# Seguridad del protocolo SIP en la VoIP

***Security of protocol SIP in the VoIP***

**Rodney del Valle Torres, María Luisa Herrera Corbelle**

Universidad de las Ciencias Informáticas

*rodneyvt@uci.cu*

**Resumen**

Este trabajo tiene como objetivo mejorar la seguridad del Protocolo de Inicio de Sesión (SIP) en la Voz sobre IP (VoIP). Para esto se presentan dos propuestas que tienen como línea fundamental el cifrado de este protocolo.

En el trabajo se abordan las características fundamentales del protocolo de señalización SIP y los mecanismos de establecimiento y liberación de una sesión en este. Se exponen además las principales características, propósitos, ventajas y desventajas que se obtienen con la implementación de las dos propuestas citadas anteriormente.

**Palabra Claves:** Protocolo, señalización**, s**eguridad

***Abstract***

*The objective of this paper is to improve the security of Session Initiation Protocol (SIP) in Voice over Internet Protocol (VoIP). For achieving this, two proposals are presented, aimed at ciphering this protocol.*

*Within this paper the principal characteristics of the signing protocol SIP are studied as well as the establishment mechanisms and the termination of a session on it. It is shown the main characteristics, purposes, advantages, disadvantages of the implementation of the two proposal already stated.*

***Key words:*** *protocol, signing, security.*

## Introducción

La VoIP es una de las tecnologías que está actualmente disponible en el mundo la cual consiste en la transmisión del tráfico de voz y video sobre una red IP. Esta permite que las llamadas telefónicas sean soportadas sobre la redes de datos existentes en lugar de utilizar líneas telefónicas tradicionales, lo cual ofrece muchos beneficios a los proveedores de servicios así como a los usuarios finales.

Muchas son las empresas que están dispuestas a adoptar la VoIP debido al ahorro que representa, siendo irrelevante la distancia y duración de las llamadas desde el punto de vista de los costos. Además ofrece mayor flexibilidad y movilidad a los usuarios, unificando su estructura de comunicación. También brinda la posibilidad de añadir nuevos servicios y funciones no disponibles con el servicio telefónico tradicional.

La VoIP utiliza diferentes protocolos para la señalización, siendo SIP uno de los más utilizados actualmente por las ventajas en cuanto a dispositivos y servicios que ofrece con respecto a los demás protocolos existentes. Usando SIP es posible implementar servicios telefónicos básicos y avanzados, además de soportar comunicaciones entre usuarios de redes IP y, con el empleo de pasarelas, entre usuarios de otras redes incluyendo terminales de la Red Telefónica Pública Conmutada (RTPC). El problema de su utilización está en que a pesar de las ventajas que este protocolo ofrece, hay que estar consciente de los riesgos que conlleva su uso, ya que posee grandes vulnerabilidades en cuanto a su seguridad y por tanto está propenso a diferentes ataques. Si bien este problema en la actualidad no preocupa demasiado al usuario, garantizar la seguridad en el entorno VoIP es clave.

Protocolo de Inicio de Sesión SIP (SIP).

El protocolo de señalización SIP se basa en el modelo cliente/servidor donde las sesiones son formadas por transacciones basadas en peticiones y respuestas. Funciona en combinación con otros protocolos con el fin de proporcionar servicios completos a los usuarios. Entre estos protocolos se encuentran el Protocolo en Tiempo Real (RTP) para intercambiar directamente el tráfico de audio/video una vez establecida la sesión, el Protocolo de Control en Tiempo Real (RTCP) que trabaja junto con RTP para informar sobre la calidad de servicio ofrecido por este último, y el Protocolo de Descripción de Sesión (SDP) para describir el contenido multimedia de las sesiones. Sin embargo, a pesar de trabajar en sintonía con estos protocolos, la funcionalidad básica y el funcionamiento de SIP no dependen de ninguno de estos protocolos.

SIP es un protocolo de nivel de aplicación independiente de las capas de transporte y de red, por lo que puede hacer uso tanto de un nivel de transporte TCP, como UDP, aunque las implementaciones más comunes usan SIP sobre UDP por su simplicidad y velocidad con respecto a TCP. En la figura 1 se muestran varios de dichos protocolos anteriormente citados.

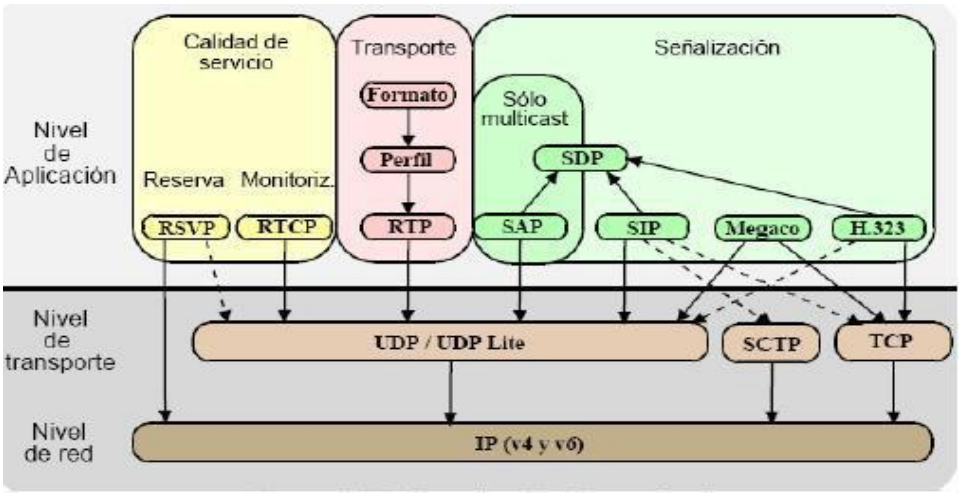


Fig. 1 SIP y demás protocolos.

Estructura del mensaje SIP.

El protocolo SIP define dos tipos de mensajes: petición y respuesta. El mensaje de petición es emitido desde el cliente terminal al servidor terminal. El encabezado del mensaje de petición y respuesta contiene campos similares:

- *Star Line*: se usa para indicar el tipo de paquete, la dirección y la versión de SIP.
- *General Header*: el encabezamiento general contiene informaciones como:
  - *Call-ID*: se genera en cada llamada para identificarla. Contiene la dirección del dominio de host.
  - *Cseq*: se inicia en un número aleatorio e identifica en forma secuencial a cada petición.
  - *From*: es la dirección del orígen de la llamada y se encuentra presente en toda petición y respuesta.
  - *To*: es la dirección del destino de la llamada y se encuentra presente en toda petición y respuesta.
  - *Vía*: sirve para recordar la ruta de petición, por eso cada Proxy en la ruta añade una línea de vía.
- *Additionals*: además del encabezado general pueden transportarse campos adicionales, por ejemplo, *Expire* que indica el tiempo de validez del registro y *Priority* que indica la prioridad del mensaje.

Las figuras 2 y 3 muestran ejemplos de mensajes de petición y respuestas SIP. En ellas se puede ver como está estructurado y compuesto el mensaje SIP, además de los parámetros que contiene.


Fig. 2 Ejemplo de un mensaje de petición SIP.


Fig. 3 Ejemplo de un mensaje de respuesta SIP.

Establecimiento y liberación de una sesión SIP.

En el flujo habitual de establecimiento de una sesión SIP el usuario ingresa la dirección lógica de la persona con la que quiere comunicarse, además de que puede indicar al terminal las características de la sesión que quiere establecer (voz, video, etc.), o estas pueden estar implícitas por el tipo de terminal del que se trate. El agente usuario SIP que reside en el terminal, actuando como agente usuario cliente envía la petición (en este caso con el método INVITE) al servidor que tiene configurado. Este servidor se vale del sistema DNS para determinar la dirección del servidor SIP del dominio del destinatario (el dominio lo conoce pues es parte de la dirección lógica del destinatario). Una vez obtenida la dirección del servidor del dominio destino, encamina hacia allí la petición.

El servidor del dominio destino establece que la petición es para un usuario de su dominio y entonces se vale de la información de registro de dicho usuario para establecer su ubicación física. Si la encuentra, entonces encamina la petición hacia dicha dirección, mientras le envía al servidor origen un mensaje de que lo esta intentando 100 (Trying). El agente usuario destino si se encuentra desocupado enviara señales de tono con el código 180 (Ringing) hasta llegar al agente usuario origen. Cuando el usuario destino finalmente acepta la invitación, se genera una respuesta de 200(OK) que indica que la petición fue aceptada. La recepción de la respuesta final es confirmada por el agente usuario cliente origen mediante una petición con el método ACK. Esta petición no genera respuestas y completa la transacción de establecimiento de la sesión.

Durante el proceso de inicio de sesión, llega un momento en el que ambos teléfonos se comunican directamente, sin pasar por el proxy ya que han aprendido las rutas gracias a los encabezados de los mensajes SIP. Después comienza la comunicación y la transferencia de información hasta que alguna de las parte decida colgar el teléfono. La parte que decida finalizar la comunicación manda un mensaje BYE al otro agente usuario. El otro agente usuario envía un reconocimiento del mensaje BYE (200 OK) y la sesión se da por terminada. En la figura 4 se muestra el establecimiento y liberación de una sesión SIP.

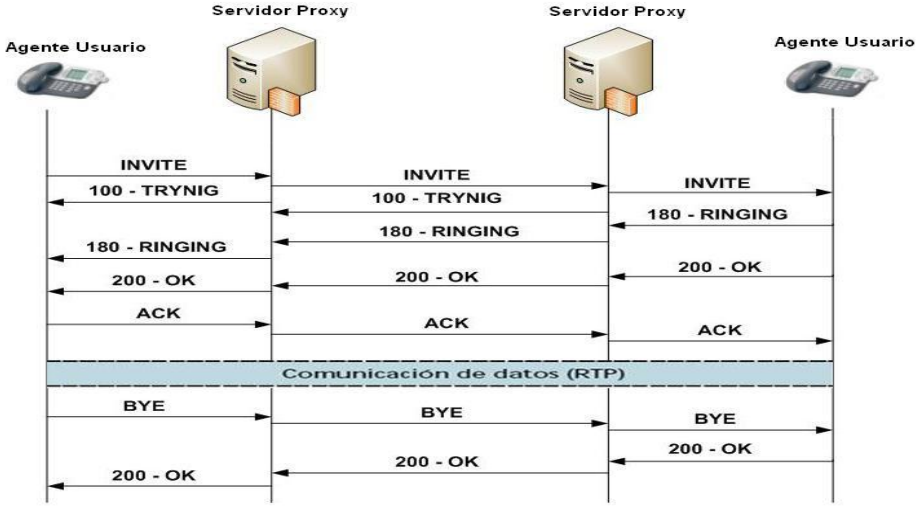


Fig. 4 Establecimiento y liberación de una sesión SIP.

## Propuestas de seguridad para el protocolo SIP

La seguridad del protocolo SIP es un aspecto fundamental a la hora de establecer y finalizar una sesión. A continuación se presentan dos propuestas para mejorar dicha seguridad ya sea para la comunicación de terminal a terminal, como de proxy SIP a proxy SIP. Ambas propuestas tienen en común el algoritmo criptográfico y el lenguaje de programación.

- Algoritmo criptográfico seleccionado.

El algoritmo criptográfico que se propone para garantizar la seguridad del protocolo SIP es el AES. El mismo fue escogido principalmente por ser un algoritmo simétrico siendo el proceso de encriptar/desencriptar mucho más rápido que en los asimétricos. El detalle anterior se ha tenido en cuenta ya que la VoIP requiere una alta inmediatez.

En comparación con su predecesor DES, el AES es rápido tanto en software como en hardware y requiere poca memoria para efectuar el proceso de encriptar/desencriptar. También proporciona mayor rapidez y menor costo computacional que el 3DES, pudiendo ser implementado en equipos con bajo requerimiento de memoria como puede ser un teléfono VoIP. Es un cifrado por bloques no una red de sustitución/permutación. Como nuevo estándar de cifrado, se está utilizando actualmente a gran escala, es decir es uno de los más potentes y más utilizados a nivel mundial, por su gran seguridad y estabilidad.

Una de las ventajas que presenta el algoritmo AES con respecto a otros algoritmos simétricos es la longitud de la clave con niveles de seguridad de 128, 192 y 256 bits, dependiendo la fortaleza del sistema de la longitud de dicha clave.

Una desventaja del uso de este algoritmo no está asociada a su seguridad sino a la hora de distribuir la llave secreta, pues como es un algoritmo simétrico, es la misma para encriptar/desencriptar. Debido a esto no se debe utilizar la variante de intercambiar la llave por la red ya que un atacante puede interceptarla y así obtener el texto claro. Para resolver este problema el administrador de la red debe insertar la llave manualmente en cada uno de los dispositivos que hagan uso de dicho algoritmo criptográfico propuesto. En caso de que en algunos de los dispositivos se cambie dicha clave se debe actualizar con esta a los demás.

- Lenguaje de programación seleccionado.

El lenguaje de programación que se propone a utilizar para la realización de la aplicación es C debido a las ventajas que presenta en comparación con otros lenguajes, como es su versatilidad. Además C puede compilar el código para varios sistemas operativos haciendo la aplicación multiplataforma y ofrece el acceso a memoria de bajo nivel mediante el uso de punteros.

Este lenguaje presenta otras ventajas como el hecho de que no requiere de ningún software adicional para ser ejecutado, pues otros como el código de C# requiere el framework de .NET y Java requiere la maquina virtual. Se pudiera usar otros como Delphy o Turbo Pascal pero C es mas orientado al trabajo con el hardware.

### Propuesta 1: Seguridad del protocolo SIP de terminal a terminal desde el inicio hasta la finalización de la sesión.

El objetivo de esta propuesta es tratar de lograr la máxima seguridad posible desde el establecimiento hasta la finalización de una sesión SIP. Esta seguridad estaría presente tanto para el terminal que quiera establecer una sesión con otra terminal dentro de una misma red como para el que se encuentre fuera de ella.

Para lograr lo expuesto anteriormente, se propone realizar una aplicación implementada en C que va a contener además del algoritmo criptográfico simétrico AES, otras funcionalidades como la de agregarle al protocolo SIP un identificador de tres

caracteres formado cada uno por 8 bits. Este identificador se utilizaría como prefijo del protocolo SIP cada vez que sea encriptado y se encontraría en un fichero de almacenamiento en la aplicación.

La aplicación estaría ejecutándose en cada servidor SIP, ya sea proxy, de registro, de redireccionamiento o de localización. Esta estaría escuchando por un puerto diferente al 5060, que sería el mismo que utilizaría dicha aplicación en los restantes elementos de la arquitectura SIP para comunicarse entre sí. La comunicación de la aplicación con el servicio SIP en los servidores y terminales sería por el puerto 5060 que es el nativo para este protocolo. En la aplicación se tendría un registro de las terminales que tengan activado o no el modo seguro, estando inicialmente todas en modo inseguro (este sólo se cambiaría cuando en la aplicación terminal sea activado el modo seguro).

La aplicación al recibir un mensaje SIP verificaría si está encriptado o no, comparando los primeros tres caracteres con el identificador que tiene almacenado. Si la comparación es válida desencriptaría a partir del bit 24 y pasaría el mensaje desencriptado al servidor SIP. En caso de que no fuera válida, entonces esta verificaría el modo en que se encuentra el emisor que si está en modo inseguro lo tomaría como texto claro y si no el mensaje no sería compatible con el formato esperado por lo que se desecharía.

En el momento en que el servidor envía un mensaje, este pasaría por la aplicación la cual verificaría si el destino es seguro o no. De esta forma se crearía una condición en esta para que todos los mensajes de respuesta por parte del servidor SIP a las terminales que estén en modo inseguro se le envíen sin encriptar y en caso de estar en modo seguro encriptados.

En el caso de las terminales, si es una PC la aplicación se ejecutaría cuando se ejecute el softphone (para esto sería necesario modificar el código del mismo). La aplicación utilizaría el mismo puerto de escucha de la aplicación en los servidores, y el puerto 5060 para comunicarse con el softphone. Esta aplicación si está en modo seguro encriptaría los mensajes salientes y desencriptaría los entrantes. Para esto brindaría la opción de que sea activado o no dicho modo, teniendo una funcionalidad que le avisaría a la aplicación servidora el estado de activación.

Si el terminal es un teléfono IP se propone el uso de SIPSEC, mostrado en la figura 5, que es un dispositivo compuesto por un par de conectores RJ-45 hembra (entrada y salida) por donde deben fluir los datos, además de un microcontrolador capaz de entender el flujo Ethernet en el que estaría implementada la aplicación. La función de avisar al servidor de que es un medio seguro, sería cuando se conectara el dispositivo a la red, y en caso de que se deje de usar SIPSEC, el usuario no podría comunicarse.

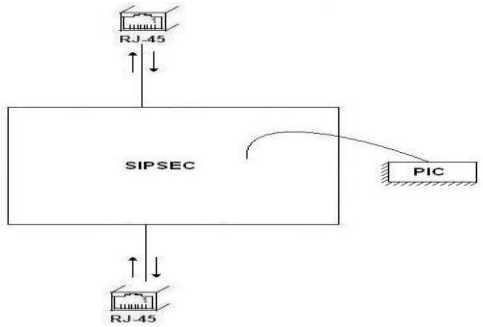


Fig. 5 SIPSEC.

En el momento que se establece la sesión SIP entre las terminales, los participantes de la sesión intercambiarán directamente su tráfico de audio/video a través del protocolo RTP. Para brindarle seguridad al protocolo RTP se propone el uso de SRTP, el cual

es un perfil del protocolo RTP que es capaz de proporcionar autenticación mediante cifrado, además de confidencialidad, integridad y no repudio tanto para los mensajes de RTP como para los de RTCP. Este protocolo consigue una mayor calidad de servicio en una conexión VoIP, una menor sobrecarga, manteniendo la eficiencia de compresión de la cabecera RTP. También proporciona alta tolerancia a la pérdida de paquetes y reordenación, presentando un sistema de cifrado robusto.

En la figura 6 se muestra un diagrama de flujo que describe los procesos que se realizarían desde la llegada del mensaje hasta su envío en cualquier elemento de la arquitectura SIP propuesta.

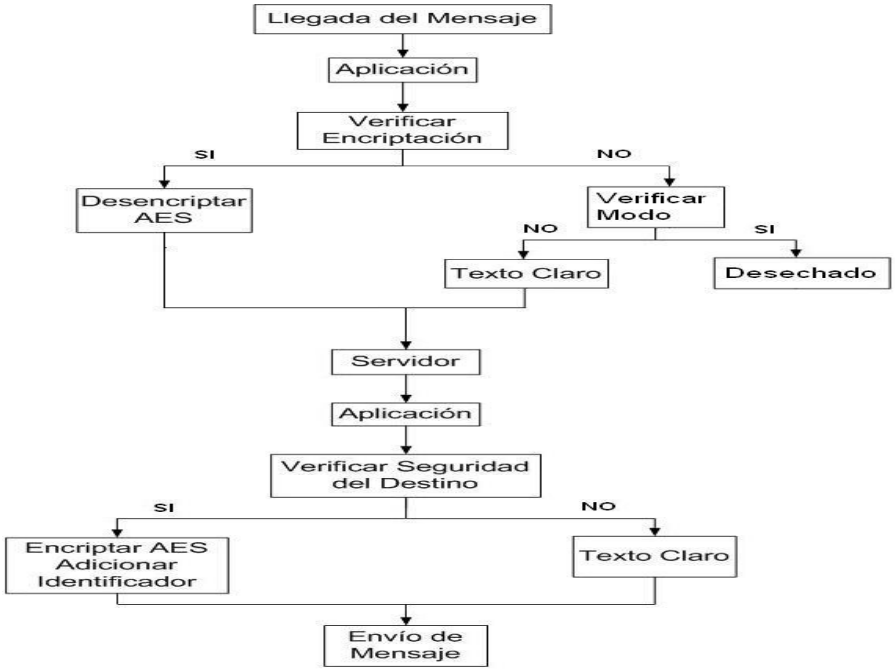


Fig. 6 Diagrama del flujo del mensaje en un servidor con la aplicación ejecutándose.

En la figura 7 se muestra el diseño de una arquitectura SIP protegida basada en lo propuesto anteriormente.

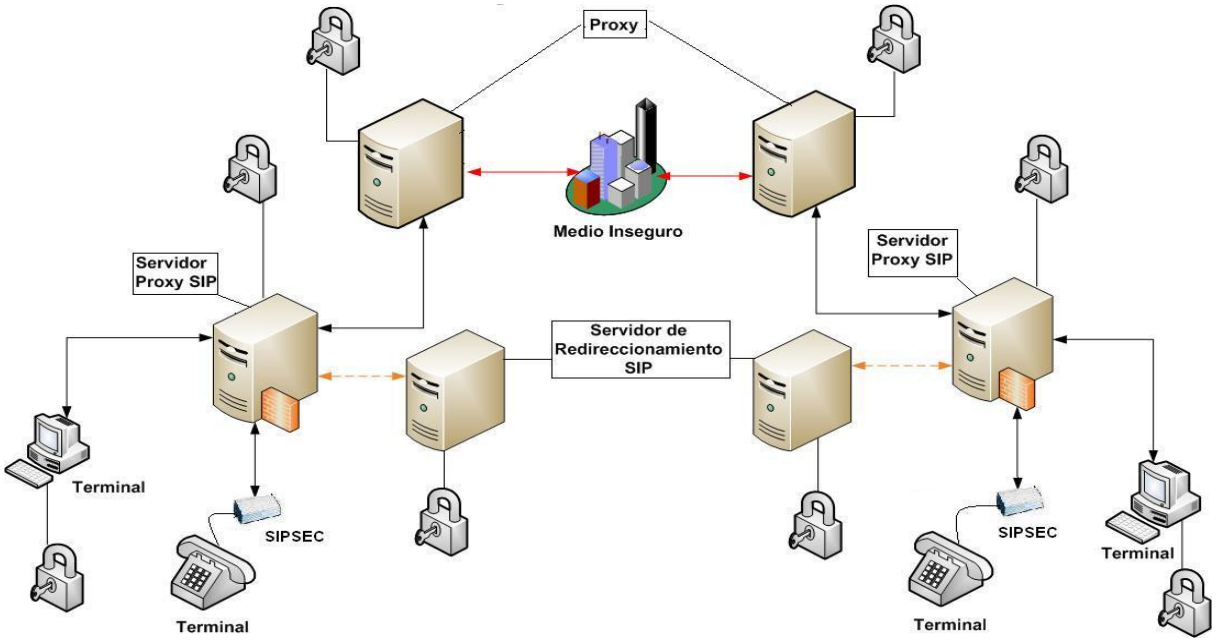


Fig. 7 Seguridad establecida de terminal a terminal para redes SIP.

Esta propuesta ofrece las siguientes ventajas:

- Los mensajes no viajarían en ningún momento en texto claro, ni dentro ni fuera de la red SIP. Esto proporciona que en todo momento el proceso de señalización sea seguro, evitando la eficacia de los ataques por parte de cualquier intruso fuera o dentro de la red.

- Permite procesar los mensajes SIP provenientes de las terminales PC, tanto con su identificador como sin él.

- En las terminales PC le brinda al usuario la opción de escoger un medio seguro o no, en el momento de enviar o recibir un mensaje SIP.

La desventaja que presenta esta propuesta es que en el caso de los teléfonos IP, si se desconectara SIPSEC, el usuario no podría comunicarse.

Propuesta 2: Seguridad del protocolo SIP en la red externa

El objetivo de esta propuesta es garantizar la seguridad del protocolo SIP en el momento que el mensaje es enviado fuera de su red. Dentro de la red interna estaría viajando en texto claro y solo se le daría seguridad al salir al medio externo.

Para lograr lo anteriormente planteado, se propone realizar una aplicación implementada en C que va a contener además del algoritmo criptográfico simétrico AES, otras funcionalidades, como la de agregarle al protocolo SIP un identificador de tres caracteres formado cada uno por 8 bits. Este identificador se utilizaría como prefijo del protocolo SIP cada vez que sea encriptado y se encontrarían en un fichero de almacenamiento en la aplicación (igual que la Propuesta 1). Esta aplicación estaría ejecutándose solamente en el último elemento físico de la arquitectura SIP.

Al llegar un mensaje al último servidor SIP de la red interna, la aplicación verificaría si está encriptado o no, comparando los primeros tres caracteres con el identificador que tiene almacenado. Si la comparación es válida desencriptaría a partir del bit 24, y pasaría el mensaje desencriptado al servidor para que este lo procese y si no es válida se le aplicaría la política de seguridad al mensaje que consiste en verificar su origen. Si el mensaje proviene de una red interna este se procesaría, y en caso de una red externa este se desecharía.

En el momento de enviar un mensaje, la aplicación ejecutándose en el último servidor SIP de la red interna verificaría el destino, para saber si será encriptado o no. Si el mensaje va para la red interna no sería encriptado y en caso de ir a la red externa entonces este se enviaría encriptado.
En la figura 8 se muestra la arquitectura SIP estando protegido el mensaje al salir a una red externa pero viajando en texto claro dentro de la red interna.

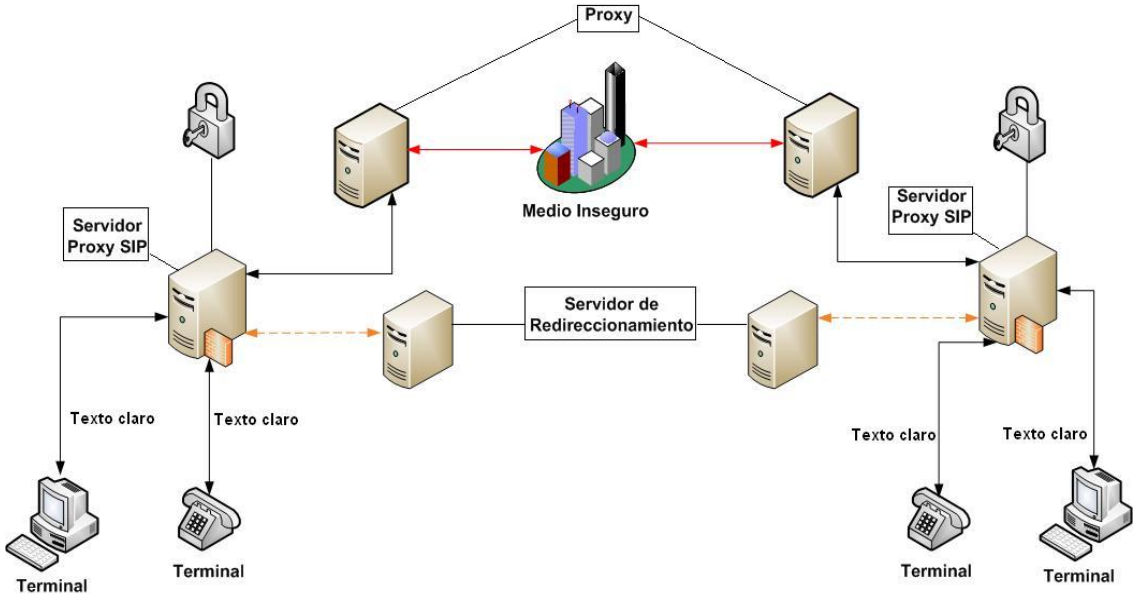


Fig. 8 Seguridad establecida de Proxy SIP a Proxy SIP.

Esta propuesta ofrece las siguientes ventajas:

- El mensaje SIP viajaría encriptado por la red externa asegurándose el contenido de cada mensaje al salir al medio exterior.
- La no implementación de SIPSEC comparado con la Propuesta 1

La desventaja que presenta esta propuesta es que dentro de la red interna los mensajes viajarán en texto claro dándole la posibilidad a un atacante de realizar cualquier ataque dentro de la red y obtener así el contenido del paquete.

## Conclusiones

Con la realización de este trabajo se debe destacar que:

- La VoIP es una tecnología que ofrece un conjunto de ventajas y servicios para la comunicación a través de redes IP. Para esto utiliza diferentes protocolos, donde su seguridad depende en gran medida de la seguridad de estos.
- SIP, el cual es uno de los protocolos de señalización que utiliza la VoIP debido a su flexibilidad y ventajas, además de los servicios que este proporciona, es uno de los protocolos más difundidos a nivel mundial. Debido a esto, la seguridad del mismo es de gran importancia por ser el objetivo de muchos tipos de ataques.
- De acuerdo a la seguridad que se quiera brindar se escogería una u otra propuesta, debido a que:

  - La propuesta 1 tiene como objetivo la integridad de los mensajes SIP en toda su trayectoria, es decir, de extremo a extremo en la comunicación SIP. Esta presenta como desventaja la complejidad en la construcción de SIPSEC.

- La propuesta 2 tiene el objetivo de asegurar la integridad de los mensajes SIP pero solo entre servidores SIP (mensaje cifrado sólo en la red externa). Tiene como desventaja que los mensajes viajarían en texto claro en el intercambio de información entre terminal y servidor SIP (red interna).

**Referencias Bibliográficas**


- **Castañeda, Rodolfo.** Protocolos para voz IP. *Protocolos para voz IP*. [Online] 2005. [Cited: Abril 05, 2008.] http://www.cudi.edu.mx/primavera_2005/presentaciones/rodolfo_castaneda.pdf.

- **Francois Bounoure, Anibal Coppo, Diego Csernoch, Bruno Pravisani, Daniel Serrano.** SIP SESSION INITIATION PROTOCOL. *SIP SESSION INITIATION PROTOCOL*. [Online] Diciembre 2006. [Cited: Marzo 20, 2008.] http://www.fiuba6662.com.ar/6648/presentaciones/2006/Informe%20SIP.pdf.

- **Pouzols, Federico Montesino.** SIP: Sesion Initiation Protocol. *SIP: Sesion Initiation Protocol*. [Online] Mayo 2003. [Cited: Marzo 25, 2008.] www.rediris.es/mmedia/gt/gt2003_1/sip-gt2003.pdf .

- **Seguridad en SIP - Session Initiation Protocol.** ***Seguridad en SIP - Session Initiation Protocol***. [Online] Mayo 26, 2006. [Cited: Abril 10, 2008.] www.eslomas.com/index.php/archives/2006/05/26/seguridad-en-sip-session-initiation-protocol.

- **Simon Znaty, Jean-Louis Dauphin , Roland Geldwerth.** SIP : Session Initiation Protocol. *SIP : Session Initiation Protocol*. [Online] 2005. [Cited: Marzo 25, 2008.] http://www.efort.com.

- **Tobias Glemser, Reto Lorenz.** Seguridad en la Voz sobre IP – Protocolos SIP y RTP. *Seguridad en la Voz sobre IP – Protocolos SIP y RTP*. [Online] Marzo 2005. [Cited: Marzo 03, 2008.] www.compuven.net/Contenidos/Revistas/Hakin9/Hakin9-Seguridad-VoIP-Protocolos-SIP-y-RTP.pdf.

- **Vázquez, Miguel Fernández.** Algoritmo Criptográfico AES para protección de datos. *Algoritmo Criptográfico AES para protección de datos.* [Online] Septiembre 2007. www.iit.upcomillas.es/pfc/resumenes/46ea7511774d8.pdf.