MÉTODOS APLICADOS PARA MEJORAR LA SEGURIDAD EN SISTEMAS VOZ/IP

PEDRO JAVIER BAYTER SÁNCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

MÉTODOS APLICADOS PARA MEJORAR LA SEGURIDAD EN SISTEMAS VOZ/IP

PEDRO JAVIER BAYTER SÁNCHEZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

ING. JOEL CARROLL VARGAS
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico éste trabajo a mi abuelo paterno, que por circunstancias de la vida hoy no se encuentra conmigo, pero me dejó la mejor enseñanza que pude tener y fue a nunca rendirme, a siempre interesarme por el estudio, que a pesar de las adversidades que se presentaron durante el camino siempre me inculcó que el estudio es la única herramienta para salir adelante en la vida, por esto y mucho más quiero dedicarle esta etapa de mi vida porque fue gracias a su crianza que hoy estoy culminando este gran paso.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y adquirir conocimientos muy valiosos para nuestro futuro laboral y personal, también quiero agradecer a cada uno de los tutores y asesores que me acompañaron durante el proceso reconociendo que durante mis estudios cumplieron un papel muy importante brindándome todo su apoyo y colaboración para hoy poder culminar esta meta trazada en mi vida.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

GLOSARIO

CALL MANAGER o CUCM:Es un software desarrollado por Cisco System, creado para el tratamiento de las llamadas y sobre todo para la voz sobre IP, permite tener mayor control sobre la plataforma IP

CUPS: Protocolo de comunicación creado por Cisco System, para usar de forma propietaria en las soluciones desarrolladas por la compañía.

GATEKEEPERS: Es el encargado de permitir los accesos dentro de un sistema, es casi como el portero de un edificio.

GATEWAYS: Encargado de permitir las conexiones entre las redes, es la puerta de enlace que indica porque red viaja el tráfico.

H.225: Es un protocolo que se usa en la comunicación de voz por IP, se encarga de señalizar las llamadas dentro de la red.

H.245: Es un protocolo que se usa en la comunicación de voz por IP, se encarga de controlar el tráfico multimedia dentro de la red.

H.323: Este protocolo también se encarga del control del tráfico multimedia en la red cuando hablamos de VoIP.

H.235: Es un protocolo de seguridad en las redes de datos, asociado a las llamadas de VoIP.

H.450: Protocolo que se usa dentro de las redes de VoIP que permite que dentro de la solución se puedan hacer transferencias de llamadas, llamadas en espera entre otras opciones.

IAX2: Es un protocolo que tiene como tarea poder comprimir los datos que se transmiten en una llamada por medio de una red de datos.

MIKEY: Protocolo encargado de la seguridad al momento de establecer la llamada, es quien se encarga de compartir las llaves públicas y también permite el ahorro de ancho de banda en la llamada.

POKE: Es un ataque de denegación de servicio, que lo que hace es que inunda la red con muchos paquetes para que el sistema colapse.

PROTOCOLO SIP: Este protocolo hace posible que el tráfico de multimedia y voz se transmita sobre una red IP.
RTP: Es el protocolo que se encarga de hacer que la voz se transmita en tiempo real.

SDES: Es un protocolo de seguridad que permite cifrar las llamadas para que no se puedan interceptar.

SRTP: Es un protocolo de seguridad, que se encarga de proteger cada paquete que se transmita por la red durante una llamada de VoIP

TERMINALES: Son todos aquellos dispositivos con los que interactúan los usuarios finales que usan día a día la solución, para nuestro caso un ejemplo sería el teléfono IP.

UDP:Este protocolo permite la comunicación entre dos terminales de forma rápida, es decir no tiene que verificar que el nodo al cual se envía el mensaje esté encendido para poder enviarlo, el protocolo lo envía sin importar si se recibe o no.

ZRTP: Protocolo de seguridad que permite que al realizar la conexión se envíen llaves públicas que permitan una conexión exitosa.

VOIP: Es una plataforma para poder usar las redes IP y transmitir voz, esto permite comunicar distintas sedes de una empresa ubicadas en zonas geográficas diferentes.

RESUMEN

La presente monografía tiene como objetivo realizar un estudio sobre los diferentes puntos de falla en la seguridad de las plataformas VoIP, se quiere ahondar en los diferentes ataques que esta plataforma recibe al estar expuesta dentro de una plataforma de datos como la IP, también conocer sus ventajas.

Para comprender de una mejor manera los aspectos que se van a tartar en este documento, se hace necesario revisar el panorama de una forma en general sobre la actualidad de las soluciones de VoIP. También se debe estudiar el funcionamiento de la tecnología ya mencionada, describiendo la arquitectura de la red asociada a los protocolos SIP y los demás protocolos que intervienen en la solución.

Es necesario realizar una clasificación de las vulnerabilidades que puedan existir en las tecnologías que intervienen en la solución de VoIP y a qué tipo de ataques se está expuesto, todo esto es variable dependiendo del tipo de tecnología que se use dentro de la red.Se trabajará en la investigación y documentación de los diferentes protocolos que ayuden a mejorar la seguridad enfocados a las redes de VoIP y protocolos SIP, estos son protocolos generales que dentro de su funcionamiento está la gestión contraseñas y cifrados, entre otros que pueden ayudar a la seguridad.

También se estudian diferentes mecanismos para la detección de intrusiones que puedan generar daños y pérdidas económicas sobre las redes para las empresas, dentro de los cuales se estudiará su funcionamiento y como protegerse.

Dentro de los estándares que se analizaran en este trabajo se hará énfasis en los protocolos usados para VoIP (H323, SIP, RTP, MGCP, SCCP e IAX), con la finalidad de entender como los hackers aprovechan las vulnerabilidades existentes en nuestras redes.

La solución sobre la cual se trabajará en este documento será la solución de uso libre Asterisk, es una herramienta que presta muy buena solución y a bajo costo.Dada las circunstancias y herramientas presentes en las redes de comunicaciones, existen compañías que se especializan en implementaciones de soluciones de Voz/IP que redefinen la forma en como las compañías se comunican llevando a una reducción significativa de costos y mejorando la calidad del servicio prestado a sus clientes.

ABSTRACT

The purpose of this monograph is to carry out a study on the different points of failure in the security of VoIP platforms, it is intended to delve into the different attacks that this platform receives when exposed within a data platform such as IP, also to know its advantage.

In order to better understand the aspects that are going to be dealt with in this document, it is necessary to review the panorama in a general way about the current state of VoIP solutions. The operation of the aforementioned technology must also be studied, describing the network architecture associated with SIP protocols and the other protocols involved in the solution.

It is necessary to carry out a classification of the vulnerabilities that may exist in the technologies that intervene in the VoIP solution and what type of attacks it is exposed to, all this varies depending on the type of technology that is used within the network. We will work on the investigation and documentation of the different protocols that help improve security focused on VoIP networks and SIP protocols, these are general protocols that include password and encryption management, among others that can help the security.

Different mechanisms are also studied for the detection of intrusions that can generate damages and economic losses on networks for companies, within which their operation and how to protect themselves will be studied.

Within the standards that will be analyzed in this work, emphasis will be made on the protocols used for VoIP (H323, SIP, RTP, MGCP, SCCP and IAX), in order to understand how hackers, take advantage of existing vulnerabilities in our networks.

The solution on which we will work in this document will be the Asterisk free use solution, it is a tool that provides a very good solution and at a low cost.Given the circumstances and tools present in communication networks, there are companies that specialize in implementations of Voice / IP solutions that redefine the way in which companies communicate, leading to a significant reduction in costs and improving the quality of service provided to Your clients.

INTRODUCCIÓN

Durante los últimos años las compañías que se enfocan en brindar servicios Telco, se han encargado en realizar grandes aportes que impulsan la evolución de las tecnologías, dicha evolución ha generado gran impresión de forma positiva en las personas y las compañías, todo esto porque se ha visto cambios drásticos y de gran valor en internet y todo lo que tenga que ver con soluciones del protocolo IP, dentro de todos los servicios que en esta infraestructura se puede ofrecer, la voz sobre IP es la que mayor ventaja toma teniendo en cuenta la facilidad con la que se puede establecer una comunicación por medio de las redes IP.

Dentro de los servicios que se aprovechan de las redes IP, está la VoIP, que une la voz y los datos en una sola red, esto es gracias al protocolo SIP, esto hace posible que mediante una red de datos se pueda transportar voz, se puedan hacer llamadas telefónicas, en la red se puede transportar datos y voz de forma simultánea sin que Ninguno de los dos servicios se vea afectado. Esto supone ahorro en costos de infraestructura para la red.

Sin embargo, esta tecnología al igual que cualquier otra que sea de telecomunicaciones tiene problemas relacionados con la seguridad, dado que VoIP se apoya en los protocolos propios de la red de datos hace que herede los problemas de seguridad que esta trae de forma inherente, cabe aclarar que también existen ataques que son exclusivos de VoIP.

La interconexión de las redes de datos significa que incluso la mayoríalas respuestas básicas terminan teniendo un efecto dominó o no intencionado consecuencias. Mantener un equilibrio entre seguridad y beneficiode las muchas oportunidades proporcionadas por el despliegue de nuevas tecnologías cibernéticas están demostrando ser uno de los problemas más complejos existentes sobre VoIP.

El presente trabajo tiene como objetivo poder realizar un estudio sobre la seguridad en redes VoIP.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En repetidas ocasiones se ha dicho que la telefónica IP no es segura, esto dado que es un servicio que viaja en muchas ocasiones sobre la Internet, pero cabe aclarar que esto no es totalmente cierto, es necesario tener claridad entre prestadores de servicios overthe top (OTT), que son quienes prestan el servicio a través de internet y empresas de telecomunicaciones que son empresas dedicadas a prestar el servicio en la red LAN de la empresa que toma el servicio, de todas maneras si existen algunos riesgos más puntuales que son propios de las redes IP, se pueden categorizar de la siguiente manera:

- Accesos desautorizados y fraudes.Una de las más grandes e importantesamenazas sobre las redes de Voz/IP, están directamente relacionados con accesos no autorizados a una red de Voz/IP como ejemplo podemos citar la obtención de credenciales de algún usuario de forma ilegal y una vez obtenido el acceso sobre el sistema de Voz/IP se realizan llamadas de forma indiscriminada a diferentes partes incluyendo llamadas a larga distancia internacional, esto ocurre principalmente en entornos empresariales.

  Evitar que esto suceda es tarea de control y registro de las llamadas realizadas y que usuario las realiza para validar que efectivamente este usuario tiene dichos acceso.

- Ataques de denegación de servicio. Los llamados DDoS o ataques de denegación de servicios distribuidos. Son ataques DoS simples, pero que al realizarlos de manera ordenada y de diferentes computadoras llegan a generar un gran daño sobre la red es aquí donde los sistemas VoIP suelen ser vulnerables a los DDoS, esto dado a que son muy dependientes de garantías en la calidad de servicio, dado que las redes IP donde se desarrollan las llamadas telefónicas necesitan una tolerancia relativamente baja a problemas de rendimientos de la red.

  Diversos entes investigadores han determinado que las diferentes aplicaciones de voz sobre IP como puede ser la ya muy conocida Skype de uso personal pueden ser usada para lanzar ataques de denegación de servicio distribuidos. En caso de que se llegue a encontrar un fallo en la aplicación o en su protocolo podría ser usada en contra de los usuarios quetienen instalada la App en sus ordenadores, haciéndolos vulnerables a ataques de seguridad.

- Ataques a los dispositivos. Se debe tener claridad que los dispositivos que se usan dentro de un sistema de Voz/IP son tan puntos vulnerables, así como lo puede llegar a ser el sistema operativo o el firmware que ejecutan. Según Coolier, Endler y Hill[1], son muy frecuentes los ataques de fuzzing con que provocan cuelgues o reinicios sobre los dispositivos cuando estos intentan procesar dichos paquetes.

[1] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.477

- Vulnerabilidades de la red subyacente. Como dice Jhonston[2],uno de los mayores problemas es quizás la interceptación de la comunicación “eavesdropping” traduce algo como “escuchar secretamente”, es el método por el cual se puede conocer la captura de información por parte de un intruso. En términos de seguridad informática, se habla de la interceptación de las conversaciones VoIP por parte de intrusos.

1.2 FORMULACIÓN DEL PROBLEMA

Dada la masificación que ha tenido la Voz sobre IP (VoIP) en el mercado, se presentan muchos problemas de seguridad que los atacantes aprovechan para suplantar o para sacar provechos económicos de la solución a la cual puedan acceder.
Uno de los problemas más latentes es la actualización de los sistemas que soportan la solución, de los más reconocidos son Asterisk que corre sobre Linux y que este debe tener un buen robustecimiento en el S.O para evitar que por alguna vulnerabilidad expuesta se puedan filtrar y generar un problema sobre la solución.
Otro de los problemas tiene que ver con los teléfonos IP que se usan dentro de la solución, estos equipos también tienen un sistema operativo y que estos si no se actualiza el Firmware, también puede ser un punto débil dentro de la solución que terminan afectando el correcto funcionamiento de la solución.
Por otro lado, el robustecimiento de las credenciales de usuarios que de una u otra manera tienen acceso a la solución es un punto que se debe mirar con lupa para mitigar una fuga de información o un punto débil dentro de la solución que pueda llegar a afectar el funcionamiento, esto muchas veces es pasado por alto en las organizaciones, pero es algo que realmente ayuda a mitigar cualquier fuga en la solución que llegan a representar problemas económicos.

En este trabajo se analizarán las vulnerabilidades inherentes a los protocolos de VoIP y también aquellas que se heredan por estar soportada en una red de datos. De forma paralela se realizará estudios para analizar las contramedidas y protocolos de seguridad ya existentes que permitan de forma efectiva mitigar todas las vulnerabilidades encontradas. A partir de esto se ejecuta un plan de seguridad en donde se involucre todo los contemplado en la solución que va desde la capa de enlace hasta la capa de aplicación. Esto permite establecer consideraciones para el diseño a implementar de la red que nos va a permitir prepararnos para generar planes que nos lleven a mitigar ataques a la solución de VoIP.

¿Qué tan importante es aplicar hardening para mejorar la seguridad dentro de una solución para VoIP y cuanto influyen las vulnerabilidades que representa una red IP, teniendo en cuenta que es quien soporta la solución?

[2] JHONSON.B. Alan. SIP Understanding the Session Initiation Protocol Fourth Edition. Artechhouse. Boston. 2016. p. 410.

2 JUSTIFICACIÓN

La seguridad sobre las redes informáticas de las compañías son necesarias tenerlas protegidas dado que son las autopistas por donde corre toda la información crítica de la compañía.Para poder proteger las redes de una compañía, se hace necesario realizar diseños y diferentes simulaciones que permitan realizar análisis a los diferentes paquetes que corren sobre las redes.La VoIP admite que una organización, cuente con una única infraestructura de red, mitigando los puntos de falla, y asimismo admite una gestión más fácil, sencilla y completa sobre la infraestructura de las comunicaciones.

Por estas razones, VoIP es una variante que permite el beneficio a varios sectores, mediante de la integración de los diferentes servicios de telecomunicaciones, ofreciendo beneficios en la disminución de gastos telefónicos, adicional a todas las ventajas que esta tecnología nos ofrece comparado con los servicios de telefonía habitual.

Cada vez que el crecimiento de esta tecnología se hace más evidente, también se hacen más visibles las diferentes vulnerabilidades que se heredan de las redes de datos que soportan la solución. Todas estas vulnerabilidades implican mucho más de lo que podamos pensar con respecto a que las llamadas puedan ser interceptadas y escuchadas de forma ilegal, esto tiene un trasfondo que va más allá y que implica que los sistemas de telefonía IP puedan ser usados de forma tal que se generen llamadas de larga distancia a través de la red telefónica de forma fraudulenta generando altos costos a las empresas víctimas.

Si se mira hacia una empresa de prestación de este servicio como Telco o las empresas de Call Center, las consecuencias pueden ser mayores, esto debido que se pueden exponer datos importantes de los clientes.Es por esto que la seguridad sobre las soluciones de VoIP es tan importante tener en cuenta para poder generar valor y confianza sobre los usuarios y clientes.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Determinar las amenazas dirigidas a los protocolos de Voz sobre IP, basado en metodologías para investigación de vulnerabilidades.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar información sobre el uso de sistemas Voz/IP en redes empresariales, que permita evidenciar y documentar posibles fallas de seguridad en la implementación del sistema.

- Establecer las posibles amenazas y riesgos asociados a las redes de datos en donde se implementan servicios de Voz sobre IP.

- Documentar las mejores prácticas de seguridad informática que permita el aseguramiento de plataformas y/o sistemas de Voz/IP.

4 MARCO TEORICO

4.1 ANTECEDENTES

Para el desarrollo de esta monografía se tomaron como referencias otros trabajos similares orientados a la seguridad de las redes VoIP, que permiten mejorar la seguridad de las redes dentro de un ambiente corporativo.

Tesis “consideraciones sobre laseguridad en las redes de telecomunicaciones soportes devoz sobre ip (voip) en cuba”, trabajo de grado presentado por Aslan Santana Vásquez a la Universidad Central “Marta Abreu” de las Villas en el año 2007 para optar al título de Máster en Telemática. En estatesis se recolecta información sobre los protocolos que se usan dentro de una solución de VoIP, dado detalles sobre cada vulnerabilidad conocida a los que estos protocolos están expuestos permitiendo documentar cada las fallas y como mitigar cada riesgo encontrado en estas vulnerabilidades que permitan mejorar la seguridad en estas plataformas, permitiendo sean usados como referencia en esta monografía.

Artículo “seguridad en VoIP: Ataques, Amenazas y Riesgos”, documento presentado por Roberto Gutiérrez Gilen laUniversidad de Valencia. En este artículo el autor detalla el protocolo SIP y los estándares que usan cada protocolo, también se detalla algunas técnicas de ataques a las cuales está expuesta la plataforma de solución VoIP realizando una amplia introducción sobre la seguridad de las redes VoIP, que permite tomar algunos apartes para ser usados en esta monografía como material de apoyo.

Monografía “seguridad VoIP: ataques y contramedidas en sistemas de código abierto”, trabajo de grado presentado por Antonio Carrasco Hirueloa la Universidad abierta de Cataluña en el año 2019 para optar al título de Máster universitario en seguridad de las tecnologías de la información y de las comunicaciones. En esta obra se detalla información sobre la historia de la seguridad en las telecomunicaciones y la importancia que estas tienen al momento de soportar las comunicaciones de las plataformas de VoIP, también detalla el uso empresarial para la VoIP y la importancia en el crecimiento de las comunicaciones que esta plataforma permite generar, en el documento se hace énfasis en las plataformas de código abierto que son una opción bastante viables para las compañías que quieren migrar a las plataformas de VoIP.

Tesis “análisis comparativo entre alternativas libres y propietarias para la migración de telefonía tradicional a telefonía ip, evaluación de las soluciones propuestas basada en la aplicación de un modelo roi orientado a una pequeña y mediana institución financiera e implementación de un proyecto piloto en la cooperativa coopera ltda”, tesis presentada por María Esther Piedra Orellana y Lucía Marcela Solórzano Valencia a la Universidad Politécnica Salesiana Sede Cuenca de Ecuadoren el año 2011 para optar al título de Ingeniero de Sistemas. Esta tesis tiene como finalidad el planteamiento de alternativas para la implementación de una plataforma de telefonía IP para una cooperativa de la ciudad de Cuenca en Ecuador, también se realizó un análisis de la red de datos de esta cooperativa para entregar un informe con todas las consideraciones técnicas a tener en cuenta para poder llevar a cabo la implementación de la solución de VoIP. Dentro de este artículo se analiza muy detalladamente la solución de código abierto Asterisk, permitiendo conocer los

protocolos que este usa los Códecs necesarios para este tipo de plataforma, también detalla las posibles vulnerabilidades asociadas a la solución de código abierto, así como las soluciones que se puedan presentar al momento de realizar la implementación de la solución.

Proyecto “seguridad en VoIP: aplicaciones de señuelos”, documento presentado por Elena Krasheninnikovaen laUniversidad Politécnica de Madrid en el año 2013 para optar por el título de Máster universitario en Ingeniería de redes y servicios telemáticos. En este proyecto el autor pretende llevar a cabo un estudio de los aspectos de las redes VoIP con enfoques de señuelos dentro de la red IP, en donde se desea llevar a cabo el análisis de varios señuelos ya existentes y validar la posibilidad de ser implementados dentro de las redes de VoIP e identificar las ventajas o inconvenientes que se puedan presentar, este proyecto también abarca un análisis de infraestructura sobre la red IP de una compañía basada en protocolo SIP y demás protocolos usados dentro de una plataforma de telefonía IP. Este proyecto permite tomar algunos apartes para ser usados en esta monografía como material de apoyo.

4.2 MARCO CONCEPTUAL

VoIP. VoIP traduce “VoiceOver Internet Protocol” que hace referencia a la transferencia de voz en paquetes IP sobre redes de datos como puede llegar a ser Internet o una red privada de datos.

Protocolo SIP. Según Gutiérrez[3],es un protocolo simple de señalización y control utilizado para telefonía y videoconferencia sobre las redes IP. Fue creado por el IETF MMUSIC WorkingGroupy su estructura está basada en otros protocolos como STMP y HTTP con los que guardacierta similitud. SIP es un protocolo abierto y ampliamente soportado que no depende deningún fabricante. Su simplicidad, escalabilidad y facilidad para integrarse con otrosprotocolos y aplicaciones lo han convertido en un estándar de la telefonía IP.

Denegación de servicio. Como afirma Gutiérrez[4], son intentos de ataques mal intencionados con el fin de degradar seriamente el rendimiento de la red o un sistema incluso llegando al punto de impedir la utilización del mismo por parte de usuarios legítimos. Algunas técnicas se basan en el envío de paquetes especialmente construidos para explotar algunas vulnerabilidades en el software o en el hardware del sistema, saturación de los flujos de datos y de la red o sobrecarga de procesos en los dispositivos.

Footpriting. Según Gutiérrez[5],se conoce como Footpriting al proceso de acumulación de información de un entorno de red especifico, usualmente con el propósito de buscar formas de introducirse en el entorno.

Eavesdropping. Como afirma Gutiérrez[6],“escuchar secretamente”, es el término con el que se conoce a la captura de información (cifrada o no) por parte de un intruso al que no iba dirigida dicha información. En términos de telefonía IP, estamos hablando de la interceptación de las conversaciones VoIP por parte de individuos que no participan en la conversación.

Vulnerabilidad. Según Carrasco[7]**,** es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos

Escucha, secuestro y modificación de llamadas. Según Carrasco[8], en estos tipos de amenazas un usuario malintencionado sin autorización puede interceptar las llamadas, oírlas, modificarlas e incluso eliminarlas o variar su finalidad. Debido a la falta de cifrado y técnicas que permitan a un atacante esnifar el tráfico relacionado, se podría conseguir adivinar contraseñas, alterar los destinatarios de las llamadas o incluso evitar su curso. Al mismo tiempo, la escucha y copia de las llamadas, del tipo que sea, implican igualmente una importante falta de privacidad. Ataques más avanzados en este marco permitirían alterar con ruido las llamadas e incluso conseguir hacerse pasar por una persona con fines maliciosos.

Interrupción o degradación del servicio. Como afirma Carrasco[9]**,** además de la opción siempre presente de recibir ataques por delincuentes como simple juego, o bien con fines empresariales e incluso nacionales, no siempre las amenazas suponen una intencionalidad o factor humano. Una amenaza puede suponer también un desastre físico como una inundación o algún tipo de desastre natural que haga que cualquier capa superior sostenida por estos soportes físicos o hardware impida su uso. Dentro de este tipo de amenazas se puede ver vulnerado el principio de disponibilidad de la información.

Asterisk. Según Piedra y Solorzano[10]**,** es una aplicación de código abierto y gracias a que fue desarrollada con la colaboración de toda la comunidad OpenSource del mundo, es posible obtener soporte de variadas fuentes, y la capacidad de respuesta ante problemas de implementación no puede ser igualada por una empresa privada. Se trata de una solución multiplataforma como Windows o MAC, pero fue diseñada para Linux por lo que tiene más soporte en esta última.

Protocolos de señalización. Como afirma Piedra y Solorzano[11]**,** el objetivo de la VoIP es dividir en paquetes los flujos de audio para transportarlos sobre redes basadas en IP. Los protocolos de las redes IP originalmente no estuvieron diseñados para la transmisión el tiempo real de audio o cualquier otro tipo de medio de comunicación. La PSTN está diseñada para la transmisión de voz, sin embargo, tiene sus limitaciones tecnológicas. Es por esto que se crean los protocolos para VoIP, cuyo mecanismo de conexión abarca una serie de transacciones de señalización entre terminales que cargan dos flujos de audio para cada dirección de la conversación.

4.3 MARCO HISTORICO

Como dice Regis[12], al comienzo de las redes de telefonía de voz, los sistemas y servicios siempre se consideraron seguros. La razón de esto proviene de la filosofía de “Bell Telephone Company”. Las compañías Bell siempre tendían un cable telefónico desde la Oficina Central hasta la ubicación del cliente. Se utilizaron diferentes formas, pero para esta discusión, los cables telefónicos eran cables dedicados que iban desde el CO a lo largo de una ruta de línea de poste telefónico hasta la ubicación del usuario final (es decir, residencia, negocio, etc.).

---

[3]GUTIERREZ G. Roberto. Seguridad en VoIP: Ataques, Amenazas y riesgos. Universidad de Valencia. p.6
[4]Ibíd., p. 14
[5]Ibíd., p. 16
[6]Ibíd., p. 13
[7]CARRASCO H. Antonio. Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Universidad Cataluña. p.27
[8]CARRASCO H. Antonio. Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Universidad Cataluña. p.28
[9]Ibíd., p. 30
[10] PIEDRA O. María y SOLORZANO V. Lucia. Análisis comparativo entre alternativas libres y propietarias para la migración de telefonía tradicional a telefonía IP. Cuenca. Marzo 2011. p. 27
[11] Ibíd., p. 27
[12] REGIS J, BUD Bates, Securing VoIP, Keeping your VOIP, Network Safe: Syngress, 2015. p.21

Según Regis[13], una vez surge el internet, que se da para que los estudiantes pudieran tener acceso a información tales como datos, archivos y correos, empieza el crecimiento de una nueva era, es aquí donde surgen muchos servicios apoyados en esta red, entre ellas la telefónica IP, que es soportada por las redes de datos empresariales y soportada por internet de una forma más global, como al principio la Internet era muy insegura, todos los problemas que traía esa red, era heredada por la red de VoIP, cuando esta red incursiona en el mercado trajo consigo a simple vista una forma más económica de implementar a bajo costo un servicio de telefonía, pero también trajo consigo una cantidad de problemas de seguridad asociadas a las llamadas que al principio pusieron en duda su efectividad o si el uso de esta red era necesaria implementar, con el paso del tiempo esto ha ido mejorando hasta hoy día que existen compañías dedicadas a soportar esta plataforma.

4.4 MARCO TECNOLÓGICO

Como dice Collier[14], en las actividades diarias, que ejecuta el ser humano, es muy importante aprovechar los medios disponibles para obtener una mayor eficiencia en el desarrollo de la persona, así como también en el ámbito laboral, es por esto que se debe impulsar desde todos los ámbitos el uso de las TIC teniendo en cuenta que mejora de forma sustancial el desarrollo y desempeño en las actividades del ser humano, para este trabajo, se quiere impulsar el uso de las comunicaciones de la Voz sobre las redes IP, generando una mayor eficiencia y eficacia en las comunicaciones entre las personas ubicadas geográficamente en sitos distintos, esto conlleva a que la comunicación sea más eficiente y por ende a que las actividades del ser humano dentro de un marco social y colectivo mejore las condiciones en la que se desarrollan las actividades.

A lo largo de este trabajo se busca evidenciar algunas falencias a las que está expuesta la solución de VoIP, y también se brindan algunas posibles soluciones desde el ámbito técnico y humano, haciendo énfasis en que los dos aspectos (técnico y humano) son sumamente importantes a la hora de mejorar la seguridad, también hacemos énfasis en el uso del software libre como lo es Asterisk, esto dado que existe una comunidad muy grande que está dispuesta a brindar apoyo cuando sea requerido.

4.5 MARCO LEGAL

Según el marco legal de las TIC en Colombia[15], la Ley 1331 del 30 de julio de 2009, que propender por brindarle a todos los ciudadanos colombianos un marco normativo al sector de las tecnologías de la información y comunicaciones. Con el desarrollo de esta ley, se busca garantizar la libre competencia, el uso eficiente de la infraestructura y algo muy importante vela por la protección de los derechos de los usuarios.

[13] Ibíd., p. 9
[14] COLLIER M, ENDLER D, Hacking Exposed Unified Communications, 2014, p. 22
[15] Marco legal que sustenta las TIC en Colombia: marco legal de las TIC en Colombia. [En línea]. 2012. (Recuperado el 12 de abril 2020.). 2012.

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

Según los artículos del marco legal de las TIC en Colombia:

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

5 IDENTIFICACIÓN DE LA INFORMACIÓN SOBRE EL USO DE SISTEMAS VOZ/IP EN REDES EMPRESARIALES

5.1 PROTOCOLO DE COMUNICACIONES DE VOZ POR TCP/IP (VOIP)

Como dice Gutiérrez[16], es un protocolo de transferencia de voz sobre internet, gracias a este protocolo podemos unir dos servicios que se manejaban por separado como lo son la transferencia de Voz y de Datos.

Esta tecnología se encarga de transportar la voz, encapsulándola para transportarla en redes de datos o de internet en paquetes, logrando aprovechar al máximo la red convirtiéndola en homogénea.

Gracias a este protocolo se presenta mayor aprovechamiento de la red, por donde por un mismo medio podemos transportar datos y voz, en este caso por una misma línea de servicio se amplía las ventajas reduciendo costos de inversión sobre la infraestructura y mantenimientos, para la telefonía tradicional, se requiere una mayor infraestructura, tales como centrales conectadas unas con otras por medio de cables de cobre y/o Fibra Óptica, que representa una gran inversión.

Por el lado de la tecnología de la Voz sobre IP, nos permite comprimir la voz para que se pueda transportar por redes compartidas donde también se prestan otros servicios, sin necesidad de fijar anchos de bandas exclusivos.

Pero no todo puede ser dicha en un ambiente donde cada día aumenta la velocidad con la que se actualizan los componentes tecnológicos, para ello se resumen en los siguientes tres componentes: Seguridad, Fiabilidad y Calidad de servicio, VoIP estar basado sobre el protocolo IP se heredan muchos de los problemas de este protocolo, tales como perdidas de paquetes, demora en la transmisión de los paquetes de un extremos a otro, esto supone un gran problema para la VoIP, pero son cosas que con la evolución de las tecnologías involucradas se van solucionando.

Mirando desde el lado de la seguridad, las llamadas VoIP transitan por Internet o redes de datos que en su mayoría suelen ser inseguras si no se toman las medidas necesarias para convertirlas en seguras, pero aun así se pueden encontrar vulnerabilidades que presentan un peligro a la seguridad de este servicio.

5.2 INFRAESTRUCTURA VOIP

Según Gutiérrez[17], dentro de la infraestructura que una red VoIP necesita como base, es necesario indicar tres elementos:

[16] GUTIERREZ G. Roberto. Seguridad en VoIP: Ataques, Amenazas y riesgos. Universidad de Valencia. p.3
[17] Ibíd., p. 4

- Terminales: son aquellos dispositivos que permiten a los usuarios finales hacer uso de la solución VoIP implementada, estos pueden ser físicos o virtuales (software) los físicos son los dispositivos tales como teléfonos parecidos a los tradicionales y los softwares como SoftPhone que se instalan en un PC y también funcionan como teléfonos tradicionales.

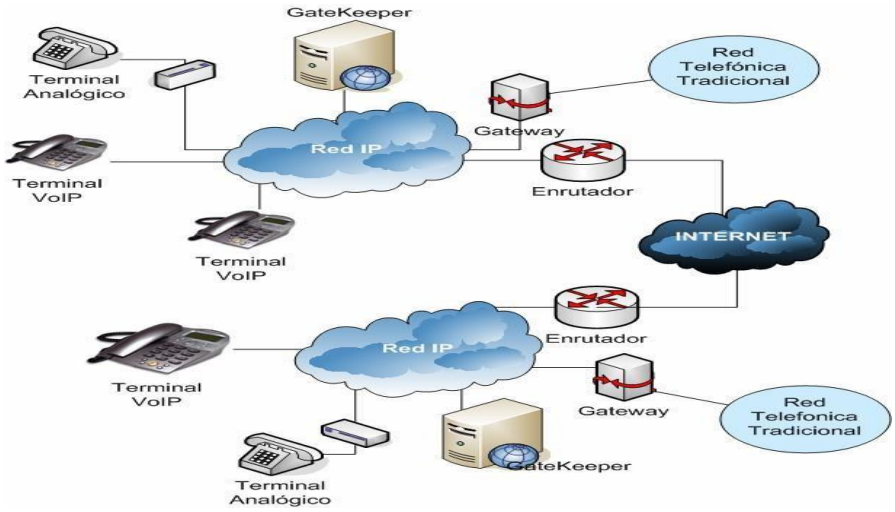
- Gateways: es quien se encarga de hacer las conexiones entre las redes análogas o digitales y la central de VoIP.

- GateKeepers: es quien realiza la autenticación de los usuarios, enrutamientos, control del ancho de banda, es el servidor de Voz sobre IP.

La siguiente ilustración muestra la conexión de dos sedes de una misma empresa a través de internet

Figura 1. Infraestructura red VoIP

Fuente. Estructura de red básica conectadas telefónicamente a través de internet.http://www.servervoip.com/blog/wp-content/uploads/Estructura-de-red-basica-conectadas-telefonicamente-a-traves-de-Internet.png, 2015



5.3 PROTOCOLES Y ESTÁNDARES VOIP

Según Gutiérrez[18], el servicio que ofrece la VoIP abarca una gran cantidad de protocolos, sumado a que la telefonía IP tiene la obligación de cumplir con los mismos servicios que ofrece la telefonía tradicional y generar un plus en cuanto a economía se trata, requiere de estándares, protocolos y servidores, siendo estos objetivos claros para ataques

[18] GUTIERREZ GIL, Roberto. Seguridad en VoIP: Ataques, Amenazas y riesgos: Universidad de Valencia. p.6

cibernéticos, se hablara de los protocolos más importantes sobre este tipo de comunicaciones como lo son: H.323 y SIP

H.323 es el protocolo de comunicación para la multimedia usado a través de redes de paquetes, ha sido tanta su evolución que hoy día es un estándar para la VoIP, el protocolo H.323 es encargado de garantizar los distintos talantes de la comunicación de la VoIP tales son la transmisión de la voz, el direccionamiento, control de transmisión, compresión de la voz y la señalización, sobre el protocolo H.323, se ciñe el estándar RTP (Protocolo de transporte de tiempo real).

5.4 PROTOCOLO SIP

Según Gutiérrez[19] este es un protocolo de señalización y control, que permite el tráfico sobre redes IP de videoconferencias y telefonía, la estructura del SIP se basa en los protocolos SMTP y HTTP, se ha convertido en un estándar de la VoIP gracias a su versatilidad y que no depende de un solo fabricante.SIP por ser un protocolo de señalización se encarga de establecer, controlar y terminar cada sesión de la comunicación, cada vez que se establece la comunicación empieza el intercambio de paquetes RTP, que son los que se encargan de transportar la voz, también involucra SDP, que es el protocolo que negocia el tipo de codificación, cantidad de participantes, entre otros, el protocolo SIP es de aplicación y corre sobre UDP y TCP.

A nivel de seguridad el protocolo SIP representa algún tipo de riesgo, dado que este usa al menos 3 puertos en donde por lo menos uno es estático haciéndolo susceptible a ataques de secuestros de registros, esto ocurre porque al ser dos puertos dinámicos hace que el cortafuegos no pueda garantizar el tráfico por esos puertos.El protocolo H.323 durante su funcionamiento usa entre 7 y 11 puertos, de los cuales dos solo son estáticos y los otros son aleatorios, haciendo también que el cortafuegos no funcione sobre los servicios que corren sobre esos puertos de forma eficaz.

Tabla 1. Protocolos y puertos que usan

No se encuentran elementos de tabla de ilustraciones.	**Puertos**
SessionInitiationProtocol (SIP)	TCP/UDP 5060,5061
SessionDescriptionProtocol (SDP)	Encapsulación SIP
Media Gateway Control Protocol (MGCP)	UDP 2427,2727
Skinny Client Control Protocol (SCCP/Skinny)	TCP 2000,2001

[19]Ibíd., p. 9

Real-time Transfer Control Protocol (RTCP)	RTP+1
Real-time Transfer Protocol (RTP)	Dynamic
Secure Real-time Transfer Protocol (SRTP)	Dynamic
Inter-Asterisk eXchange v.2 (IAX2)	UDP 4356

Fuente. Seguridad en VoIP: Ataques, Amenazas y riesgos.

5.5 COMPARATIVO SOFTWARE DE PAGO VS SOFTWARE LIBRE

Como dice Piedra y Solorzano[20], la telefonía IP es conocida como la telefonía del futuro, por lo que representa una gran responsabilidad a partir de los tipos de software de uso privativo y de uso libre, por lo que en este informe he querido trabajar con dos tipos de software que representan cada uno de los ya mencionados.Para el uso del software libre nos enfocaremos en Asterisk y para software de uso privativo hablaremos de Cisco UnifiedCommunications Manager.

5.5.1 Software de uso libre. Asterisk.

Según Piedra y Solorzano[21],es una aplicación de código abierto,desarrollada por la comunidad OpenSource a nivel mundial, gracias a esto se puede conseguir soporte de distintas comunidades en el ámbito del software libre, esto hace que la respuesta a los diferentes incidentes que se puedan presentar supere con amplitud el soporte que se puede recibir si tenemos en cuenta que los foros están siendo rápidamente contestados y se cuenta con una gran base de conocimiento en la web que dan solución a los incidentes que podamos presentar y que en el pasado alguien los haya presentado.

Asterisk se puede encontrar para plataformas Windows, Mac y Linux, pero su origen fue para Linux por lo que es más fácil encontrar soporte para esta plataforma. La solución para VoIP basada en la plataforma Asterisk permite diseñar a la medida un sistema de telefonía, permitiendo crecimientos escalables dependiendo de los requerimientos de la compañía, algo bueno de la telefonía IP en general es que permite conectar varias sedes por medio de un enlace de comunicaciones, ahorrando costos de llamadas de largas distancias.

La variedad de protocolos que permite Asterisk es bastante variada, así como los códecs que usa para la comprensión de la voz permitiendo optimizar las redes y no generando saturación, requiere de Hardware adicional para brindar el servicio, tales como teléfono IP, la central Asterisk permite armar otras funcionalidades adicionales y complementarias a la voz IP.La infraestructura que soporta Asterisk es muy variada, entre ellas están las tarjetas

[20] PIEDRA O. María y SOLORZANO V. Lucia. Análisis comparativo entre alternativas libres y propietarias para la migración de telefonía tradicional a telefonía IP. Cuenca. Marzo 2011. p. 27
[21]Ibíd., p. 28

Digium o cualquiera otra tarjeta genérica, una de las ventajas más notorias es que Asterisk puede coexistir con la telefonía tradicional y la telefonía IP, haciendo un sistema hibrido.

5.5.2 Software de uso propietario. Cisco UnifiedCommunications Manager.Una de las empresas líderes en el mundo para la telefonía IP es Cisco, que ofrece paquetes muy abiertos y bastante completos en soluciones IP incluyendo terminales para los clientes finales, proporcionando servicios uniformes bajo una misma plataforma que ayuda a mantener conectadas las diferentes sedes de una compañía sin importar las distancias, con tener un canal de comunicación entre las sedes se da la comunicación de forma transparente.

Cisco ofrece diferentes modelos de equipos para brindar servicios de telefonía IPdependiendo el tamaño de la compañía se puede instalar un Router que permita hacer la labor de VoIP, las empresas más grandes ya necesitan de servidores dedicados para ofrecer un mejor servicio.Cuenta con soporte para el protocolo de modo privativo de Cisco SCCP; también SIP además de una gran diversidad de códecs de audio, dentro del soporte existe una gran variedad de teléfonos IP, en los que se pueden encontrar teléfonos básicos, hasta los teléfonos de gama alta con mayores prestaciones.

El soporte que necesitan las herramientas y plataformas de Cisco se deben contratar con los partner autorizados por dicha firma, esto hace que el mantenimiento y el soporte se haga un poco costo en términos económicos, cabe resaltar que Cisco escoge muy bien a las empresas que la representan a nivel mundial para garantizar que las personas que prestan los servicios y manipulan sus equipos estén capacitados para hacerlo, esto en parte genera un poco más de confianza pero no quiere decir que se cumpla a cabalidad, cabe la posibilidad que personas que no tengan los conocimientos necesarios realicen configuraciones en equipos generando fallas de seguridad en la solución.

Los equipos que usa Cisco no son precisamente los más económicos en el mercado, cuando se contrata un proyecto con el fabricante Cisco, ellos indican que se debe usar todos los equipos de la marca para poder garantizar la efectividad de la solución, esto encarece mucho los proyectos dados que los equipos no son muy económicos.El soporte de forma libre no es muy común de encontrarlo para esta plataforma en comparación de Asterisk, dado que las comunidades de Cisco no son muchas y de forma abierta, toca pagar suscripciones que te permitan acceder a dicho material de apoyo para dar soluciones a los inconvenientes presentados.

5.6 SOFTWARE DE USO PROPIETARIO: AVAYA AURA APPLICATION SERVER 5300

Según Avaya[22], el Portafolio de comunicaciones multimedia de Avaya ofrece una amplia gama de servicios multimedia de próxima generación en una variedad de configuraciones de red, que incluyen el Servidor de comunicaciones multimedia y el Servidor de aplicaciones Avaya Aura. La solución del Servidor de aplicaciones proporciona una poderosa solución

[22] AVAYA. Application Server 5300Overview. Marzo 2019.

que admite seguridad mejorada y alberga un conjunto completo de características del protocolo de inicio de sesión (SIP), una amplia gama de clientes basados en el Protocolo de Internet (IP) y componentes de puerta de enlace y servidor de medios para la interoperabilidad SIP

Application Server 5300 se basa en las fortalezas de MCS 5100. La solución está diseñada para implementaciones empresariales donde se requieren operaciones seguras. La solución combina servicios y aplicaciones de cliente multimedia SIP seguras, con Inter funcionamiento, enlace troncal y enrutamiento escalables, y se integra en el entorno de intercambio privado de sucursales (PBX) del cliente y migraclientes PBX a servicios IP y SIP de próxima generación. Esta solución se puede incluir en entornos IP independientes y proporcionar las aplicaciones multimedia SIP más recientes, como mensajería instantánea (IM), presencia y llamadas de video. La solución mejora la experiencia de comunicación general y lleva a los usuarios al siguiente nivel de integración de aplicaciones

5.7 SOFTWARE DE USO PROPIETARIO: AUDIO CODES ONE VOICE

AudioCodesOneVoiceOperations Center (OVOC) es una solución de gestión de red de voz que combina la gestión de dispositivos de red de voz y la calidad de la supervisión de la experiencia en una única aplicación intuitiva basada en la web. Esta plataforma permite a los administradores adoptar un enfoque integral para la gestión del ciclo de vida de la red al simplificar las tareas cotidianas y ayudar a resolver problemas desde la detección hasta la corrección.

Gracias al claro diseño de GUI de OVOC, los administradores del sistema pueden administrar el ciclo de vida completo de los dispositivos y elementos VoIP desde una única ubicación centralizada, ahorrando tiempo y costos. Las tareas que normalmente serían complejas y llevarían mucho tiempo, como realizar análisis de causa raíz, agregar nuevos dispositivos a la red VoIP e iniciar actualizaciones masivas de software, ahora se pueden llevar a cabo de manera rápida y fácil.

Por estas razones y por temas económicos al momento de poder hacer pruebas en un laboratorio vamos a usar en el resto de la monografía la plataforma **Asterisk**

6 ESTABLECER LAS POSIBLES AMENAZAS Y RIESGOS ASOCIADOS A LAS REDES DE DATOS EN DONDE SE IMPLEMENTAN SERVICIOS DE VOZ SOBRE IP.

6.1 AMENAZAS SOBRE LAS REDES VOIP.

Actualmente cuando se busca atacarunsistema de comunicaciones, casi siemprese busca poder generar una denegación de servicios, extorción, robo de información u obtener algún tipo de servicio de forma gratuita tales como llamadas.

Según Peter[23], hoy día la mayoría de los ataques a entornos VoIP lo que buscan es poder robar llamadas desde alguna de las centrales y con ellos poder generar algún ingreso económico, estos ataques generan a las compañías deudas millonarias ya que casi siempre las llamadas son de tipo internacional y si no se evidencia el ataque de forma oportuna las empresas se llevan una sorpresa cuando reciben las cuentas de facturación del servicio de telefonía por parte del PSTN.

Para poder hacer una descripción lo más exacta posible sobre las posibles amenazas en los entornos VoIP se hace necesario tener claros conceptos que nos permitan tener claridad del entorno.El activo es el recurso del cual dispone una compañía que permite desarrollar ciertas actividades cotidianas, dichos activos se van deteriorando y esto genera una depreciación en su valor y muchas veces ocasionan que ya no presten el mismo servicio para desarrollar las actividades generando esto a su vez un riesgo dentro de la empresa.

Según Peter y Ari[24], las vulnerabilidades llevándolas al enfoque informático representa debilidad o un posible fallo dentro de un aplicativo poniendo en riesgo la seguridad informática abriendo puertas a posibles ataques que comprometen la disponibilidad, integridad y la confidencialidad de la información, por lo que se hace necesario establecer procedimientos que permitan encontrarlas y mitigarlas para tenerlas controladas.

Las amenazas son aquellas acciones generadas debido a las vulnerabilidades existentes que permiten atentar contra la seguridad de un aplicativo. Las amenazas suelen derivar de ataques, eventos físicos o por malas decisiones dentro de una compañía que por lo general suelen ser negligencias. Alliance (VoIPSA). Es una organización sin ánimo de lucro que está confirmada por varias compañías y universidades del sector de las telecomunicaciones deformada por variasempresas que se dedican a la ciberseguridad.

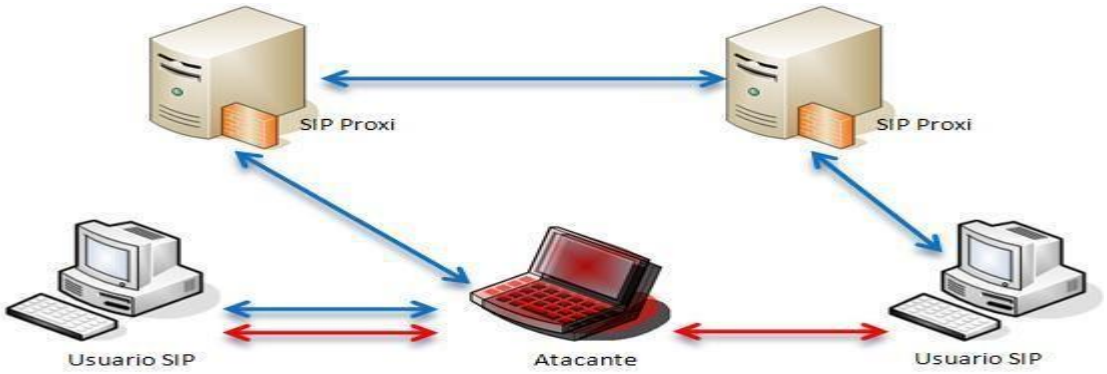
6.2 SECUESTROS DE LLAMADAS.

Con este tipo de amenazas se busca interceptarllamadas para efectuar actos ilegales o delictivos para modificar su finalidad, un atacante con conocimientos y con las herramientas necesarias puede conseguir contraseñas, cambiar el curso de una llamada incluso puede escucharla y llegarla a grabar así generando una falta grave a la privacidad pudiendo hacerse pasar por personas para generar extorsiones y demás delitos con fines lucrativos.

Para mitigar estos riesgos existen certificados como el TLS, que, aunque ayudan a la seguridad, muy pocas veces se implementan.Se debe tener claridad que un ataque genera impacto sobre la Integridad, confidencialidad y la disponibilidad del servicio.

[23]PETER T, ARI T, Securing VoIP Networks, 2008, p. 43
[24] Ibíd., p. 27

Figura 2. Secuestro de llamadas SIP



Fuente. Secuestro de llamadas SIP.https://docplayer.es/docs-images/84/90159952/images/74-0.jpg, 2020

6.3 ACCESOS NO AUTORIZADOS.

Los entornos de VoIP tienen consigo varios sistemas que permiten realizar diferentes tareas como el control de llamadas, administración, tarificación entre otras funciones.

Estos sistemas contienen información importante que, si llegan a ser comprometidos, los pueden usar en contra de la compañía para lograr el acometido de un fraude. Si esto llegara a ocurrir dentro de una empresa puede ocurrir que sus consecuencias sean nefastas dado que los datos (facturación, registros, datos de cuentas, entre otros) se usarían para cometer fraudes contra la empresa.

Según Wallingford[25], dentro de las amenazas más importantes de estas redes encontramos los accesos no autorizados o accesos desautorizados, dado que este tipo de acceso se hacen por haber obtenido una cuenta de algún usuario de la compañía y quien lo consigue puede efectuar llamadas a larga distancia nacional y larga distancia internacional. Una forma de controlar esto es realizando diariamente un control sobre las llamadas salientes, con esto podremos evidenciar comportamientos anormales que nos lleven a sospechar de que no está bien y tomar correctivos a tiempo.

[25] WALLINGFORD T, O'Reilly Media, Inc. All rights reserved,2006, p.228

6.4 DENEGACIÓN DE SERVICIOS

Según Carrasco[26], los entornos de VoIP tienen consigo varios sistemas que permiten realizar diferentes tareas como el control de llamadas, administración, tarificación entre otras funciones.Estos sistemas contienen información importante que, si llegan a ser comprometidos, los pueden usar en contra de la compañía para lograr el acometido de un fraude. Si esto llegara a ocurrir dentro de una empresa puede ocurrir que sus consecuencias sean nefastas dado que los datos (facturación, registros, datos de cuentas, entre otros) se usarían para cometer fraudes contra la empresa.

Como dice Peter y Ari[27], dentro de las amenazas más importantes de estas redes se encuentra los accesos no autorizados o accesos desautorizados, dado que este tipo de acceso se hacen por haber obtenido una cuenta de algún usuario de la compañía y quien lo consigue puede efectuar llamadas a larga distancia nacional y larga distancia internacional. Una forma de controlar esto es realizando diariamente un control sobre las llamadas salientes, con esto podremos evidenciar comportamientos anormales que nos lleven a sospechar de que no está bien y tomar correctivos a tiempo.

6.5 FRAUDE Y ABUSO.

Estas amenazas representan uso inapropiado que se asocian a abusos de los servicios o fraudes, esto se materializa en ataques, suplantación de identidad o en la evasión de facturación de las llamadas.

Como afirma Carrasco[28] existe un ataque denominado TollFraud, que es el que se presenta con mayor frecuencia al momento de sufrir un ataque, consiste en generar muchas llamadas de larga distancia internacional, para de esta manera poder generar alguna remuneración, esto lo logran haciendo tratos con personas estafadoras que reciben el servicio y lo venden a otros usuarios a bajo costo y sin ningún tipo de compromiso, una vez se puede acceder a la central IP de la compañía de forma fraudulenta, los estafadores implementan unos robots que les permita de forma rápida generar llamadas a cualquier destino, ocasionando altos costos económicos a la empresa.

[26] CARRASCO HIRUELO. Antonio, Documento de la Universidad de Cataluña Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Cataluña. 2019. p.30
[27] PETER T, ARI T, Securing VoIP Networks, 2008, p. 28
[28] CARRASCO HIRUELO. Antonio, Documento de la Universidad de Cataluña Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Cataluña. 2019. p.29

6.6 ACCESOS O DETERIORO DE EQUIPOS.

Como dice Carrasco[29] esta amenaza está relacionada con la capa física, los equipos que componen la solución deben ser actualizado con frecuencias y deben contar con contraseñas seguras, existen otros elementos que hacen parte de la capa física que también sugieren una amenaza tales como discos duros, servidores expuestos o con acceso físico no supervisado.

6.7 AMENAZAS DEL FACTOR HUMANO.

Según Carrasco[30] la intervención del ser humano en los distintos sistemas de información sugiere el mayor riesgo que pueda representar una solución, a nivel de máquinas y dispositivos se suponen fallos de asociados con defectos de los elementos, pero quizás el mayor riesgo es la configuración y parametrización que se realiza por medio de la mano del ser humano, esto sugiere un grupo de amenazas al que se expone cualquier sistema de voz moderno.

6.8 ATAQUES A LOS DISPOSITIVOS.

Gran cantidad de los ataques que existen hoy día que son dirigidos a las redes de datos, van dirigidos a: Hardware y el Software de los equipos, lo que involucra dentro de una solución de VoIP a los teléfonos, Servidores IP, Gateways como potenciales para un atacante.

Según Gutiérrez[31], se debe tener en cuenta que en una solución de VoIP las vulnerabilidades también se encuentran en los Sistemas Operativos o Firmware que corre sobre cada uno de los dispositivos que componen la solución, dentro de estos son muy frecuentes los ataques de tipo Fuzzing que envían paquetes malformados para provocar sobre carga en el sistema operativo y generar que se sature el sistema operativo generando indisponibilidad, otro tipo de ataque conocido es Flooders que tiene como objetivo explorar y encontrar que servicios están corriendo y que puertos están abiertos en los dispositivos de VoIP.

Otro de los aspectos que hacen que un dispositivo sea un punto de falla dentro de una solución VoIP es su incorrecta configuración, cuando en la solución se dejan puertos y contraseñas por defecto se acrecienta la vulnerabilidad y la posibilidad que un ataque sea efectivo, los servicios corren en dichos puertos por defecto y están más expuestos a ataques de DoS, desbordamientos de Buffer o cualquier otro tipo de ataque que el atacante conozca, afectando o comprometiendo el dispositivo IP.

---

[29] CARRASCO HIRUELO. Antonio, Documento de la Universidad de Cataluña Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Cataluña. 2019. p.29

[30] Ibíd., p. 29

[31] GUTIERREZ GIL. Roberto.Seguridad en VoIP: Ataques, Amenazas y riesgos, Universidad de Cataluña. p. 16

Dentro de las vulnerabilidades que hacen parte de una solución VoIP también se deben mencionar los teléfonos IP que usan los usuarios finales, estos si no tienen la configuración de forma correcta también comprometen a la solución de cara a un ataque de seguridad, dado que pueden ser un punto donde el atacante irrumpa en la red y con leer la configuración del servidor al que apuntan dejaremos servido en bandeja un ataque al servidor IP.

6.9 ATAQUES A SOLUCIONES VOIP.

Carrasco[32] afirma que un entorno de soluciones para la Voz IP cuenta con variados elementos informáticos para su funcionamiento, haciendo que sean más comunes los ataques cibernéticos, los sistemas tradicionales de telefonía antiguos que son basados en conmutación de servicios, también sufren de ataques tales como denegación de servicios o enmascaramiento de llamadas, para el caso los sistemas de voz modernos soportado por VoIP sufren también los mismos ataques que se enfocaban en la telefonía tradicional, sumando las falencias de todos los elementos que la conforman tales como redes IP y sus componentes como tarjetas de red, cifrado de información, servidores, puertos, servicios entre otros.

Teniendo en cuenta que la Voz IP corre sobre redes de datos y que tiene que convivir con todo lo que estas redes ofrecen en cuanto a servicio y ataques, es de aclarar que para VoIP lo más difícil de gestionar es la correcta implementación y configuración de cada uno de los servicios que ofrece con la finalidad de evitar los ataques que pueden llegar a comprometer la disponibilidad y confiabilidad del servicio, los ataques como ya los hemos mencionados pueden llegar a ser de tipo de denegación de servicios, Malware para interceptar información o el secuestro de la misma.

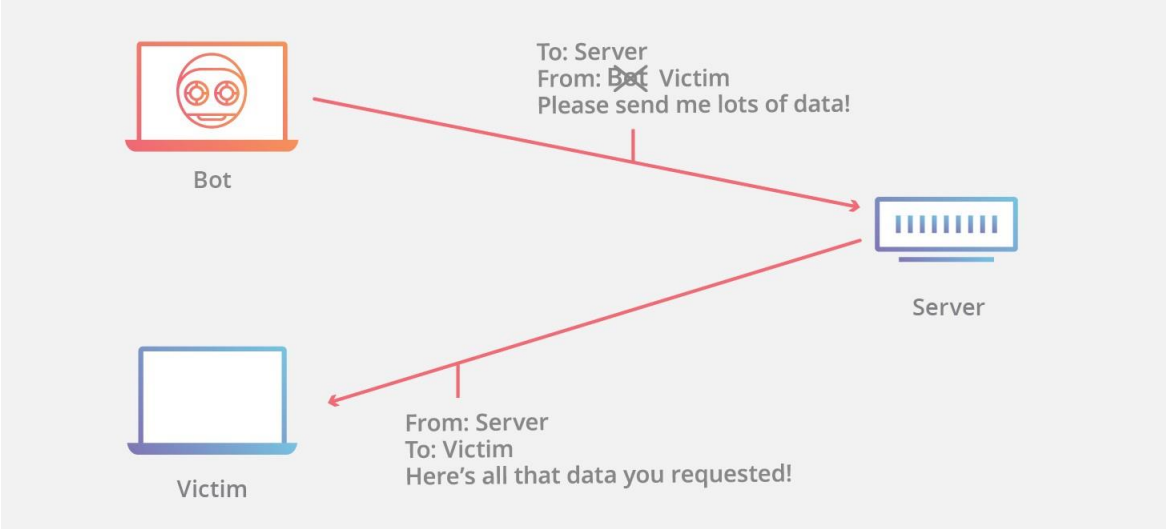
La investigación realizada nos indica que la mayoría de los ataques involucran los protocolos SIP y RTP asociados con la señalización de los paquetes, dado que su uso en la actualidad es el más común en este tipo de soluciones, el protocolo SIP está basado en características propias de la comunicación de correo electrónico y HTTP. En todos los ambientes estos protocolos están publicados y expuestos a ser analizados, estos tipos que son de tipo Textos comúnmente viajan por la red, por lo que analizarlos es muy fácil.Por otro lado, el RTP es usado como medio de transporte por muchos protocolos en la actualidad que involucran voz y video como los son H.323 O SCCP.

[32] CARRASCO HIRUELO. Antonio, Documento de la Universidad de Cataluña Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Cataluña. 2019. p.31

6.10 VULNERABILIDADES SUBYACENTES A LA RED.

Según Carrasco[33] la tecnología VoIP debido a que corre sobre la infraestructura de una red de datos o Internet, está muy expuesta a vulnerabilidades propias de la solución VoIP y de la solución de red de datos, la mayoría de ataques por no decir que todos, que van dirigidos hacia la red IP tales como denegación de servicio, inundación de paquetes sobre la red IP, van a poner en riesgo el servicio, la confiabilidad y la disponibilidad de la Voz sobre IP, también será susceptible a los diferentes ataques de bajo nivel como lo son la fragmentación IP, Spoofing, Secuestro de sesiones, entre otros ataques.

Figura 3. Secuestro de llamadas por método Spoofing



Fuente: Viemes.https://www.cloudflare.com/img/learning/ddos/glossary/ip-spoofing/ip-spoofing.png, 2020

De los mayores problemas que se puedan identificar es quizás la interceptación o eavesdropping que traduce (escuchar secretamente), por medio de este método de intrusión se llega a la captura de información cifrada o no cifrada, orientándolo a la telefonía IP estamos haciendo referencia a la interceptación de las conversaciones por quienes de forma inescrupulosa intervienen para captar conversaciones que no les corresponde.

Como dice Carrasco[34] la técnica de eavesdropping para la VoIP a comparación de las redes tradicionales de datos, no presenta mucha diferencia, esta técnica es capaz de interceptar diferentes comunicaciones en donde se obtiene toda clase de información sensible y confidencial, esta técnica usualmente interactúa de forma pasiva en las conversaciones,

[33] CARRASCO HIRUELO. Antonio, Documento de la Universidad de Cataluña Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Cataluña. 2019. p.33
[34] GUTIERREZ GIL. Roberto.Seguridad en VoIP: Ataques, Amenazas y riesgos, Universidad de Cataluña. p. 44

esto no quiere decir que pueda cambiar su actuar pasando a un poco más agresiva cambiando los datos de un paquete de voz o haciendo redireccionamientos para que los datos no lleguen a su destino, mientras su función es trabajar de forma pasiva solo escuchando, es prácticamente imposible detectar el ataque, cuando pasa a modo activo o agresivo es donde se puede evidenciar el ataque.

Según Gutiérrez[35], para interceptar una comunicación es tan sencillo como usar un sniffer en la red, si los datos no viajan cifrados serán más fáciles de interceptar y de descifrar los datos, hoy día es más común encontrarnos dentro de redes conmutadas cosa que hace que para que alguien al interior quiera escuchar nuestra red por medio de un sniffer no le será tan fácil, el tráfico que no vaya dirigido a un equipo en especial no es tan fácil de descifrar, se necesitará de técnicas más avanzadas y especializadas como un (Main in theMidle) usando envenenamiento ARP, entre las herramientas más usadas se encuentra Ettercap, Cain&Abel, también existen herramientas de distribución Linux como Dsniff y Vomit.

Las redes inalámbricas son en muchos casos un punto más de fallas que el intruso va a explotar, esto es posible si el atacante cuenta con herramientas avanzadas, si por parte de quien configura y administra la red, deja huecos de seguridad tales como actualizaciones de dispositivos o parámetros incorrectos, si el atacante alcanza la red Wifi desde allí podrá lanzar un ataque a la red VoIP.

6.10.1 Encontrando objetivos. Como dice Collier y Endler[36] cuando el atacante analiza las posibles redes a atacar, debe tener en cuenta cual de todas es más fácil de acceder, esto lo hace por medio de sondeos sobre las redes para validar cual tiene más vulnerabilidades que le permita acceder más rápido y sin perder tanto tiempo, una vez determinado esto, debe concentrarse recolectar la mayor información posible referente a su víctima. Esta información que se ha recolectado le sirve para determinar qué tipo de ataque usará que le permita tener éxito en el objetivo trazado.

Estos métodos para obtener información se llevan a cabo con técnicas que van de menos a más hablando en niveles de instrucción, es decir ataques menos invasivos que van solo desde escucha, hasta ataques más agresivos que secuestraninformación o interfieren en el destino de dicha información. Esto se hace para evitar ser detectados muy temprano en el ataque y de esta manera el atacante realiza un footprinting que le permite obtención de la mayoría de información que esté pública y accesible correspondiente al objetivo fijado.

El siguiente paso consiste en recolectar la mayor información posible de los equipos conectados a la red, servicios que corren sobre estos equipos, puertos que usan, direcciones IP entre otros aspectos que el escaneo pueda obtener y que sean de utilidad para el Hacker, la información recolectada apoyada de otras herramientas que el atacante pueda usar le permitirán obtener información sensible, tales como vulnerabilidades, agujeros de seguridad asociadas al sistema operativo, actualizaciones de aplicativos,

[35]Ibíd, p. 14
[36] COLLIER Mark, ENDLER David. Unified Comunications and VoIP. 2014. p.52.

ataques de enumeración, entre otros, con esto lo pueden explotar y encontrar una posible vía de entrada a los diferentes sistemas.

Un ejemplo que dan Collier y Endler[37], de un ataque de enumeración sería usar fuerza bruta dirigido a los servidores que soportan el servicio de VoIP con la finalidad de obtener el listado de extensiones telefónicas IP habilitadas. Esta información sería demasiado útil para el atacante ya que con ella podría ejecutar otro tipo de ataques en la red tales como inundaciones INVITE o secuestro de información y registros.

6.10.1.1 Footprinting. Según Gutiérrez[38], este método de ataque informático es conocido por tener la habilidad de recolectar la mayor cantidad de información posible de un entorno de red especifico, esto tiene la finalidad de encontrar múltiples formas para poder acceder por algún agüero de seguridad que presente el entorno de red al que se quiere atacar.

Casi todas las herramientas básicas necesarias para la etapa de exploración a la red las podemos encontrar en el buscador Google. Las diferentes herramientas que puedes encontrar en este buscador te permiten realizar análisis sobre la página web corporativa de una empresa y el dominio, también permite realizar búsquedas sobre correos electrónicos, direcciones de contacto, teléfonos, entre otros que le permiten al atacante realizar ataques de suplantación de identidad e ingeniería social.

6.10.1.2 Protocolos VoIP y sus vulnerabilidades. Según Regis[39], los protocolos se clasifican en:

- Señalización:Veremos los protocolos de señalización H.323 Y SIP, también veremos el protocolo que interviene en el establecimiento de esta señalización como lo es SDP.

- H.323: Este protocolo es recomendado por la unión internacional de telecomunicaciones. El protocolo H.323 define los requisitos necesarios para sistemas multimedias que basan el transporte de la información en una red de datos, dado que se puede presentar que la calidad de servicio sobre este medio no sea garantizado, este protocolo es muy completo hablando de las funcionalidades que cumple sobre las soluciones de VoIP, este protocolo incluye a la solución de forma embebida la calidad de servicio (QoS), esto ayuda a que no se necesario de otro tipo de software o Hardware para garantizar la transmisión de la voz.

- El protocolo H.323 usa otros protocolos para cumplir su función. RTP: Se usa para transportar la Voz.

[37] COLLIER Mark, ENDLER David. Unified Comunications and VoIP. 2014. p.52.
[38] GUTIERREZ GIL. Roberto.Seguridad en VoIP: Ataques, Amenazas y riesgos, Universidad de Cataluña. p. 16
[39]REGIS J. Securing VoIP. El Sevier. 2015. p.71.

- H.245: Protocolo para el control de comunicaciones multimedia.

- H.450: Servicios suplementarios como transferencia de llamadas, llamadas en espera, entre otros servicios.

- H.235: Describe la seguridad del protocolo H.323

- H.225: Se usa para la señalización de las llamadas y empaqueta los mensajes.
- RAS: Usa los mensajes H.225 para garantizar la comunicación entre el Gateway y el Gatekeeper, además controla el ancho de banda que se usa en la comunicación.

- Ataque H.225: este tipo de ataques consisten en amenazas de denegación de servicios, este ataque se genera por vulnerabilidades existentes en los mensajes de instalación de H.225

- Ataque H.245: Este también es una amenaza de Denegación de servicio, la vulnerabilidad que se explota está relacionada con el mensaje que describe las capacidades del terminal que recibe la llamada, el mensaje TCS es transmitido antes de iniciar la llamada, determinando la versión del firmware y capacidad del terminal.

- Malformación de mensajes RAS: este tipo de ataques también es de denegación de servicio, estos aprovechan las vulnerabilidades con las que cuenta el RAS cuando envía los paquetes al GateKeeper y hace que una estación H.323 se comunique con otra estación en la red para generar inundación de paquetes, ocasionando la desconexión de los teléfonos y la generación de broadcast en la red.

- Protocolo SIP: Este protocolo se encarga de establecer la llamada en la telefonía IP y administrar la señalización que se usa para establecer, modificar y terminar las llamadas, este protocolo se caracteriza por ser de uso libre y abierto que no depende de ningún proveedor, este protocolo soporta audio, video y videoconferencia incluyendo mensajería instantánea.

6.10.1.3 Protocolo SIP. Según Gutiérrez[40], los protocolos que usa el protocolo SIP se clasifican en:

- RTP: conocido como protocolo de transporte de tiempo real, una vez que el SIP establece la llamada, RTP se encarga de transportar la voz. SDP: Conocido como protocolo de descripción de sesión, estos mensajes son transportados por el protocolo SIP para poder negociar de mejor manera las capacidades de cara a los participantes.

[40] GUTIERREZ GIL. Roberto.Seguridad en VoIP: Ataques, Amenazas y riesgos, Universidad de Cataluña. p. 6

- Ataque a hashes digest: como dice Gutiérrez[41], esta es una amenaza de acceso no autorizado, la autenticación digest es utilizada para validar la identidad de los usuarios que pertenecen al sistema de VoIP, este tipo de autenticación fue inicialmente desarrollada para ser usada con el protocolo HTTP, que era basado en un mecanismo en HAS, para evitar que las contraseñas de los usuarios se envíe por texto plano, es decir la contraseña se cifra, el método de hashes digest se encargan solo de cifrar la contraseña pero no el mensaje.El ataque por hashes digest, una vez se capturen los paquetes SIP, es posible obtener la contraseña del usuario, dejando vulnerable la seguridad y que se puede atacar de dos modos:

- Método de fuerza bruta: este ataque permite descubrir las contraseñas probando todas las combinaciones posibles hasta encontrar la que permite el acceso al atacante.

- Método de diccionario: este ataque lo que hace es que crea una serie de combinaciones con todas las palabras que se encuentran en el diccionario que crea el atacante.

- Suplantación de Identidad: esta amenaza utiliza la vulnerabilidad en el mensaje que se envía REGISTER. Dado que el registro del usuario es la primera acción que sucede al momento de registrar el inicio de sesión en la plataforma VoIP, la comunicación entre el cliente y el servidor se debe establecer de forma segura, esto es muy importante dado que, si un atacante nos suplanta, la comunicación establecida no se garantiza y puede ser escuchada por quien no corresponde.Para poder hacer contrapeso a este riesgo, el sistema envía dos secuencias de caracteres de forma aleatoria, una secuencia es para identificar la comunicación (noncey) y otra para identificar el dominio del usuario (realm), con esto se puede garantizar que los mensajes en caso de ser interceptados no funcionen en otra comunicación.

6.10.1.4 Protocolos propietarios. Como dice Regis[42], los protocolos que se usan de forma propietario para las soluciones de VoIP, SCCP y IAX2, estos protocolos son usados de forma masiva en redes de Voz sobre IP

- SCCP: este protocolo de uso propietario de Cisco es usado para la comunicación con las terminales definiendo el conjunto de los mensajes que se transmiten entre un cliente IP (teléfono o software) y la central telefónica.Es un protocolo bastante liviano que permite establecer comunicaciones de forma eficiente con todos los dispositivos de sistema Cisco y el Callmanager, este último funciona tal cual un proxy señalizando las llamadas iniciadas por medio de otros protocolos que se integran, tales como el H.323, SIP.

[41]Ibíd., p. 22
[42] REGIS J. Securing VoIP. El Sevier. 2015. p.170.

- Vulnerabilidades asociadas al Call Manager (servidor VoIP): Las vulnerabilidades asociadas a las centrales telefónicas tienen asociaciones con protocolos propietarios y también otras se asocian a protocolos de la capa de transporte que son propios de una red de datos tales como TCP y UDP.

- CUCM y CUPS: los dos protocolos tienen vulnerabilidades que permiten ataques remotos asociados a la alteración de los mensajes por protocolos TCP, UDP e ICMP, a todas estas vulnerabilidades el propietario de los protocolos (CISCO) ha liberado los parches de seguridad necesarios para corregirlos.

- Callmanager: estos servidores pueden sufrir ataques debido a vulnerabilidades que se presentan en los puertos por defecto que trae la solución, tales puertos son TCP 2000 o 2443, dichos puertos son usados por SCCP.

- Vulnerabilidad UDP: esta afecta el IPSec orientado a CUCM y CUPS, aquellos servicios que usan el puerto 8500 por el protocolo UDP, esta vulnerabilidad propiamente no permite que el hacker pueda tener acceso a las llamadas que emite el servidor Cisco, pero si puede afectar otras características que afectan la capacidad correcta de transferir las llamadas.

- IAX2: Este protocolo se desarrolló orientado a la solución de uso libre Asterisk, este protocolo tiene como misión la tarea de minimizar el consumo de una llamada en el ancho de banda al momento de transmitir la información, este protocolo es binario y no de texto, con esto mejora la compresión de los datos transmitidos.

- Ataque POKE: es un ataque de denegación de servicios, que, por medio de envíos masivos de paquetes, vuelven al sistema vulnerable en cuanto a la estabilidad, en este caso el atacante podría interceptar todas las llamadas y los números de teléfonos entrantes afectando el normal procesamiento de las llamadas.

- Inundación con IAX: Este es otro tipo de ataques de denegación de servicios, envía muchos mensajes de gran tamaño con la finalidad de hacer que el equipo receptor colapse, esto es posible dado que IAX2, no autentica todos los mensajes.

- Ataque de espera: corresponde a una amenaza de tipo de denegación de servicios que usa la vulnerabilidad QUELCH. Por medio de este mensaje, el sistema detiene el audio que se transmite en el momento por la solución, lo que ocasiona que, si se detienen muchas llamadas y quedan en cola, esto hace que el ancho de banda colapse y afecte no solo a la solución de VoIP si no a todos los servicios que corren en la red.
- Protocolo SRTP: Es conocido como el protocolo de transporte de tiempo real seguro, este protocolo provee seguridad a los protocolos asociados RTP y RTCP

- SRTP: este protocolo provee seguridad en el paquete transmitido sin incrementar de forma exagerada el tamaño del paquete, este protocolo encripta el paquete cuando se transmite.

- SDES: es un protocolo que se usa para intercambio de llaves que permitan realizar el intercambio de las llaves correspondiente al protocolo SDP, las llaves que se negocian son criptográficas que permiten mayor robustez.

- ZRTP: es un protocolo de encabezado RTP que permite establecer llaves de inicio de sesión que involucran el protocolo Diffie Hellman, pero el protocolo ZRTP no requiere compartir llaves, esto se transcribe en que se anule un servidor certificador y las llaves no quedan expuestas a los diferentes ataques.

- MIKEY: es un protocolo que permite el intercambio de llaves para SRTP, este protocolo tiene como característica un bajo consumo del ancho de banda al momento de proteger los datos, adicional permite negociar la llave presentando mejoras de SDP, esto sucede en el momento que se establece la sesión con el protocolo SIP.Puede funcionar de 3 formas distintas

  Modo de intercambio de llaves pre-compartido (PSK): Es de los modelos más eficientes que pueden existir al momento se compartir las claves.

  Modo de intercambio de llaves públicas (PKE): Este modelo se encarga de crear una llave propia encriptada, basada en llaves públicas, este modelo necesita mayor performance del servidor.

  Modo de intercambio de llave Diffie-Hellman (DH): Este modelo no es malo, pero es quizás el que mayor número de elementos necesita para funcionar, dado que necesita una entidad certificadora para poder funcionar y solo permite el intercambio de llaves ente dos terminales.

6.11 INGENIERÍA SOCIAL Y/O PHISHING DE VOZ.

Según Gutiérrez[43], este tipo de ataques involucran a un atacante que por medio de engaños llega hasta su víctima, haciéndola creer que está accesando a páginas oficiales de alguna entidad, pero lo que realmente está haciendo es que por medio de un estudio previo de sus gustos y/o aficiones, lo lleva hasta una página fraudulenta para poderle robar, ya sea dinero o su identidad en internet, como tomando usuarios y contraseñas de alguna cuenta que para el atacante genere valor.

Orientado hacia los posibles ataques que se puedan recibir desde la Voz IP, el atacante puede hacer que el funcionario de una empresa marque a un IVR falso y digite en este toda

[43] GUTIERREZ GIL. Roberto.Seguridad en VoIP: Ataques, Amenazas y riesgos, Universidad de Cataluña. p. 35

la información que necesita, en cualquier caso, el Phishing siempre busca engañar a los usuarios.

Vamos a hablar un poco sobre el capital humano, este que es quizás el más complejo por la formación que tenga, no siempre en una compañía los usuarios deben saber de tecnología, pero si deben tener claro los riesgos que corren cuando se usa la tecnología y más aún la tecnología de una empresa ya que puede ser la pieza del eslabón que se rompe y por la cual se puede afectar la economía de una empresa.

Como dice Gutiérrez[44], se debe evaluar la seguridad humana, esto siempre ayuda en los casos de ataques dirigidos por IVR, durante las fases de exploración y enumeración, los atacantes buscan establecer algún tipo de contacto con sus víctimas, que les permita ahondar más sobre la empresa a la que están atacando, esta información al principio suele ser útil, esto puede generar mayor interés del atacante sobre la compañía que está atacando, es por esto que invertir en capacitar al personal de las compañías sobre la ciber delincuencia en muchas ocasiones pueden salvar las finanzas.

Es importante que se plantee las siguientes preguntas: ¿Los agentes del centro de llamadas conocen los problemas de seguridad que tiene la empresa?

Según Collier, Endler y Hill[45], si el atacante es capaz de descubrir DID o extensiones de los usuarios, es posible que los agentes experimenten acosos, SPAM de voz que le impide que pueda realizar su trabajo de forma correcta, llamadas de phishing en donde se les solicita realizar alguna actividad que comprometa la seguridad de la empresa o del propio funcionario, existen diferentes métodos de aplicar ingeniería social y TDoS dentro de un sistema de Voz IP.

Un TDoS, es una denegación de servicio telefónico, es decir en vez de inundar con paquetes la red como lo haría un DoS normal, este se encarga de inundar el sistema de VoIP con muchas llamadas, que hace que colapse el sistema impidiendo que las llamadas se puedan contestar y brindar el servicio que la compañía ofrece, este término fue brindado por el FBI en el año 2010.

Como ya lo mencioné antes, la ingeniería social es algo a lo que debemos ponerle mucha atención dado que es un tema muy amplio y los usuarios que estamos frente a una computadora con conexión a internet debemos saber cómo identificar si nos están haciendo ingeniería social para luego por medio de un Phishing engañarnos y robarnos información o dinero.

Uno de los sectores más atacados con frecuencia, son los servicios financieros, los atacantes o delincuentes cibernéticos, buscan al interior del banco los funcionarios que constantemente están procesando información, tales como tarjetas de créditos, pagos de créditos, a quienes llaman con información parcial de un cliente, tales como nombres,

[44]Ibíd., p. 36
[45] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.289.

números de cuentas, la referencia de un crédito o cualquier otra información que le permita persuadir al agente del banco para que le entregue más información para poder extraer dinero, este tipo de ataques son un poco más exigentes, va necesitar de un delincuente muy convincente al momento de persuadir al agente, que este debe ser muy incauto, estar sobre cargado de trabajo o estar un poco disperso al momento de atender la llamada, esto no tiene mucho éxito siempre, pero algunas veces encuentran la victima perfecta y terminan robando dinero de la cuenta del banco de un cliente.

Es cierto que cada vez más los clientes están usando los servicios de internet o aplicaciones móviles, pero también sabido que este tipo de actividades también está expuesto a muchas amenazas, es por esto que muchos clientes todavía prefieren usar el servicio telefónico especialmente para transacciones financieras como traslados de fondos de una cuenta a otra.

Como dice Collier, Endler y Hill[46], la ingeniería social se ha vuelto mucho más fácil para los atacantes y difícil de detectar para las empresas, hoy día el atacante pude falsificar un número telefónico y hacerlo pasar como real cubriendo todas sus huellas con los diferentes aplicativos que puedes encontrar en Internet, los atacantes consiguen información básica de los objetivos, tales como nombres, apellidos, apellido de soltera de la madre, fechas de nacimientos, entre otros, esta información suelen ser posibles respuestas de seguridad de cuentas o cualquier otra información que esté en internet y sea útil para el atacante, con el tiempo necesario y toda la información que pueda recopilar se pueden realizar múltiples llamadas por medio de un IVR dirigido a los objetivos que previamente han sido estudiados y con toda la información conseguida es factible que en algún momento caiga en la trampa del atacante.

Recopilación de información personal:según Carrasco[47], la recopilación de información personal como el número de afiliación a un centro médico, fecha de nacimiento, el apellido de soltera de la madre y el número de teléfono como una forma de obtener información crítica de la cuenta es cada vez más fácil. Un atacante armado con información básica puede usar las redes sociales para recopilar datos más importantes. Se pueden utilizar varios recursos en Internet para recopilar información personal básica:

Según Collier, Endler y Hill[48], Facebook es un gran lugar para recopilar información básica, los usuarios publican habitualmente números de teléfono, direcciones e información que se pueden usar para preguntas de seguridad tales como nombres de mascotas, escuelas secundarias a las que asistieron y enlaces a familiares, que se pueden usar para determinar datos importantes de las personas, que permiten armar una base de datos con todos esos datos y luego orientar las campañas de Phishing de manera más efectiva a esos usuarios. Otros sitios de redes sociales en los cuales también se puede recolectar información sensible de los usuarios son: Twitter, Instagram, Tumbler y LinkedIn.

[46] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.289
[47] CARRASCO HIRUELO. Antonio, Documento de la Universidad de Cataluña Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Cataluña. 2019. p.34
[48] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.292.

Figura 4. Redes Sociales

Fuente. Redes sociales.https://red.computerworld.es/archivos/201802/redes-sociales-hombre.jpg, 2020

6.11.1 Elegir un centro de contacto específico como objetivo. Como afirman Collier, Endler y Hill[49], la ingeniería social, normalmente se dirige a un agente de llamadas telefónicas, pero también es útil saber los procedimientos de seguridad de la empresa donde labora el usuario. Algunos procedimientos de seguridad pueden ser más débiles que otros o, pueden requerir una información de autenticación que le resulta difícil recopilar. Es posible que algunos centros de contacto le den más valor al número que llama, lo que hace que la suplantación de identidad sea más útil. Como dice Collier, Endler y Hill[50], que algunos centros de contacto sean menos seguros, puede encontrar que algunos parecen tener muchos agentes sin experiencia, o con más sobrecarga laboral y es posible que otros tengan muy poca correlación entre varias llamadas y consultas en una cuenta.

SegúnCollier, Endler y Hill[51], un mecanismo de seguridad que utilizan algunos centros de contacto es devolver a llamada al número registrado en la cuenta de los clientes. Esto mitiga la suplantación de números de llamada, porque la devolución de llamada irá al número real del usuario en lugar de al atacante. Una forma en que los atacantes pueden abordar esto es hacer una llamada por separado para cambiar el número de teléfono de la cuenta, utilizando el motivo por el que el usuario se ha "mudado". La transacción financiera ilícita debería realizarse rápidamente antes de que se notifique al usuario real del cambio en su cuenta. Ya sea que el atacante pueda identificar una organización financiera con procedimientos de seguridad débiles.

[49] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.291.
[50] Ibíd., p. 293
[51] Ibíd., p. 292

6.11.2 Ingeniería social para contramedidas de fraude financiero. Como dice Collier, Endler y Hill[52], la protección de la información personal es fundamental, aunque cada vez es más difícil, los usuarios deben hacer todo lo posible por no divulgar información personal más de lo necesario y evitar colocar voluntariamente en Internet información que no necesite compartir. Algunos sitios lo encontrarán de todos modos, pero no hay ninguna razón para facilitárselo. Desafortunadamente, una vez que la información está disponible en línea, es difícil, si no imposible, eliminarla. Se puede detener a los atacantes de ingeniería social poco sofisticados si llaman continuamente desde el mismo número o con números de partes del país o del mundo donde una empresa no opera.

Estas llamadas se pueden detectar o bloquear con una lista negra básica. Las personas que llaman también pueden ser detectadas o bloqueadas al analizar el audio si bloquean su número de llamada.Bloquear el número que llama realmente facilita la detección del atacante

Una de las mejores recomendaciones para identificar y defenderse con éxito contra ataques de ingeniería social a través de líneas de voz es tener la capacidad de analizar patrones de llamadas y correlacionarlos con actividades fraudulentas de ingeniería social conocidas o sospechadas. Una vez que se detecta una actividad sospechosa, la capacidad de registrar y analizar esas llamadas para determinar si representan ingeniería social es clave. Las llamadas de ingeniería social confirmadas o sospechosas pueden redirigirse a agentes más experimentados o al equipo de seguridad. Las listas negras se pueden utilizar para bloquear futuras llamadas de números que se sabe que están asociados con la ingeniería social.

Según Porter[53], la empresa SecureLogix tienen firewall de voz y productos IPS que pueden monitorear este tipo de actividad y bloquear los números para evitar que vuelvan a llamar con la intención de realizar un fraude.Otra contramedida es emplear alguna forma de autenticación, que no sea información personal tradicional. Una estrategia de autenticación se basa en demostrar que el consumidor es realmente quien dice ser. Existen diferentes formas de esto, pero la más prometedora es el uso de datos biométricos para la autenticación del cliente que realizar la llamada. La idea es que los consumidores se inscriban, capaciten al sistema para que los reconozca y luego se confirmen cuando llamen. Esta tecnología no es perfecta, los consumidores deben optar por el servicio y entrenar el sistema, y aunque la precisión no es perfecta, está mejorando cada vez más.

6.11.3 Contraparte a la ingeniería social. Collier, Endler y Hill[54], afirman que lamejor forma de hacer contrapeso a la ingeniería social es la educación, desafortunadamente no es fácil hacer que todos estén a la vanguardia de la tecnología y los riesgos que esta lleva consigo, así como también la forma de identificar una posible amenaza o riesgo en la internet o en las redes de cómputo, en general nunca se debe compartir información sensible a personas desconocidas o en quienes no se confíe.

[52] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.298
[53] PORTER Thomas. Practical VoIP Security. Editorial Syngress. 2006. p. 99
[54] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.300

6.11.3.1 Phishing de voz. Según Collier, Endler y Hill[55], Es una técnica que se usa para el robo de identidad, normalmente es dirigido a un objetivo específico, ya sea un usuario o una empresa, los ciberdelincuentes crean sitios web muy parecidos a los sitios reales, en muchas ocasiones son realizados a la medida para un grupo de usuarios dependiendo de los gustos o hobbies que estos tengan, pero esto se hace con una previa recopilación de información de ese grupo de usuarios, esto se hace por ingeniería social que se mezcla con muchas técnicas de robo de información que existe en la internet, entonces una vez con la información suficiente del objetivo es donde entre el Phishing, este llega por medio de un correo electrónico comúnmente y es donde el usuario es engañado y llevado a un sitio web falso que se le parece muy familiar pero dicho sitio está lleno de Spam y demás virus que se introducirán a su computadora para luego poder ejecutar el cometido del ciberdelincuente, que orientado a la voz sería poder encontrar la central telefónica, contraseñas guardadas en el PC y que sean asociadas con la central telefónica y una vez tienen este acceso pueden sacar llamadas a su antojo y peor aún si logran tener acceso a la central telefónica pueden tener acceso a la información del servicio SIP y realizar llamadas a cualquier parte del mundo perjudicando de esta manera a la empresa que fue vulnerada y llenando los bolsillos del atacante que vende esos minutos a usuarios que muy seguramente no saben que son obtenido de forma ilícita.

Como dice Collier, Endler y Hill[56], el phishing por voz, es muy similar al phishing por correo electrónico, el atacante envía mensajes de correo electrónico que, en lugar de tener un enlace para hacer clic tienen un número legítimo para llamar, que normalmente es un número 01-8000, en este caso el atacante puede generar llamadas de voz solicitando a la víctima que vuelva a llamar al número 01-8000. Cuando la víctima devuelve la llamada, el atacante la recibe con un IVR falso que intenta recopilar los números de cuenta de la víctima y otra información.

El phishing de voz necesariamente necesita que el atacante configure un IVR falso, con la intención de engañar a las víctimas para que ingresen información confidencial o cualquier información personal que pueda ser útil para el atacante por medio de la cual pueda obtener más información para realizar por ejemplo alguna transacción financiera de forma ilícita. El IVR grabará audio, que se pueden reproducir y decodificar fácilmente, plataformas como el software Asterisk han facilitado mucho la configuración de este tipo de IVR, cabe aclarar que por ser una herramienta de código abierto los ciberdelincuentes lo aprovechan, no es que el software sea malo o esté más propenso a sufrir ataques, si está bien configurado será tan seguro como un software de Voz IP de pago.

El phishing de voz se basa en la credulidad efectiva de una víctima que confía en un número de teléfono más que en un enlace de correo electrónico. Por un costo muy bajo, un atacante puede configurar el IVR a través de un proveedor SIP que es más difícil de rastrear que un servidor web comprometido. Además, la naturaleza de SIP hace que este tipo de ataque sea aún más factible porque la mayoría de los servicios SIP otorgan a sus clientes un número ilimitado de llamadas por una tarifa mensual a muy bajo precio.

[55] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.301
[56] Ibíd., p. 301

6.11.4 Contraparte al phishing de Voz. Según Collier, Endler y Hill[57], para contrarrestar el Phishing de voz en una empresa y evitar que lleguen a los empleados de la compañía, existen muchas soluciones en el mercado, empresas se dedican a brindar soluciones y mitigar el riesgo cuando de Phishing de voz se trata, es decir son soluciones anti-Spam enfocadas a los correos electrónicos que por medio de inteligencia artificial pueden determinar un posible ataque por medio de Phishing, estas herramientas deben ser configuradas e implementadas por sus fabricantes y/o Partner calificado para implementar la solución. Dentro de las diferentes soluciones más conocidas en el mercado encontramos a las compañías: Sophos, Barracuda, McAfee, Symantec.

La educación hacia los usuarios dentro de una compañía es algo muy importante, es algo que la empresas deben hacer, invertir en educar a sus funcionarios, esto sin duda alguna va ayudar mucho a la seguridad de una empresa, es muy fácil llegar a un usuario inexperto o que no sea capaz de reaccionar ante un ataque de Phishing ya sea por correo o de voz, esta falta de conocimiento le puede costar a una empresa pérdidas millonarias, es mejor tener empleados capacitados y que sean capaz de evidenciar una posible estafa para luego evitar problemas a futuro.

Cuando se presentan phishing de voz, el empleado debe evitar devolver las llamadas a IVR dedicados a la estafa, debe reflexionar si él ha solicitado dicho servicio o no, debe saber que datos les están solicitando y si es prudente entregarlos a un desconocido, todo esto hace que un empleado esté del lado de la seguridad informática.

Los ataques de ingeniería social y phishing de voz seguirán aumentando. La ingeniería social, puntualmente en los Call Center financieros, es un problema que ha empeorado mucho debido a la capacidad de recopilar información personal básica desde Internet y de esta manera falsificar el número de la llamada.

El phishing de voz es una evolución del phishing por correo electrónico y es más eficaz debido al nivel de confianza que aún se mantiene para las llamadas telefónicas y porque estos mensajes rara vez se bloquean. Además, las redes VoIP han facilitado que las llamadas de phishing de voz sean asequibles. Configurar un número 01-8000 y un IVR falso es más sencillo que nunca. La recolección de información personal desde Internet, ingeniería social y phishing de voz aumenta enormemente la amenaza de fraude financiero.

7 DOCUMENTAR LAS MEJORES PRÁCTICAS DE SEGURIDAD INFORMÁTICA QUE PERMITA EL ASEGURAMIENTO DE PLATAFORMAS Y/O SISTEMAS DE VOZ/IP.

[57] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.312

7.1 MEJORES PRÁCTICAS PARA LA SEGURIDAD EN LA INFRAESTRUCTURA.

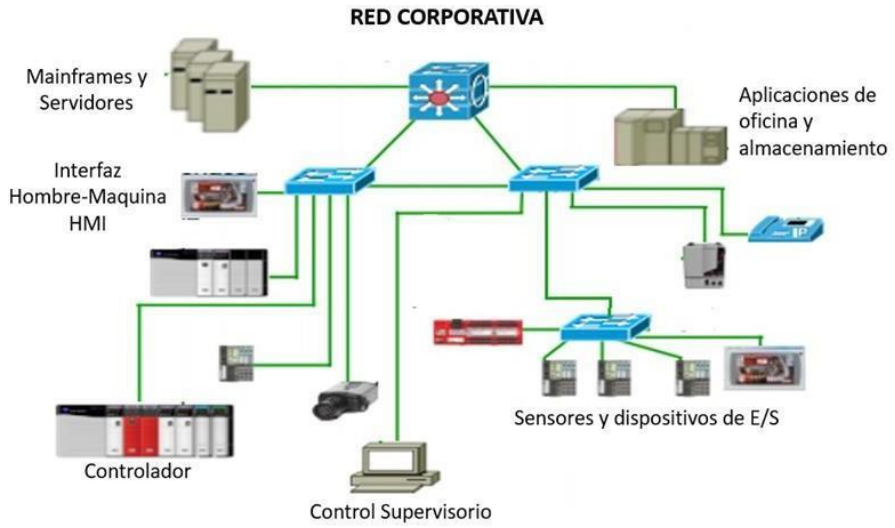
Como diceCollier, Endler y Hill[58], si se tiene en cuenta todos los problemas ya mencionados durante la recopilación de la información, se hace necesario destacar algunas buenas prácticas que se deben tener en cuenta a la hora de implementar una red de datos por la cual vamos a transmitir voz, recordemos que una de las ventajas en cuanto a implantación y bajo costo de las redes de VoIP es que usan las redes de datos ya existentes en las compañías pero que esto también puede jugar en contra si no se hace una correcta configuración y parametrización.

a. Los equipos activos tales como Modem, Router y/o Switch, deben ser administrados mediante el protocolo HTTPS en caso de ser accesados por la web y usar también el protocolo SSH, estos accesos deben estar limitados por una lista de accesos (ACL).

b. Las Vlan´s deben estar separadas, una de las recomendaciones que se hace a nivel de seguridad, es separar la Vlan de voz de la Vlan de datos, con la finalidad de poder segmentar el tráfico por segmentos de redes distintos.

c. Los ID de las Vlan deben ser cambiados por el que trae por defecto el Switch, uno de los errores más comunes es que dejan activo la Vlan 1 y por esa Vlan transmiten datos y esto se presta para que los atacantes puedan de forma más fácil encontrar la información.

Figura 5. Red Corporativa



[58] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.407

Fuente: Red corporativa. https://isamex.org/intechmx/wp-content/uploads/2017/09/figura01-Small.jpg 2020

Lo anterior son solo algunas de las buenas prácticas que se deben tener en cuenta al momento de implementar la solución de VoIP en ambientes corporativos y de forma local, pero cabe aclarar que esto lo debe asegurar el área de infraestructura de la compañía, es algo que se debe tener en cuenta como básico y necesario para iniciar con una implementación para garantizar la seguridad y el correcto funcionamiento de la solución.

Collier, Endler y Hill[59], aseguran que VoIP es una tarea importante si va a proteger la información, sibien las organizaciones a menudo piensan en la seguridad en términos decarpetas y archivos, la información hablada por voz puede ser igualmenteimportante.Muchas empresas suelen decir que la comunicación de VoIP que ellos utilizan, es de uso interno y que no tienen problemas con la seguridad, pero ya vimos que, si tenemos una red de datos mal implementada o con falencias, esto va a afectar la seguridad del VoIP.

También es de aclarar que el aseguramiento de esta plataforma o solución va mucho más allá de la red de datos que la soporta, es de aclarar que esto es igual que cualquier otra solución que soporte la operación de una compañía y es de constante soporte y mantenimiento, las actualizaciones de seguridad al S.O que soporta la plataforma es vital, la actualización del Hardware también es vital, la actualización del Firmware de la plataforma a medida que vaya siendo mejorada, también se debe actualizar y el monitoreo constante de los Log que genera.

La plataforma son de vital importancia para saber el estado y la salud del sistema, pero muchas empresas evitan mirar esto debido al alto costo que esto puede llegar a tener, si, desafortunadamente asegurar VoIP en la forma y manera correcta muchas veces resulta engorroso haciendo que el proceso se vuelva costoso implicando muchas veces el cambio de Hardware por obsolescencia tecnológica representando esto para la compañía el gasto de un dinero adicional, sumado a esto el pago de las horas al profesional capacitado correctamente para ejecutar dicha actividad.

7.1.1 SIP Sobre SSL / TLS. Como dice Collier, Endler y Hill[60], cuando se habla sobre SSLv3 y TLSv1, que se usa por medio del protocolo TCP y por el puerto 5061, cifrar la información con SSL / TLS, es un método bastante efectivo que permite proteger la información de la sesión SIP de posibles ataques.

Como ya se ha abarcado en este documento, SIP es un protocolo de texto sin cifrar que puede ser manipulado y monitoreado por atacantes pasivos en la red. Además, el método de autenticación utilizado por SIP es autenticación de resumen, que es vulnerable a un ataque de diccionario sin conexión. Un ataque de diccionario fuera de línea por sí solo es una preocupación; sin embargo, combinado con el hecho de que la mayoría de los agentes de usuario SIP utilizan códigos de cuatro dígitos para las contraseñas, en ocasiones los

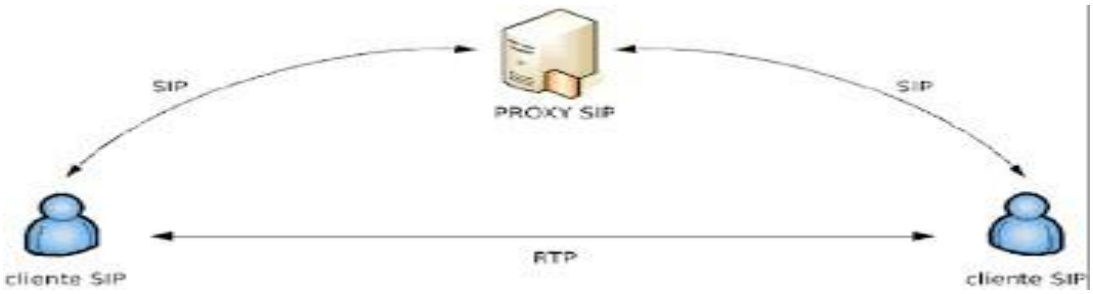
[59] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.408
[60] Ibíd., p. 463

usuarios utilizan los últimos cuatro dígitos de la extensión del teléfono, facilitando esto que la autenticación SIP sea muy vulnerable a los atacantes.

7.2 RTP SEGURO.

Según Collier, Endler y Hill[61], Secure RTP (SRTP), según definición en el RFC 3711, es un protocolo que agrega cifrado, confidencialidad e integridad a la parte de voz real de las llamadas VoIP que utilizan RTP y RTCP (Protocolo de control en tiempo real), envolver el tráfico SIP o H.323 sobre TLS protege la información de autenticación; sin embargo, la parte más importante de la llamada es probablemente el flujo de medios real que contiene el audio. Una infraestructura SIP que usa TLS con un flujo de medios RTP de texto sin cifrar aún permite a los atacantes espiar o inyectar audio en las llamadas y adquirir información confidencial.

Figura 6. Encripción de la voz con SRTP



Fuente. Enscipción de la voz. https://encryptedtbn0.gstatic.com/images?q=tbn%3AANd9GcTr0qn_4ZoDhppHnlwq18qAP2qWfQpht-ejpw&usqp=CAU, 2020

7.3 SRTP Y PROTECCIÓN DE MEDIOS CON CIFRADO AES.

Según Thermos y Takanen,[62]SRTP utiliza el Estándar de cifrado avanzado (AES) como cifrado para el cifrado, que se puede utilizar con dos modos de cifrado. Los dos modos de cifrado que se pueden usar con AES son el modo de contador de enteros segmentados (SICM), que es el predeterminado, y el modo f8. Un tercer cifrado, que es el cifrado NULL, también se puede utilizar con AES, pero nunca debería implementarse, ya que no proporcionaría cifrado al flujo de medios.

[61] COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, p.607
[62]THERMOS Peter y TAKANEN Ari.Securing VoIP Networks. Pearson Education, Inc. 2007. p. 249

7.3.1 SRTP y protección de autenticación e integridad con HMAC-SHA1. Como dice Thermos y Takanen[63], además de AES, que proporciona cifrado a la carga útil, SRTP puede proporcionar integridad de mensaje a la parte del encabezado del paquete con HMAC-SHA1. HMAC (código de autenticación de mensajes hash con clave) es una función hash criptográfica para verificar simultáneamente tanto la integridad de los datos como la autenticidad de un mensaje. Los HMAC se utilizan a menudo con la función hash SHA-1, considerada como HMAC-SHA1. Con esta técnica, se etiquetará un hash HMAC-SHA1 al final de un paquete para proporcionar integridad entre dos puntos finales de VoIP. La adición de integridad garantizará que los paquetes de VoIP no sean susceptibles a ataques de reproducción, que aún pueden ocurrir incluso con el cifrado AES del flujo de medios.

7.3.2 Método de distribución de claves SRTP. Según Thermos y Takanen[64], un problema importante para SRTP es si el proceso de intercambio de claves se produce en texto sin cifrar, lo que puede suceder si una infraestructura de VoIP utiliza SIP o H.323 sin un túnel TLS. Por lo tanto, la clave maestra SRTP se puede capturar a partir de paquetes SIP o H.323 de texto sin formato, y un atacante podría descifrar cualquier paquete SRTP cifrado capturado a través del cable. Si SRTP se utiliza con fines de seguridad, asegúrese de que TLS se utilice con SIP o H.323; de lo contrario, se reduce el beneficio de seguridad de SRTP.

7.3.3 ZRTP y Zfone. Como dice Thermos y Takanen,[65] para ZRTP, una extensión de RTP, aplica el acuerdo de claves Diffie-Hellman (DH) a los paquetes SRTP existentes al proporcionar servicios de administración de claves durante el proceso de configuración de una llamada VoIP entre dos terminales. Se mantiene alejado de la capa de sesión, como SIP y H.323, y se centra únicamente en SRTP. ZRTP se utiliza para generar claves en los inicios de sesiones SRTP.

Según Dwivedi[66], ZRTP es similar a PGP (Pretty Good Privacy), ya que intenta garantizar que no se produzcan ataques man-in-the-middle (hombre en el medio) entre dos puntos finales. Para resolver estos problemas, utiliza una cadena de autenticación corta (SAS), que es un valor hash de las claves DH. El hash SAS se comunica a ambos extremos de VoIP mediante ZRTP, cada extremo verifica el valor de SAS para garantizar que los valores hash coincidan y que no se hayan producido alteraciones.

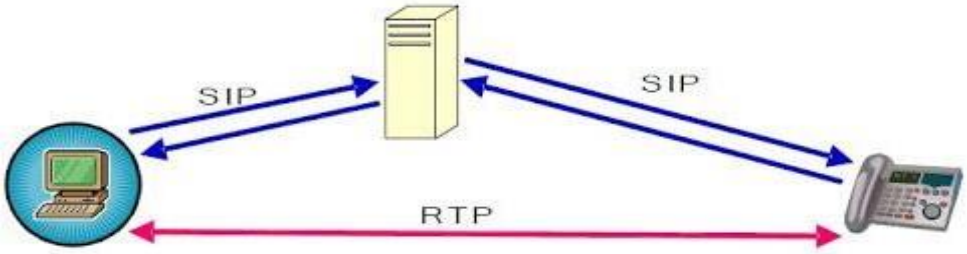
Para concluir este capítulo, se pretende dejar en claro que asegurar las redes de VoIP no es una tarea fácil, pero es importante. Si bien el proceso puede ser engorroso, la implementación de SIPS, SRTP o ZRTP puede reducir drásticamente la superficie de ataque en una red VoIP.

La capacidad de proporcionar cifrado tanto en la capa de sesión como en la capa de medios puede garantizar que los usuarios reciban el mismo nivel de seguridad que tendrían si usaran sistemas telefónicos tradicionales. Además, la comunicación de audio sensible,

[63]THERMOS Peter y TAKANEN Ari.Securing VoIP Networks. Pearson Education, Inc. 2007. p. 221
[64] Ibíd., p. 249
[65] Ibíd., p. 284
[66] DWIVEDI Himanshu. Haking VoIP – Protocols, Attacks, and countermeasures. 2009. p.199

desde llamadas internas sobre información de existencias hasta preocupaciones de privacidad sobre datos personales, podría tener la obligación de ser tan segura como cualquier otra entidad (por ejemplo, archivos y carpetas) en la red que contenga el mismo tipo de información. Por último, los teléfonos de software que utilizan SRTP pueden implementar nuevas tecnologías como Zfone, lo que permite a los usuarios seguridad adicional en teléfonos de software que podrían no proporcionarla de forma nativa.

Figura 7. Cifrado RTP en protocolo SIP



Fuente.https://lh3.googleusercontent.com/proxy/b3cBsJDpkbWoEPZ7bf2qDUi8AUlkcn4k6IF796aUSVPnKmZ32ZeXaX3iRGgo0Qz0XIZ0NmR6wQvgHT4iFTkoBFofIFRtyfpNv0WoGpRH8QctmyKfDQoHW_jXxttnUFCgkCxqKzPtfJcIswWoLCOpB_Tdf4TQ, 2020

8 CONCLUSIONES

Durante la investigación realizada, se realizó el levantamiento de la información necesaria que nos llevara a identificar las amenazas más relevantes o conocidas que afectan a la solución de VoIP, estas amenazas están ligadas a los diferentes protocolos que usa esta solución, también debe lidiar con los problemas de los protocolos de las redes de datos, así como son la configuración en estas dado que es donde se soporta la solución IP. Se pudo evidenciar el tipo de amenazas dirigidas que existen y que son un peligro latente para este tipo de solución.
También se logró documentar los protocolos que usan las redes VoIP, conociendo sus vulnerabilidades, pero también como hacer para que estas vulnerabilidades se mitiguen.

La implementación de una solución de comunicaciones basada en VoIP en una organización, requiere del análisis de ciertos factores tales como el sistema actual de comunicaciones de la empresa, la arquitectura o modelo de comunicación a implementar (modelo de sitio único, múltiples sitios con procesamiento independiente de llamadas o múltiples sitios con procesamiento de llamada distribuido), distribución geográfica de la empresa, ancho de banda disponible, costos, entre otros para poder determinar cuál de las soluciones que están en el mercado puede ser la más adecuada para la empresa.Dentro del análisis que se realiza para la implementación se debe tener en cuenta todos los elementos de la red que intervienen para poder evidenciar posibles fallos y poderlos corregir.

La investigación y documentación de esta monografía nos lleva a entender que las redes de datos por sí solas no son tan vulnerables o las vulnerabilidades propias son bajas, el problema radica en que estas soluciones de Voz son soportadas por redes de datos, redes ya existentes que en muchas ocasiones son mal configuradas y no son actualizadas de forma correcta, es cuando entendemos que la Voz sobre IP es un conjunto de protocolos que se unen para hacer posible una solución con muchas bondades.

Dentro de este trabajo se detallaron los protocolos, puertos, equipos activos y pasivos que juegan un papel importante dentro de las redes de datos apalancando la solución VoIP.

Dentro del alcance y como finalidad este trabajo busca documentar las fallas asociadas a la solución de VoIP, pero también es necesario investigar y documentar las posibles soluciones, cuáles son las mejores prácticas al momento de implementar estas soluciones, es por esto que en el desarrollo del objetivo 3 se detalla de forma muy completa las buenas prácticas a tener en cuenta.

9 RECOMENDACIONES

El presente trabajo está enfocado a servir como guía al momento de realizar una implementación de un sistema de comunicaciones IP por lo tanto los autores recomiendan apoyarse constantemente en las hojas de especificaciones de los productos expuestos, debido a la constante y rápida actualización por parte de fabricantes.

Para la mejora y continuación del presente trabajo se recomienda al lector a investigar sobre la seguridad en un sistema de comunicaciones IP, teniendo en cuenta que teléfonos IP, los PBX, Gateway y demás elementos de un sistema de comunicaciones IP no están exentos de ser atacados por virus o hacker, que pueden en un determinado momento extraer información de la compañía o bien hacer colapsar el sistema de comunicaciones de la empresa.

10 BIBLIOGRAFÍA

ALANA B. Johnston. SIP: Understanding the Session Initiation Protocol. 4ª ed. Boston Artech House.2015, 410p

ASLAN S. Vásquez. Consideraciones sobre la seguridad en las redes de telecomunicaciones soportes de voz sobre ip (voip) en cuba. 2007, 40p.

BRYANT R, Madsen L, Van Meggelen Asterisk, the definitive guide, 4ª ed. O'Reilly Media, 2013, 86p.

CARRASCO HIRUELO. Antonio, Documento de la Universidad de Cataluña Seguridad VoIP: ataques y contramedidas en sistemas de código abierto. Cataluña. 2019, 30, 31, 33, 34p.

COLLIER Mark, ENDLER David y HILL Mc Graw. Unified Comunications and VoIP. 2014, 52, 289, 291, 292, 294, 298, 300, 301, 312, 407, 408, 477, 607 p.

GUTIERREZ G. Seguridad en VoIP: Ataques, Amenazas y Riesgos. 2014, 3, 4, 6, 13, 14, 16, 35, 44p.

JHONSON.B. Alan. SIP Understanding the Session Initiation Protocol Fourth Edition. Artechhouse. Boston. 2016, 416p.

KRASHENINNIKOVA E. Seguridad en VoIP: aplicaciones de señuelos. Madrid. 2013, 56p.

LAPSLEY P. Exploding the phone: Thee Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell. New York: Grove Press.2013, 91p.

PIEDRA O. María y SOLORZANO V. Lucia. Análisis comparativo entre alternativas libres y propietarias para la migración de telefonía tradicional a telefonía IP. Cuenca. 2011, 27, 28p.

PORTER T. Practical VoIP Security. Canada: Syngress Publishing. 2016 99p.

REGIS J. Securing VoIP. El Sevier. 2015, 21, 71, 170p.

WALLINGFORD T. VoIP Hacks Beijing: O´REILLY. 2015, 228p.

AUDIOCODECS. Management Product & Solutions. Abril 2020. Disponible en https://www.audiocodes.com/solutions-products/products/management-products-solutions/one-voice-operations-center

AVAYA. Application Server 5300Overview. Marzo 2019. Disponible en https://downloads.avaya.com/css/P8/documents/100174168.

BAUMANN R, Schmid C. Voice Over IP - Security and SPIT. Septiembre 2006. Disponible en http://rainer.baumann.info/public/voip.pdf

COLLIER M. VoIP Vulnerabilities – Registration Hijacking. Junio 2005. Disponible en https://download.securelogix.com/library/Registration_hijacking_060105.pdf

COLLIER M. Basic Vulnerability Issues for SIP Security. Marzo 2005. Disponible en https://download.securelogix.com/library/SIP_Security030105.pdf

CUTILI, Catania, García, Problemas y herramientas en la seguridad de redes de transmisión de datos universitarias. El caso de la Universidad Nacional de Cuyo. 2012, Disponible en http://dspace.redclara.net/bitstream/10786/832/1/10-2_Problemas_y_herramientas.pdf

DRUID. VoIP-Attacks. 2007. http://druid.caughq.org/presentations/VoIP-Attacks.pdf

GUTIERREZ. Ramírez. Seguridad en VoIP: Ataques, Amenazas y Riesgos, 2020Disponible en http://www.it- docs.net/data/896.pdf

GRANADOS& CARDENAS. Implementación de Voz/IP como solución a obsolescencia del PBX análogo,septiembre2014, Disponible en https://repository.usta.edu.co/bitstream/handle/11634/3586/Cardenasoscar2014.pd f?sequence=1#page=1&zoom=auto-99,792

INCIBE.Glosario de términos de ciberseguridad. Febrero 2017. Disponible en https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

LIBERONA,M.Seguridad en Voz/IP. noviembre, 2010Disponible enhttp://www.telematica.utfsm.cl/telematica/site/artic/20121011/asocfile/20121011110145/liberonamaria.pdf.

LÓPEZ, A. El portal de ISO 27001 en español. 2020. Disponible en https://www.iso27000.es/glosario.html,

Marco legal que sustenta las TIC en Colombia: marco legal de las TIC en Colombia. [En línea]. 2012. (Recuperado el 12 de abril 2020.) Disponible en http://ticcentroeducativosantateresa.blogspot.com/2012/04/marco-legal-que-sustenta-las-tic-en.html, 2012.

MCAFEE., Las vulnerabilidades de VoIP. 2020. Disponible en http://www.microsa.es/biblioteca/McAfee/McAfee_Vulnerabilidades_de_VoIP.pdf

MCCARRON J. A Brief Overview of VoIP Security. 2020. Disponible en http://www.infosecwriters.com/text_resources/pdf/Voip_JMccarron.pdf,

NETWORK WORLD, Aumentan los ataques cibernéticos a través de VoIP. 2016. Disponible en https://www.networkworld.es/seguridad/aumentan-los-ataques-ciberneticos-a-través-de-voip

SIERRAH. Estado del arte de la seguridad VoIP, 2014, Disponible en http://ojs.urepublicana.edu.co/index.php/ingenieria/issue/view/20/8

SCHOLZ H. SIP Stack Fingerprinting and Stack Difference Attacks. 2020. Disponible en https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Scholz.pdf.

VOIPSA. VoIP Security and Privacy Threat Taxonomy. Octubre 2005. Disponible en http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf