Servicio de Voice Over Internet Protocol (VoIP)

Jorge Álvarez – 201721065-6

Valentina Barreda – 201721010-9

UTFSM

Asignatura: Redes de Computadores I

Profesor: Agustín González Valenzuela

Fecha: viernes, 24 de agosto, 2018

Resumen

La telefonía digital o VoIP es la que permite hacer llamadas de voz y sesiones multimedia a través de internet, usada en la gran mayoría de aplicaciones de comunicaciones entre usuarios. En este proyecto se busca, a nivel general, estudiar y analizar el funcionamiento de VoIP de manera de ser capaces de entender su envío y recibo.

La capa en la que sucede el empaquetamiento de la voz es la capa de aplicación, en esta se poseen distintos protocolos para iniciar la conexión y hacer el envío de voz. Dentro de los protocolos vemos que la mayoría se encapsulan en la capa de transporte dentro de UDP. Al ver los paquetes enviados y recibidos en un software de sniffing como WireShark, actualmente, no se es capaz de identificar si hubo una llamada VoIP, por la encriptación de los protocolos de inicio de sesión y porque en los paquetes enviados durante la llamada se identifican sólo UDP. Si se conoce la estructura y el tipo de protocolos de la capa de aplicación, es posible decodificar UDP y poder analizar la llamada (esto con una aplicación con protocolo conocido) todo con el objetivo de poder ver el proceso completo de las llamadas por Voice over Internet Protocol, para finalmente decodificar de tal manera de poder escuchar los mensajes de voz enviados por los interlocutores.

Introducción

Voice over Internet Protocol es un grupo de tecnologías de software y de hardware que permiten el envío y llegada de voz y sesiones multimedia a través del protocolo internet. Esta tecnología al recibir la señal de voz proveniente del usuario, la transforma a una señal digital para que así sea procesada, es decir, se codifique según protocolo, luego esta señal se comprime y se empaqueta de manera de que pueda ser enviada a través de internet. Una vez que los paquetes llegan al destino, se comienza el proceso inverso, o sea, estos se desempaquetan, descomprimen y finalmente se transforma la señal digital para que el usuario pueda escuchar el mensaje. Este proceso es lo suficientemente rápido para que la conversación sea fluida.

Se puede apreciar que es un servicio que requiere sus propios protocolos y encriptación de datos para poder llevarse a cabo, hoy en día la mayoría de las aplicaciones que utilizan este servicio poseen sus propios protocolos encriptados en base 64, por lo que, aunque se ha intentado hacer ingeniería inversa, no se ha logrado comprenderlos para decodificarlos. Con este contexto, el programa de *sniffing* Wireshark, al presenciar una llamada VoIP, capta paquetes del protocolo UDP, pero al analizar si hubo una llamada no hay datos. A continuación, al conocer el funcionamiento de VoIP, se buscará la manera de hacer un análisis de una llamada.

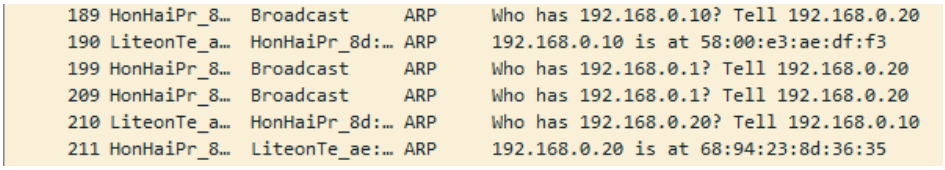
Funcionamiento básico del servicio

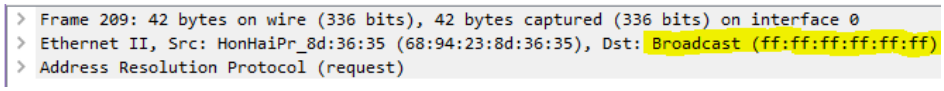
Los proveedores de este servicio buscan parecerse a la telefonía tradicional (PBX), además de ofrecer el servicio de poder efectivamente llamar desde un teléfono digital (teléfono IP) a uno análogo, usando un adaptador (ATA), la empresa Vonage ofrece estos servicios, además existen las centrales telefónicas virtuales y de nube (iPBX o cloudPBX respectivamente) que facilitan un número y el servicio completo, ejemplos de estos son el OpenSource Asterisk, para utilizarlo se puede usar un softphone, el cuál es libre la elección del usuario. Por otro lado, son muchas las aplicaciones que utilizan telefonía digital, dentro de los más famosas se encuentran las llamadas de *Whatsapp*, las de *Facebook*, *Hangouts* y *Skype* siendo esta última una de las más antiguas y ocupadas. Estas aplicaciones son un proveedor de segunda generación, es decir, proveen una red cerrada para el uso de usuarios privados y sólo se puede llamar entre usuarios de la misma aplicación, esto lo hacen a través del uso de sus propios protocolos para el envío de paquetes como es el protocolo MSNP24, creado en por Microsoft que desde 2014 usa *Skype*. Por último, existen los proveedores de tercera generación que usan la VoIP federada, que es descentralizada y permite la conexión entre distintos dominios.

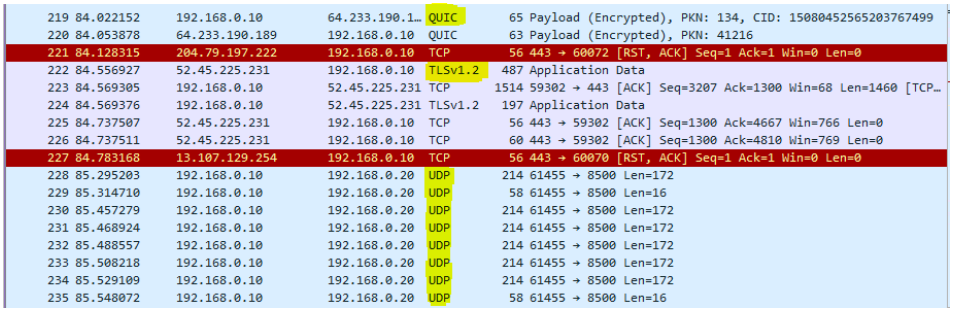
Los protocolos que se han desarrollado para este servicio son de la capa de aplicación los cuales permiten los distintos sucesos para efectuar la llamada ya descritos. En su mayoría estos se encapsulan en UDP, debido a que, como protocolo de transporte, es mucho más conveniente para envío de datos en tiempo real, ya que no le da importancia al orden de los paquetes o la pérdida de algunos de estos, sin embargo, se utiliza TCP para la invitación a la llamada, para mantener las sesiones abiertas y controlar ciertos aspectos de la señal. Para iniciar la sesión dentro de TCP existen el protocolo H.323 (define otros protocolos del mismo estilo como H.255, H.245, Q.931 etc.) y en UDP existe SIP (Session Initiation Protocol), siendo este último más popular que el primero. Hoy en día SIP en su mayor parte es encriptado con el protocolo TLS (Transport Layer Security). Para el control de señal y manejo de sesión existe MGCP (Media Gateway Control Protocol), ahora, para el verdadero transporte existe RTP (Real Time Protocol) que proporciona funciones de transporte de extremo a extremo para aplicaciones de transmisión de datos en tiempo real en servicios de red a través de multidifusión o unidifusión, en adición, existen complementos como RTCP (Real Time Control Protocol) que monitorea a escala y tiene mínimas funcionalidades de control e identificación, o la versión WebRTP para funcionar en la world wide web. Como RTP es el encargado del envío de datos, entonces, dentro de los paquetes UDP, podemos encontrar los paquetes de voz, decodificarlo y efectivamente escuchar la llamada. La decodificación depende del codec (codification - decodification), el tipo de codec se explicita en el header RTP (12 bytes) en 7 bits de *Payload type,* Se procederá a hacer esta decodificación de UDP a RTP en una aplicación simple sin encriptación desconocida, para observar el proceso real.

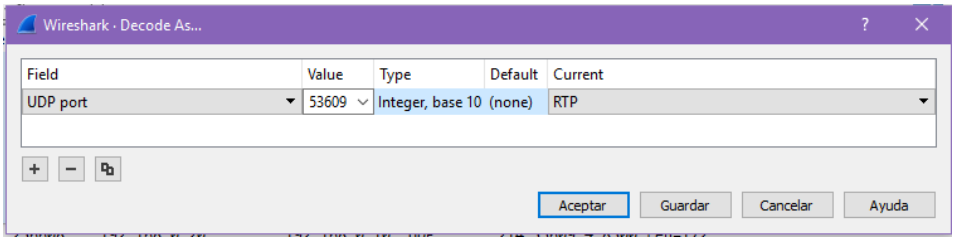
Resultados

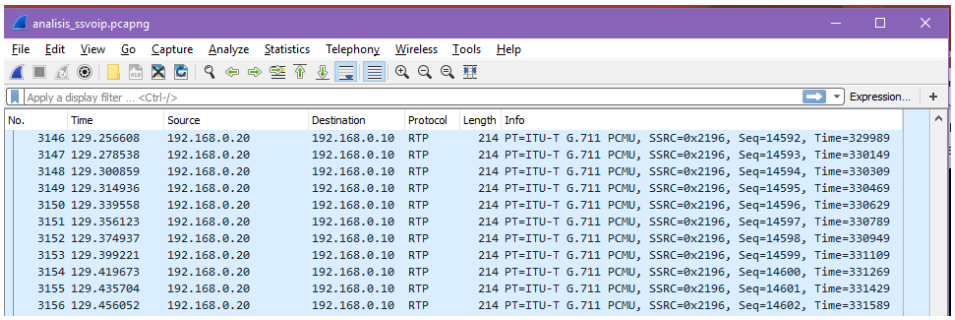
La demostración se hace por medio de un softphone que utiliza las IP dentro de una LAN, este es gratuito, que permite fácil decodificación. Se hace una llamada desde el 192.168.0.10, como se comprueba en la segunda captura, ya que el hace uso del protocolo TLSv1.2 (transport layer security, versión mejorada de SSL) que encripta el mensaje SIP, por lo que no se puede acceder a los flujos de este protocolo. En la primera captura se puede observar el uso de ARP (de manera Broadcast ya que Dst ff:ff:ff:ff:ff:ff) para obtener la dirección MAC de 192.168.0.20 (destino). Se efectúa la llamada a través de UDP. Sabiendo que RTP se ubica por debajo de UDP de decodifica como RTP, esto se observa en la captura 4 y 5. Por último se procede a hacer un análisis de stream (6ta captura) y finalmente es posible hacer una reproducción del stream.

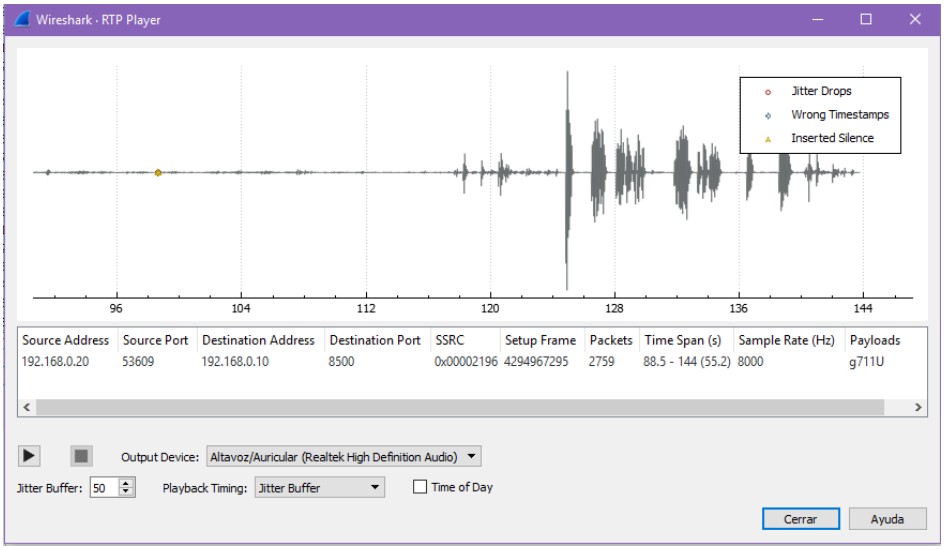












Conclusiones

Las comunicaciones actuales por razones de comodidad y precio se llevan a cabo en su gran mayoría por servicios de telefonía digital, en su ámbito más popular, existen las aplicaciones gratuitas de llamada y chat. Estas, si bien se basan en los protocolos ya existentes, suelen utilizar protocolos propios privados con el fin de encriptar sus datos y darles seguridad a sus usuarios, por esta razón no es posible identificar una llamada de voz por IP en un software de *sniffing*, pero si se conoce la estructura y protocolos de este servicio, además de las características de la aplicación, es posible decodificar lo visible para obtener los datos de los paquetes de voz. Efectivamente, el protocolo RTP (*real-time protocol*) es el encargado de encriptar, según la aplicación decida (uso específico de codec), la voz, por lo que al decodificar UDP como RTP y luego decodificar, este según el codec identificado en la cabecera RTP en el campo *Payload Type*, así es posible analizar la llamada y reproducir lo que dijeron los interlocutores.

Esto es un ejemplo, primero, del funcionamiento de principio a fin del empaquetamiento y envío de voz por IP en una llamada en tiempo real, pero además esto revela la evolución en la seguridad de datos y a la vez lo cuidadoso que hay que ser al elegir una aplicación de servicio de telefonía digital, ya sea como una PBX virtual o de nube o una aplicación de computador o celular móvil, ya que si utiliza los protocolos conocidos, entonces se es capaz de *sniffear* todas las interacciones de los usuarios perdiendo la privacidad y con peligro posible de un ataque.

El desarrollo de los servicios de voz sobre el protocolo de internet, o telefonía digital, ha sido notable, desde la llegada de Skype en 2003, hasta el día actual en el que existen múltiples aplicaciones para el mismo servicio con distintos públicos, ventajas y desventajas. Si bien se estuvo en lo correcto al decir hace 15 años que esto era la tecnología del futuro, no pensamos que la telefonía digital sea un remplazo de la telefonía tradicional, por las claras desventajas en casos de falta de conexión, baja calidad de conexión, la pérdida de paquetes y el uso de CPU de la aplicación por computador, por lo que un uso de ambas tecnologías es lo mejor en cuanto la búsqueda de la mejor conexión entre las personas alrededor del globo.

Referencias

[1] Schulzrinne, H., Casner S., Frederick R., Jacobson V. (2003) RTP: A Transport Protocol for Real Time Applications (Request for Comments: 3550). Fuente: https://www.rfc-editor.org/rfc/rfc3550.pdf

[2] Shade P. (2012) VoIP Analysis Fundamentals with Wireshark… Obtenido de: https://sharkfestus.wireshark.org/sf12

[3] Telefonía VoIP, qué es, cómo funciona, ventajas y desventajas. Obtenido de: http://www.telefoniavozip.com/voip/

[4] Session Initiation Protocol. Obtenido de: https://en.wikipedia.org/wiki/Session_Initiation_Protocol

[5] How to Listen to VoIP Conversations with Wireshark without Capturing the Call Setup. Obtenido en: https://skinnyrd.com/how-to-listen-to-voip-conversations-with-wireshark-without-capturing-the-call-setup/

[6] VoIP Calls. Obtenido de https://wiki.wireshark.org/VoIP_calls

[7] How Vonage Works. Obtenido de https://www.vonage.com/personal/why-vonage/how-vonage-voip-service-works

[8] Real-time transport Protocol. Obtenido de: https://en.wikipedia.org/wiki/Real-time_Transport_Protocol

[9] Microsoft Notification Protocol. Obtenido de : https://es.wikipedia.org/wiki/Microsoft_Notification_Protocol

[10] SSuite Voip PC Phone (software) Obtenido de : https://www.ssuiteoffice.com/software/voippcphonelanchat.htm

[11] RTP header image. Obtenido de: https://www.researchgate.net/profile/Jaime_Lloret/publication/315479711/figure/fig4/AS:537631830310912@1505192825052/RTP-header.png

[12] Asterisk. Obtenido de: https://en.wikipedia.org/wiki/Asterisk_(PBX)