Científica, vol.19, núm. 2, pp. 47-51, julio-diciembre 2015.
ISSN 1665-0654, ESIME Instituto Politécnico Nacional México

Sistema de video llamadas seguras empleando una PBX-Asterisk

Rafael **Soria-Vargas**
Marco Antonio **Acevedo-Mosqueda**
Jaime **Hernández-Castillo**
Miguel **Sánchez-Meraz**

Instituto Politécnico Nacional,
Sección de Estudios de Posgrado e Investigación,
Escuela Superior de Ingeniería Mecánica y Eléctrica.
Edificio Z-4 3er Piso, Col. Lindavista,
Del. Gustavo A. Madero, CP 07738, Ciudad de México. MÉXICO.
Tel. 57296000 ext. 54757

correo electrónico (email): raphacujae@gmail.com
marcoantonio.acevedo@gmail.com
jhdezc_01@hotmail.com
miguel_sm7008@yahoo.com.mx

Recibido 13-11-2014, aceptado 15-03-2015.

Resumen

En el mercado internacional existen diversos proveedores de telefonía de VoIP, sin embargo, muchos carecen de seguridad en sus servicios. La mayoría de ellos se vende por la capacidad que tienen para realizar comunicaciones telefónicas a través de internet, pero casi ninguno proporciona una comunicación segura. La privacidad y confidencialidad de las conversaciones telefónicas son los principales atributos que presenta este proyecto de investigación, utilizando un sistema de comunicaciones de VoIP implementado en una PBX-Asterisk. El sistema se conforma por una centralita Asterisk en la versión 11.6, montado sobre un sistema operativo de Linux llamado Centos en la versión 6. Se implementó el servicio de videollamadas seguras entre extensiones. El protocolo de señalización utilizado para la VoIP fue el *Session Initiation Protocol* (SIP) y para la seguridad se empleó el *Secure Real-time Transport Protocol* (SRTP) o protocolo seguro de transporte en tiempo real.

Palabras clave: Astersik, internet, seguridad, voz sobre IP, tiempo real.

Abstract
(Secure Video Call System Using Asterisk PBX)

In the international market there are various VoIP telephony providers, but many lack confidence in their services. Most of them sold the ability to make phone calls via internet communications, but almost none provide secure communication. Privacy, confidentiality of telephone conversations are the main attributes having this research project using a VoIP communications system implemented in a PBX-Asterisk. The system is made up of an Asterisk PBX in version 11.6, mounted on an operating system called Linux Centos version 6. Video service, secure calls between extensions was implemented. The signaling protocol used for VoIP was the Session Initiation Protocol (SIP) and security Secure Real-time Transport Protocol (SRTP) or Transport Protocol Secure Real Time was used.

Key words: Asterisk, internet, security, voice over IP, real time.

1. Introducción

La necesidad de realizar comunicaciones seguras por internet ha inspirado la conformación de un proyecto de investigación que satisfaga dichas necesidades elementales de los usuarios. Mediante este artículo se muestra cómo se pueden suplir dichas necesidades implementando un *sistema de videollamadas seguras*. Dicho sistema está conformado por tecnologías libres, lo que le da al proyecto la completamente libertad de la utilización de software como Linux que es la base para la obtención de los resultados que se presentan.

2. Desarrollo

El sistema de comunicaciones que se presenta está conformado por la centralita PBX-Asterisk que corre sobre un sistema operativo de Linux. A grande rasgos, se utiliza un servidor Asterisk y diversos softphones de escritorio o aplicaciones móviles comerciales. La PBX-Asterisk se instalará en un servidor que será quien atienda las llamadas realiza-

das por los usuarios, ya sea desde una aplicación móvil o una aplicación de escritorio. Estos usuarios pueden conectarse utilizando una *Red Fast Ethernet*, WiFi o en una red de servicios móviles con tecnologías como 3G y LTE; la idea es que se encuentren utilizando alguna tecnología que permita el acceso a la IP del servidor de VoIP. La figura 1 muestra con más detalles el sistema VoIP.

De la figura 1 se desglosa que los requerimientos para que funcione el diseño propuesto son:

- Un servidor de VoIP Asterisk
- Una conexión a internet
- Equipos terminales

En cuanto al servidor Asterisk, se seleccionó la versión 11.6, ya que forma parte del conjunto de versiones de Asterisk que son estables y que tienen programados soportes técnicos a largo plazo. El sistema operativo seleccionado para instalar Asterisk fue la distribución de Linux Centos 6.0. Después de varias pruebas en diferentes sistemas, en Centos se logró el mejor funcionamiento del servicio. El servidor Asterisk es compatible con la mayoría de los protocolos de señalización como H.323, IAX y SIP. En el caso particular del diseño se empleó señalización SIP. Esta es utilizada para que el origen y el destino de una llamada VoIP puedan aprender unos de otros sobre la dirección de red y el puerto, esto permite la

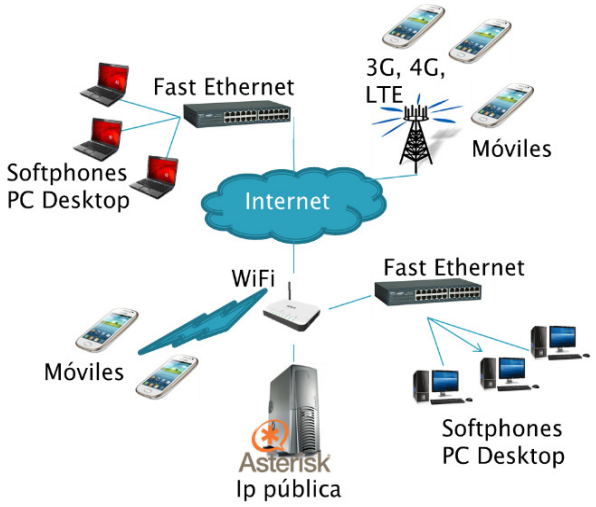

Fig. 1. Mapa del sistema VoIP.

negociación de los protocolos, servicios y formatos a utilizar para la conexión de medios de comunicación [1].

El servidor Asterisk cuenta con un conjunto de parches que hacen funcionar el sistema. Dichas aplicaciones extras fueron seleccionadas ya que el software de Asterisk carecía de determinadas funciones necesarias para los objetivos propuestos, tal es el caso de la función de cifrado de la voz mediante el SRTP y en particular los códecs de audio Speex, Vp8 y Opus. Cabe señalar que la selección de Speex como códec de audio se debió a que muchos de las aplicaciones clientes probadas utilizaban dicho códec. Además, la mejor calidad de audio experimentada se presentó usando el códec Speex. En cuanto al VP8 destacar que es un códec de video con mucha documentación, perteneciente a google, por lo que tiene un largo soporte.

Servicio con los que cuenta el sistema

El sistema está conformado por tres servicios, uno principal y dos secundarios:

Servicio principal

- Comunicación de voz cifrada.
- Comunicación de voz y video cifrado.

En cuanto al servicio principal, la voz cifrada, se utilizó SRTP para proporcionar seguridad en las comunicaciones. Este servicio se pudo probar ejecutando el software Wireshark, se evidencia claramente que la voz ha sido cifrada, puesto que al tratar de capturar la llamada, solo se escucha ruido. A modo de comparación se exhibirán varias figuras donde se ponen de manifiestos las diferencias entre una comunicación cifrada y una en claro. La figura 2 muestra una llamada SIP de VoIP sin cifrar.

Luego de enviar los INVITE, se transmiten los tonos de timbre atrás o lo que es lo mismo, los mensajes RINGING para notificar que se está estableciendo la llamada y que hay tono de timbre. Además se envía un mensaje de OK en conjunto con la descripción del códec que se usará [2]. En este caso se notifica que el códec a utilizar será el g711u. A este mensaje se le responde con un ACK o mensaje de reconocimiento de que ha llegado bien la información y que se puede enviar el audio a partir de este punto. Como se ve luego del ACK se envía el audio embebido en el protocolo RTP o protocolo de tiempo real y como se puede ver, exactamente se ha utilizado el códec

Fig. 2. Llamada en claro.

g711u como se había descrito en el SDP. Una vez que se ha finalizado la conversación uno de los *peers*, envía un mensaje de BYE para completar la fase de finalización de llamada a lo que se le responde con un OK y se cierra el audio [2]. En esta imagen se destaca que no se ha utilizado seguridad, evidentemente el audio no ha sido cifrado y viaja en claro en el protocolo RTP.

La figura 3 muestra la llamada SIP de VoIP pero utilizando el cifrado. En esta llamada se ha utilizado el protocolo SRTP o protocolo de tiempo real seguro que encripta el mensaje de audio para ser transmitido.

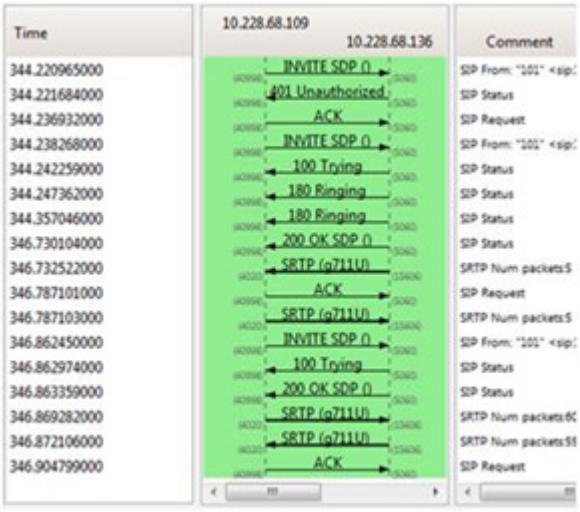

Fig. 3. Llamada cifrada.

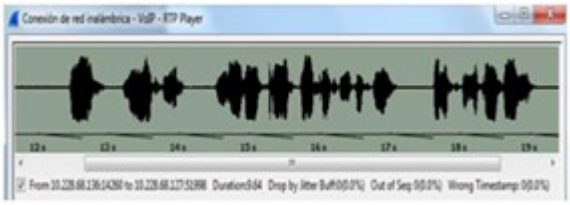

Fig. 4. Captura del audio en claro.

Como se puede apreciar al igual que en la figura 2, se comienza el establecimiento de la llamada con los mensajes de INVITE. Este mensaje sólo es usado para identificar de los participantes: el que llama y el que recibe la llamada, se envía un Unauthorized como respuesta lo que significa que se le está solicitando al peer que inicio la llamada que se autentifique para poder establecer la comunicación. A esta petición se responde con un ACK y luego se envían un INVITE con la autenticación y la descripción de la sesión y se le responde con un ACK, Luego se envía nuevamente el INVITE y se responde con un TRYING para notificar que se está intentando el establecimiento y acto seguido se envían dos mensajes de RINGING notificando timbre o tono. Además, se transmite un mensaje de OK, para decir que se ha aceptado la llamada [3] y se comienza a enviar el audio utilizando el códec g711u. La diferencia entre lo que se muestra en esta figura 3 y la anterior figura 2 es que el audio aquí va dentro del protocolo SRTP, por lo que la llamada se está realizando a un nivel que su audio ha sido cifrado.

Si atacáramos el sistema con una aplicación que detectara la llamada de VoIP, el resultado de capturar los paquetes de la llamada no cifrada sería el que se muestra en la figura 4. Si hiciéramos lo mismo a la llamada que ha sido cifrada entonces obtendríamos una señal con ruido como se muestra figura 5.

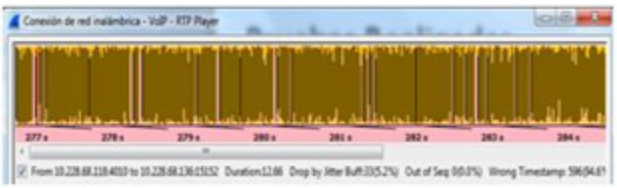

Fig. 5. Captura del audio en claro.

En la figura 4 claramente se ve la forma de onda de un archivo de audio y es perfectamente escuchable.

De la figura 5 es evidente que no se puede definir la forma de onda de los paquetes capturados y si se reprodujera dichos paquetes solo se escucharía ruido.

Para las llamadas de video cifrado también se hicieron pruebas las que arrojaron la siguiente imagen. En la figura 6 no se ha puesto todos los mensajes desde el establecimiento hasta la finalización de llamadas, solo se ha puesto el envío de los datos de audio y video a modo de que se pueda ver como se han cifrado ambas cosas. Podemos determinar que estamos en presencia de una comunicación de video cifrada, porque en la figura se muestra claramente el uso del códec de video VP8, este códec, esta embebido dentro del protocolo SRTP. También se muestra como se envían mensajes de audio. Dichos mensajes son codificados utilizando el códec opus y se ve en la figura cómo también viajan dentro del protocolo SRTP.

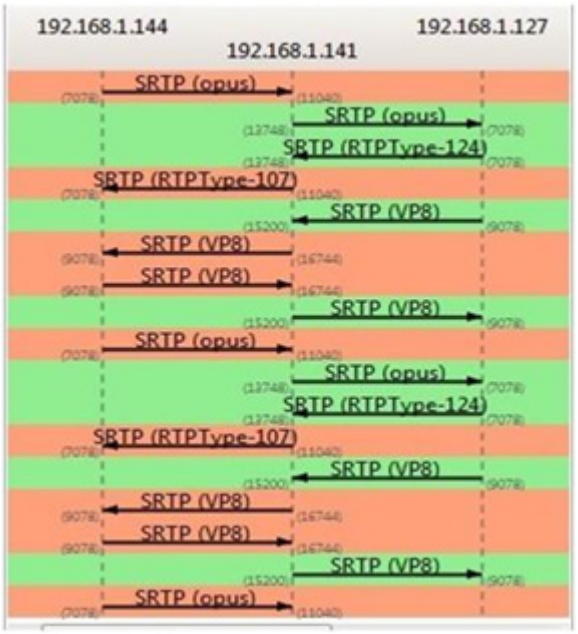

Fig. 6. Flujo de video cifrado.

¿Por qué utilizar Asterisk?

Asterisk es el líder mundial en plataformas de telefonía de código abierto. Es un software que puede convertir un ordenador de propósito general en un sofisticado servidor de comunicaciones VoIP. Es utilizado por empresas de todos los tamaños para mejorar su comunicación, incluyendo a *Google*, *Yahoo*, IBM, e incluso el Ejército de EE.UU. Actualmente las soluciones *Open Source* representan el 18% de las centralitas telefónicas instaladas en todo el mundo (según el *Eastern Management Group*) y Asterisk es el líder en el mercado de código abierto de centralitas VoIP (VoIP PBX) [3].

Ventajas que proporciona Asterisk

1. Asterisk es un software gratuito, y se dispone del código fuente para lo que se desee.
2. Cualquier sistema compatible con Linux puede utilizarse con Asterisk
3. Se puede utilizar cualquier tipo de terminales que contengan señalización SIP, IAX o H.323, que son los tres protocolos más usados en la actualidad.
4. Pertenece a Digium quien garantiza el funcionamiento de Asterisk y ofrece soporte técnico para sus versiones [3]
5. Asterisk es un sistema de comunicación bien seguro, debido a que su código es visible, cualquier detección de fallo de seguridad, es rápidamente publicado [3].

3. Conclusiones

El éxito de las pruebas realizadas demuestra el cumplimiento de los objetivos trazados. Se ha mostrado como es posible la realización de un sistema de video llamadas utilizando seguridad. Además, se han destacados rasgos importantes como la flexibilidad del sistema y de las configuraciones al haberse implementado en Linux. Destacar además que el sistema es compatible con varios códecs de audio y de video, lo que da la oportunidad de trabajar con diferentes tipos de software clientes. Se hace notar que todas las pruebas se realizaron satisfactoriamente en el Laboratorio de Telecomunicaciones de la Sección de Posgrado e Investigación, en la Escuela Superior de Ingeniería Mecánica y Eléctrica del Instituto Politécnico Nacional (Unidad Zacatenco), Ciudad de México.

Referencias

[1] John G. Van Bosse, Y.O., *Signaling in Telecommunication Networks*. 2007, New Jersey: John Wiley & Sons, Inc.

[2] Handley H., Y.O., *Request for Comments 2543 SIP: Session Initiation Protocol*. 1999.

[3] Boucadair, M., *Inter-Asterisk Exchange (IAX): Deployment Scenarios in SIP-Enabled Networks*. John Wiley & Sons Ltd. ed. 2009, Francia: John Wiley & Sons, Ltd.