Enfoque UTE, V.7-N.2, Jun.2016, pp.25 - 40
http://ingenieria.ute.edu.ec/enfoqueute/
e-ISSN: 1390-6542 / p-ISSN: 1390-9363
Recibido (Received): 2016/04/27
Aceptado (Accepted): 2016/06/23

Seguridad de la Telefonía IP en Ecuador: Análisis en Internet

(Security of IP Telephony in Ecuador: Online Analysis)

José Estrada[1], Mayra Calva[2], Ana Rodríguez[1], Christian Tipantuña[1]

Resumen:
La telefonía es un servicio global, y por ello las redes telefónicas han sido un objetivo codiciado de los ciberdelincuentes. Ahora que la voz se puede transportar a través del protocolo IP y que múltiples servicios se integran en un modelo convergente mediante Internet, los incentivos para atacar los sistemas telefónicos y los atacantes son, sin duda, más numerosos. Además, el desarrollo de aplicaciones telefónicas basadas en software libre ha permitido la masificación del uso de telefonía IP, sin que la conciencia sobre los riesgos de seguridad inherentes se haya incrementado. En vista de la vigente e intensiva adopción de sistemas de telefonía IP en el Ecuador, se realizó una exploración basada en información pública para determinar estadísticas sobre los sistemas telefónicos conectados a Internet en Ecuador. En base a estos datos y a los recopilados por un prototipo de telefonía IP deliberadamente vulnerable, se realizó un análisis preliminar de las vulnerabilidades y amenazas de estos sistemas telefónicos. Se encontraron cientos de sistemas telefónicos públicamente disponibles en Internet, muchos con versiones desactualizadas y, por tanto vulnerables, de soluciones de telefonía IP basadas en Asterisk. En pocos días, se identificaron miles de interacciones maliciosas sobre el sistema de telefonía IP publicado en Internet en Ecuador.

Palabras clave: telefonía IP; seguridad; Ecuador; Asterisk, vulnerabilidades; amenazas

Abstract:
Telephony is a global service and thus telephone networks have been a coveted target for criminals. Now that voice can be transported over IP and that multiple services are integrated in a convergent model through Internet, there are more incentives to attack and more attackers. Moreover, the development of open source telephone applications has encouraged the massive use of IP telephony, but not an increased awareness about embedded security risks. Due to the current and intensive adoption of IP telephony systems in Ecuador, we conducted an exploration based on public information to obtain statistics about telephone systems connected to Internet in Ecuador. Additionally, using a deliberately vulnerable IP telephony system, we collected more data to do a preliminary analysis of threats to such systems. We found that hundreds of telephone systems were publicly available on the Internet and using outdated versions of Asterisk-based applications. We also found thousands of malicious interactions on the IP telephony system we deployed on the Internet.

Keywords: IP telephony; security; Ecuador; Asterisk; vulnerabilities, threats

[1] Escuela Politécnica Nacional, Quito – Ecuador ({jose.estrada, ana.rodriguez, christian.tipantuna} @epn.edu.ec)
[2] Escuela Politécnica Nacional, Quito – Ecuador (maycanetz@gmail.com)

1. Introducción

La telefonía es un mecanismo cotidiano de comunicación. Gracias a la masificación en el uso de Internet, la telefonía ha evolucionado y ha permitido la creación de nuevos servicios a su alrededor. Desde Skype y Google Talk hasta Facebook y Whatsapp, un sinnúmero de aplicaciones en la red soportan comunicaciones por voz que se han hecho tan comunes para los usuarios como las llamadas por teléfono móvil o convencional. De hecho, la telefonía IP es una tecnología donde pueden converger una gran cantidad de servicios de comunicaciones en torno al transporte de la voz.

Por otro lado, las empresas han encontrado en la telefonía IP una solución para ahorrar costos (transportando, por Internet, la voz entre sus sucursales), flexibilizar la comunicación entre sus empleados y con sus clientes, integrar sus sistemas de comunicaciones (voz, correo electrónico, mensajería instantánea), y, especialmente, disponer de una posición de presencia corporativa mediante un novedoso sistema automático e interactivo para atención al cliente (IVR). Así, las ventajas de los servicios de telefonía IP han revolucionado el entorno de comunicaciones empresariales.

Además, gracias al desarrollo de software libre, nuevas aplicaciones para la red han surgido y, ya que no tienen costo, se encuentran al alcance de cualquiera, incluso para su desarrollo. Así aparece Asterisk (Bryant, Madsen & Van Meggelen, 2013), que permite construir un sistema de telefonía IP completo, aprovechando los recursos incluso de una computadora personal. Esta aplicación ha logrado tanta popularidad que, alrededor de ella, se han generado varios proyectos para el desarrollo de interfaces web de gestión como Elastix (Puente, 2015) y FreePBX (Sangoma, 2014), también basadas en software libre. Estas interfaces, que le han robado algo de protagonismo a Asterisk, han permitido que sea más sencillo todavía implementar una plataforma de telefonía IP, muchas veces sin la necesidad de contratar los servicios de una empresa especializada.

El bajo costo inicial de implementación gracias al software libre y la gran versatilidad que ofrece la telefonía IP han promovido una adopción sin precedentes de esta tecnología, tanto en la empresa pública, como en la empresa privada. Ecuador no es la excepción, y durante los últimos 6 años ha vivido un importante proceso de migración hacia la telefonía IP, tal como se describe más adelante.

Los protocolos de comunicaciones en los que se basa la telefonía IP no fueron concebidos para ofrecer mecanismos de protección de la información. Además, la consciencia de los riesgos latentes en Internet aún no está desarrollada en los administradores de tecnología. Por ello, miles de dispositivos vulnerables (mal configurados o con software desactualizado) se encuentran disponibles en Internet, aun cuando muchas veces no era necesario que fuesen públicos. Entre

esos dispositivos se encuentran, sin duda, sistemas de telefonía IP instalados sin tomar en cuenta las normas de seguridad de información básicas.

La vulneración del servicio de telefonía IP puede llegar a ser crítica pues los sistemas que se implementan usualmente tienen conexión con recursos que dan acceso a otras redes de comunicaciones (e.g. un red telefónica fija o móvil) cuyo uso representa un costo económico. Así, la explotación de una vulnerabilidad de un sistema de telefonía podría permitir el uso fraudulento de esos recursos y provocar un perjuicio económico considerable a la organización atacada.

En Ecuador, este tipo de fraude empieza a darse con cierta frecuencia, especialmente a partir del uso de software libre para las aplicaciones de telefonía (especialmente Elastix y FreePBX). La facilidad de puesta en marcha que ofrecen estas aplicaciones lleva a que muchas de las implementaciones se realicen sin la ayuda de un experto, lo que incrementa el riesgo de vulnerabilidad. Asimismo, estas aplicaciones integran la telefonía con otros servicios como correo electrónico, mensajería instantánea y CRM, que hacen de su mantenimiento una tarea más complicada y sujeta a errores.

Aunque estos riesgos empiezan a manifestarse en Ecuador en eventos graves de fraude telefónico, no existe información pública que permita determinar su impacto o el nivel de vulnerabilidad que tendrían las plataformas de telefonía IP en el país. En este artículo se exponen los resultados de un esfuerzo por explorar el uso de telefonía IP en el Ecuador y de poner de manifiesto a algunas de las serias vulnerabilidades de las plataformas telefónicas que se encuentran públicamente disponibles en Internet.

El resto del artículo está organizado como sigue: en la Sección 2, se expone una modesta descripción de la telefonía IP en Ecuador; en la Sección 3, se describen los escenarios utilizados para analizar las amenazas del servicio de telefonía IP en el país; en la Sección 4 se exponen los resultados de un análisis exploratorio activo de las plataformas de telefonía IP; en la Sección 5, se presentan los resultados del análisis pasivo de las amenazas a la telefonía IP en el Ecuador; en la Sección 6, se discuten los riesgos de la telefonía IP en Ecuador; y en la Sección 7, se exponen las conclusiones de este trabajo.

2. La Telefonía IP en Ecuador

La Telefonía IP es una tecnología que ha ido calando silenciosamente en la infraestructura de comunicaciones de las empresas, y muy lentamente en las instituciones públicas del Ecuador. No existen estadísticas ni notas de prensa que registren la penetración de dicha tecnología en el país. Lo que sí se puede notar es la evolución de la telefonía fija corporativa que ya ofrece conexión de última milla en base al protocolo de Internet (IP) (Corporación Nacional de Telecomunicaciones, 2016). En lo que respecta a telefonía fija, la Corporación Nacional de Telecomunicaciones (CNT) ofrece servicios de troncales telefónicas con protocolo IP, permitiendo a las instituciones contratar

desde 5 canales (troncales) telefónicos SIP a través de una conexión de datos que usualmente llega mediante fibra óptica.

Por otro lado, la voz transmitida sobre el protocolo de Internet (VoIP) ha sido noticia en el Ecuador solamente cuando se ha relacionado con aplicaciones (usualmente móviles) de uso masivo, como Whatsapp (El Comercio, 2015) y Skype (El Universo, 2016). La interacción con este tipo de aplicaciones es lo más cercano que los usuarios comunes y corrientes se encuentran de la telefonía IP en el país, pues gran parte de su comunicación telefónica se reduce a la realizada usando el teléfono móvil.

En Ecuador, la telefonía IP se empieza a estudiar aproximadamente en el año 2005, aunque, para entonces, países más desarrollados llevaban casi una década aplicándola. Seguramente, a raíz de la reducción de costos del servicio de acceso a Internet y al significativo incremento de las capacidades ofrecidas es que la telefonía IP comienza a ser adoptada con mayor intensidad a nivel nacional, a partir de 2009.

La telefonía IP, como un conjunto de servicios que se ofrecen en torno al transporte de la voz a través de protocolo IP, viene siendo adoptada en instituciones tanto públicas como privadas con el fin de aprovechar algunas de sus ventajas como: posibilidad de reutilización de la red de datos interna para tráfico de voz, mayor cantidad de aplicaciones telefónicas, facilidad de integración con otros servicios en la red y mayor control sobre el tráfico de voz.

Otra de las razones para la adopción de sistemas de telefonía IP es el ahorro de costos derivado del transporte de la voz mediante Internet. Esto podría permitir a varias sucursales de una empresa comunicarse sin costo, o a sus clientes contactarse telefónicamente con ellas usando su servicio de acceso a Internet. El uso de este beneficio implica, en muchos casos, hacer disponible el servicio de telefonía en Internet para que sea públicamente accesible desde otras sucursales o desde las premisas de los clientes. Se desprende, entonces, que esta reducción de costos está sujeta a exponer los sistemas de telefonía IP a un gigantesco universo de posibles atacantes en Internet.

Finalmente, la aparición de herramientas de software libre como Asterisk o la distribución Elastix (basada en Asterisk) que facilitan la implementación de servicios de telefonía IP a bajo costo (pues no están sujetas a licenciamiento) ha impulsado aún más la adopción de la telefonía IP en el Ecuador. Sin embargo, esta conciencia de relativa facilidad en la implementación de telefonía IP podría llevar a las instituciones que requieran ese servicio a desplegarlo por su cuenta, prescindiendo de los servicios más rigurosos ofrecidos por proveedores calificados.

A continuación, se describen varios esfuerzos realizados como parte de este trabajo para obtener datos adicionales sobre el estado de la telefonía IP en Ecuador y de los correspondientes riesgos

de las plataformas de telefonía que se encuentran públicamente disponibles en el espacio ecuatoriano en Internet.

2.1 La Telefonía IP según el Portal de Compras Públicas

Con el fin de obtener información sobre las tendencias de adopción de telefonía IP en el sector público del Ecuador, consultamos el portal del Sistema Nacional de Compras Públicas (Instituto Nacional de Compras Públicas, 2016). Este portal, por disposición de la Ley Orgánica del Sistema Nacional de Compras Públicas (LOSNCP), publica la información relevante de los procedimientos de contratación. La información que se obtuvo incluye: objeto del proceso de compra, provincia en la que se realizó, presupuesto referencial, y fecha de publicación y, con base en esos parámetros, intentamos ilustrar en la Figura 1 la evolución de las compras de telefonía IP en el Ecuador. Aunque los resultados obtenidos no se pueden extrapolar inmediatamente para diagnosticar, en general, la situación de la telefonía IP en el país, sí son un punto de partida importante, ya que no existen estadísticas oficiales al respecto.

Antes de 2009 no se encontraron procesos relacionados con la compra de telefonía IP (sistemas, componentes o servicio). En este año, se ejecutaron 6 procesos de compra y en 2013 llegaron a ser 24. La inversión total realizada en los rubros descritos, de acuerdo a los datos obtenidos, casi alcanza los 28 millones de dólares. Tal como se puede observar en la Figura 1, la inversión en telefonía IP pasó de cero a 16 millones de dólares en 4 años (2009 a 2013) en el sector público, luego de lo cual ésta se ha ido reduciendo paulatinamente. Esta información refleja claramente la tendencia creciente en la utilización de telefonía IP que inicia de manera tardía en comparación con otros países más desarrollados tecnológicamente. Las provincias con mayor cantidad de procesos de compra de telefonía IP son Pichincha (56%), Guayas (14%), Azuay (10%) y Tungurahua (6%) de un total de alrededor de 105 procesos realizados durante los últimos 7 años.

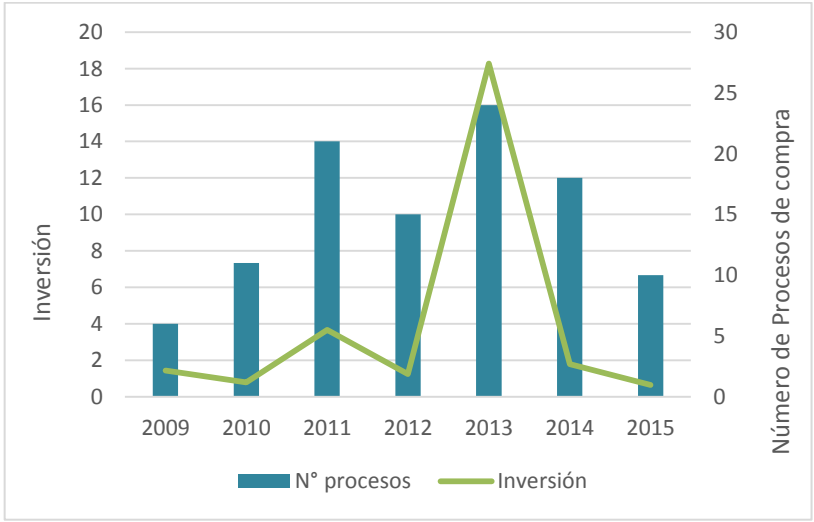


Figura 1. Evolución de las Compras de Telefonía IP en el Sector Público de Ecuador a partir del año 2009

Aunque las tendencias de adopción de la tecnología resultan reveladoras, es posible obtener más información relacionada, por ejemplo, con las marcas de los sistemas que se adquieren en el sector público, e incluso de sus correspondientes versiones de software. Si se investiga con mayor profundidad en los documentos habilitantes de los procesos de compra (pliegos, términos de referencia, resolución de adjudicación, etc.), que también son públicos, es posible intuir información sobre los sistemas telefónicos que le interesa adquirir o que adquirió la institución (generalmente los proveedores se identifican con una sola marca). Mediante esa información podría complementarse el mapa de la telefonía IP en Ecuador.

2.2 Censo en Internet

Los datos expuestos en la sección anterior dan una ligera idea de la tendencia en el uso de la telefonía IP en el país. Sin embargo, dicen muy poco sobre el número de sistemas de telefonía IP que actualmente se encuentran operativos ya que no están incluidos aquellos funcionando en la empresa privada. Por otro lado, conocer, por ejemplo, qué aplicaciones de telefonía IP son las más utilizadas en Ecuador, ayudaría a entender el impacto que podrían tener los problemas de seguridad de estos sistemas. No existe un censo con respecto al uso de la telefonía IP en Ecuador, pero la intuición y la experiencia nos hacen pensar que, al igual que ocurre con otros servicios, aunque con frecuencia no sea necesario conectar un sistema telefónico a Internet, muchos administradores lo conectarán por descuido, o por el simple hecho de que es posible hacerlo.

Así, otra aproximación para medir de alguna manera el impacto de la telefonía IP en el Ecuador se realizó mediante el motor de búsqueda Shodan (Allen, 2012). Shodan permite encontrar dispositivos conectados a Internet en base a distintos filtros y en base a información que se ha recopilado a partir de banners de servicios de red públicos y configurados por defecto. Usamos Shodan para determinar la cantidad de sistemas de telefonía IP conectados a Internet en Ecuador. Aunque es claro que no todos los sistemas de telefonía IP del país están conectados a Internet y que no todos los que lo estén publican un banner con información indexada en Shodan, la muestra obtenida es útil para tener una idea del panorama de la telefonía IP en el país, no solo considerando la cantidad de sistemas en funcionamiento, sino también los tipos de soluciones utilizadas. Esto, sin duda, podría ayudar a orientar de mejor manera el análisis de la seguridad

De este análisis con Shodan, utilizando solamente el filtro de país (country:EC) y la palabra SIP para la búsqueda en los banners indexados, se encontraron 512 dispositivos identificados como servidores SIP. De ellos, casi el 50% se ubica geográficamente en la ciudad de Quito, el 43% en Guayaquil, el 8% en Cuenca, etc. Se puede notar que existe cierta correspondencia de estos resultados con los obtenidos en la sección anterior, en lo que respecta a las provincias que mayor penetración tendrían del uso de telefonía IP. Se encontró también que el 22% de esos dispositivos están conectados a la red de la Corporación Nacional de Telecomunicaciones, un porcentaje

similar a Telconet, el 10% a Satnet, el 7% a Netlife, el 6% a Puntonet, y el 6% a Etapa. Quizás lo más interesante que se encontró tiene que ver con el tipo de servicios utilizados en estos dispositivos. La mayoría, el 27%, usan FreePBX (que incluiría a Elastix), el 5% usaría la solución DenwaPBX, el 5% Grandstream, y el 3% Asterisk puro. Las soluciones basadas en Asterisk estarían presentes en un 30% de los dispositivos encontrados.

De la muestra obtenida, se puede concluir que la solución de telefonía IP más popular en Ecuador sería FreePBX, pero hay que recordar que Elastix, la solución ecuatoriana, está construida sobre FreePBX. Es muy probable, por tanto, que en realidad la solución de telefonía IP más popular sea Elastix, al menos entre las que están directamente conectadas a Internet. Curiosamente, soluciones que son también muy populares en el mercado ecuatoriano de telefonía IP como Cisco y Avaya aparecen marginalmente (3 y 2 veces respectivamente). Esto podría significar que pocos de estos dispositivos se conectan a Internet o que los banners que generan están adecuadamente configurados para no publicar información potencialmente sensible. Es evidente, entonces, que un gran porcentaje de las soluciones de telefonía IP que se encuentran públicamente disponibles en Internet están basadas en Asterisk.

Si un sistema de telefonía IP se conecta directamente a Internet, éste se expone a graves riesgos. En principio, estos riesgos están vinculados con la revelación de información de las versiones de las soluciones utilizadas. Un atacante podría descubrir un dispositivo de telefonía IP funcionando con una versión desactualizada de software y por ello, seguramente, vulnerable. Luego, podría utilizar esa información para buscar o implementar ataques que aprovechen esa vulnerabilidad.

3. Escenarios de Análisis

Una vez que se ha intentado retratar el estado de la telefonía IP en Ecuador, se descibe en las siguientes secciones los escenarios de prueba construidos para evaluar, en cierta medida, la seguridad de los sistemas de telefonía IP en Ecuador, utilizando una metodología no intrusiva de recopilación de información. A continuación, se explica brevemente esta metodología, y se exponen los dos escenarios de pruebas utilizados para obtener información sobre las potenciales vulnerabilidades.

3.1 Metodología

La metodología utilizada para explorar las vulnerabilidades de los sistemas de telefonía IP en Ecuador se dividió en dos fases: una exploración activa y una pasiva.

La primera fase consistió en un análisis activo en el que se sondeó el espacio de Internet asignado al Ecuador con el fin de encontrar instancias del servicio de telefonía IP conectadas. Luego, con esta información, en base a las instancias en línea, se determinó, cuando fue posible, la aplicación telefónica utilizada y su versión correspondiente. Cabe destacar que esta información

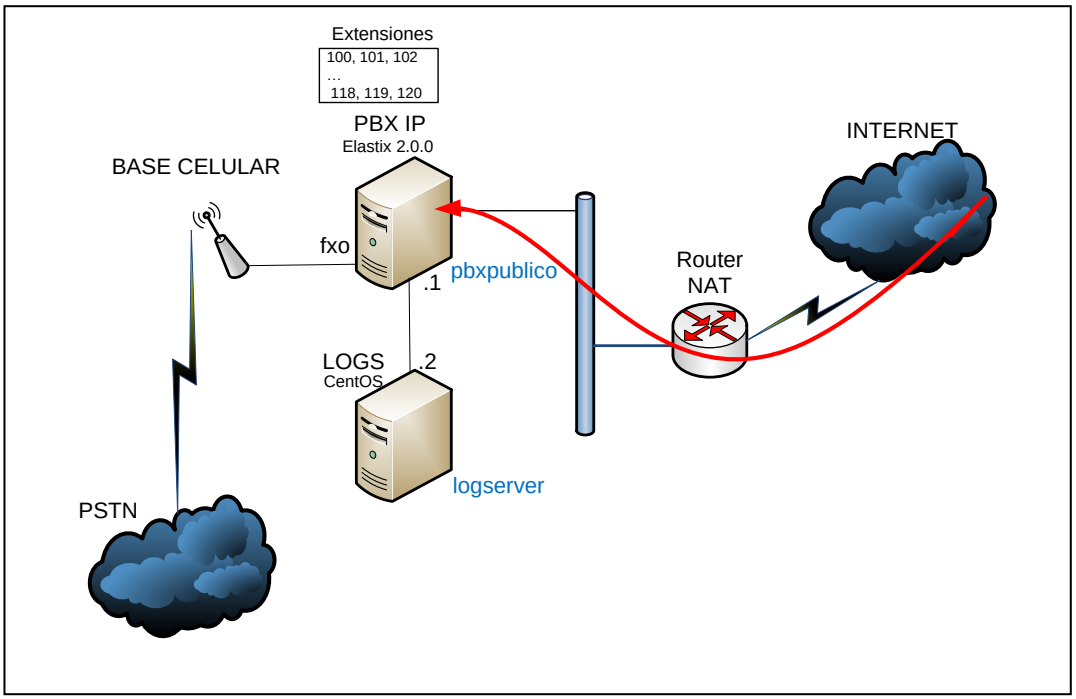
se obtuvo con éxito haciendo una sola petición a cada instancia disponible, y únicamente en aquellos casos en los que esta información estaba contenida en el campo User-Agent de la respuesta SIP a dicha petición. Los datos de las aplicaciones telefónicas y sus versiones encontradas luego fueron analizados, entre otras cosas, para determinar el nivel de vulnerabilidad de las mismas mediante una consulta simple en los sitios web de los desarrolladores de dichas aplicaciones sobre los problemas de seguridad de las versiones encontradas.

La segunda fase de este análisis consistió en instalar un prototipo de telefonía IP que se encuentre disponible públicamente en Internet y configurarlo de modo que fuese deliberadamente vulnerable (un *honeypot* de telefonía IP). El objetivo fue atraer ataques de Internet con el fin de analizarlos y determinar su impacto.

Finalmente, se trató de recopilar información sobre la seguridad de los sistemas de telefonía IP en Ecuador, consultando con algunos organismos ecuatorianos involucrados en la temática.

3.2 Escenario de Análisis Activo

Para el análisis activo, se consideraron fundamentalmente todos los dispositivos conectados a Internet ubicados en los rangos de direccionamiento asignados a Ecuador. Los rangos de direccionamiento IP que se analizaron se obtuvieron de (IP2Location, 2016). Como ya se indicó previamente, el objetivo fue encontrar los dispositivos, en el espacio de direccionamiento ecuatoriano, que implementen algún servicio relacionado con telefonía IP. Ya que normalmente este servicio implementa el protocolo SIP (protocolo de señalización para telefonía más popular), el proceso de búsqueda consistió básicamente en identificar aquellos dispositivos con servicios basados en SIP.



La herramienta utilizada para esta prueba se llama svmap que es parte de un conjunto de herramientas de auditoría de sistemas de telefonía IP, basadas en Python, agrupadas bajo el nombre de *SipVicious* (EnableSecurity, 2012). A través del campo User-Agent de la respuesta SIP generada por los sistemas analizados, *svmap* podría determinar el nombre y la versión del servicio de telefonía IP que está ejecutándose. Evidentemente, esto no es posible si el sistema está configurado para no revelar esta información (configuración recomendable).

Aunque las pruebas realizadas implican una ligera interacción con cada instancia de telefonía IP encontrada, esta interacción no es más intensiva que la generada por una petición ICMP mediante la herramienta ping.

3.3 Escenario de Análisis Pasivo

El objetivo del análisis pasivo fue obtener información que permita intuir el nivel del riesgo existente en Internet para una aplicación de telefonía IP. Para ello nos planteamos atraer atacantes a un prototipo de sistema de telefonía IP deliberadamente vulnerable y accesible a través de Internet.

El prototipo se conectó directamente a Internet y se instaló con la versión 2.0.0 de Elastix. Adicionalmente, el prototipo se conectó a la red de telefonía móvil, a través de una base celular y un gateway telefónico, tal como se observa en la Figura 2.

El prototipo se configuró de tal manera que tuviese, entre otras, las siguientes vulnerabilidades: vulnerabilidad a *fingerprinting* (Dassouki, Safa & Hijazi, 2014), vulnerabilidad a enumeración de extensiones, identificadores de terminales equivalentes a números de extensiones, canales SIP con contraseñas débiles (es decir, canales sin contraseñas, con contraseñas iguales a sus identificadores, y canales con contraseñas que usen palabras de diccionario), y software de terceros (VtigerCRM) desactualizado.

La vulnerabilidad a *fingerprinting* está relacionada con la posibilidad de que un tercero sea capaz de determinar el sistema operativo y la aplicación de telefonía IP que se ejecuta en nuestro sistema. Por otro lado, la vulnerabilidad frente a ataques de enumeración supone, en Asterisk (o sus derivados), la posibilidad de que un atacante encuentre los números de varias de las extensiones que se pueden conectar a una central telefónica. Luego, ya que estos números suelen usarse también como identificadores de los terminales telefónicos en el proceso de registro y autenticación con la central, si un atacante puede averiguar uno de esos identificadores, solo le faltaría la contraseña para suplantar a un terminal y usar los recursos telefónicos fraudulentamente. Cabe destacar, además, que la versión utilizada de Elastix es una versión antigua y, por tanto, vulnerable, entre otros, a ataques de inyección SQL (Exploit Database, 2015).

Finalmente, al prototipo se conectó un servidor de logs encargado de recibir todos los registros de los eventos generados en los servicios de Elastix, con el fin de disponer de esa información aunque se recibiese un ataque que inutilice por completo el prototipo.

3.4 Fuentes de Información Oficiales

Otra fuente de información importante sobre la problemática de la seguridad de los sistemas de telefonía IP en Ecuador está constituida, sin duda, por las instituciones oficiales que manejan los servicios de telefonía y los organismos de regulación y control a los que llegan las denuncias del fraude cometido a través de dichos servicios. Entre las primeras tenemos a la Corporación Nacional de Telecomunicaciones (CNT), proveedor principal de telefonía fija a nivel nacional y que, en principio, tendría la capacidad de encontrar indicios de fraude telefónico al detectar patrones anómalos de tráfico. Luego, en el campo de la regulación y control, se tiene a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) que, a través del Ecucert, sería el encargado de recibir denuncias sobre estos ataques y plantear buenas prácticas para que no vuelvan a ocurrir.

4. Riesgos de la Telefonía IP en Ecuador: Resultados del Análisis Exploratorio Activo

A continuación se discuten los resultados obtenidos del análisis exploratorio activo para determinar, solamente en base a la aplicación de telefonía IP y sus versiones, el nivel de vulnerabilidad que podrían tener estos sistemas de telefonía.

4.1 Resultados del Análisis Exploratorio

De las pruebas realizadas en el mes de diciembre de 2013, se encontraron cerca de 800 dispositivos conectados a Internet en Ecuador con un servicio de telefonía IP basado en SIP funcionando. De estos dispositivos, un porcentaje importante (37%) ejecutaban soluciones basadas en Asterisk, y de ellas el 73% utilizaban FreePBX (seguramente Elastix) mientras que el 27% restante usaba Asterisk puro sin interfaz gráfica de gestión. Además, del total de sistemas telefónicos encontrados, el 15% usaban soluciones de Grandstream, 12% usaban alguna solución de la empresa Innomedia, 8% de Denwa, y aproximadamente el 12% no revelaba información sobre el nombre o la versión de la aplicación que ejecutaba.

La información encontrada sobre el uso de soluciones basadas en Asterisk (especialmente Elastix y FreePBX) conectadas a Internet muestra que muchas empresas están poniendo en marcha centrales telefónicas de bajo costo y que además están haciéndolas disponibles públicamente.

Enfocando el análisis a los dispositivos encontrados que funcionan con FreePBX (la mayoría sería Elastix), se descubrió que solamente un número aproximado al 2% de los dispositivos con esta distribución tenían instalada una versión actualizada (la 2.12 o 2.13, liberadas en 2015), el 20% tenía instalada la versión 2.10 o 2.11 liberadas hace solo 3 años pero que son vulnerables a

ataques de ejecución remota de comandos (Exploit Database, 2014). Finalmente, el 76% de los dispositivos ejecutando FreePBX tenían instalada una versión igual o inferior a la 2.8 que también poseen graves vulnerabilidades de seguridad (Exploit Database, 2010) (Androulidakis, 2016).

Por otro lado, de los dispositivos con Asterisk llano instalado, el 30% tenían una versión 1.6 y prácticamente todos tenían releases vulnerables (1.6.2.23 o inferiores) (Terán, 2012). Un 25% de los dispositivos con Asterisk utilizaba la versión 1.8, y de ellos algunos poseían un release vulnerable. Finalmente, casi un 50% de los dispositivos con Asterisk llano no entregaron información sobre las versiones instaladas.

Del breve análisis realizado en párrafos anteriores se puede concluir que existen en Internet en Ecuador, muchos dispositivos de telefonía IP públicamente disponibles. La gran mayoría de esos dispositivos ejecutan soluciones derivadas de Asterisk, especialmente Elastix/FreePBX (seguramente porque su instalación y configuración es relativamente sencilla y libre de licencias). El problema radicaría en varios factores: primero, que probablemente muchos de esos dispositivos no necesitan estar conectados a Internet a disposición de miles de atacantes; segundo, que la configuración por defecto que ofrecen estas soluciones de software libre no es la más adecuada porque en ocasiones revelan demasiada información; y, tercero, que la mayoría de esos dispositivos ejecutan versiones derivadas de Asterisk que están desactualizadas y que tendrían serias vulnerabilidades.

4.2 Análisis A Posteriori (*footprinting*)

Una vez que un atacante ha descubierto un sistema de telefonía IP público en Internet, así como el nombre de la aplicación telefónica y su versión, éste podría fácilmente indagar, de manera pasiva mediante un buscador en Internet, las vulnerabilidades que le afectan. Recordemos que si una aplicación instalada tiene una versión más moderna, es muy probable que la antigua tenga serios problemas de seguridad. Además, podría también encontrar código capaz de explotar estas vulnerabilidades, que aparece en Internet tan pronto como una vulnerabilidad es descubierta.

Identificado el objetivo, las posibilidades de ataque solo están limitadas por la imaginación del atacante. Por ejemplo, usando la herramienta svwar de SipVicious, un atacante podría implementar un ataque de enumeración para determinar los números de las extensiones a las que da servicio el sistema de telefonía IP. La información sobre estos números de extensiones podría ser muy útil luego para obtener las contraseñas respectivas, considerando que es común utilizar el mismo número de extensión como contraseña. De hecho, esta verificación (si la contraseña es la misma que el número de extensión) se puede realizar, junto con otras pruebas (si la extensión no tiene contraseña) utilizando otra herramienta de *SipVicious* llamada *svcrack*. Disponer de los números de extensión (identificadores de terminal en soluciones basadas en Asterisk) y su

correspondiente contraseña permitiría que el atacante registre su terminal en la central telefónica y haga uso de sus recursos.

4.3 Información de Fuentes de Información Oficiales

Aunque los ataques a sistemas de telefonía IP en Ecuador son realizados comúnmente a través de la conexión de dichos sistemas a Internet, el fraude (producto del ataque inicial) se consuma a través de la generación de tráfico utilizando la conexión de estos sistemas hacia la red de telefonía pública (fija o móvil) mediante el uso doloso de los recursos telefónicos pagados por la institución afectada. Por esta razón, los proveedores de aquellos servicios de telefonía pública estarían en plena capacidad de detectar comportamientos fraudulentos. Así ocurre actualmente con la CNT de Ecuador, empresa que posee la mayor cantidad de abonados de telefonía fija, y que puede identificar patrones poco comunes en la generación de llamadas (llamadas a destinos poco usuales, por ejemplo). Luego de detectar indicios de fraude, el proveedor suspende el servicio y reporta el incidente a la Arcotel para su investigación.

La división en la Arcotel encargada de atender este tipo de incidencias se llama Ecucert. Irónicamente, la mayor parte del tiempo, estos incidentes son detectados inicialmente por estos organismos y no por las instituciones afectadas.

Los únicos datos oficiales sobre la seguridad de los sistemas de telefonía IP en Ecuador fueron provistos por la Arcotel. Aunque la información es muy limitada por las obligaciones que tiene esta institución para el manejo privado de la información de las empresas que han recibido ataques, ésta puede servir para tener otra visión aparte de la estrictamente exploratoria que se expuso previamente.

A partir de las estadísticas tomadas desde hace 3 años, se han documentado en promedio unos 240 casos anuales relacionados con vulneración de sistemas de telefonía IP que terminan en fraude. Esto quiere decir que terminan en un perjuicio económico para la empresa afectada que va de los 1000 a 9000 dólares antes de ser detectado. El fraude lo realiza comúnmente un atacante que logra tener contacto con la PBX IP de una empresa (casi siempre mediante Internet) y empieza a utilizar esa PBX para sacar llamadas internacionales mediante las troncales disponibles hacia la PSTN.

Entre las marcas de las soluciones más afectadas se encuentran: Elastix, Cisco y Avaya. Entre las provincias donde se localizan estos incidentes se tiene: Pichincha, Guayas, Imbabura, Azuay, Manabí, Azogues y Santo Domingo. Los destinos más comunes de las llamadas cuando se toma el control de los recursos de estos dispositivos son: Sierra Leona, Mónaco, Austria, Serbia, Barbados, Montserrat, Guinea, Luxemburgo, Estonia, Somalia, Albania, entre otros.

5. Amenazas a la Telefonía IP en Ecuador: Evaluación en Prototipo Pasivo

Tal como se explicó en la Sección 3, el análisis pasivo permitió evaluar las amenazas a un sistema de telefonía IP deliberadamente vulnerable y basado en Asterisk (Elastix 2.0.0). Tal como con un honeypot, el objetivo de este prototipo es atraer a atacantes con el fin de analizar ciertos patrones que ayuden a entender un poco más los problemas de seguridad de este tipo de servicios tan crítico e igualmente vulnerable.

Los eventos generados en el prototipo público se analizaron entre el 29 de diciembre de 2015 y el 3 de enero de 2016. La información de estos eventos se extrajo del archivo de log full (ubicado en /var/log/asterisk/) y que guarda básicamente la información de todos los procesos que tienen que ver con el servicio de telefonía implementado. Cabe destacar que, luego de solo 6 días de estar en línea, se generaron 739 MB de logs relacionados con el servicio de telefonía, lo que revela la agresividad de las interacciones a las que se enfrentó el prototipo.

También se analizaron los logs contenidos en el archivo secure (dentro de /var/log) para tener una idea de los intentos de login remoto que se realizaron sobre el sistema desde Internet. Para empezar, se detectaron 4825 intentos de login remoto fallidos; de estos, 66 con el usuario root, y 13 con el usuario asterisk. La mayoría de estos intentos provienen de Estados Unidos, Indonesia y China.

Del mismo modo, se detectaron una enorme cantidad de intentos fallidos de registro SIP en la PBX IP (11441 intentos). La mayoría de estos intentos se realizaron a la extensión 100 (10705 intentos), y a la 101 (543 intentos). Además, todos estos intentos se originaron en solamente 9 direcciones IP. El 93% de los intentos se originaron en Francia y el resto en Estados Unidos, Alemania y Países Bajos.

Se detectaron también 667 intentos de registrar terminales utilizando números de extensiones que no existían en el prototipo. Estos intentos se originaron en 12 direcciones IP, la mayoría de ellos provenientes de Francia y Países Bajos. Los números de extensiones utilizadas van desde el 1 hasta el 10000, fundamentalmente. Se observó también varios procesos exitosos de registro (170), la gran mayoría desde Palestina y Francia. Finalmente, se encontraron 537 intentos de llamada desde el prototipo a través de la troncal telefónica conectada.

6. Ilustración de los Riesgos de Seguridad de la Telefonía IP en Ecuador

Para ilustrar los riesgos de seguridad de la telefonía IP en Ecuador, imaginemos a la empresa A que tiene 20 empleados. Motivada por el auge de la telefonía IP, y apasionada por el software libre, la gerencia de A decide encargar a Pedro, el administrador de tecnología, la implementación de un prototipo de sistema telefónico basado en Asterisk. Se espera que Pedro implemente un sistema de telefonía que permita a los empleados, dentro de la red de datos, comunicarse entre sí

y con la PSTN a través de 5 troncales analógicas (líneas telefónicas) contratadas con el proveedor local y dos bases celulares para comunicaciones móviles. Además, se encarga a Pedro que mediante este sistema de telefonía se permita a los clientes llamar a la empresa usando su conexión de Internet, para que no tengan que pagar la llamada cuando quieran comunicarse con A. Pedro es un buen empleado, ha trabajado antes con Linux, y aunque tiene muy claros los conceptos de telefonía, jamás ha implementado una solución de telefonía IP. Pedro encuentra un tutorial en Internet para instalar Asterisk, un poco antiguo, pero muy claro, así que decide seguirlo al pie de la letra. Luego de un par de días de pruebas, Pedro logra montar el sistema tal como le ha pedido la gerencia, y funciona tan bien que lo dejan trabajando. Luego Pedro se embarca en otros proyectos tecnológicos de la empresa y se olvida, por un tiempo, del sistema telefónico que acaba de instalar.

Sin percatarse de ello, Pedro instaló una versión desactualizada de Asterisk que, por defecto, es vulnerable a ataques de enumeración. Ya que el sistema está publicado en Internet, empieza a recibir escaneos muy intensivos de atacantes que intentan aprovecharse de esta vulnerabilidad. Puesto que las extensiones que creó se encuentran en un rango estándar (1000-10000), los atacantes no tardan en descubrirlo. Una vez con la información de los números de extensión, los atacantes descubren que las contraseñas de cada una de ellas es el mismo número de extensión. Pedro no imaginó que el sistema quedaría funcionando en producción, por lo que usó contraseñas fáciles para no olvidarlas y luego sí que olvidó cambiarlas.

Una vez con los parámetros de autenticación de varias extensiones, los atacantes registran sus terminales (suplantando usuarios internos) y así consiguen acceso al plan de marcado de la plataforma de telefonía, con lo que empiezan a utilizar los recursos de salida hacia otras redes de comunicaciones (PSTN). Además, otro atacante se logra registrar como invitado y, ya que Pedro no fue muy minucioso al configurar el plan de marcado para controlar las cuentas de invitado, resulta que sus llamadas también tienen acceso a las troncales. Todo esto sucede sin que Pedro lo note.

Luego de un mes de que la plataforma de telefonía quedó en marcha, la empresa A recibe una notificación del proveedor de telefonía fija sobre un patrón anómalo de llamadas salientes debido al cual el servicio se ha suspendido. En ese momento, Pedro se da cuenta de que se ha cometido un fraude contra su empresa a través de la plataforma de telefonía que instaló por el que deberá pagar cerca de diez mil dólares.

7. Conclusiones

Ante la evidente falta de información sobre los recursos de telefonía IP en el Ecuador, este artículo ha presentado algunos datos sobre las amenazas que estos enfrentan, especialmente cuando están conectados directamente a Internet. Del análisis exploratorio, se desprende que cientos de

estos sistemas están públicamente disponibles en Internet en Ecuador, que tendrían ejecutando software desactualizado y, por ello, vulnerable. Además, de los resultados se desprende que la mayoría de esos sistemas funcionan con aplicaciones basadas en Asterisk, particularmente Elastix y FreePBX. Casi no se descubren sistemas basados en Cisco, Avaya u otras soluciones de pago. Ya que estas soluciones licenciadas sí son populares en ciertos sectores de la empresa pública y privada ecuatoriana, esta estadística nos hace suponer que las implementaciones basadas en Asterisk no estarían siendo aseguradas adecuadamente ya que estarían revelando demasiada información en el contexto de Internet. Esto sería una consecuencia directa de la "facilidad" que ofrecen las soluciones de software libre para su implementación, lo que estaría impulsando iniciativas de instalación de plataformas de telefonía IP sin asesoramiento especializado. Finalmente, se descubrieron graves amenazas a plataformas de telefonía IP basadas en Asterisk (Elastix) cuando éstas se conectan directamente a Internet sin adecuados mecanismos de protección. Estas amenazas se plasman en miles de interacciones que se originan en diversas partes del mundo en actividades de enumeración de extensiones, ataques de fuerza bruta, registro de terminales no autorizados, e intentos de uso no autorizado de troncales telefónicas (fraude); todo inmediatamente después de conectar el sistema de telefonía IP a la red.

La seguridad de estos sistemas de telefonía se podría ver comprometida, en primera instancia, porque su conexión a una red pública de comunicaciones le pondría en contacto con sinfín de fuentes de ataque que se encuentran permanentemente monitoreando este espacio público. El uso de una u otra solución de telefonía no implica necesariamente una implementación vulnerable. Sin embargo, el empleo de versiones desactualizadas de software, la configuración incorrecta del plan de marcado, la innecesaria conexión a redes externas (especialmente a Internet), y, en general, la falta de dominio técnico de la solución telefónica que se implementa (parámetros por defecto), frecuentemente derivan en fraude y un importante perjuicio económico para la víctima.

Bibliografía

Allen, L. (2012). Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Packt Publishing Ltd.

Androulidakis, I. I. (2016). VoIP and PBX Security and Forensics: A Practical Approach.

Bryant, R., Madsen, L., & Van Meggelen, J. (2013). Asterisk: The definitive guide. " O'Reilly Media, Inc.".

Corporación Nacional de Telecomunicaciones. (2016). Troncal Telefónica IP - Telefonía | Corporación Nacional de Telecomunicaciones. [en línea] Disponible en: https://www.cnt.gob.ec/telefonia/plan-corporativo/troncal-telefonica-ip-2/ [Visitado 12 Ene. 2016].

Dassouki, K., Safa, H., & Hijazi, A. (2014, March). End to End Mechanism to Protect Sip from Signaling Attacks. In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on (pp. 1-5). IEEE.

El Comercio. (2015). Las llamadas por WhatsApp no pueden ser restringidas en Ecuador, según el Gobierno. [en línea] Disponible en: http://www.elcomercio.com/actualidad/llamadas-whatsapp-restringidas-ecuador-gobierno.html [Visitado 12 Ene. 2016].

El Universo. (2016). Skype reporta que algunos usuarios tienen problemas para realizar llamadas. [en línea] Disponible en: http://www.eluniverso.com/vida-estilo/2015/09/21/nota/5140421/skype-reporta-que-algunos-usuarios-tienen-problemas-realizar [Visitado 12 Ene. 2016].

EnableSecurity. (2012). SIPVicious. [en línea] Disponible en: http://blog.sipvicious.org/ [Visitado 1 Ene. 2016].

Exploit Database. (2010, Septiembre 24). FreePBX <= 2.8.0 Recordings Interface Allows Remote Code Execution. Disponible en: https://www.exploit-db.com/exploits/15098/ [Visitado 31 Ene. 2016].

Exploit Database. (2014, Marzo 12). FreePBX 2.11.0 - Remote Command Execution. Disponible en: https://www.exploit-db.com/exploits/32214/ [Visitado 30 Ene. 2016].

Exploit Database. (2015, Marzo 7). Elastix 2.x - Blind SQL Injection Vulnerability [en línea] Disponible en: https://www.exploit-db.com/exploits/36305/ [Visitado 1 Ene. 2016].

Instituto Nacional de Compras Públicas. (2016). Ingreso al Sistema - Compras Públicas. [en línea] Disponible en: https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/ [Visitado 1 Ene. 2016].

Ip2location. (2016). Block Visitors by Country | IP2Location.com. [en línea] Disponible en: http://www.ip2location.com/blockvisitorsbycountry.aspx [Visitado 1 Ene. 2016].

Puente, G. B. (2015). Elastix Unified Communications Server Cookbook. Packt Publishing Ltd.

Sangoma. (2014). FreePBX. [en línea] Disponible en: https://www.freepbx.org/ [Visitado 1 Ene. 2016].

Terán, F. (2012). Nuevas fallas de seguridad Zero Day descubiertas en Asterisk 1.6.2, 1.8 y Asterisk 10. [en línea] Sinologic :: Tu web favorita sobre VoIP. Disponible en: https://www.sinologic.net/blog/2012-04/nuevas-fallas-de-seguridad-zero-day-descubiertas-en-asterisk-1-6-2-1-8-y-asterisk-10.html [Visitado 1 Ene. 2016].