Modelo Sip Seguro para una Comunicación extremo a extremo sobre IPV6

Sip Security Model for End to End Communication on IPv6

Ross M. Benites[1], José L Quiroz[2], Raúl Villafani[3]

[1] INICTEL-UNI, Lima 41
[2] INICTEL-UNI, Lima 41
[3] INICTEL-UNI, Lima 41

RESUMEN

Las implementaciones VoIP hoy en día se han incrementado considerablemente, sin embargo no en todos los escenarios se tiene en cuenta los mecanismos de seguridad adecuados. Este último punto es muy importante a considerar el día de hoy , sobre todo por el agotamiento de las direcciones IPV4 y el despliegue hacia IPV6 de muchos de los servicios, donde aparecerán nuevas amenazas a la seguridad que trataran de opacar el gran auge de la tecnología VoIP. Si bien IPv6 fue desarrollado para solucionar muchas vulnerabilidades en seguridad que actualmente se ven presentes en IPv4, el hecho es que no logra alcanzar aún estas metas según pruebas realizadas.
El protocolo SIP, el actor principal de la tecnología VoIP , requiere de la implementación de mecanismos de seguridad . Los escenarios actuales requieren terminales de usuario de alto rendimiento y soporte para adaptarse a mecanismos de seguridad heterogéneos o asumir relaciones de confianza.
Sin embargo debemos tener en cuenta que hay varias combinaciones de soluciones de seguridad que son proporcionados por usuarios finales y los servidores.

En este trabajo se expone un modelo de seguridad aplicado a un escenario experimental VoIP sobre el Internet de Próxima Generación (IPv6), que utiliza la seguridad salto a salto y extremo a extremo**.**

El escenario propuesto se encuentra sobre una red local con direcciones IPv6. Utiliza dos servidores *Asterisk* implementados bajo las mismas características que cumplen la función de SIP *Proxy*, y se encuentran conectados mediante un enlace troncal SIP – TLS. Se utilizan además dos terminales de usuario (teléfonos IP) provenientes de una marca comercial conocida, registrados cada uno mediante el protocolo SIP-TLS a cada servidor *Asterisk*.

En trabajos anteriores, se han realizado varios estudios sobre el rendimiento del uso de VoIP sobre IPv4 e IPv6 comparando los resultados [1], evaluación de mecanismos de seguridad para mantener la autenticación de usuario, confidencialidad e integridad de la señalización y media de los mensajes VoIP sobre las redes IPv4 [2] y [3].
Este trabajo se esboza en un marco de seguridad, donde se presenta un escenario basado en una red VoIP en IPV6 utilizando TLS y SRTP.

TLS es utilizado para la seguridad en el establecimiento de la sesión con mecanismos de autenticación salto a salto y SRTP (*Secure Real Time Protocol*) para la seguridad del establecimiento del *stream* de media. Nos enfocaremos en analizar y evaluar la seguridad de los mensajes en este escenario sobre el protocolo de transporte seguro (TLS).

Descriptores: *sip, tls ,ipv6, srtp*

ABSTRACT

VoIP deployments today have increased considerably, but not all the scenarios consider appropriate security mechanisms. This last point is very important to consider today, especially the depletion of IPv4 addresses

and the deployment of many services IPv6, where will new security threats to try to overshadow the great technology boom VoIP. Although IPv6 was developed to solve many security vulnerabilities are currently present in IPv4, the fact is that still fails to achieve these goals by testing.
The SIP protocol, the main actor of VoIP technology requires the implementation of security mechanisms. The current scenarios require high-end user performance and support to adapt to heterogeneous security mechanisms or assume trust relationships. But keep in mind that there are various combinations of security solutions that are provided by end users and servers.
This paper presents a security model applied to an experimental scenario VoIP over Next Generation Internet (IPv6), which uses hop by hop security and end to end.

The proposed scenario is on a local network with IPv6 addresses. Use two Asterisk servers implemented under the same characteristics that act as SIP Proxy, and are connected via SIP trunk - TLS. They also use two user terminals (IP phones) from a known trade mark registered by each SIP-TLS protocol for each server Asterisk.

In previous work, there have been several studies on the performance of VoIP using IPv6 and IPv4 and comparing the results [1], evaluation of security mechanisms to support user authentication, confidentiality and integrity of the signaling and media messages VoIP over IPv4 networks [2] and [3].
This paper outlines a framework of security, which presents a scenario based on a VoIP network in IPv6 using TLS and SRTP.

TLS is used for the security session establishment authentication mechanisms hop by hop and SRTP (Secure Real Time Protocol) for the safety of the establishment of media stream. We will focus on analyzing and evaluating the security of the messages in this scenario the secure transport protocol (TLS) .

Keywords: *sip, tls ,ipv6, srtp*

1. INTRODUCCIÓN

Los servicios basados en VoIP son actualmente muy populares debido a las múltiples oportunidades que brindan, es por ello que en un entorno donde se ha desarrollado tan ampliamente deben considerarse aspectos muy importantes como la migración y seguridad necesaria.
Los servicios basados en el protocolo SIP toman un rol muy importante pues brindan grandes ventajas al permitir la adhesión de más servicios debido a la simplicidad del protocolo. Este protocolo actualmente se transporta sobre el Protocolo de Internet v4, el cual actualmente forma la nube del Internet con sus varias limitaciones, pero que podría ir migrando a la versión 6 el cual ya se encuentra en proceso de despliegue.
IPv6 fue desarrollado como un reemplazo a la actual red IPv4 debido al agotamiento de este ultimo. Aunque IPv6 aun no ha sido adoptado, el estado actual de IPv4 es que se han agotado ya las direcciones disponibles, es así que la adopción de IPv6 y la migración de servicios es una tarea que se realizara en el muy corto plazo.

La seguridad para voz sobre IP (VoIP) puede ser dividida en dos aspectos. Seguridad en la señalización de la llamada y seguridad en la sesión de media.

En este trabajo se propone un escenario VoIP seguro sobre Ipv6 en el cual se analiza y describe los mecanismos de seguridad necesarios para la realización de una comunicación segura.
Los resultados se obtendrán del uso los protocolos utilizados: TLS (Transport Layer Security) y SRTP (Secure Real Time Protocol) que tienen como

función mantener la encriptación de la señalización y la media.

Comunicaciones VoIP Seguras

La mayoría de los mecanismos de seguridad en el proceso de gestión de claves en la señalización SIP tiene cuatro etapas:

- Negociar el conjunto de cifrado.
- Realizar la autenticación mutua mediante una clave a largo plazo.
- Establecer una sesión segura al compartir una clave de sesión.
- Cambio de la clave de sesión en la sesión segura.

a) Protocolo de Inicio de Sesión (SIP)

Es un protocolo de señalización que se utiliza para la gestión de la sesión en la comunicación multimedia. SIP ha sido definido por Internet Engineering Task Force (IETF) y sus

especificaciones se encuentran en el RFC 3261 [4]. SIP trabaja igual que el modelo HTTP, mediante solicitud de modelo de respuesta de transacción, es decir, una petición de cliente invoca un método en el servidor y la envía al servidor .Es independiente de la capa de transporte y se le permite utilizar protocolos de transporte fiable como UDP o los protocolos de transporte no fiable como TCP, TCP sobre TLS / SSL, etc.

TLS

TLS (Transport Layer Security) [5]. Seguridad de la capa de transporte, es un protocolo criptográfico que permiten realizar comunicaciones seguras a través de la red de Internet.
La figura 1 muestra el protocolo de enlace TLS. Primero el cliente inicia con un mensaje Client Hello al cual el servidor debe responder con un mensaje Server Hello. Si el cliente ha recibido un certificado que contiene la llave publica del servidor RSA Key, el cliente cifra un secreto pre-compartido elegido al azar con el y envía al servidor ClientKeyExchange. En tercer lugar el cliente luego emite un mensaje ChangeCipherSpec anunciando que los parámetros se han cargado, seguidos por un mensaje final que ya ha sido encriptado con la nueva configuración.

El servidor hace lo mismo por su lado. Por ultimo, el cifrado e intercambio de datos de aplicación se puede iniciar ahora.

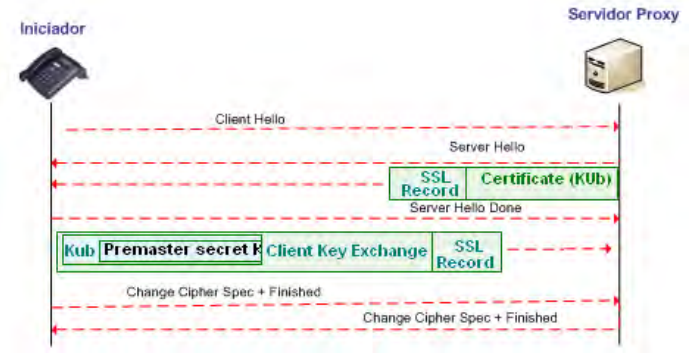

FIGURA 1. TLS Handshake Protocol

b) Protocolo de Tiempo Real (RTP)

Real Time Transport Protocol es un protocolo de transporte que se encarga de la entrega de datos como son audio y video sobre las redes IP en tiempo real extremo a extremo.Se utiliza en conjunto con SIP o H.323, RFC 3550 [6].

SRTP

El Secure Real-time Transport Protocol (o SRTP) define un perfil de RTP, que proporciona cifrado, autenticación del mensaje e integridad, y protección contra reenvíos a los datos RTP en aplicaciones unicast y multicast. Se encuentra definido en el RFC 3711 [7]. SRTP se encarga de encriptar la carga del paquete RTP. Con el fin de garantizar la protección de la cabecera, SRTP proporciona la comprobación, autenticación e integridad de la información de encabezado RTP con funciones HMAC-SHA1 y AES. Es importante destacar que SRTP no agrega cabeceras particulares (es decir no aumentan la longitud del paquete) lo que permite mantener determinada QoS.

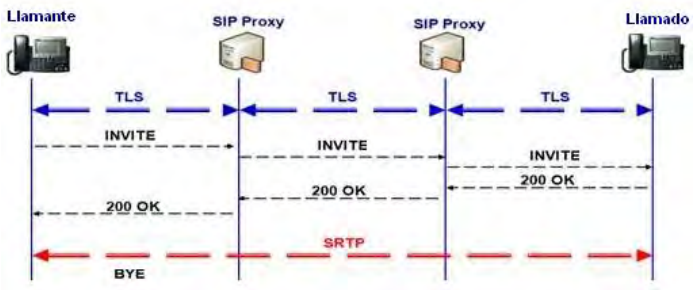

FIGURA 2. SIP basado en comunicaciones VoIP seguras

SDES

SDES (SDP Security Description for Media Streams) especifica un mecanismo para negociar los parámetros de cifrado de flujos de medios en general y para SRTP en particular. SDES está estandarizado por el IETF y especificado en el RFC 4568 [8].
Se introduce un nuevo atributo SDP llamado "crypto", que puede ser utilizado por SRTP para establecer parámetros criptográficos. Puesto que las claves son transportados dentro del mensaje SDP, SDES sólo es adecuado si el SDP está protegido, por ejemplo, con IPSec, TLS, SIP S / MIME, o medios similares. De lo contrario el flujo de los medios de comunicación no se puede considerar como seguro si las llaves no son protegidas.

2. EXPERIMENTAL

La demostración es realizada utilizando como base el escenario trapezoidal SIP estándar, como se muestra en la *Figura 3.*

Escenario de Pruebas:
El escenario propuesto se encuentra sobre una red local con direcciones Ipv6, en este escenario se tienen los elementos de red como User Agent Client (UAC) y User Agent Server (UAS). Los dos servidores Proxy SIP (UAS) se encuentran implementados utilizando software Open Source Asterisk versión 1.8.2.4 sobre Sistema Operativo Linux Debian Lenny 5.0.6.
Cada servidor SIP Proxy se encuentra configurado sobre Pcs de similares características (CPU: Intel core 2 Duo E 8500 3160 Ghz, RAM: 1GB).

Los User Agent Clients (UAC) son teléfonos IP de la marca SNOM modelo S300 con firmware 8.2.35 los cuales tienen soporte para IPv6, autenticación TLS y cifrado SRTP.

Todos los elementos de red se encuentran conectados a un switch Cisco 2960. Adicionalmente se tiene los analizadores de paquetes (Wireshark y Sipv6 Analyzer) que se encuentra conectado al switch en modo monitor.

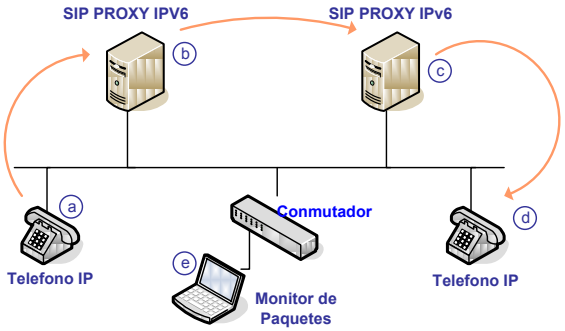

FIGURA 3. Escenario de Red Local IPV6 VoIP basado en SIP – TLS

Procedimiento:
La figura 3 muestra el escenario de interconexión. Se ha utilizado el escenario estándar trapezoidal SIP. La red VoIP local basado en SIP con direcciones IPv6 incluye Agentes de Usuario (SIPv6), y Servidores SIP IPv6 y los analizadores "Wireshark" y "SIPv6 Analyzer".
Las llamadas son realizadas provenientes del UAC (Figura 3 ⓐ) y son enviadas al servidor Proxy adjunto al UAC (Figura 3 ⓑ) .El servidor Proxy SIP Procesa los paquetes encriptados (Mensajes SIP – TLS) y los redirige hacia el Proxy SIP adjunto (Figura 3 ⓒ) . Este último enlace, entre servidores SIP Proxy se da mediante un enlace troncal SIP-TLS donde existe una mutua autenticación (Figura 4). A sus ves este último envía el mensaje a su UAC adjunto (Figura 3 ⓓ). Luego la respuesta del

UAC es reenviada de regreso al UAC que inicio la llamada (Figura 3 ⓐ) a través del último servidor Proxy adjunto.
EL flujo de los paquetes son monitoreados en la red IPv6 haciendo uso de "Wireshark", un analizador de protocolos bastante completo. Debemos mencionar que los paquetes capturados son analizados utilizando la llave publica de la autoridad certificadora, pues de lo contrario seria imposible decodificar toda la transacción SIP.

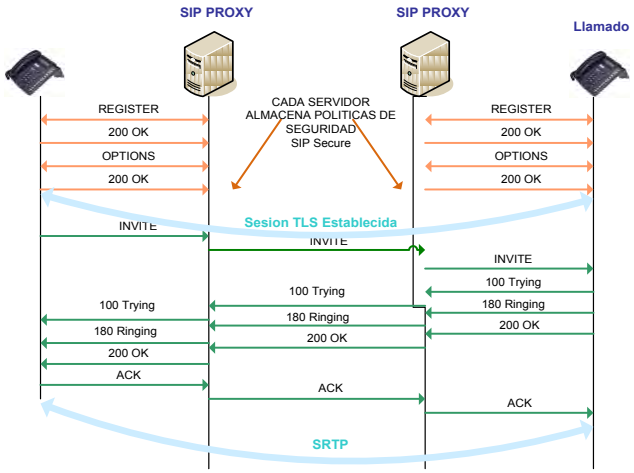

FIGURA 4. Proceso de Registro y Escenario de Red Local IPV6 VoIP basado en SIP – TLS

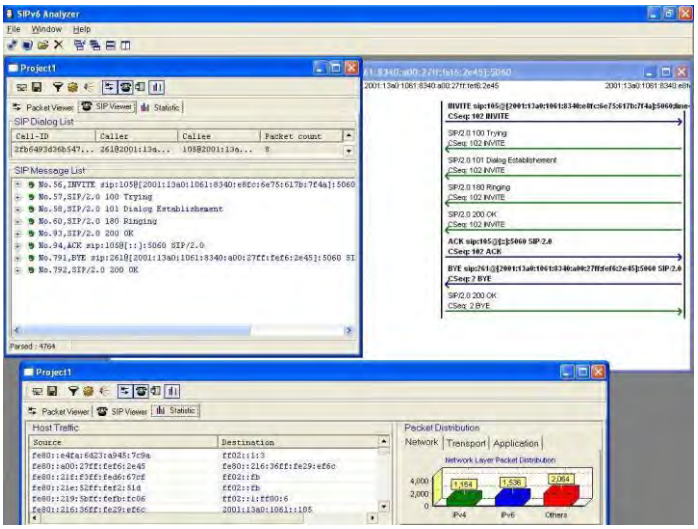

FIGURA 5. Captura del Analizador SIPv6Analyzer

3. RESULTADOS Y DISCUSIÓN

Haciendo uso de la interfaz gráfica de usuario (GUI) del Analizador SIPv6Analyzer que se muestra en la figura 5 se hizo una captura de paquetes con señalización SIP, en varias sesiones, donde se incluyen varias de las transacciones realizadas, que incluyen desde, hacia, el ID de las llamadas y los campos de las cabeceras. Este analizador nos permite construir el dialogo SIP en IPv6 en función de la fuente y direcciones IP de destino (figura 6).
Este primer análisis nos muestra un escenario donde la señalización y la media viajan de manera transparente a cualquier usuario y puede ser fácilmente utilizado para alterar y atacar un escenario VoIP sobre Ipv6.

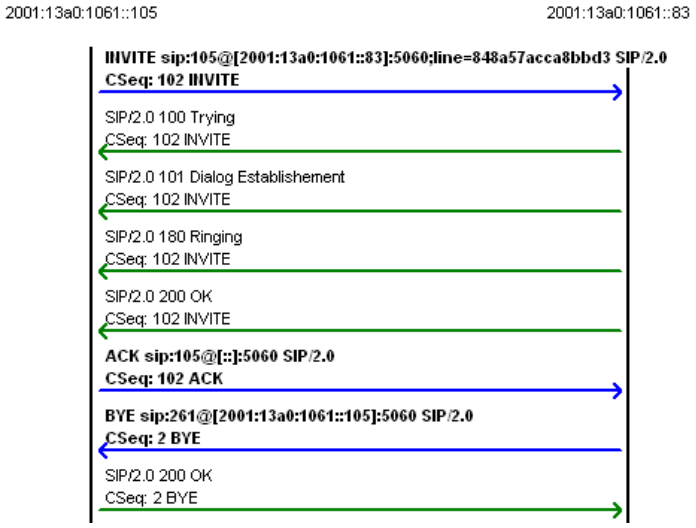

FIGURA 6. Captura SIP utilizando SIPv6Analyzer

En el segundo análisis, se hizo una captura de la señalización, haciendo uso de la herramienta Wireshark, que en un inicio solo nos muestra paquetes TLS y encripta la señalización SIP.
A continuación se muestra un fragmento de un paquete INVITE. Para realizar esta captura se utilizo la llave pública de la autoridad certificadora como se menciono anteriormente.

INVITE sip:260@[fe80::216:36ff:fe39:ec9d] SIP/2.0
Via: SIP/2.0/TLS
[fe80::216:36ff:fe29:eb9d]:5061;branch=z9hG4bK5aaaf4f1;rport
Max-Forwards: 70

From: "Rosa Palacios"
<sip:105@[fe80::216:36ff:fe29:eb9d]>;tag=as7837923d
To: <sip:260@[fe80::216:36ff:fe39:ec9d]>
Contact: <sip:105@[fe80::216:36ff:fe29:eb9d]:5061;transport=TLS>

User-Agent: Asterisk PBX 1.8.4.2
[...]

v=0
o=alice 1993816404 1993816404 IN IP6 fe80::216:36ff:fe29:eb9d
s=Asterisk PBX 1.8.4.2
c=IN IP6 2001:13a0:1061::105
t=0 0
m=audio 18234 RTP/AVP 0 3 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:4Mnln8yqvZH1613RsJbswgbmzhv06uyHPOlrph81
a=direction:both
a=rtpmap:0 PCMU/8000
[...]

En la solicitud INVITE se utiliza SIP sobre TLS, mientras que en el SDP del mensaje se aprecia el parámetro "*crypto" que solicita el uso de cifrado AES para la negociación de la media.*

CONCLUSIONES

En la actualidad ya algunos proveedores se encuentran en proceso de despliegue de Ipv6, y gradualmente en la fase inicial de los servicios sobre esta red tal como es VoIP basado en SIP.
Con el proceso de despliegue de este servicio hemos presentado un escenario para demostrar y promover el funcionamiento de una red VoIP sobre este nuevo internet, con los parámetros de seguridad necesarios utilizando herramientas capturadoras de trafico para analizar hasta donde son nuestros sistemas VoIP para esta red de nueva generación son seguros, y así evitar que nuestros sistemas y comunicaciones sean vulnerados.

AGRADECIMIENTOS

Agradecemos a la Instituto Nacional de Investigación y Capacitación en Telecomunicaciones por brindarnos los ambientes necesarios para realizar las investigación, y muy especialmente a los investigadores del Área de Conmutación y Transmisión de la DIDT – INICTEL-UNI.

REFERENCIAS

[1] Yasinovskyy, R. Wijesinha, A.L. Karne, R.K. Khaksari, G. "A comparison of VoIP performance on IPv6 and IPv4 networks", Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS , 2009 page 603, ISBN 978-1-4244-3807-5.

[2] JoongMan Kim SeokUng Yoon HyunCheol Jeong YooJae Won, "Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP", 2008, Vol 2, page 356 , ISBN 978-0-7695-3492-3

[3] Subramanian, S.V. Dutta, R. , "Comparative Study of Secure vs. Non-secure Transport Protocols on the SIP Proxy Server Performance: An Experimental Approach **",** Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 , page 301, ISBN 978-1-4244-8093-7

[4] RFC 3261, Junio 2002. "SIP: Session Initiation Protocol", http://www.ietf.org/rfc/rfc3261.txt

[5] RFC 2246, Enero 1999. "The TLS Protocol", http://www.ietf.org/rfc/rfc3261.txt

[6] RFC 3550, Julio 2003, "RTP: A Transport Protocol for Real-Time Applications", http://www.ietf.org/rfc/rfc3550.txt

[7] RFC 3711, Marzo 2004, "The Secure Real-Time Transport Protocol (SRTP)", http://www.ietf.org/rfc/rfc3711.txt

[8] RFC 4568, Julio 2006. "The Secure Real TimeTransport Protocol (SRTP)" ,http://www.ietf.org/rfc/rfc4568.txt

[9] Guillet, T. Serhrouchni, A. Badra, M. "Mutual Authentication for SIP: A Semantic Meaning for the SIP Opaque Values", New Technologies, Mobility and Security, 2008. NTMS. , 2008, page 1, ISBN 978-1-42443547-0

[10] Jaesic Choi Kangseok Chae Jaeduck Choi Souhwan Jung "Demonstration of Spam and Security Mechanism in SIP-Based VoIP Services", Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, page 1 ISBN 978-1-4244-2308-8

[11] http://wiki.snom.com

[12] http://www.wireshark.org

[13] http://www.asterisk.org

E-mail: rossmery309@gmail.com
rbenites@inictel-uni.edu.pe