gateway Controllers* (o *Session Gateway Controllers)*, equipos especializados en protocolos VoIP y con características de seguridad (filtrado con inspección de estados), y control de calidad de servicio. Además ofrecen nativamente capacidades, obligatorias para los operadores, de interceptación legal de las comunicaciones **[9].** Entre los fabricantes de estos equipos se encuentran, por ejemplo, Acme Packet, Edgewater Networks o NetRake. Por otro lado, en una gama más baja, están los cortafuegos SIP como son los de Borderware, Ingate, e Interetex Data AB. Todos éstos ofrecen datos concretos de rendimiento aplicables a VoIP: *throughput*, número máximo de llamadas soportadas y la tasa máxima de establecimiento de llamadas. Además aseguran una latencia pequeña y, más importante, constante para el tráfico con un mayor nivel de integración con otros elementos de la arquitectura VoIP. En la tabla adjunta se muestran las características de los *Gateway Controllers* de gama alta.

Como desventaja cabe reseñar que estos dispositivos son de reciente aparición, por tanto, poco maduros, de empresas que aún no están consolidadas en el mercado, con poca presencia local y con una política de precios que puede no ajustarse a las necesidades reales de una organización.

Por último, deben introducirse sistemas de monitorización. Tanto para detectar ataques de cualquier tipo a la infraestructura de la red como para analizar el comportamiento de la misma (tráfico, dispositivos, nivel de llamadas, etc.) y poder anticiparse a posibles problemas de capacidad y escalabilidad.

Aunque pueda ser más tentador, y claramente más barato, utilizar las infraestructuras existentes puede no ser lo más recomendable a largo plazo, dadas las características específicas de este servicio. Así, habrá que analizar la capacidad de utilizar nuevas infraestructuras (y nuevos equipos) para garantizar el correcto funcionamiento de la red.

Así pues, uno debe estar dispuesto antes de entrar de lleno en un despliegue para probar concienzudamente las distintas alternativas y evaluar "en casa" los problemas de seguridad y la capacidad de escalabilidad de éstas para tomar la decisión más adecuada, obligando a los fabricantes o buscando asistencia externa en caso de no disponer de conocimiento propio.

Antes de entrar de lleno en un despliegue se debe estar dispuesto a probar concienzudamente las distintas alternativas y evaluar "en casa" los problemas de seguridad y la capacidad de escalabilidad de éstas para tomar la decisión más adecuada, obligando a los fabricantes o buscando asistencia externa en caso de no disponer de conocimiento propio.

Conclusiones

La tecnología VoIP está aún en desarrollo con protocolos en constante evolución, las organizaciones u operadoras que quieran desplegarla (o estén desplegándola ya) tienen que pensar que podrán estar utilizando una combinación de protocolos y que tendrán que dar soporte a todos ellos. Deberán pensar en cómo asegurar la confidencialidad de las llamadas con una arquitectura de cifrado sostenible y cómo garantizar la seguridad de los distintos elementos que conforman el servicio integral VoIP.

No vaya a ser que cuando pase uno de un entorno "de juguete" (que siempre funciona) a un entorno real, se encuentre con que su cabeza peligra porque el presidente de la compañía no puede recibir llamadas en una red saturada o porque un número significativo de usuarios de la red ha conseguido defraudar a la compañía haciendo pasar sus llamadas a la factura de otro. ■

Javier Fernández-Sanguino
División de Seguridad
GERMINUS
jfernandez@germinus.com

REFERENCIAS

[1] The Trivial Cisco IP Phones Compromise, Security analysis of the implications of deploying Cisco Systems' SIP-based IP Phones model 7960, Ofir Arkin, septiembre 2002.

[2] Security Considerations for Voice Over IP Systems, Recommendations of the National Institute of Standards and Technology, D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, NIST SP-800-58, enero 2005.

[3] Challenges in Securing Voice over IP, Thomas J. Walsh, D. Richard Kuhn, NIST, IEEE Security and Privacy vol 3 num 3, mayo-junio 2005.

[4] La inseguridad en plataformas VoIP, Pablo Carretero y Daniel Solís, SIC noviembre 2004, nº 62.

[5] SIP: Session Initiation Protocol, Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. y E. Schooler, RFC 3261, junio de 2002. Disponible en ftp://ftp.rfc-editor.org/in-notes/rfc3261.txt

[6] PROTOS (Security Testing of Protocol Implementations) Test-Suite: c07-sip, Universidad de Oulu, disponible en http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html

[7] CA-2003-06 Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP), CERT/CC, 21-2-2003, disponible en http://www.cert.org/advisories/CA-2003-06.html

[8] Performance and Security Analysis of SIP using IPsec, Thomas Bowen, John Haluska, Panayiotis Thermos y Steven Ungar, Telcordia Technologies. NIST, enero 2004.

[9] Council Resolution of 17 January 1995 on the lawful interception of telecommunications
Official Journal of the European Communities, noviembre 1996