UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

ESTUDIO DE FRAUDES EN EL SERVICIO MÓVIL DE INTERNET

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELÉCTRICO

JAVIER ELÍAS YARMUCH MUÑOZ

PROFESOR GUÍA:
CLAUDIO IGNACIO ESTÉVEZ MONTERO

MIEMBROS DE LA COMISIÓN:
CLAUDIO ANDRÉS GARRETÓN VENDER
SANDRA LORENA CÉSPEDES UMAÑA

SANTIAGO DE CHILE
2015

RESUMEN DE LA MEMORIA
PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELÉCTRICO
POR: JAVIER ELÍAS YARMUCH MUÑOZ
FECHA: ABRIL, 2015.
PROF. GUÍA: Dr. CLAUDIO ESTÉVEZ

"ESTUDIO DE FRAUDES EN EL SERVICIO MÓVIL DE INTERNET"

En el mundo de las telecomunicaciones, los fraudes existen desde que se empezaron a masificar los servicios de telefonía fija. En esos tiempos, se disminuían costos y evadían pagos de manera ilegal, como por ejemplo, el cargo extra por llamadas internacionales o por llamadas de teléfono fijo a móvil. Dado el avance tecnológico, la televisión digital, el Internet móvil y la enorme oferta de servicios y aplicaciones que un teléfono móvil ofrece, las posibilidades de hacer fraude son mucho mayores.

El presente estudio se focaliza en los fraudes más masificados, en particular en servicios de Internet móvil. Para llevar a cabo este análisis, se hicieron pruebas en distintos escenarios en todos los servicios que ofrece un operador móvil. Estas pruebas consistieron en intentar explotar distintas vulnerabilidades existentes conocidas en el servicio, como por ejemplo la conexión vía VPN en Internet móvil. Se sometieron a pruebas los tres operadores más grandes del país.

Los resultados de las pruebas permiten concluir que actualmente el fraude es posible tanto en Chile como en el extranjero, y que los operadores están trabajando para disminuir las vulnerabilidades existentes. Se puede señalar también que el volumen de fraude es sustancial (cada conexión irregular puede llegar a ser del orden de 2 Mbps en descarga y 0,5 Mbps en subida), lo que puede causar un gran daño a los operadores móviles en el ámbito comercial y de planificación de redes.

La importancia de este estudio consiste en la recopilación de los métodos más viralizados para hacer fraude y así poder tomar acciones por parte de los operadores. En consecuencia, se genera una optimización de los recursos de red disponibles.

Tabla de Contenido

Tabla de Ilustraciones.

Capítulo 1: INTRODUCCIÓN

Este estudio está orientado a diagnosticar y probar las distintas formas de vulnerar las plataformas de cobro y evadir costos de navegación desde el punto de vista de un usuario casual, es decir, sin conocimiento avanzado en redes y protocolos. Para esto, el trabajo realizado contempla a cabalidad el proceso de extracción de conocimiento de aplicaciones web que dan soporte a discusiones u opiniones en línea. En esa categoría se encuentran los foros y redes sociales, en donde se acumula e intercambia la mayor cantidad de información relacionada con el tema. Se continúa realizando una evaluación realista, mediante la simulación de todas las técnicas encontradas para realizar fraude en todos los escenarios posibles, midiendo el ping y la velocidad de la conexión, para finalmente analizar el impacto y las potenciales pérdidas por parte del operador móvil.

1.1. Motivación

El constante aumento de dispositivos inteligentes, la introducción de nuevas tecnologías de conexión móvil (LTE) y la convergencia de las comunicaciones a la mensajería instantánea y redes sociales ha producido un aumento considerable en el tráfico de Internet móvil. Según Cisco, "Casi la mitad de mil millones (497 millones) de dispositivos móviles y conexiones se agregaron en 2014. La cantidad global de dispositivos móviles alcanzó un total de 7.4 mil millones, aumentando de los 6.9 mil millones del 2013. Los smartphones son el 88% del aumento registrado, agregándose 439 millones de ellos en el 2014" [1]. Además, Cisco pronostica que el aumento del tráfico será considerable en los próximos años, llegando a 24.3 Exabytes por mes para el año 2019. [1]

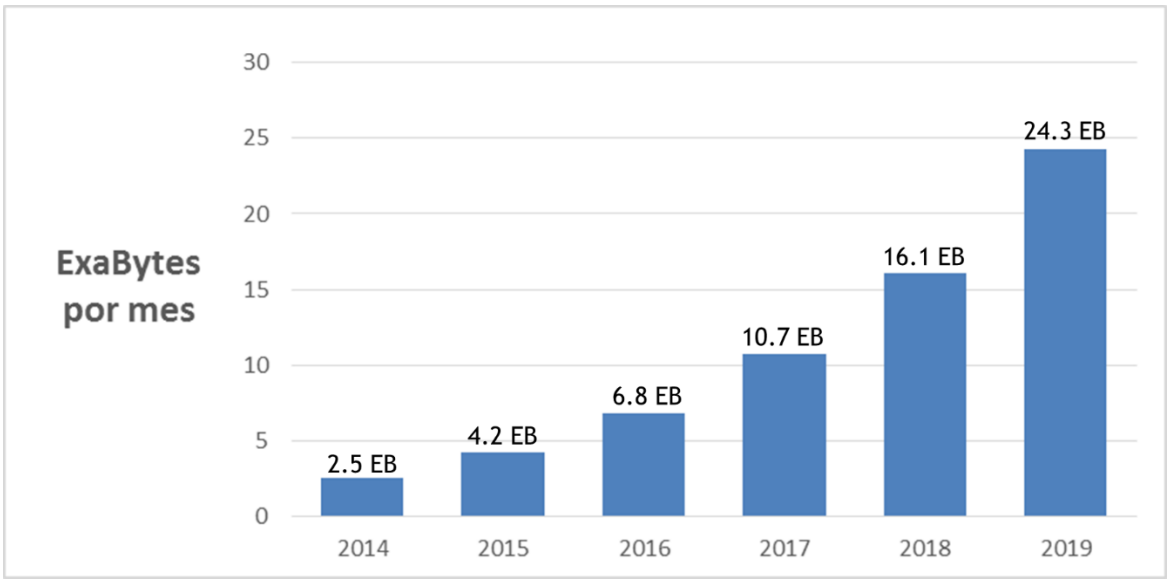

Figura 1: Cisco VNI Mobile 2015 estima que el tráfico mensual de datos móviles ascenderá a 24.3 Exabytes (24 300 000 Terabytes) el año 2019 [1]

En Estados Unidos, la consultora "Chetan Sharma consulting", especialistas en estudios en el mercado móvil, señala que los ingresos por datos móviles superaron a los ingresos por servicios de telefonía y de mensajes cortos (SMS, *Short Message Service*) a finales del año 2013 [2]. Además indica que el crecimiento en los ingresos de los datos móviles ha sido exponencial, tal como muestra la Figura 2. En base a estas afirmaciones, claramente el aumento del tráfico presentó una gran oportunidad para los operadores móviles para aumentar los ingresos, enfocándose más en los servicios de Internet móvil que los servicios de voz y SMS.

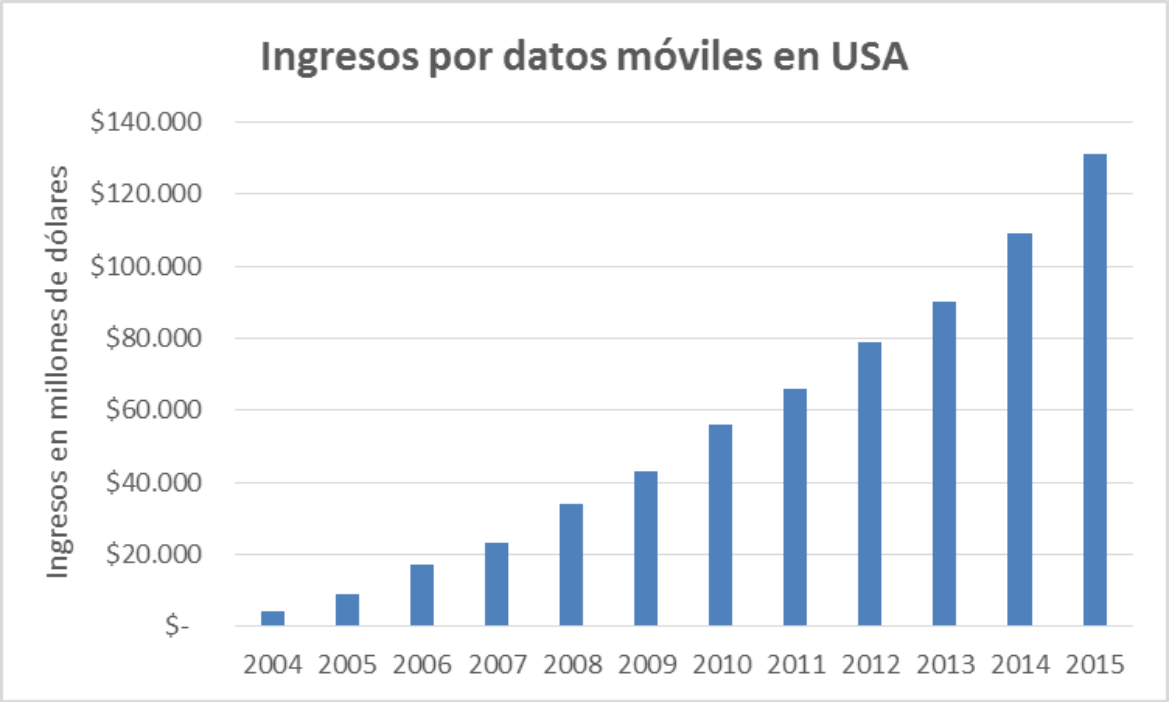

Figura 2: Ingresos anuales por datos móviles en millones de dólares estimados por Chetan Sharma Consulting, 2015. [2]

Pero con la oportunidad viene el riesgo. Si antes la evasión era de los costos de los servicios de voz, ahora es de los servicios de datos. El aprovechamiento de las vulnerabilidades de las plataformas de cobro se convirtió en un tema sumamente importante para los operadores móviles, ya que estos fraudes ponen en peligro las oportunidades que el mercado actual presenta. Por lo tanto, este estudio ayudará a entender y detectar los ataques, y además se discutirán las repercusiones que producen a los operadores y a los demás usuarios que ocupan la misma red.

1.2. Alcances

Como se señaló anteriormente, este estudio se desarrolla con el propósito de detectar y probar las distintas formas de vulnerar las plataformas de cobro. Para esto, se necesita estudiar todos los protocolos y puertos que están involucrados en la navegación móvil de un usuario común. Los protocolos y puertos más conocidos por ser utilizados para cometer fraude y que serán sometidos a pruebas son:

- Protocolos: TCP, UDP, ICMP y DNS.

- Puertos: 21, 53, 80, 110, 123, 137, 443, 995, 1194, 1985, 4343, 8080, 8484, 9200 y 9201.

Además, durante el proceso se requiere implementar distintos códigos y utilizar una serie de programas, los cuales permiten enmascarar todo el tráfico del usuario en un solo tipo de protocolo y puerto que no esté siendo tarificado. Algunos de estos programas son:

- TroidVPN
- DroidVPN
- OpenVPN Connect
- YourFreedom
- SimpleServer

1.3. Objetivos

1.3.1. Objetivo General

El objetivo general es diagnosticar y probar las distintas maneras de vulnerar el servicio de Internet móvil en los sistemas de operadores móviles, de manera que se logren cuantificar las pérdidas incurridas por la explotación fraudulenta de dichas vulnerabilidades.

1.3.2. Objetivos Específicos

- Demostrar que el servicio de Internet móvil tiene vulnerabilidades y que además son conocidas por algunos usuarios, los cuales explotan de forma fraudulenta dichas vulnerabilidades para obtener el máximo provecho.
- Replicar los fraudes y revelar en los sistemas cuáles son los parámetros de configuración que explotan. Además, establecer cuáles son las características, velocidad y estabilidad de cada uno de los fraudes.
- Calcular el impacto en los ámbitos técnico y comercial en que incurren los operadores del servicio de Internet móvil, debido a la existencia de prácticas fraudulentas de uso del servicio.

1.4. Estructura de la Memoria

La estructura utilizada en esta memoria es la siguiente:

- **Capítulo 1. Introducción**: Se introduce y motiva al lector en el tema investigado y se presentan los alcances, objetivos y estructura de la memoria.

- **Capítulo 2**. **Contextualización**: En este capítulo se describen los conceptos generales básicos que dan marco a la memoria, es decir, que lo colocan en un contexto. Al final de este capítulo se termina explicando cuál es el aporte del proyecto al conocimiento en el campo en que este se ha desarrollado.

- **Capítulo 3**. **Implementación**: En este capítulo se describen las actividades del plan de trabajo que permiten desarrollar el proyecto. Se replica cada fraude con sus respectivas aplicaciones, se revisan los parámetros de configuración que utiliza cada uno y se expone el impacto en el ámbito técnico y comercial de dichas vulnerabilidades para la empresa y para los demás usuarios.

- **Capítulo 4**. **Análisis de Resultados**: Se lleva a cabo un análisis cualitativo y cuantitativo de los fraudes implementados. Se expondrán y discutirán los resultados obtenidos en la realización de las actividades. Se estudiará la efectividad de estudios anti-fraudes como este.

- **Capítulo 5**. **Conclusiones**: Se presentarán las conclusiones del trabajo a la luz de los resultados obtenidos. Se realizarán recomendaciones en el sentido de abordar aspectos o actividades en proyectos futuros.

Capítulo 2: CONTEXTUALIZACIÓN

El objetivo del presente capítulo es ubicar al lector en el entorno en el cual se desarrolla este trabajo de título.

2.1. Internet

El Internet es una red informática descentralizada que permite la conexión entre computadoras a través de protocolos de comunicaciones. En otras palabras, Internet es una red de redes, por la cual millones de computadores, notebooks, tablets y smartphones se pueden conectar entre sí. Además, diariamente se agregan a la red nuevos dispositivos que tienen otra función, pero que se conectan a Internet para agregar funcionalidades como los sensores, webcams y consolas de video juegos. Por lo tanto, Internet es una red grande, creciente, heterogénea y muy compleja. En este capítulo se explicarán los conceptos básicos y su funcionamiento, los cuales son conocimientos necesarios para comprender cómo se efectúan los fraudes en Internet.

2.1.1. Elementos Principales de Internet

En un principio, los dispositivos que estaban conectados a Internet eran bastante limitados en comparación con los que hoy existen, por lo que se utilizaban para hacer tareas mucho más livianas. En ese tiempo, cuando la cantidad de computadores que estaban conectados no alcanzaba el millón, no era muy complicado entender el funcionamiento de la red. Hoy, el Internet se ha convertido en una gigantesca red que interconecta millones de dispositivos. A esto se le suma el servicio de Internet móvil que proveen los operadores móviles, lo que permite a más dispositivos integrarse día a día a la red.

A veces, no es práctico que dos dispositivos de comunicaciones se conecten directamente mediante un enlace directo. Esto es válido si los dispositivos están muy alejados o si existe un conjunto de dispositivos que necesitan conectarse entre ellos en instantes de tiempo diferentes. Por lo tanto, cada dispositivo se conecta con los demás a través de red de enlaces de comunicaciones. Las redes de enlaces están compuestas por nodos e interconexiones entre ellos. Los nodos son elementos que se encuentran entre los dispositivos, los cuales son capaces de recibir información, almacenarla un intervalo breve y posteriormente reenviarla al siguiente nodo. Estos nodos son los conocidos enrutadores y switches. La interconexión que hay entre los nodos y los dispositivos puede ser por medios guiados o por el aire. En la categoría de medios guiados se encuentran el par trenzado, el cable coaxial y la fibra

óptica. En el caso de la transmisión inalámbrica, se encuentra la radiotransmisión, que incluye las microondas, la transmisión por ondas de luz, entre otros. Dependiendo del tipo de interconexión que se usa, se puede transmitir a distintas velocidades, las cuales se miden en bits/segundo. Los distintos tipos de enlaces y elementos que componen Internet son ilustrados en la Figura 3.

La conmutación de paquetes es la forma de transmisión de información preferida en las redes de enlaces. Esto consiste en enviar los datos en secuencias de pequeñas unidades llamadas paquetes. Cada uno de ellos contiene en sí mismo la información del emisor, el receptor y otras cosas más dependiendo del tipo de datos y el protocolo. La parte reservada para transportar esta información se denomina cabecera. Como se verá más adelante, estas mismas cabeceras serán las encargadas de engañar a las plataformas que hacen el cobro en los operadores móviles, ya que hay mecanismos para modificar cada campo de la cabecera.

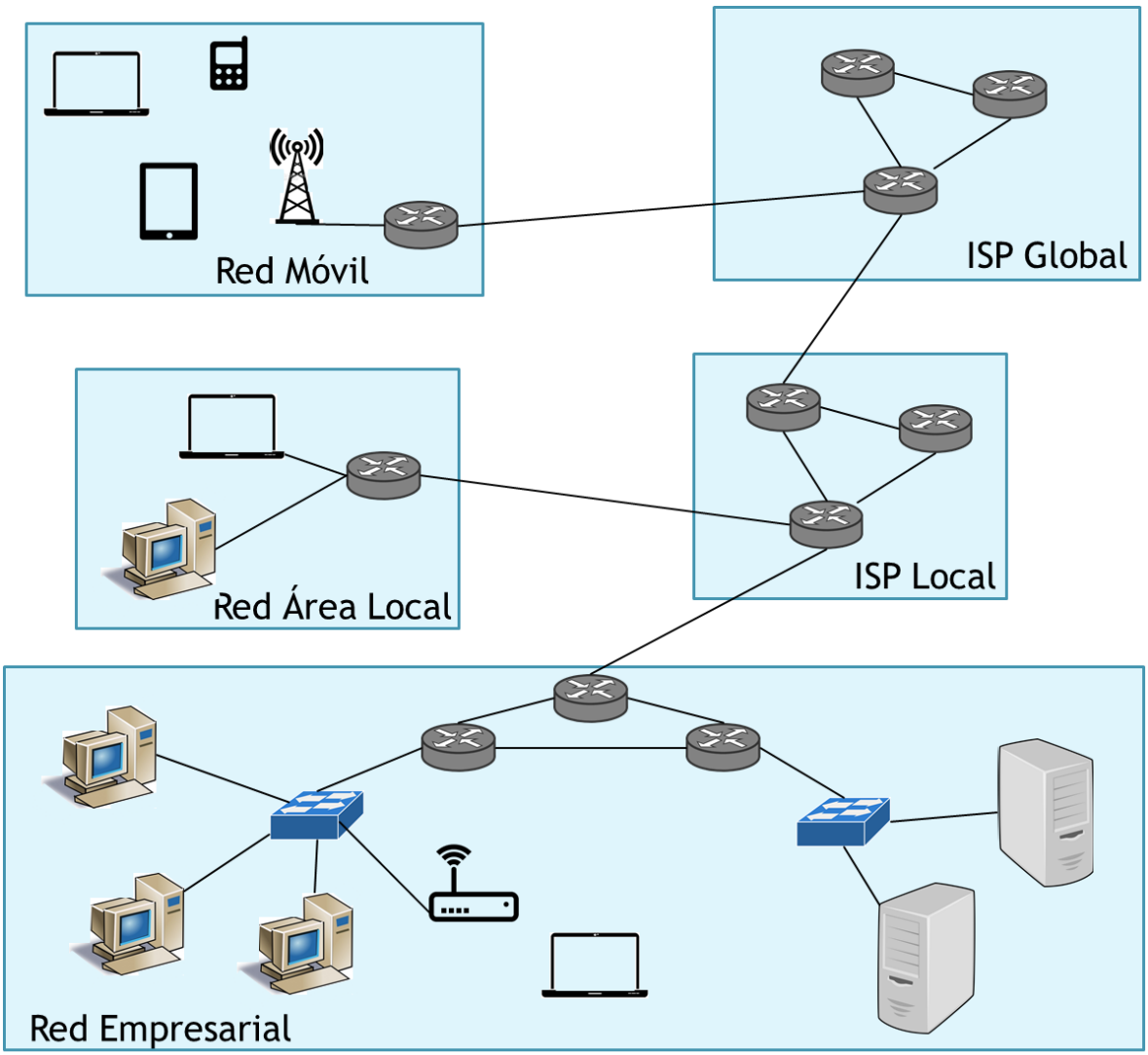

Figura 3: Algunos componentes esenciales de Internet. [3]

Todos los dispositivos necesitan tener acceso a Internet de alguna forma y son los proveedores de servicios de Internet (ISP, *Internet Service Provider*) quienes entregan esta prestación. Los ISP conectan a sus usuarios a través diferentes tecnologías como la línea de abonado digital mediante módem, la conexión inalámbrica por el sistema global para las comunicaciones móviles (GSM, *Global System for Mobile Communications*) o mediante fibra óptica. Dentro de la gran cantidad de dispositivos que están siendo conectados por los ISP, no solo se encuentran los usuarios "clientes", sino que también están los servidores, los cuales se encargan de proveer los sitios web. Por lo tanto, como los ISP conectan todo, se consideran los cimientos de Internet.

Para entender bien cómo funcionan los ISP hay que señalar que estos tienen distintas jerarquías, es decir, hay unos más grandes y unos más chicos. Como se ilustra en la Figura 4, los ISP más pequeños son interconectados por los más grandes. Los más pequeños o de nivel inferior son los más cercanos a los usuarios. Estos son los más conocidos porque ofrecen el servicio de Internet directamente a la población. Más arriba, se encuentran los ISP de nivel superior, los cuales pueden ser nacionales o internacionales. Estos no son tan conocidos y su estructura está compuesta por enrutadores y enlaces de alta velocidad. Estos mismos son los que interconectan continentes mediante enlaces de fibra óptica que cruzan océanos completos.

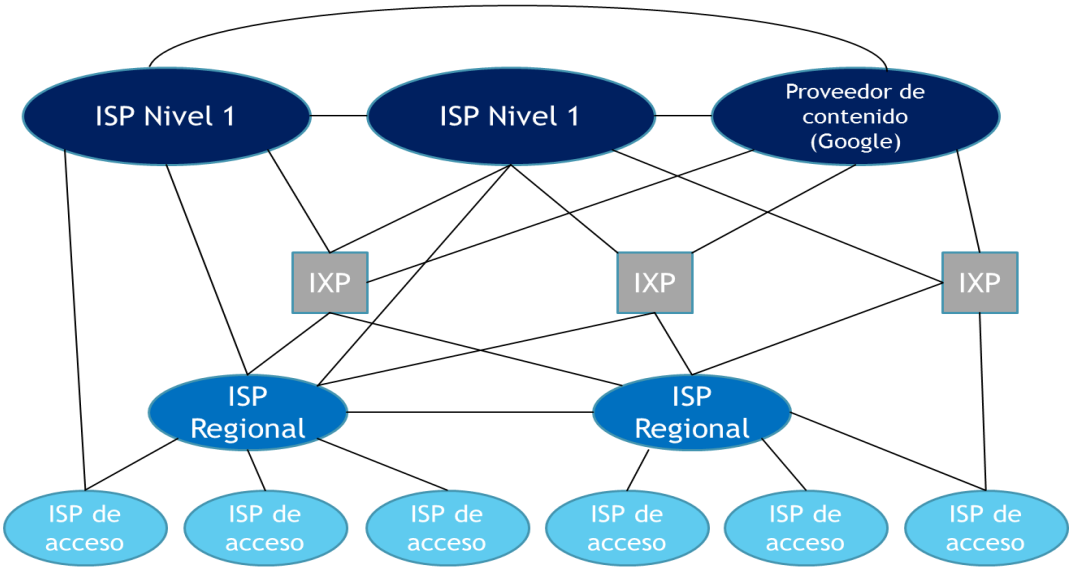

Figura 4: Interconexión de los ISP. [4]

La parte más importante de todo lo que se ha repasado hasta ahora son las cabeceras de los paquetes que se utilizan para transmitir la información. Dichas cabeceras son distintas y su contenido depende del protocolo. Los protocolos más importantes y conocidos son el protocolo de control de transmisión (TCP, *Transmission Control Protocol*) y el protocolo de Internet (IP, *Internet Protocol*). Además de ellos, se pueden encontrar el protocolo de datagramas de usuario (UDP, *User Datagram Protocol*), el protocolo de mensajes de control de Internet (ICMP, *Internet Control Message Protocol*) y el sistema de nombres de dominio (DNS, *Domain Name System*). Estudiar la manera en que se utilizan estos protocolos es de suma importancia, ya que ellos son fundamentales para el funcionamiento de Internet. Por lo tanto, gran parte de este capítulo está dedicado a revisar el uso de dichos protocolos en

los dispositivos y nodos de la red. Además, se explicará que los fraudes profundizados más adelante se aprovechan de vulnerabilidades relacionadas a estos mismos protocolos.

2.1.2. Internet Móvil

El Internet móvil nace a partir de la evolución de la telefonía móvil. En un principio, los dispositivos móviles solo permitían hacer llamadas y algunas cosas más como jugar, hacer anotaciones, enviar SMS, etc. Pero enseguida fueron creciendo las necesidades de los usuarios y el acceso a distintos contenidos aumentó.

El primer servicio de contenidos inalámbricos ofrecido por estos dispositivos era el protocolo de aplicaciones inalámbricas (WAP, *Wireless Application Protocol*). La tecnología WAP permite que los usuarios de los dispositivos móviles puedan acceder a servicios disponibles en Internet, sin embargo, tiene muchas limitaciones en comparación a la navegación en un computador.

Posteriormente, se creó el servicio general de paquetes vía radio (GPRS, *General Packet Radio Service*) o más conocido como 2G, el cual permite la transmisión de datos mediante conmutación de paquetes. Esto significa que es posible acceder a Internet a través del protocolo TCP/IP y alcanzar velocidades de hasta 114 kbps. Más tarde se implementó una tecnología llamada tasa de datos mejoradas para la evolución de GSM (EDGE, *Enhanced Data Rates for GSM Evolution*), la cual se considera una evolución de GPRS y actúa como puente entre las redes 2G y 3G. A pesar de que EDGE sea más avanzado, no se considera como una nueva generación y se denomina 2.5G.

La tercera generación o 3G es conocida como sistema universal de telecomunicaciones móviles (UMTS, *Universal Mobile Telecommunications System*) y permite acceder a todo tipo de contenidos multimedia, ya que alcanza una velocidad máxima de 384 kbps. Esta tecnología aún está vigente en los dispositivos móviles, pero en algunos otros ya se puede utilizar 4G – LTE que corresponde a la siguiente generación. Como la gran mayoría de los operadores móviles ofrece 3G a sus usuarios, se profundizará en la arquitectura UMTS más adelante.

La cuarta generación o 4G ya está presente en los dispositivos móviles más avanzados y permite navegar a velocidades de hasta 100 Mbps. Dado que las necesidades de los usuarios han ido cambiando, las comunicaciones móviles también. Por lo tanto, esta tecnología está enfocada netamente a la transferencia de datos, ya que está basada por completo en el protocolo IP. Cada día es más común comunicarse a través de aplicaciones de mensajería como "Whatsapp" y como consecuencia se ha dejado de lado la telefonía móvil.

Como la cuarta generación está presente en el día a día de los usuarios, también se revisará en la próxima sección. [17]

2.1.2.1. Arquitectura de la Red Móvil

La arquitectura presente en todos los operadores móviles que hoy en día ofrecen servicios de Internet móvil es UMTS. Como se ve en la Figura 5, la arquitectura UMTS se puede separar en tres bloques, el primero corresponde al equipo del usuario (UE, *User Equipment*), el segundo a la red UMTS terrestre de radio acceso (UTRAN, *UMTS Terrestrial Radio Access Network*) y el tercero a la red core (CN, *Core Network*).

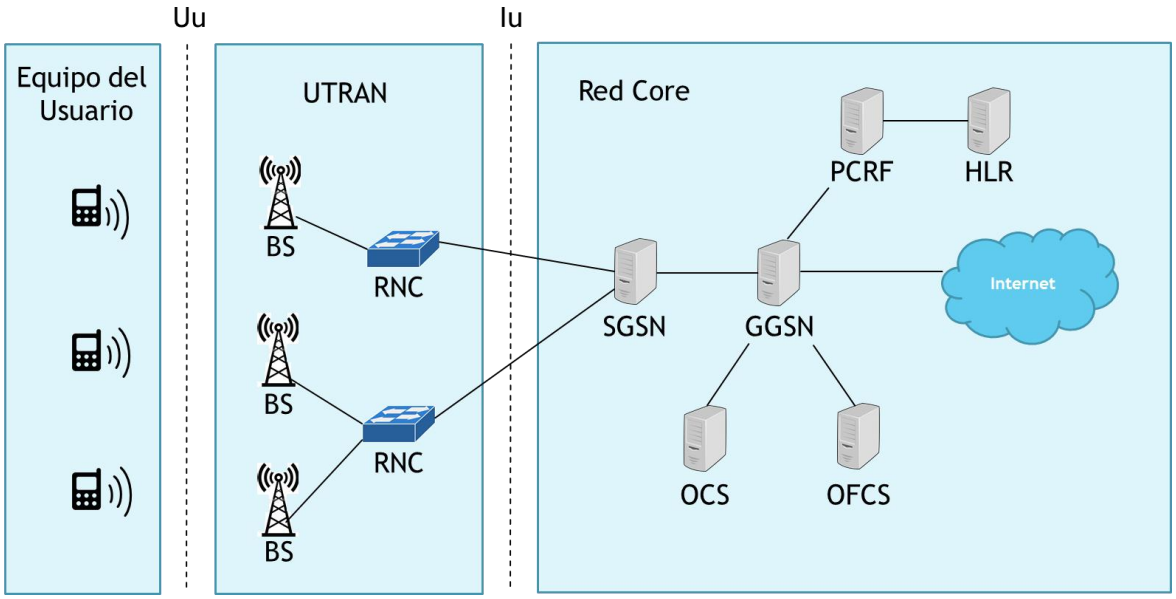

Figura 5: Arquitectura UMTS. Fuente: Elaboración propia.

El equipo del usuario corresponde al dispositivo que utiliza el cliente para conectarse a Internet. Cada uno de estos es identificado por la red por el número de suscripción del móvil (MSISDN, *Mobile Station International Suscriber Directory Number*). Cuando el operador móvil quiere verificar si el usuario tiene saldo para navegar, hacer un cobro o una recarga, se hace consultando la información asociada al MSISDN de dicho usuario. También existen otros números identificadores de dispositivos, como el identificador de equipo del sistema móvil internacional (IMEI, *International Mobile System Equipment Identity*), pero no son tan importantes como el MSISDN.

Los dispositivos se conectan a las estaciones bases (BS, *Base Station*) que son parte del segundo bloque llamado UTRAN. La comunicación entre ellos es mediante la interfaz Uu. Estas son las conocidas antenas de celulares que

se ven por las ciudades y también son llamadas "Nodos-B". Cada una está conectada a los controladores de red de radio (RNC, Radio Network Controller), los cuales se encargan de controlar la red de estaciones bases y direccionar el tráfico hacia las plataformas del operador móvil. La comunicación entre los RNC y las plataformas del operador móvil son mediante la interfaz Iu.

La plataforma que actúa como puerta de entrada al tercer bloque es el nodo de servicio GPRS (SGSN, *Serving GPRS Support Node*), el cual da acceso a los dispositivos móviles a la red del operador móvil. Además se encarga del manejo de la movilidad de los dispositivos de una estación base a otra. Este se conecta con el nodo de compuerta GPRS (GGSN, *Gateway GPRS Support Node*), el que actúa como enlace con la red exterior, es decir, con Internet. En este punto se hace un filtro de cuáles clientes pueden navegar y cuáles no, ya que para cada conexión se consulta a una plataforma llamada función de políticas y reglas de cargos (PCRF, *Policy and Charging Rules Function*). El PCRF es generalmente un "firewall" que hace una inspección profunda de paquetes (DPI, Deep Packet Inspection) y determina si las conexiones cumplen con las condiciones determinadas por el operador móvil. Esta plataforma le consulta constantemente al registro de ubicación base (HLR, *Home Location Register*) sobre las características del cliente para determinar qué servicios puede usar. Esta base de datos es conocida como el corazón de un operador móvil, ya que se encuentra toda la información de todos los clientes. Por lo tanto, no se puede modificar por cualquier entidad, así que existen otras dos plataformas muy parecidas encargadas de eso. Estas son el sistema de cobros en línea (OCS, *Online Charging System*) y el sistema de cobros fuera de línea (OFCS, *Offline Charging System*). Ambas plataformas son utilizadas para realizar los cobros a los usuarios y registrarlo en el HLR, con la diferencia que OCS lo hace inmediatamente y OFCS tarda horas e incluso días.

La tecnología 4G está presente en los operadores móviles más grandes e importantes de Chile, por lo tanto es importante entender las mejoras que introduce a la arquitectura UMTS. La cuarta generación o arquitectura LTE permite la transmisión a mayores velocidades tanto de subida como de bajada. Reduce significativamente la demora de las conexiones, lo que mejora la experiencia del usuario. Es más estable y soporta el crecimiento constante de usuarios en la red.

Para lograr estas ventajas, el primer cambio en la arquitectura es que los RNC desaparecen y sus funciones se traspasan a las estaciones base, convirtiéndolas en "eNodoB". De esta forma, las estaciones bases se comunican y controlan entre sí, utilizando otro interfaz de comunicación más complejo. Además existe otra plataforma que se encarga de la movilidad de los usuarios entre las estaciones bases llamada entidad encargada de la movilidad (MME, *Mobility Management Entity*). También, se sustituye el GGSN

por el paso de servicio (SGW, *Serving Gateway*) y el paso de red de datos públicos (PGW, *Public Data Network Gateway*), las cuales realizan las mismas tareas, pero de una manera más eficiente.

En el fondo, la evolución de 3G a 4G significa un migración de los principales servicios que ofrece un operador móvil al protocolo IP, por lo que ya no hay una red distinta para voz y datos. Esto no representa grandes cambios para la parte de Internet, pero sí para la parte de voz. Por lo tanto, para ofrecer la cuarta generación a los clientes no es necesario invertir en una red completamente nueva. En consecuencia, el PCRF, OCS y OFCS funcionan de la misma manera en ambas generaciones, por lo que los ataques que más adelante se revisarán funcionan de la misma forma si se utiliza 3G o 4G. [17]

2.2. Modelos de Capas

En general, un usuario de Internet no imagina lo complicado que es para sus dispositivos conectarse con otros. Para que esto ocurra, se requiere que ambos "hablen el mismo idioma". Lo que se comunica, cómo se comunica y cuándo se comunica debe seguir una serie de convenciones mutuamente aceptadas por los dispositivos involucrados. Es claro que debe haber un alto grado de cooperación entre los dispositivos, por lo que en vez de implementar toda la lógica para llevar a cabo la comunicación en un único proceso, esto se divide en subtareas, las cuales se realizan por separado. Entonces, en vez de disponer de un solo módulo que realice todas las tareas involucradas en la comunicación, se considera una estructura que consiste en conjunto de módulos que realizarán todas las funciones. Esta estructura se denomina arquitectura de capas y permite estudiar una parte específica de la comunicación. Además, esta forma de analizar los componentes del sistema facilita la actualización de los componentes.

Hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares de la comunicación: el modelo OSI y el modelo TCP/IP. TCP/IP es la arquitectura más adoptada para la interconexión de dispositivos, mientras que OSI se ha convertido en el modelo estándar para clasificar las funciones de comunicación. Ambos modelos se comparan gráficamente en la Figura 6.

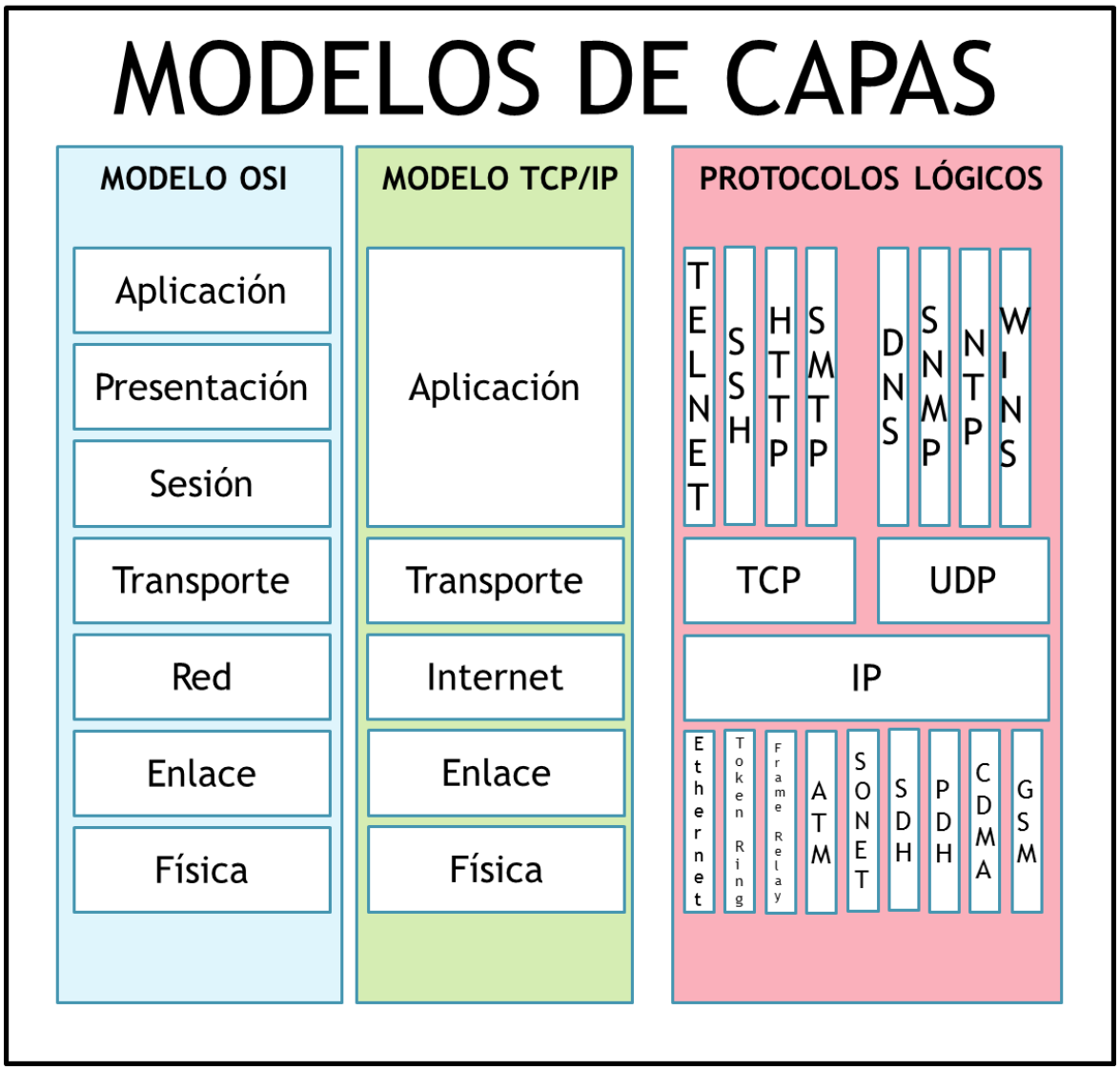

Figura 6: Modelos de capas de Internet [5]

Al contrario que en el modelo OSI, no hay un modelo oficial de referencia TCP/IP. Sin embargo, basándose en los protocolos estándar que se han desarrollado, todas las tareas involucradas en la comunicación se puede organizar en cinco capas independientes:

I. La capa de aplicación.
II. La capa de transporte.
III. La capa de Internet.
IV. La capa de enlace.
V. La capa física.

A continuación, se va a aplicar explicar cada capa del modelo TCP/IP, abordando en primer lugar la capa de aplicación y continuando hacia abajo. [18]

2.2.1. Capa de Aplicación

Por encima de todas las capas se encuentra la capa de aplicación, la cual contiene varios protocolos que se necesitan con frecuencia. Siempre que se ocupa una aplicación que se conecta a Internet se utilizará un protocolo de esta capa. Entre los protocolos más antiguos están el de terminal virtual (TELNET, *Teletype Network*), el de transferencia de archivos (FTP, *File Transfer Protocol*) y el de correo electrónico (SMTP, *Simple Mail Transfer Protocol*). El protocolo de terminal virtual permite que un usuario en un dispositivo ingrese en uno distante y trabaje ahí. Se dice que es antiguo porque actualmente se prefiere utilizar el protocolo de intérprete de órdenes segura (SSH, *Secure SHell*), el cual tiene el mismo propósito pero agrega encriptación a los comandos remotos. El protocolo de transferencia de archivos ofrece un mecanismo para transferir datos de un dispositivo a otro de forma eficiente. El protocolo del correo electrónico provee una manera de robusta para enviar y recibir correos ordenada y consistentemente. Otro protocolo que se usa a diario y que corresponde a esta capa es el protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*), el cual es el encargado de solicitar y recibir respuestas de páginas web. Es relevante saber en qué contexto se utiliza HTTP, ya que existen fraudes que se pueden realizar debido al uso de este protocolo. Cuando se navega por Internet en un buscador, generalmente es HTTP el encargado de hacer todo funcione. Primero se establece la conexión, buscando el nombre de dominio en la red para poder hacer contacto con el servidor web correspondiente. Al encontrarlo, se envía una petición con una serie de parámetros necesarios para que el servidor responda. Por último, el servidor responde y envía el sitio web solicitado en un principio. Este método de intercambio de información es el más común en Internet y por eso mismo se ha convertido en uno de los principales canales de comunicación entre los usuarios y operadores móviles. Cuando el usuario necesita saber su cuota de navegación, detalles de facturación o comprar bolsas, lo hace a través de un portal HTTP sin costos asociados. El hecho que no se cobre convierte a dicho portal en una vulnerabilidad, ya que los atacantes disfrazan todo su tráfico como si consultaran el portal, lo que les permite navegar gratis. Este fraude se estudiará más adelante, ya que se realiza en conjunto con otras herramientas. Sin embargo, el protocolo más importante a estudiar en la capa de aplicación es el DNS, ya que es uno de los más utilizados para cometer fraudes en los operadores móviles y también se intentará vulnerar en este estudio. Enseguida se verá cual es el propósito de DNS y su respectivo funcionamiento.

2.2.1.1. DNS

Este protocolo se explicará a cabalidad dado que se utiliza para hacer fraudes como se ha mencionado anteriormente. Además, se considera de la capa de aplicación, por lo que será fundamental su entendimiento en esta sección.

A pesar de que a diario se utilizan nombres como google o u-cursos para navegar por la red, ésta entiende solo direcciones binarias. Por lo tanto, de alguna manera hay que convertir los nombres propios a direcciones que la red entienda. Sería ideal tener una base de datos de acceso público que relacione todas las direcciones de los hosts con las direcciones IP. Es así que se crea DNS, una base de datos distribuida por el mundo que implementa un índice de nombres jerárquicamente basado en dominios.

Muy brevemente, el modo de usar DNS es el siguiente: Para relacionar un nombre con una dirección IP, una aplicación envía un paquete UDP con el nombre a un servidor DNS local a través del puerto 53, el cual busca el nombre y devuelve la dirección IP a la aplicación. Con la dirección IP, el dispositivo puede establecer la conexión con el sitio.

Conceptualmente, Internet se divide en varios cientos de dominios de nivel superior, donde cada uno abarca muchos hosts. Cada dominio se divide en subdominios, y éstos se dividen nuevamente, etc. Los dominios de nivel superior son de dos tipos: genéricos y de país. Los dominios genéricos son ".com", ".gov", ".net", entre otros. Los dominios de país son ".cl", ".br", ".de", etc. Cada dominio se nombra por la trayectoria hacia arriba separado por puntos. Por ejemplo, la facultad de ingeniería de la Universidad de Chile es http://ingenieria.uchile.cl/.

Hay ciertos detalles importantes con respecto a los nombres de dominio. Estos no hacen distinción entre las mayúsculas y las minúsculas, por lo que ".cl" o ".CL" son lo mismo. Además, los componentes pueden ser de hasta 63 caracteres de longitud cada uno, y los nombres completos no pueden exceder los 255 caracteres. Para crear un nombre de dominio nuevo, es necesario el permiso del dominio en el que se incluirá. De esta manera se evitan los conflictos de nombres y cada dominio puede llevar el registros de todos sus subdominios. Los nombres de dominio reflejan limites organizacionales, no redes físicas. Por ejemplo, los departamentos de informática e ingeniería eléctrica podrían ubicarse en el mismo edificio, compartir la misma red pero tener dominios diferentes. [19]

2.2.1.1.1. Servidores DNS

En teoría, un solo servidor sería capaz de contener la base de datos y responder a todas las consultas. En la práctica, este servidor se sobrecargaría

y sería inservible. En ese caso, todo Internet dejaría de funcionar, ya que ningún usuario podría hacer consultas DNS y no se podría navegar. Para evitar estos problemas, la base de datos se divide en distintos servidores.

Los servidores que tienen la base de datos oficial son llamados servidores DNS de raíz (*Root DNS Server*), los cuales se encuentran listados en http://www.root-servers.org/. Como se indica en el sitio web, existen 13 tipos de servidores de raíz distintos etiquetados de la A a la L, los cuales son operados por 12 distintas organizaciones y están dispersos por todo el mundo. Estos servidores son los encargados de tener los registros de los dominios de nivel superior, tales como .com, .net, .edu y .gov.

Cada uno de los dominios de nivel superior es administrado por servidores llamados servidores DNS de dominio de nivel superior (TLD DNS Server, *Top Level Domain DNS Server*). Estos servidores tienen el registro de todos los dominios autoritativos asociados al dominio de nivel superior correspondiente. Por ejemplo, el servidor DNS del dominio de nivel superior ".cl" tiene el registro de todos los dominios de Chile. Estos podrían ser http://www.entel.cl/, http://www.uchile.cl/ o http://www.movistar.cl/.

Para cada dominio hay un servidores que tienen el registro de todos sus subdominios. Estos subdominios podrían corresponder, por ejemplo, a distintos departamentos de una misma institución. En el caso de la Universidad de Chile, se podrían encontrar distintos subdominios como http://matricula.uchile.cl/, http://alumnos.uchile.cl/, http://ingenieria.uchile.cl/ o http://dcc.uchile.cl/. Estos servidores que contienen estos registros son llamados servidores DNS autoritativos (*Authoritative DNS Server*) y están presentes en todas las organizaciones.

Como se revisó, el funcionamiento de los servidores DNS es descentralizado y de forma jerárquica. En la Figura 7 se puede ver un esquema de la distribución de los servidores DNS.

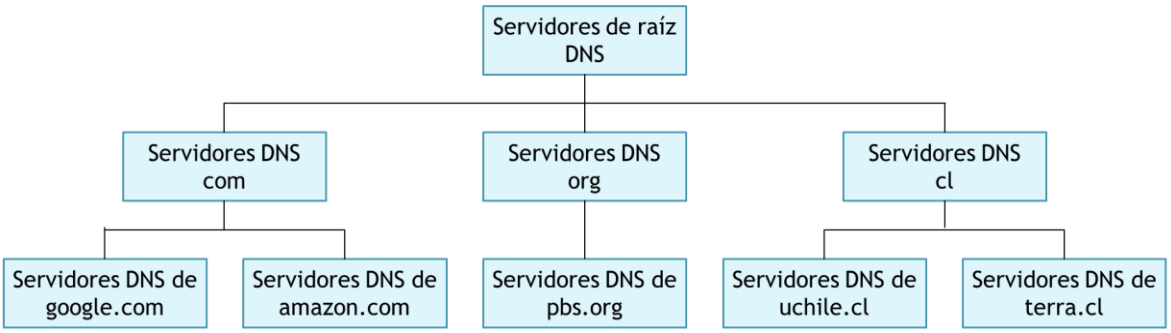

Figura 7: Jerarquía de los servidores DNS. [6]

Pero hay un tipo de servidor que no se considera en esta distribución llamados servidores locales de DNS o Resolvers. Estos servidores se encuentran en los proveedores de servicios de Internet, que en el caso de Internet móvil se encontrarían en la red del operador móvil. Cuando un dispositivo se conecta a un ISP, este proporciona al dispositivo las direcciones IP de uno o más de sus servidores locales de DNS normalmente a través del protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol).

Los dispositivos no hacen las consultas directamente a los servidores revisados anteriormente, sino que se hacen al servidor local de DNS asignado por la red. Éstos no contienen la base de datos completa, por lo tanto, cuando se les realiza una consulta, estos la reenvían a los servidores DNS correspondientes, almacenando la respuesta para futuras peticiones y ahorrar tiempo. Así, los servidores locales de DNS tienen bases de datos temporales creadas a partir de las consultas ya hechas y se completan o actualizan a medida que los usuarios navegan en la red. La forma en que se hacen las consultas se revisarán a continuación. [19]

2.2.1.1.2. Consultas DNS

Para llevar a cabo una consulta DNS, es importante señalar que el dispositivo que quiere hacer la consulta se conecta únicamente al servidor local de DNS determinado por su red. El servidor local de DNS es el encargado de reenviar la consulta del usuario a los servidores pertenecientes a la base de datos mundial y responderle.

A modo de ejemplo y simplificando el procedimiento para su mejor entendimiento, se explicará cómo se hace una consulta DNS al navegar por http://ingenieria.uchile.cl/. En primer lugar, se hace la consulta DNS cuando un programa (como un navegador) en el dispositivo de un usuario necesita conocer la dirección IP correspondiente a http://ingenieria.uchile.cl/. Entonces, se levanta un proceso en el sistema operativo del usuario, el cual pregunta al servidor local de DNS si conoce la IP asociada a ese sitio web. Si ya se navegó previamente por esta página, entonces el servidor local de DNS va a conocer la IP y va a responder inmediatamente. Pero si no se ha navegado antes por este sitio, el servidor local de DNS se encargará de preguntar a los servidores de DNS correspondientes.

El primer paso para el servidor local de DNS será preguntar al servidor de raíz de DNS más cercano la dirección IP del servidor de dominio superior ".cl". Al conocer esa IP, el servidor local pregunta al servidor de dominio superior ".cl" la dirección IP del dominio "uchile". Finalmente se consulta al

servidor del dominio "uchile" la dirección IP del subdominio "ingeniería". Al conocer por completo las direcciones IP relacionadas a http://ingenieria.uchile.cl/, el servidor local de DNS responde al usuario la dirección IP con la que se debe comunicar y se almacena esta información en caso de que se haga una futura consulta por parte de otro usuario. Este procedimiento se ilustra en la Figura 8 que está a continuación.

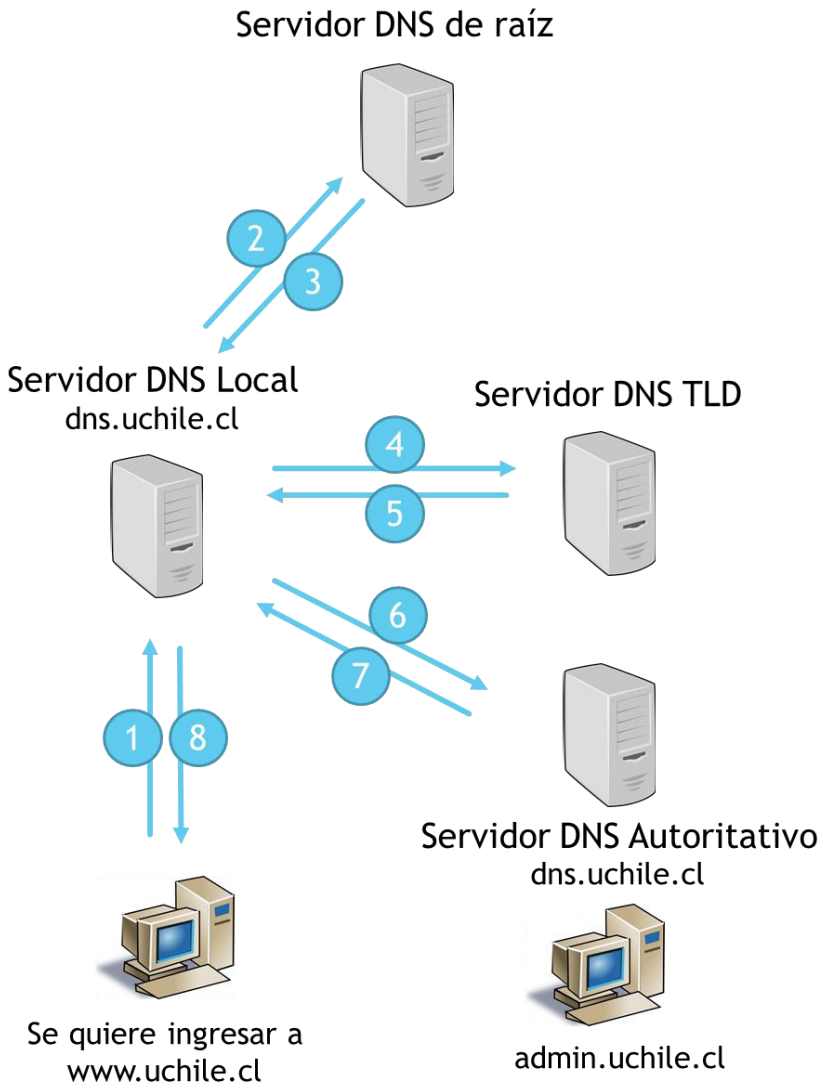

Figura 8: Interacción enumerada de los diversos servidores DNS. [7]

2.2.2. Capa de Transporte

La capa de transporte es donde se concentran la mayoría de los ataques hechos a los operadores móviles. El propósito de esta capa es proporcionar un transporte de datos confiable del dispositivo de origen al dispositivo de destino, independientemente de la red que se utilice.

Para esto, la capa de transporte provee un servicio eficiente a los procesos de la capa de aplicación. Otra manera de ver la capa de transporte es considerar que su función principal es mejorar la calidad del servicio proporcionada por la capa de Internet.

El servicio de transporte se divide en dos tipos, el orientado a conexiones y no orientado a conexiones, donde se utilizan los protocolos TCP y UDP, respectivamente. Cuando se habla de transporte orientado a la conexión significa que proporciona una garantía en el transporte de los mensajes de la capa de aplicación al destino y un mecanismo de control del flujo, es decir, adapta las velocidades de transferencia del emisor y del receptor. En cambio, el transporte no orientado a la conexión significa que no ofrece ninguna fiabilidad, ni control de flujo ni de congestión.

Hay que destacar que estos protocolos son de vital importancia para el estudio, ya que los softwares maliciosos intentan engañar por esta vía a las plataformas de cobro de los operadores móviles. Por lo tanto, se explicarán algunas de sus características en la siguiente sección.

2.2.2.1. UDP

UDP es un protocolo de transporte no orientado a la conexión. Este ofrece a las aplicaciones un mecanismo para enviar paquetes IP en bruto sin tener que establecer una conexión. Muchas aplicaciones cliente-servidor que tienen una solicitud y una respuesta usan UDP en lugar de demorarse y establecer la conexión. Como se ve en la Figura 9, UDP tiene una cabecera bastante simple. Esta cabecera es de 8 bytes y contiene los puertos de origen y destino, los cuales sirven para identificar los puntos terminales de las máquinas y determinar cuál aplicación se está comunicando. También se encuentra el campo de largo del paquete y el "*checksum*", que sirve para determinar si algún bit del paquete UDP ha sido alterado en el camino del emisor al receptor. En el lado del receptor, el protocolo UDP efectúa la revisión de este campo.

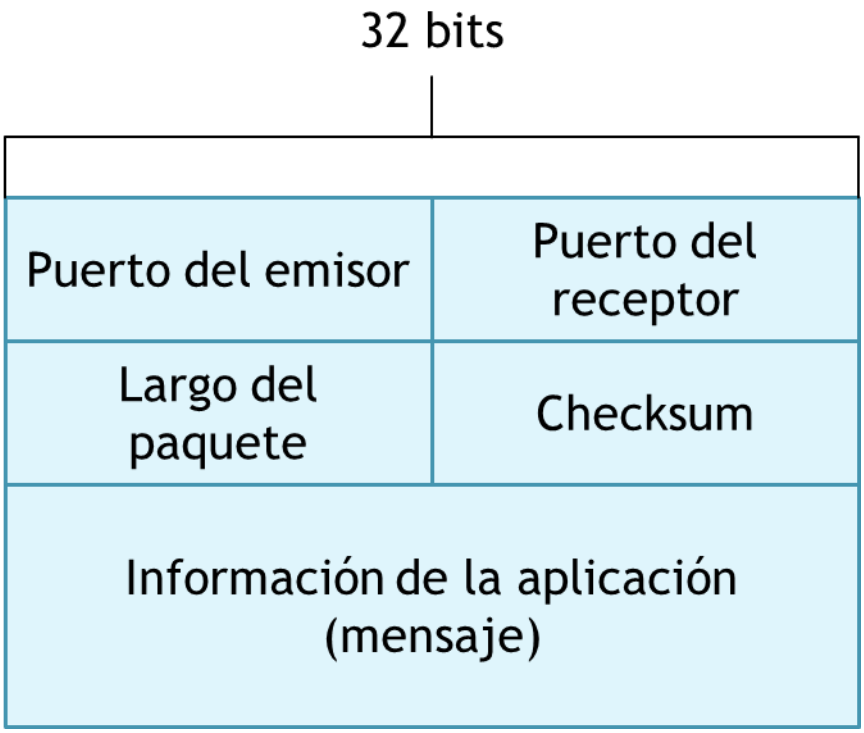

Figura 9: Estructura de un segmento UDP. [25]

Por lo tanto, la cabecera es la principal diferencia entre un paquete IP con UDP y un paquete IP solo, ya que provee los números de los puertos para ayudar a distinguir los distintos requerimientos de los usuarios y el checksum que verifica que la información llegue intacta. En algunos operadores móviles, para que funcionen ciertas aplicaciones independiente del saldo y de la cuota de navegación, se permite que algunos puertos UDP no sean tasados. De esta forma, si se modificaran todos los encabezados del tráfico por esos puertos no tasados se podría navegar gratis.

Se dice que UDP es no orientado a la conexión porque solo envía paquetes. Esto tiene beneficios, tales como un uso menor de ancho de banda y una transmisión mucho más rápida (con menor latencia) que otros protocolos. Estas características hacen que este protocolo sea uno de los preferidos para hacer fraude, ya que como se comentará en las secciones siguientes, las métodos para hacer fraude merman la conexión y es necesario utilizar un protocolo rápido.

UDP es un protocolo ideal para aplicaciones donde la latencia es crítica, como juegos o comunicaciones por voz y video, las cuales podrían sufrir cierta pérdida de paquetes sin afectar la calidad percibida por el usuario. También es ideal para aplicaciones que envían poca información pero repetidamente. Un

ejemplo de esto son las "Tablas de enrutamiento" (tablas almacenadas en los enrutadores con la información de las rutas). Como las actualizaciones se hacen periódicamente (típicamente cada 5 minutos), las actualizaciones que se pierdan son reemplazadas por las actualizaciones más recientes, haciendo que la información perdida no sea importante luego que llegó la última actualización. UDP también es utilizado para llevar información de administración de la red, como por ejemplo en el protocolo simple de administración de red (SNMP, *Simple Network Management Protocol*). UDP es preferible en este caso, ya que las aplicaciones de administración de la red deben funcionar en mayor cantidad cuando la red está saturada, precisamente cuando una conexión de difícil de conseguir. Además, como ya se mencionó, DNS también funciona sobre UDP, esto es para evitar el retraso que otros protocolos tienen al establecer la conexión con el receptor. [20]

2.2.2.2. TCP

El protocolo TCP se diseñó específicamente para proporcionar una transferencia de bytes confiable a través de una red no confiable. Además, fue diseñado para adaptarse a las propiedades de las distintas redes y para ser robusto ante muchos tipos de fallas. TCP se asegura que la información llegue sin errores, sin partes faltantes, sin duplicados y en secuencia.

El servicio TCP se obtiene haciendo que tanto el emisor como el receptor creen puntos terminales llamados sockets, donde cada socket consiste en la dirección IP del dispositivo y un puerto. A través de los sockets se establece una o varias conexiones al mismo tiempo. Todas las conexiones TCP son dúplex y punto a punto. Dúplex significa que el tráfico puede ir en ambos sentidos al mismo tiempo. Punto a punto significa que cada conexión tiene exactamente dos puntos terminales. Cada vez que se establece una conexión a través de los sockets, el emisor y el receptor deben primero hacer un "handshake" entre sí. Un "handshake" es el envío de algunos segmentos preliminares para establecer los parámetros que aseguren la transferencia de la información.

A continuación, se revisará como se hace envío de datos con TCP. Cada byte que se transfiere a través de una conexión TCP tiene su propio número de secuencia. Estos se usan para acusar recibo y para el "mecanismo de ventana de recepción". Los emisores y receptores en TCP intercambian datos en forma de segmentos, los que consisten en una cabecera TCP de 20 bytes seguida de los bytes correspondientes a los datos que se quieren transferir. El protocolo TCP decide el tamaño de los segmentos, es decir, puede enviar los datos en un solo segmento o dividir la información en muchos segmentos. Hay un límite que restringe el tamaño del segmento que se va a enviar. Cada red tiene una unidad máxima de transmisión (MTU, *Maximum Transmission Unit*),

la cual no puede ser superada. Tanto en Ethernet como en el protocolo punto a punto (PPP, *Point-to-Point Protocol*), el valor MTU estándar es de 1.500 bytes. En algunos casos, cuando un segmento es demasiado grande para transitar por una red intermedia, este puede dividirse en varios segmentos mediante un enrutador. Cada segmento nuevo recibe sus propias cabeceras TCP/IP, por lo que la fragmentación en los enrutadores aumenta la carga total.

Es necesario revisar los campos más importantes correspondientes a la cabecera TCP. Para esto, se ilustra la estructura de un segmento TCP en la Figura 10. Los campos de puerto del emisor y puerto del receptor identifican el puerto correspondiente al socket en cada uno de los dispositivos que se están comunicando. Los campos de número de secuencia y número de acknowledgement indican el número del primer byte que se envía en el actual segmento y el número del primer byte del próximo segmento que se espera recibir, respectivamente. El largo del paquete indica la longitud de la cabecera TCP. Como se mencionó anteriormente, el control de flujo en TCP se maneja usando un mecanismo de ventana de recepción de tamaño variable. El campo ventana de recepción indica la cantidad de bytes que pueden enviarse comenzando por el byte especificado en el campo número de acknowledgement. El campo checksum de Internet es una suma de comprobación de la cabecera y los datos. Este campo se revisa en cada paquete que se recibe para verificar la integridad del mismo.

También existen otros campos de menor importancia, los cuales son un sector de 6 bits que no tiene un uso en particular y seis flags que son de 1 bit cada uno. Estos flags son URG que sirve para indicar urgencia, ACK que sirve para indicar que el número de acknowlegdment es válido, PSH que indica si la información debe ser empujada inmediatamente a la aplicación, RST que indica si se debe reestablecer la conexión, SYN que sirve para establecer la conexión y FIN que sirve para finalizar una conexión.

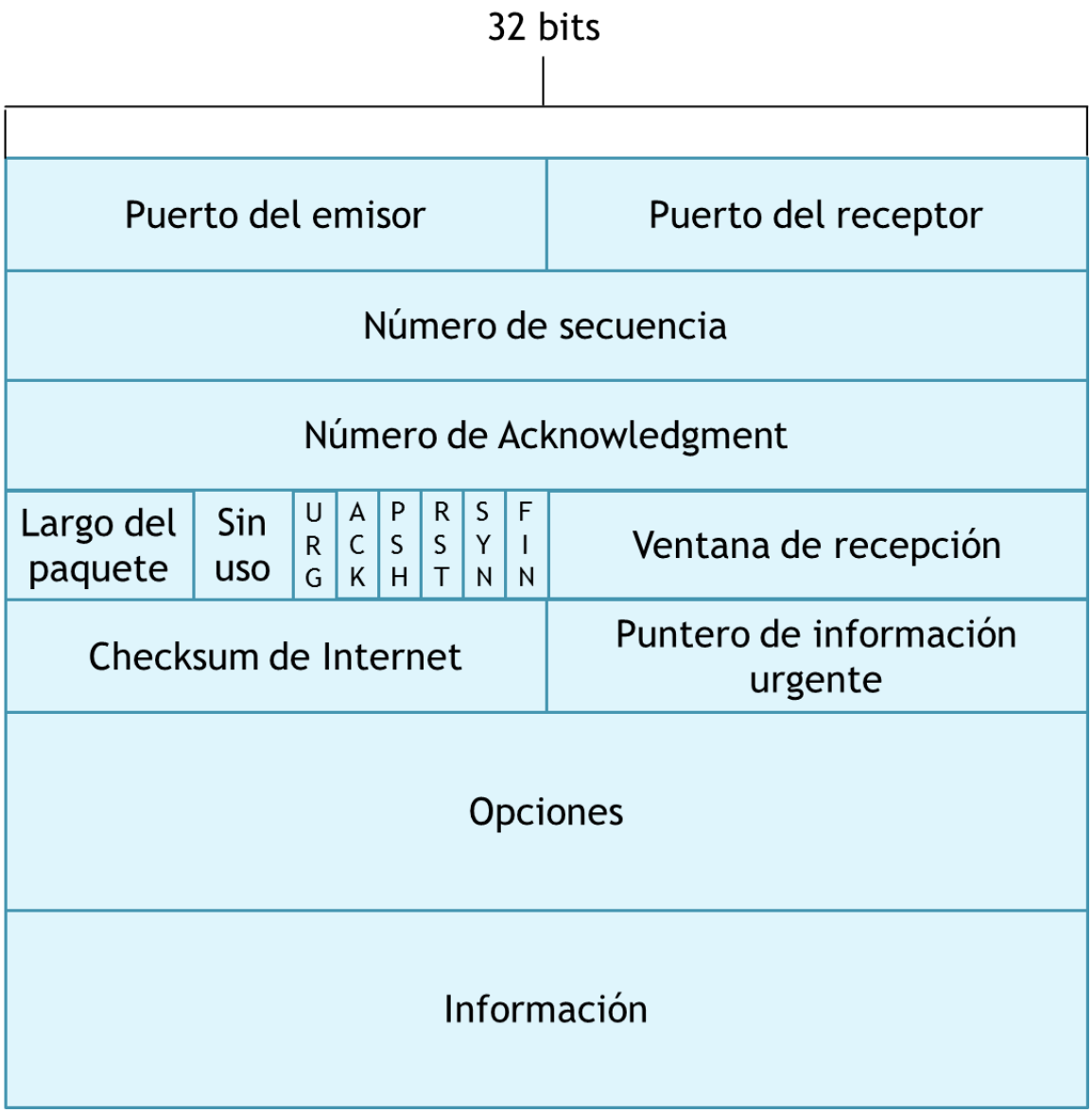

Figura 10: Estructura de un paquete TCP. [26]

En otro ámbito, el "mecanismo de ventana de recepción" es una forma de controlar el flujo a sus aplicaciones para eliminar la posibilidad de que el emisor sature al receptor. Este consiste la sincronización de la velocidad de envío de información del emisor con la velocidad de lectura de la aplicación en el receptor. Cuando un emisor envía un segmento, también inicia un temporizador. Al llegar al receptor, el protocolo TCP envía un segmento de vuelta acusando el recibo de la cantidad de bytes que le llegaron. Si el temporizador del transmisor expira antes de la recepción del acuso de recibo, el transmisor envía de nuevo un segmento, pero más corto. [21]

2.2.2.3. Comparación de Aplicaciones

Se había mencionado anteriormente que los protocolos HTTP, SMTP y FTP funcionan sobre TCP, ya que todas estas aplicaciones necesitan un servicio de transferencia confiable. Pero es importante notar que muchas aplicaciones importantes funcionan sobre UDP en vez de TCP. Para revisar esta afirmación, la Figura 11 se muestran las aplicaciones más utilizadas por los usuarios en Internet y los protocolos de transporte que ocupan. Se puede ver que tanto UDP como TCP son utilizados en aplicaciones multimedia, como telefonía por Internet (VoIP, *Voice over IP*), videoconferencias en tiempo real y streaming de audio y video. Estas aplicaciones, como son en tiempo real, toleran una baja cantidad de pérdida de paquetes y por lo mismo utilizan el protocolo UDP. Sin embargo, TCP es cada vez más usado en el transporte de datos multimedia.

Aplicación	Protocolo de la capa de aplicación	Protocolo utilizado en la capa de transporte	Puerto(s) utilizado(s)
E-Mail	SMTP	TCP	25, 587 y 465
Acceso Remoto a Terminal	Telnet	TCP	23
Web	HTTP	TCP	80
Transferencia de Archivos	FTP	TCP	20 y 21
Remote File Server	NFS	Típicamente UDP	2049
Streaming Multimedia	Depende del servicio	UDP o TCP	554 y 1755
Telefonía IP (VoIP)	Depende del servicio	UDP o TCP	4569 y 1720
Administración de red	SNMP	Típicamente UDP	161 y 162
Protocolo de Ruteo	RIP	Típicamente UDP	520
Traductor de URLs	DNS	Típicamente UDP	53

Figura 11: Tabla con aplicaciones típicas y sus respectivos protocolos. [27]

2.2.3. Capa de Internet

Cuando dos dispositivos que están conectados a redes diferentes se envían información, se necesitarán una serie de procedimientos que permitan que los datos atraviesen las distintas redes interconectadas. Ésta es la función de la capa de Internet. En otras palabras, esta capa es la encargada de trasladar la información de un dispositivo a otro a través de distintas redes. Para esto se ocupa el protocolo IP, el cual es utilizado para proveer el enrutamiento de los paquetes. Además, está implementado tanto en los dispositivos de los usuarios como en los nodos intermedios (enrutadores y switches).

2.2.3.1. Protocolo IP

Para entender el protocolo IP, es necesario saber qué es una dirección IP. Cada dispositivo y enrutador de Internet tiene una dirección IP que codifica su número de red. Esta dirección es única, por lo que es imposible encontrar dos dispositivos con la misma dirección IP.

Existen dos versiones de protocolos IP, la versión 4 (IPv4, Internet Protocol Version 4) y la versión 6 (IPv6, Internet Protocol Version 6). La versión que se ha utilizado desde que existe Internet es IPv4, pero se inventó

una nueva llamada IPv6. La razón de esto es porque eventualmente se están acabando las direcciones IPv4.

Las direcciones IPv4 son de 32 bits de longitud y están presentes en todos los encabezados de todos los paquetes que se envían en la red. En ellos, existen los campos "dirección de origen" y "dirección de destino", en donde se incluyen las direcciones IP correspondientes. El formato de cada dirección IPv4 es de la forma XXX.XXX.XXX.XXX, donde "XXX" puede ser cualquier número entre 0 y 255. Por lo tanto, el número total de direcciones IPv4 es $2^{32} = 4.294.967.296$.

Las direcciones IPv6 son de 128 bits de longitud y deberían comenzar a utilizarse luego de que las direcciones IPv4 se acaben. El formato de una dirección IPv6 es XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX donde "XXXX" es un número entre 0 y 65.535 escrito de forma hexadecimal (16 diferentes caracteres: 0-9 y a-f). Por lo tanto, el número total de direcciones IPv6 es $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$.

Por otro lado, existen otros protocolos incluidos en la capa de Internet que también son importantes. Estos protocolos corresponden a algoritmos de enrutamiento que poseen distintas redes y dependen del tamaño de dicha red. Cuando se intercambia información en una red de una organización relativamente pequeña se utilizan los protocolos de paso interiores (IGP, *Interior Gateway Protocols*). En el caso de que sea una red más grande, se utilizan los protocolos de paso exteriores (EGP, *Exterior Gateway Protocols*). [22]

2.2.3.2. ICMP

ICMP es un protocolo que sirve para informar a los dispositivos conectados a Internet sobre problemas en la comunicación. La situación más típica en donde se utiliza es cuando un paquete no puede llegar al destino. Así, se genera un mensaje ICMP que avisa al emisor lo ocurrido.

Aunque ICMP está en el mismo nivel que el protocolo IP, este utiliza a IP tal como lo hace TCP y UDP. Cuando se construye un mensaje ICMP, este se pasa al protocolo IP, el cual encapsula el mensaje con una cabecera IP, proceso que se revisará más adelante para todos los protocolos. Como los mensajes ICMP se transmiten en paquetes IP, no se garantiza su entrega.

Los mensajes ICMP tienen un tipo, un código y contienen el encabezado y los primeros 8 bytes del paquete IP que causó el error que generó el mensaje ICMP en primer lugar, de esta forma el emisor puede determinar qué paquete causó el error. Algunos tipos de ICMP se ven en la Figura 12. Hay que notar que ICMP no solo se utiliza para reportar errores.

Este protocolo es preferido por los atacantes para hacer fraude a los operadores móviles porque es imprescindible para el funcionamiento de Internet y es muy difícil de bloquear. Además es un protocolo simple y con pocos encabezados, por lo que las herramientas que se utilizan para hacer fraude demoran poco en reencapsular la información, permitiendo navegar a mayor velocidad y menor ping que con los demás protocolos.

Tipo ICMP	Código	Descripción
0	0	Respuesta a Ping
3	0	Red de destino no disponible
3	1	Host de destino no disponible
3	2	Protocolo de destino no disponible
3	3	Puerto de destino no disponible
3	6	Red de destino desconocida
3	7	Host de destino desconocida
4	0	Control de congestión
8	0	Petición de respuesta
9	0	Aviso de enrutador
10	0	Descubrimiento de enrutador
11	0	TTL expirado
12	0	Encabezado IP malo

Figura 12: Tipos de mensajes ICMP [28]

Para entender que ICMP sirve para informar varios tipos de errores, es necesario explicar algunos mensajes de la Figura anterior. Los mensajes de destino no disponible se generan cuando un enrutador no sabe cómo alcanzar el destino. El mensaje de TTL excedido se genera cuando el tiempo de vida de un paquete expira. Cuando hay un error en la cabecera IP, se genera el mensaje de encabezado IP malo. El mensaje de control de congestión puede ser enviado por un dispositivo receptor o un enrutador para solicitar al emisor que disminuya la velocidad a la cual está enviando datos. Esta se considera una forma primitiva de control de flujo comparado con el que proporciona TCP. El mensaje de respuesta a Ping proporciona un mecanismo para comprobar que la comunicación entre dos dispositivos es posible. El receptor del mensaje de Ping está obligado a responder con el mismo mensaje al emisor. Esta herramienta es comúnmente llamada “Ping”. Otra herramienta importante es

el Traceroute, el cual permite rastrear la ruta que recorre un paquete por el mundo. [22]

2.2.4. Capa de Enlace

La capa de enlace es responsable del intercambio de datos entre el sistema final y la red a la cual se está conectado. El emisor debe proporcionar a la red la dirección del destino, de tal manera que la red pueda encaminar los datos hasta el destino apropiado. El emisor puede requerir ciertos servicios, los cuales son proporcionados por esta capa. Por ejemplo, el emisor puede solicitar una determinada prioridad o necesitar la entrega fiable de información a través del enlace hasta el destino. Además de proveer distintos servicios al emisor, el trabajo de la capa de enlace es que la transferencia de un nodo a otro esté libre de errores independiente del medio de transmisión.

2.2.5. Capa Física

La capa física se encarga fundamentalmente del transporte seguro de los bits por el medio de transmisión. Para esto, debe definir cosas como el tipo de señales y valores que permite el receptor. El protocolo en particular que se use para lo que la comunicación requiera dependerá del tipo de red y de enlace que se disponga. Entre los protocolos más conocidos se encuentran Ethernet y WiFi, los cuales se utilizan para enlaces cableados y enlaces inalámbricos, respectivamente. Por ejemplo, Ethernet dispone de muchos "subprotocolos": uno para cable de cobre de par trenzado, otro para cable coaxial, otro para fibra, etc. En cada caso, la información se desplaza a través del enlace de forma diferente.

2.3. Encapsulación de Información

La encapsulación de datos es el proceso que agrega la información de los encabezados de los distintos protocolos a los datos antes de enviarlos. En casi todos los casos, los datos originales se encapsulan o envuelven en varios protocolos antes de ser transmitidos.

Cuando se envían datos en una red, estos se encapsulan con las cabeceras correspondientes a las capas superiores del modelo TCP/IP hacia las capas inferiores. Por lo tanto, el protocolo de la capa de aplicación es el que comienza el proceso incluyendo su encabezado en los datos. Luego, la capa de transporte le otorga el encabezado TCP a cada segmento recibido de la capa de aplicación. Incluso esta capa podría segmentar los datos si así lo requiere. Posteriormente, la capa de Internet implementa el protocolo IP agregando el encabezado correspondiente. Este contiene principalmente las direcciones IP del emisor y del receptor. Por último, la capa de enlace junto a la capa física incluyen su encabezado propio. Este contiene la dirección física del origen, la dirección física del destino, entre otras cosas. [18] El procedimiento recién descrito se ilustra en Figura 13 que se encuentra a continuación:

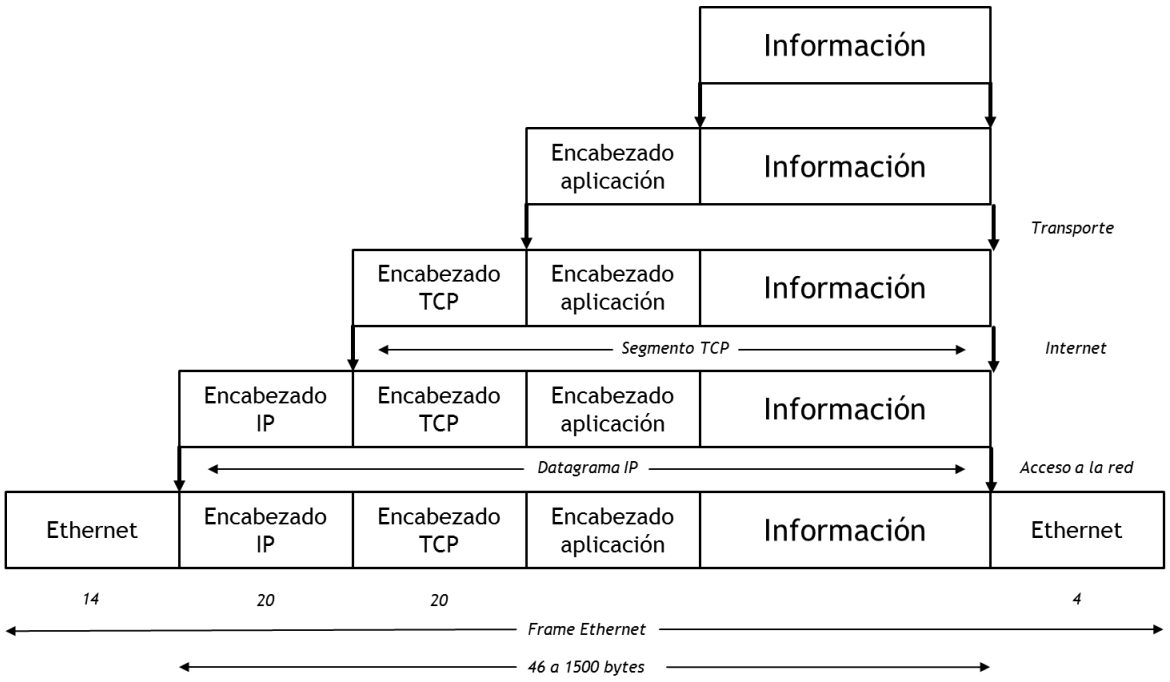

Figura 13: Diagrama de encapsulación de la información. [8]

2.4. Seguridad en las Redes

Las amenazas de seguridad de red se dividen en dos categorías: amenazas pasivas, las cuales suponen el intento de un atacante de obtener información relativa a una comunicación espiando en ella; y amenazas activas, que corresponden a modificar los datos transmitidos.

Hasta ahora la herramienta más importante para la seguridad en la red y en la comunicación es la encriptación. Con la encriptación convencional, dos dispositivos comparten una clave de encriptación y desencriptación. Esta herramienta se suele combinar en aplicaciones de red seguras y se utiliza generalmente para encriptar los datos transmitidos, sin embargo, también se utiliza para crear firmas digitales, que pueden autentificar la fuente de los mensajes transmitidos.

La seguridad de red se basa teóricamente en tres pilares fundamentales. El secreto es uno de ellos, ya que se requiere que la información que se transmite sea conocida solamente por los usuarios autorizados. La integridad de la información es otro tema importante, porque los datos que se envían o reciben deben ser leídos o modificados solamente por los que participan de la comunicación. Por último se encuentra la disponibilidad, que requiere que los datos estén disponibles únicamente a los dispositivos autorizados.

2.4.1. Ataques Pasivos

Los ataques pasivos corresponden al monitoreo de las transmisiones. El atacante pretende obtener la información que está siendo transmitida "escuchando" entre el emisor y el receptor. A esta agresión se le denomina "análisis de tráfico", la cual es bien sutil, ya que no implica la alteración de los datos, haciendo que sean muy difíciles de detectar. Así, la mejor forma de evitar estos ataques es la prevención antes que la detección.

La forma más común para prevenir el análisis de tráfico es enmascarar el contenido con la encriptación. De esta forma, el agresor podría determinar solo algunas características de los mensajes que se están enviando pero no podría saber su contenido.

2.4.2. Ataques Activos

Los ataques activos consideran la modificación de los datos que se están trasmitiendo. Entre los más comunes se encuentran el enmascaramiento, la repetición, la modificación de los mensajes y la denegación de servicio.

El enmascaramiento ocurre cuando el atacante enmascara los mensajes que desea transmitir pretendiendo engañar al receptor. Por ejemplo, este

podría enmascarar los paquetes TCP haciéndolos pasar por paquetes DNS. La principal herramienta para efectuar este ataque es el uso de aplicaciones de redes privadas virtuales (VPN, *Virtual Private Network*).

La repetición es la captura de distintos paquetes y su retransmisión constante para producir errores no esperados. Esto podría saturar fatalmente al servicio TCP, ya que existirían inconsistencias en los números de secuencia de los paquetes.

La modificación de mensajes significa alterar alguna parte de un mensaje que se está enviando para producir un efecto no autorizado. Por ejemplo, si se envía un mensaje de autorización para que un usuario acceda a cierta información, se podría modificar el nombre del usuario en el mensaje para autorizar a otro usuario.

Por último la denegación de un servicio corresponde a inhibir el funcionamiento normal de un servicio. Por ejemplo, un atacante puede perturbar una red completa, sobrecargándola con mensajes de forma que se degrade su rendimiento.

Las agresiones activas, al contrario de las agresiones pasivas, son bastante fáciles de detectar pero muy difíciles de prevenir. La detección es fácil porque es muy evidente un ataque de este tipo. Sin embargo, la prevención es complicada, ya que se requiere protección constante de toda la red.

A continuación se revisará la técnica de la encriptación, la cual se utiliza mayoritariamente para prevenir los ataques de terceros.

2.4.3. Encriptación

La encriptación, también llamada encriptación simétrica o de clave única, ha sido utilizada para las comunicaciones secretas innumerables veces en las historia por distintas culturas en todo el mundo. Por lo tanto, utilizarla como manera de prevenir ataques pareciera ser una buena idea. A continuación se encuentra una explicación breve y simple de cómo se encriptan los mensajes en Internet.

Los mensajes que se quieren encriptar son conocidos como texto normal ("*plain text*") y se transforman mediante un algoritmo de encriptación con una llave. La salida del proceso de encriptación se denomina texto encriptación ("*cipher text*"), el cual se transmite tal cual. Si un intruso intercepta la información encriptada, este no puede obtener el texto normal porque no conoce la clave de encriptación. Posteriormente, cuando el receptor esperado recibe el mensaje, este lo puede desencriptar ya que fue informado previamente de la llave. Este procedimiento se ilustra en la Figura 14.

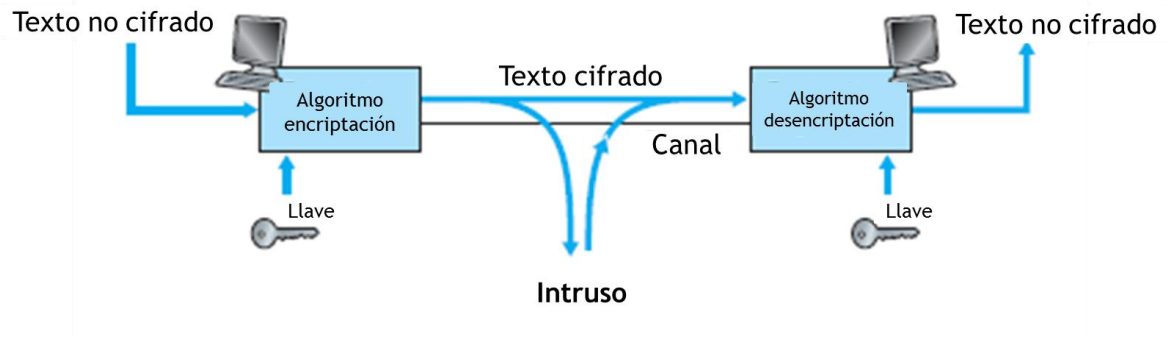

Figura 14: Elementos de Encriptación. [9]

La llave consiste en una cadena corta de caracteres que se puede cambiar con frecuencia. Esta clave es secreta y debe conocerse solo por los dispositivos involucrados en la comunicación. Sin embargo, el algoritmo de encriptación podría no ser secreto. Esto no resulta beneficioso para quienes lo utilizan, ya que al ser público puede ser vulnerado por terceros y se puede descubrir la clave. Por lo mismo, cada cierto tiempo se diseñan nuevos algoritmos de encriptación.

Por último, existe una manera de agregar una capa de seguridad extra a los algoritmos de encriptación de mensajes. Esta consiste en agregar firmas digitales, las cuales sirven para comprobar la identidad de un integrante de la comunicación. De esta forma, un receptor podría intentar verificar la identidad del emisor y fracasar, concluyendo que el mensaje que recibió podría ser falso o haber sido enviado por un tercero. [23]

2.4.4. IPsec

El protocolo de seguridad IP (IPsec, "*IP security*") permite hacer seguras las comunicaciones en una red privada o pública encriptando de una forma muy particular el tráfico IP. Su principal uso consiste en proveer conectividad segura entre dispositivos remotos a través de Internet, incluyendo autenticación de la fuente mediante firmas digitales y asegurando la integridad de los datos.

La principal característica de IPsec que le permite entregar estos servicios es que puede encriptar todo el tráfico a nivel IP, es decir, en la capa de Internet. Así, todas las aplicaciones (por ejemplo Telnet, SMTP, FTP, HTTP y muchas más), se pueden hacer seguras. De hecho, no es relevante si estas aplicaciones utilizan TCP, UDP o ICMP, ya que IPsec actúa en la capa inferior. Este servicio podría prevenir que algún intruso espíe, lo que la convierte en una de las principales herramientas para contrarrestar los ataques pasivos.

2.4.5. VPN

Las redes privadas virtuales (VPN, "*Virtual Private Network*") se desarrollaron para conectar un dispositivo en forma remota a una red local. Teóricamente, VPN permite la comunicación segura entre dos dispositivos o redes y transmite a nivel de la capa de Internet, haciendo un "túnel" seguro a través de Internet al destino planeado. La mayoría de los software de VPN incorporan métodos de encriptación estándar para enmascarar más aún los datos que se trafican.

En términos de seguridad, un intruso que quiera interceptar la información primero debe detectar por dónde está el túnel de datos y además debe descifrarla. Por lo tanto, no basta con tener la llave de encriptación para vulnerar una VPN. Pero a pesar de que el propósito de las conexiones VPN sea para aumentar la seguridad, el uso que se les da en este estudio es completamente contrario gracias a las cualidades que poseen.

El funcionamiento de una VPN se describe a continuación. Cuando se quiere transmitir información a través de una conexión VPN, esto se hace con un cliente, el cual envía los paquetes por un enlace determinado hacia un servidor. Antes de ser enviados, dicho cliente les agrega un encabezado para enrutado y encriptado, el que puede ser del tipo UDP, TCP, ICMP, SSH, FTP, HTTP, etc… Luego, cuando el servidor recibe este paquete, quita el encabezado y desencripta los datos para enviarlos al destino original. Este proceso se ilustra en la Figura 15.

A modo de ejemplo, se supone que se quiere enviar información confidencial, por lo tanto se utilizará una conexión VPN. Como se quiere ocultar el enlace por el que se transferirá, se agregará como encabezado el protocolo UDP y puerto 53. De esta manera, parecerá que son paquetes "DNS" los que viajan por la red y que la información que contienen no es importante. Este procedimiento es utilizado para vulnerar los firewall que incluyen el servicio "Deep Packet Inspection" (DPI), el cual se revisará en la sección siguiente.

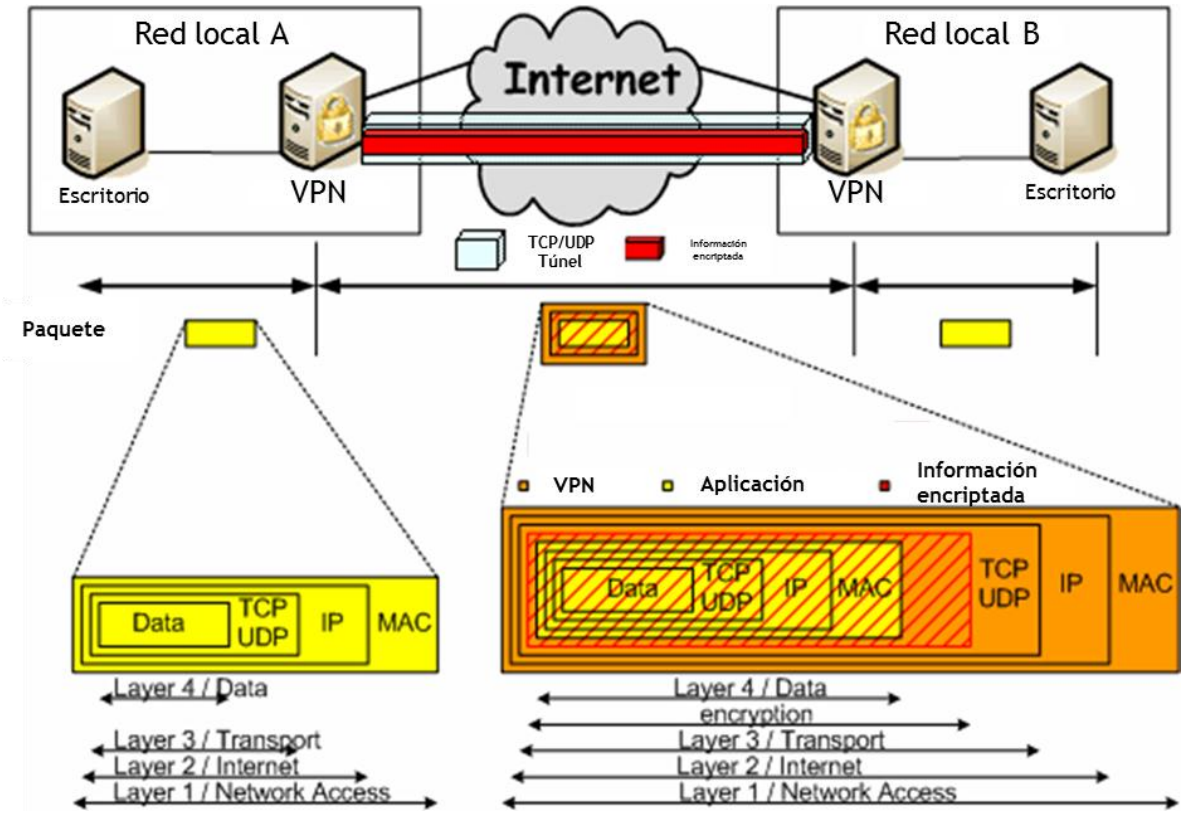

Figura 15: Esquema del funcionamiento de una VPN. Fuente: Elaboración propia.

2.4.6. Firewall

Un "Firewall" es un elemento de la red diseñado para controlar el flujo de la información que pasa por él. La revisión que este hace consiste en comparar los campos de las cabeceras de los paquetes con reglas predeterminadas por el administrador del Firewall. Estos dispositivos son realmente necesarios, porque cuando una red está conectada a Internet se vuelve visible públicamente. Estas herramientas se encuentran principalmente entre el dispositivo e Internet y permite o bloquea ciertas conexiones. Así, se torna más difícil hacer ataques a la red por parte de atacantes externos.

Existen dos tipos, por software y por hardware. Un Firewall por software es una aplicación que se instala en el dispositivo y que conoce las demás aplicaciones que se están ejecutando. Cuando es por hardware consiste en un elemento físico que se conecta entre la red e Internet, tal como se ve en la Figura 16. En ese punto, se hace una revisión a nivel de cabeceras y protocolos. A veces, es el mismo enrutador el que actúa como Firewall.

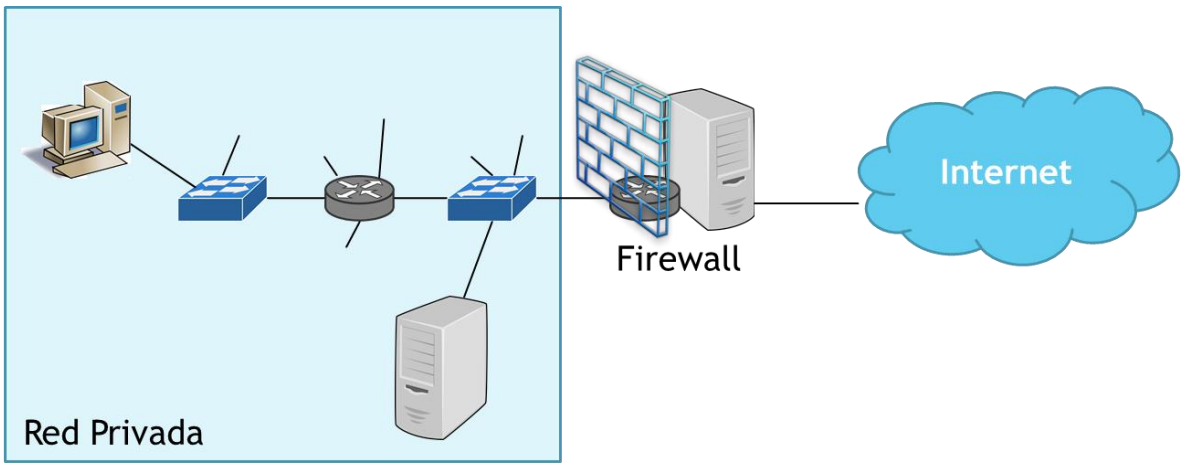

Figura 16: Firewall puesto entre la red privada e Internet. [10]

El Firewall más utilizado es el filtro de paquetes. Este funciona a nivel de la capa de transporte, de la capa de Internet y de la capa de enlace. Este tipo de Firewall permite filtrar según los encabezados del protocolo de transporte (TCP o UDP), los encabezados del protocolo IP (dirección del emisor y dirección del receptor) y la dirección física del dispositivo.

Sin embargo, un filtro de paquetes tradicional no es suficiente cuando es necesario aplicar reglas más complejas, como son las políticas de cobro en un operador móvil. Por lo tanto, en casos como estos se efectúa una "Deep Packet Inspection" o DPI, que es revisar más allá que los solo los encabezados y mirar la información que el paquete está transportando. Cuando este dispositivo observe un paquete que no cumpla con una regla establecida por el administrador, puede bloquear el acceso de esos paquetes o cobrarlos en el caso de las políticas de cobro de un operador móvil. [24]

Capítulo 3: IMPLEMENTACIÓN

El objetivo del presente capítulo es explicar cómo se efectúa el fraude en las redes de los operadores móviles y señalar las vulnerabilidades que éste explota.

3.1. Cobros de Internet en un Operador Móvil

Las redes de los operadores móviles pueden llegar a ser realmente complejas. Es necesario saber que hay muchísimos elementos de red que contribuyen a la experiencia de usuario desde el momento que se inicia la conexión de los datos, se lleva a cabo la sesión y se desconectan los datos. No es necesario conocer cada uno de los elementos para el entendimiento de este estudio, pero se revisaran los principales.

En una red 3G, como la que se ilustra en la Figura 17, uno de los elementos más importantes en el proceso de cobro y en el acceso a los datos es el GGSN. El GGSN actúa como puerta de entrada a la red pública de datos (PDN, *Public Data Network*) o más conocida como Internet. Cuando un usuario se conecta a Internet, una conexión sobre el protocolo de paquetes de datos (PDP, *Packet Data Protocol*) se establece con el GGSN. El PDP tiene una estructura tal que contiene la información del usuario, su dirección IP, la identidad internacional del suscriptor móvil (IMSI, *International Mobile Suscriber Identity*) y su MSISDN, que en otras palabras es su número de teléfono.

Posteriormente se establece un túnel entre el GGSN y el SGSN. Generalmente, el tráfico que recibe el GGSN viene encapsulado con el protocolo de túnel GPRS del usuario (GTP-U, *GPRS Tunneling Protocol - User*) desde el equipo móvil. Es importante notar que cuando se establece y termina el PDP, esto ocurre sobre otro protocolo llamado protocolo de túnel GPRS de control (GTP-C, *GPRS Tunneling Protocol - Control*). Luego, es en el mismo GGSN donde se desencapsula la información y es en enviada a Internet a través de la interfaz Gi (o Gp en el caso de roaming). En redes 4G/LTE, las tareas que lleva a cabo el GGSN son reemplazadas por el SGW y el PGW.

Actualmente existen dos tipos de cobros, cobros online o cobros offline. Las especificaciones técnicas TS32.240 del 3GPP para los cobros offline los definen como "un mecanismo donde el cobros por la información no afecta, en tiempo real, el servicio ofrecido". Por otro lado, los cobros en línea son definidos como "el cobro por la información puede afectar, en tiempo real, el

servicio ofrecido, además de requerir interacción directa con operador o servicio de control" [11]

Otro componente importante en el proceso de cobros es un nodo llamado función de políticas y de realización de cobros (PCEF, *Policy and Charging Enforcement Function*). El PCEF "aplica las políticas y reglas de cobros que recibe del sistema de cobros y/o del PCRF" [12] al tráfico del usuario. Por ejemplo, puede enviar al usuario a un portal de recargas luego de que su cuota se acabó y puede bloquear su conexión a Internet si no tiene saldo suficiente. En la realidad, las tareas que cumple el PCEF se hacen en el GGSN, en el PGW o en un filtro de paquetes DPI externo a estos elementos.

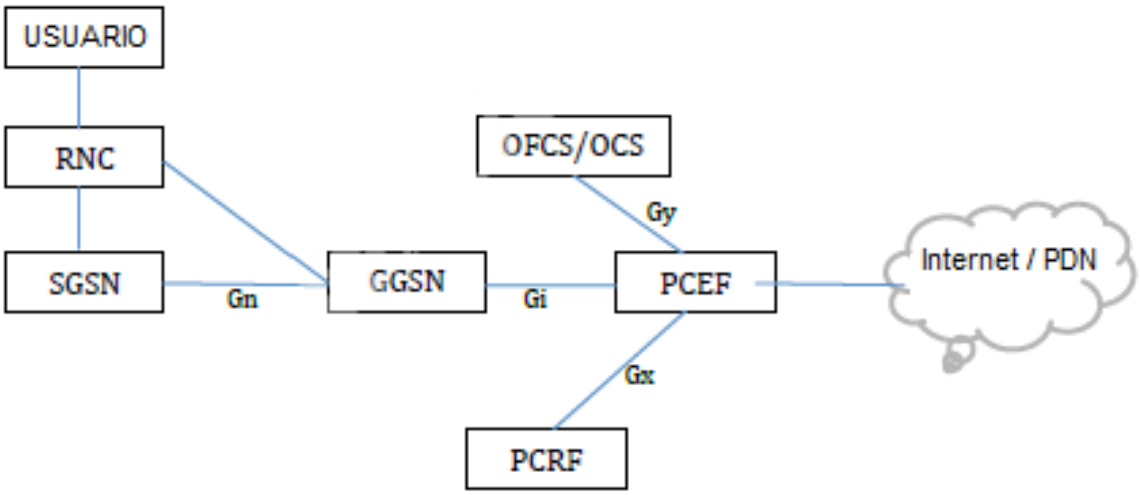

Figura 17: Esquema general Red Core 2G/3G.

La especificación técnica TS 23.002 del 3GPP identifica al PCRF como "un punto de decisión de las políticas de cobro y de control del servicio de datos. El PCRF selecciona y provee las políticas aplicables y decisiones de control de cobros al PCEF". [12]

3.2. Técnicas de Ataque a las Plataformas de Cobro de Internet

Los ataques a las plataformas de cobro se dividen en dos categorías principales: los ataques a las debilidades de las políticas de cobro y ataques por fuerza bruta.

Los ataques a las debilidades de las políticas de cobro se aprovechan de los errores de configuración del PCRF. La regla principal en este tipo de ataques es que cualquier cosa que se ofrezca gratis se puede utilizar para vulnerar el proceso de cobro. Los operadores tienden a ofrecer servicios de datos gratis debido a ofertas comerciales o por limitaciones técnicas. Por ejemplo, cuando a un usuario se le acaba la cuota de navegación de Internet, la mayoría de los operadores no permite seguir navegando, sin embargo permiten la navegación en cierto portal que sirve para recargar el saldo, comprar una "bolsa de Internet" y seguir navegando. Estos sitios web son conocidos como "páginas gratis". En este categoría se discutirán tres técnicas para evadir el cobro: La técnica de las páginas gratis, el traffic tunneling y el mal uso de proxies internos.

La segunda categoría consiste en crear errores en el sistema de cobro saturándolo con un tráfico especifico. En esta categoría se discutirán los problemas que existen con el "accounting" al producir un estado de saturación.

3.2.1. Utilizando las Páginas Gratis

¿Qué ocurre cuando a un usuario se le termina su cuota y el operador móvil necesita informarle eso? Una forma muy común es redireccionar su tráfico Web a un "portal cautivo" para informarle de su saldo y, en algunos casos, permitirle recargar saldo o comprar "bolsas" de megabytes. Pero si el usuario no tiene megabytes, ¿cómo puede acceder a este portal?

Generalmente los operadores ofrecen a sus clientes la opción de acceder gratis a un grupo de sitios web, como por ejemplo un banco para hacer recargas, redes sociales en caso de una promoción, etc… ¿Pero cómo es que un operador puede diferenciar entre los sitios que consumen su cuota y los que no?

Bueno, normalmente lo que un operador hace es que cobra "cero" por navegar en esas URL. Si un "atacante" pudiera manipular el tráfico que no va a sitios web gratis y lo disfrazara como que si va a una página gratis, entonces tendría acceso libre a Internet.

3.2.1.1. Simple Server

Cuando se hace una petición de una URL en un navegador Web, el paquete HTTP se construye con la información de la página que el usuario quiere visitar en los encabezados. Si un atacante manipula el paquete e introduce en el campo de la URL una que sea considerada gratis por el

operador, entonces podría navegar sin costo. Pero surge otro problema para el atacante, el cual es la IP de destino del paquete. Cuando un paquete llega al servidor Web con una IP de destino y una URL que no calza, este lo considera como un paquete erróneo y no le responde. Por lo tanto, ese necesario que exista un tercero o un proxy que se encargue de enviar el paquete como corresponde al servidor Web.

Simple Server es un programa gratuito que permite manipular el encabezado de los paquetes y enviarlos a un servidor proxy externo. Este servidor proxy envía y recibe correctamente la información del servidor web, para luego enviarla de vuelta al usuario con el encabezado de la página gratis. Así, se puede navegar explotando la vulnerabilidad de las paginas gratis.

Simple Server existe para dos sistemas operativos: Windows y Android. Ambas versiones son igual de configurables. A continuación se describe su funcionamiento:

En la Figura 18 se puede ver una configuración típicamente utilizada para vulnerar las paginas gratis en el operador "Operador 3". A partir de esta configuración, se explicarán los campos que la componen y que utiliza SimpleServer para conectarse:

I. Local Host: Especifica la dirección IP en la cual el programa espera recibir información.
II. Local Port: Especifica el puerto por el cual el programa espera recibir información.
III. Front Query: Sirve para agregar un string delante de la petición HTTP.
IV. Middle Query: Sirve para agregar un string en medio de la petición HTTP.
V. Back Query: Sirve para agregar un string al final de la petición HTTP.
VI. Reverse Query: Sirve para agregar un string en la respuesta a la petición HTTP.
VII. Inject Query: Se define el string que se utilizará para lo que "Inject Method" decida.
VIII. Inject Method: Define donde se modificará el paquete. Puede ser solo el encabezado "HEAD", como también la petición completa "GET".
IX. Inject Newline: Agrega, en caso de ser necesario, una nueva línea con el string que aquí se define.
X. Inject Splitline: Modifica la línea que esta entre el encabezado y la petición HTTP.
XI. Remove Port: Remueve el puerto al cual va destinada petición HTTP.
XII. Remove Path: Remueve la URL de la petición HTTP por completo.
XIII. URL Replacer: Se reemplaza toda la URL por el string definido aquí.

XIV. Request version: Dependiendo del valor definido aquí (Default, 0 o 1), el programa responderá con la información del software del cual está recibiendo la información.
XV. Advanced Mode: Define si el modo avanzado está activado o no.
XVI. Custom Header N: Define el tipo de encabezado que se agregará.
XVII. Header Value N: Se define el string que se utilizará como encabezado.
XVIII. Keep Server: Si se le pregunta a SimpleServer cual aplicación es, este responderá con este campo. Es útil en caso de existir alguna restricción a la aplicación.
XIX. HTTPS Connection: Se define si el programa permitirá conexiones HTTPS.
XX. Tunnel Proxy: Se define si el proxy se utiliza para una conexión túnel.
XXI. Server Buffer: Se establece el valor del Buffer de la aplicación.
XXII. Connection Timeout: Se establece el tiempo en segundos que la aplicación esperará por un paquete desde el servidor proxy antes de concluir que la conexión se perdió.
XXIII. Proxy Host: Especifica la dirección IP del servidor proxy que se utilizará.
XXIV. Proxy Port: Especifica el puerto del servidor proxy que se utilizara.

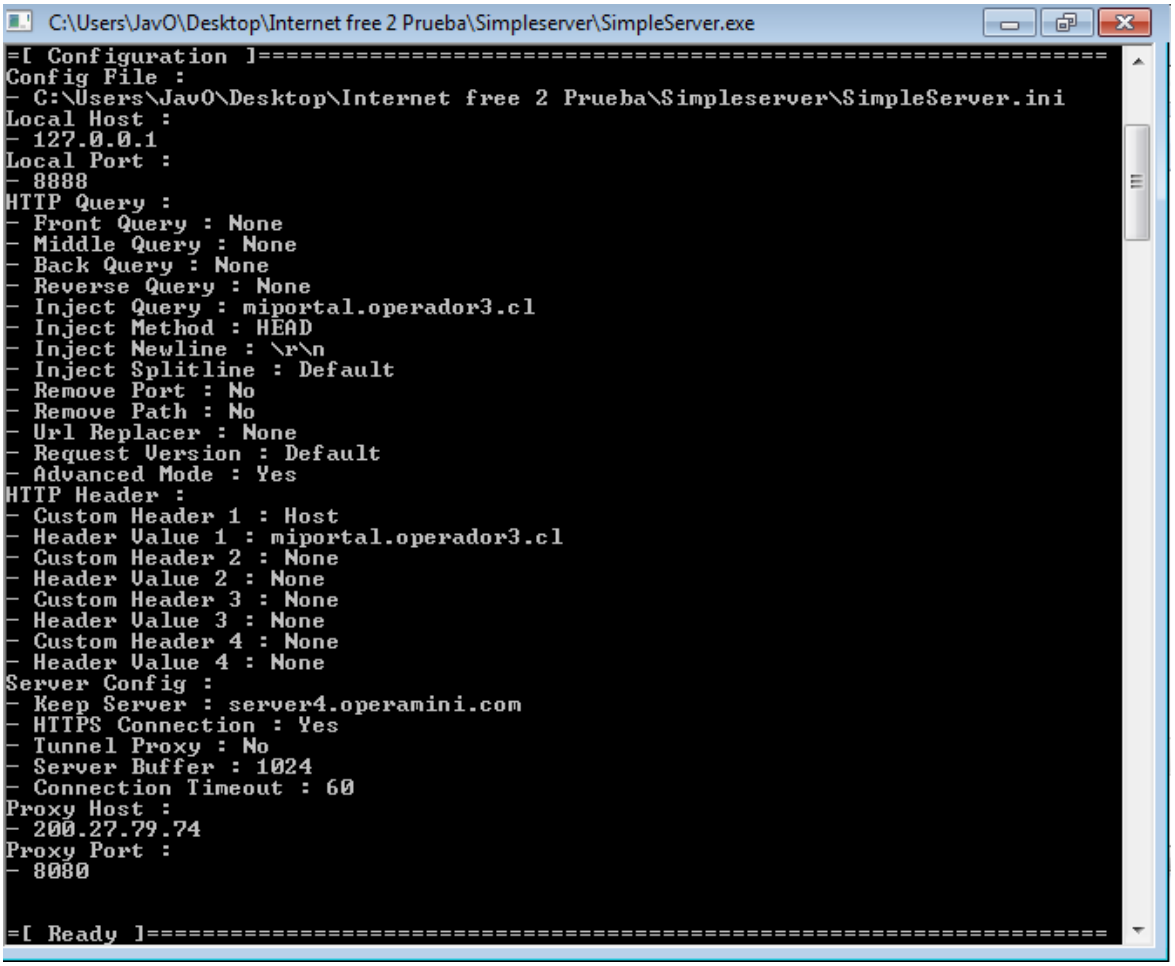

Figura 18: Configuración de Simple Server

Sabiendo qué significa cada uno de los campos, se procederá a reproducir el ataque vía paginas gratis, con el fin de navegar sin costo por Internet. La página gratis que el operador ofrece para que el usuario efectúe recargas o compre megabytes es "http://miportal.operador3.cl/". Esta página se puede ver en la Figura 19. Cuando SimpleServer indica que esta "Ready" como lo es en la parte inferior de la Figura 18, significa que está escuchando en el "Local Host" y "Local Port" definidos. Solo basta redireccionar todo el tráfico por ese "Local Host" y "Local Port" para que SimpleServer manipule la información y el fraude se realice.

Figura 19: Página gratis http://miportal.operador3.cl/.

Una forma simple de redireccionar el tráfico es mediante las opciones que entrega el navegador Web. En la Figura 20 se muestran las opciones de red que entrega un conocido navegador llamado "Firefox". La principal desventaja de hacerlo mediante el navegador es que solo el tráfico del Firefox "pasará" por SimpleServer y no el tráfico de las aplicaciones que no estén relacionadas con el navegador.

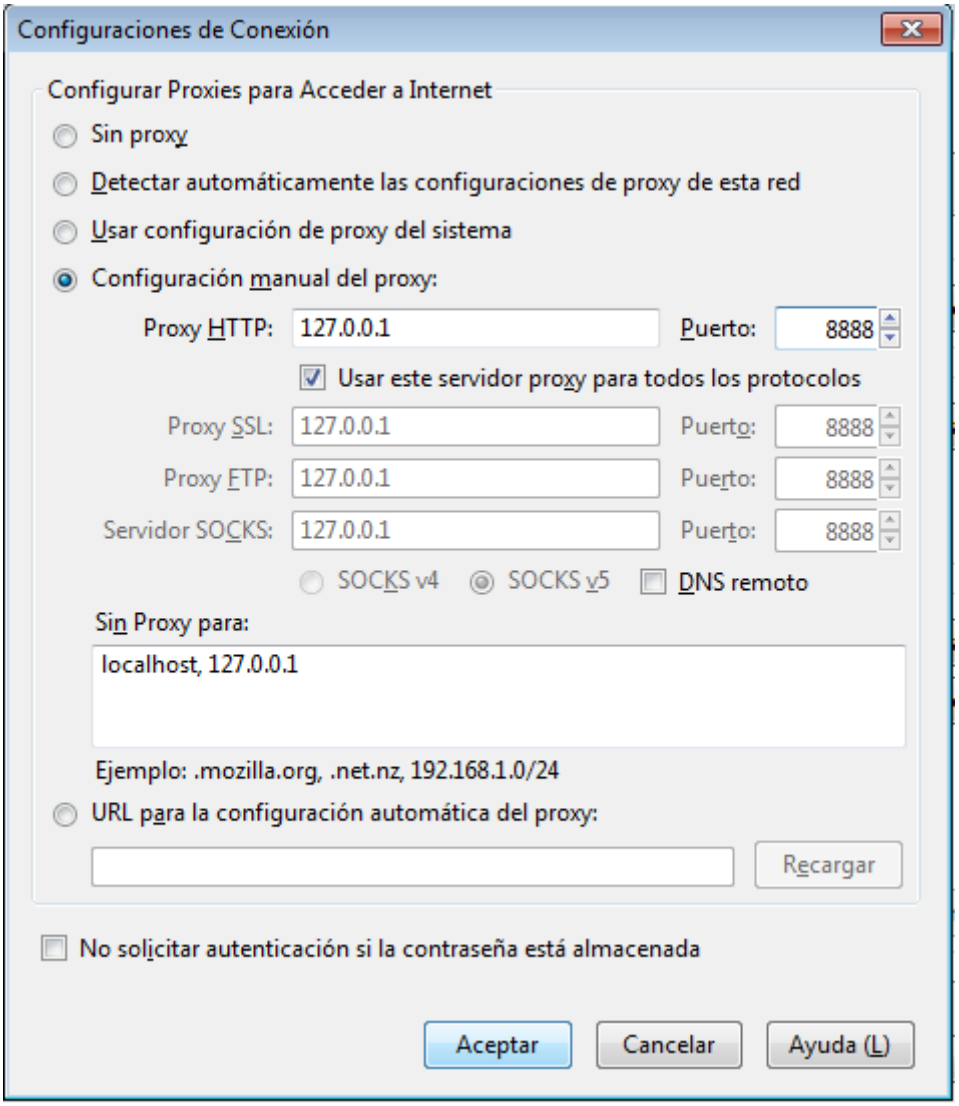

Figura 20: Opciones de red de Firefox.

Otra manera es hacerlo con un programa de VPN, el cual recibe absolutamente todo el tráfico del host y entrega la opción de redireccionarlo por donde se desee. Para esta prueba en particular se utiliza el ya mencionado OpenVPN, tal como se ve en la Figura 21.

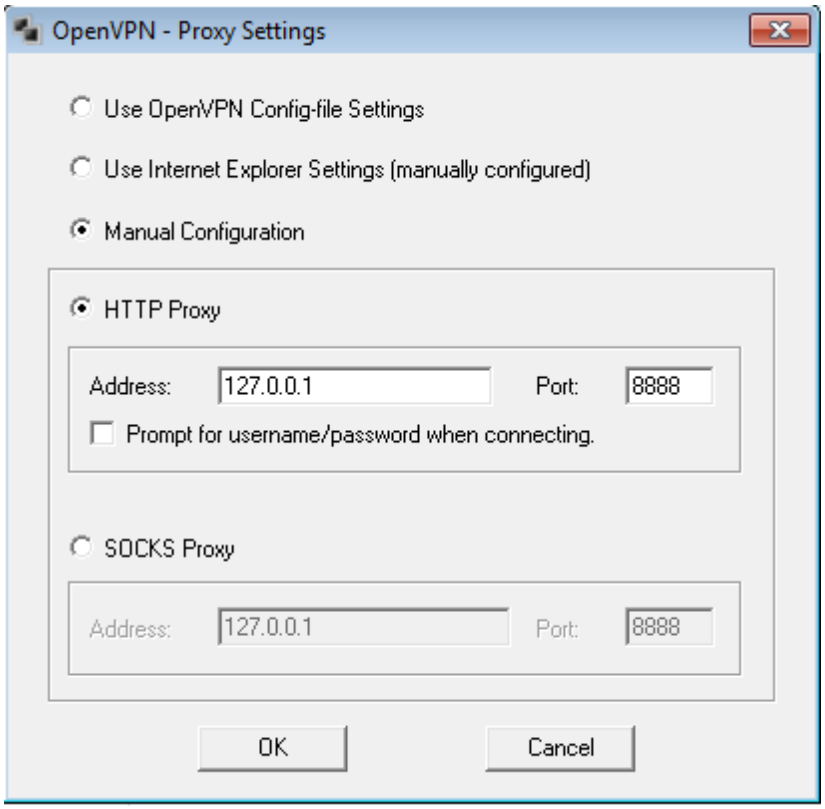

Figura 21: Opciones de Proxy de OpenVPN.

Luego de llevar a cabo estas indicaciones, se debería poder navegar sin costo. Esto se puede verificar en la consola de Simple Server, la cual muestra las conexiones que está manipulando y se puede ver en la Figura 22.

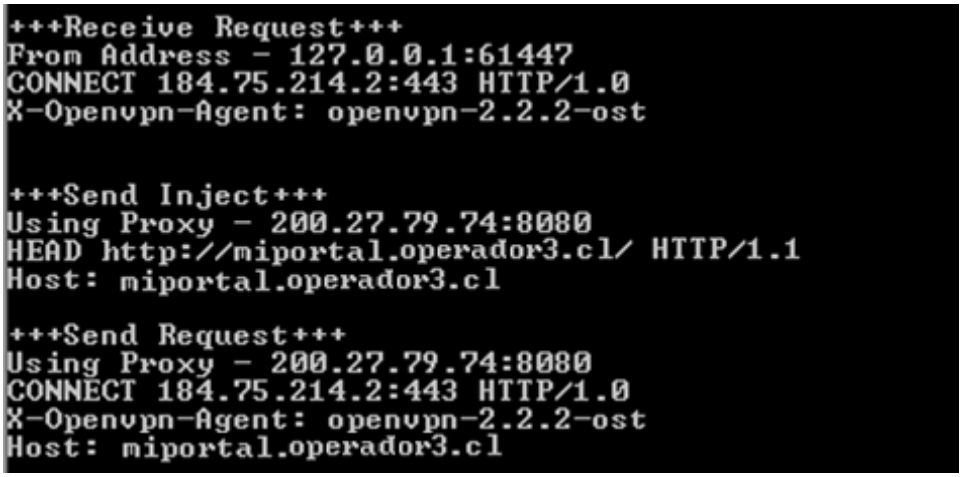

Figura 22: Consola de SimpleServer cuando se establece una conexión.

Para tener una idea más clara del funcionamiento de SimpleServer en conjunto con una conexión VPN, se incluye en la Figura 23 un esquema que ilustra de qué manera están relacionados los programas y elementos que forman parte de este fraude.

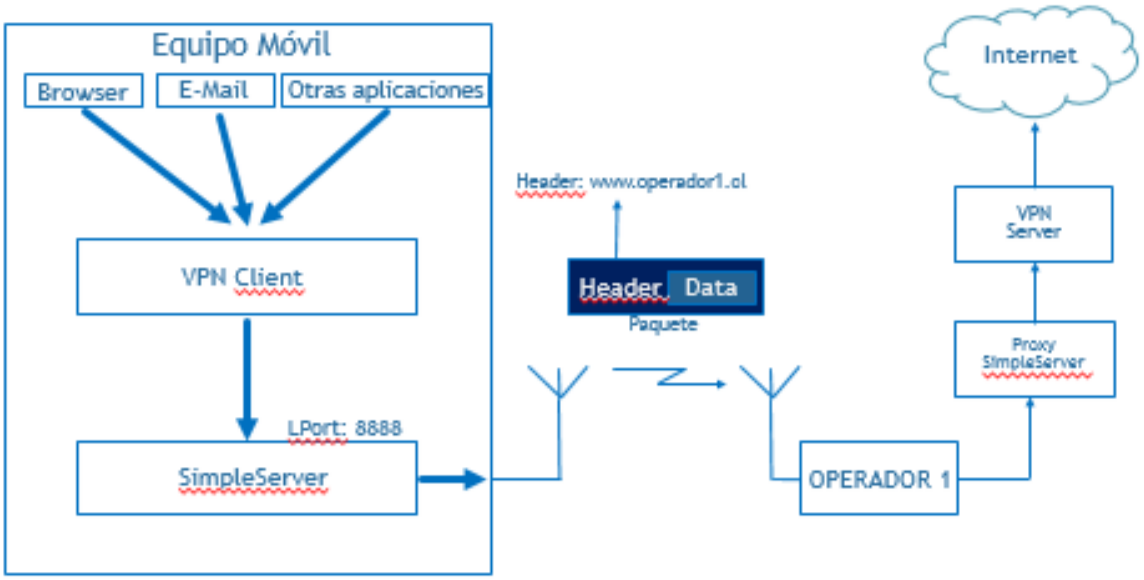

Figura 23: Esquema de funcionamiento de SimpleServer + Conexión VPN.

3.2.2. Traffic Tunneling

Un túnel de datos consiste en volver a empaquetar la información que se quiere enviar con otro protocolo y puerto. Un ejemplo de túnel es cuando se utiliza una conexión VPN, ya que se encripta la información, se empaqueta con un protocolo determinado por el usuario y se envía. Hay que notar que la encriptación de la información no es obligatoria para un túnel de datos. Este tipo de ataque se aprovecha de protocolos y puertos que están siendo cobrados a "cero", ya que corresponden a servicios que permiten el funcionamiento de Internet. Un ejemplo son las consultas DNS o mensajes ICMP, los cuales son imprescindibles para Internet. En algunos casos, el motivo de cobrar "cero" por esos protocolos es porque el volumen de tráfico es (o debería) ser tan pequeño que no "vale la pena" cobrarlo. A esto se le suma que el número de consultas DNS es tan alto, que esto podría afectar el desempeño de las plataformas de cobro. Otras veces es solo un descuido por parte de quienes configuraron y establecieron las políticas de cobro en el PCRF.

Existen muchas aplicaciones para establecer un túnel de datos en Windows, Mac OS X, Linux, iOS y Android. Las preferidas son los mismos VPNs por lo fácil que son de configurar y utilizar. Esta vez, se analizarán ataques en Android con distintos clientes VPN. Estas aplicaciones ofrecen la posibilidad de establecer una conexión VPN con sus propios servidores VPN gratis o a cambio de un pequeño pago en algunos casos. Según los desarrolladores de estas aplicaciones, el propósito de sus programas es proveer seguridad para el tráfico de datos en la red en la que el host se encuentra, sin embargo es común que se use con fines maliciosos.

3.2.2.1. DroidVPN

DroidVPN es uno de los preferidos por los usuarios porque permite conectarse sin muchas configuraciones. En particular, "DroidVPN" permite navegar 100 megabytes diarios y luego es necesario pagar para seguir navegando (o esperar 24 horas). Como se ve en la Figura 24, basta seleccionar un servidor, presionar ON y esperar a que conecte.

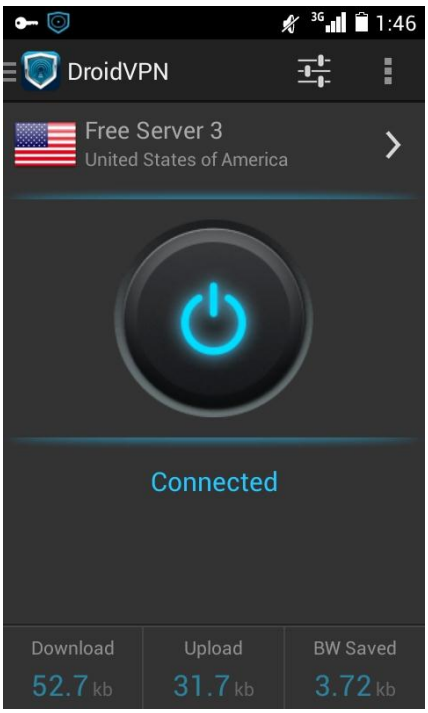

Figura 24: Menú principal de DroidVPN.

No es necesario configurarlo, ya que el mismo programa se encarga de revisar que protocolos y puertos están siendo cobrados. En la Figura 25, se puede ver a DroidVPN haciendo un escaneo de la red.

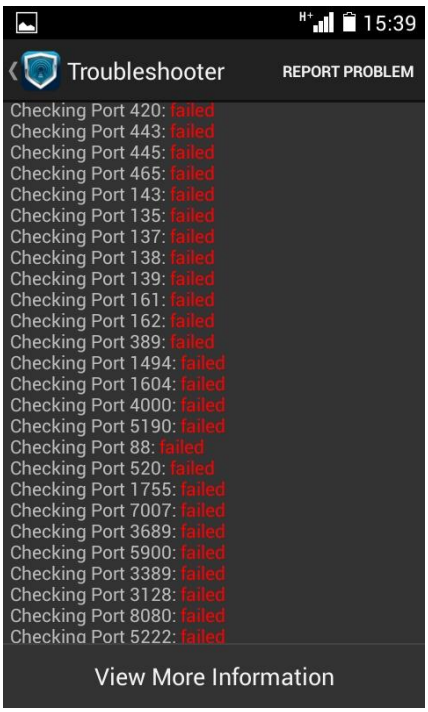

Figura 25: DroidVPN escaneando protocolos y puertos no cobrados.

Se debe mencionar que una aplicación que se configure prácticamente sola tiene pros y contras. El gran beneficio ya mencionado es que es fácil de utilizar, pero eso tiene como consecuencia que le quita libertad al usuario para modificar cosas a su elección.

3.2.2.2. YourFreedom

YourFreedom es una aplicación que cumple con el mismo propósito que DroidVPN, sin embargo es completamente distinta. YourFreedom es descrita por sus desarrolladores como "El túnel VPN todo en uno, la solución anti-censura y de anonimato". Esta aplicación, como todo cliente VPN, establece una conexión con un servidor externo (servidor de YourFreedom) y redirecciona todo el tráfico del host por ahí. Soporta el túnel de datos sobre múltiples protocolos, incluyendo HTTP, HTTPS y DNS. En la Figura 26 se ilustra un esquema que indica cómo se evade un Firewall con YourFreedom.

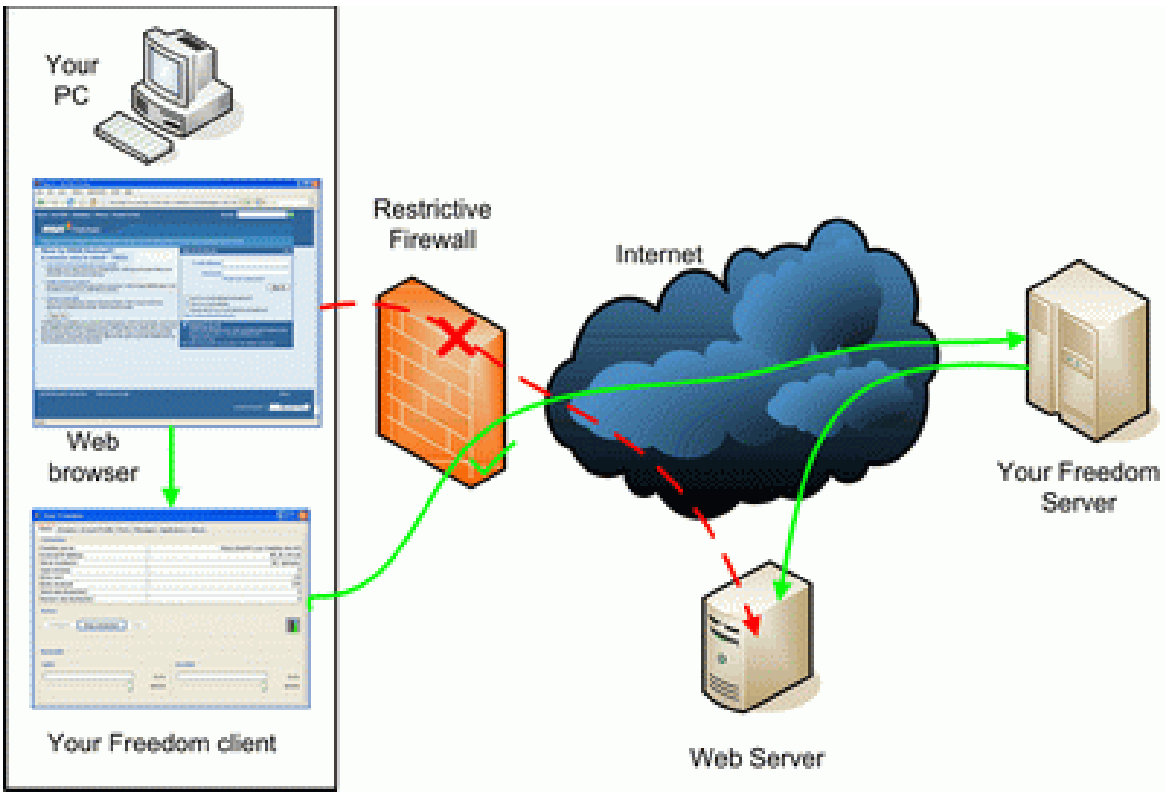

Figura 26: Funcionamiento de YourFreedom [16]

La característica más importante de YourFreedom es que permite establecer un túnel de datos sobre DNS. Los operadores móviles e incluso los hotspots de Wi-Fi de los aeropuertos descuidan el cobro de este protocolo. El único problema es que el servicio funciona gratis solo durante una hora y a una velocidad reducida. Es necesario pagar para poder usarlo ilimitadamente.

Los paquetes DNS son normalmente de pequeño tamaño, por lo tanto se tienden a excluir de los cobros. Esto se hace no cobrando todo el tráfico que pasa por el puerto UDP 53 o enrutando el tráfico hacia un servidor DNS externo antes de que pase por la plataforma PCRF.

YourFreedom se aprovecha de esto reempaquetando los datos como tráfico DNS y conectándose a sus servidores VPN a través del puerto UDP 53. Se revisa en la Figura 27 cómo la aplicación ya está conectada a un servidor en Alemania y está navegando:

Figura 27: Menú principal de YourFreedom para Android.

Además, en la Figura 27 se pueden ver otros elementos del menú principal de YourFreedom, como por ejemplo se puede revisar cuantos datos se han subido y descargado, y a la velocidad que se hace. En la Figura 28 se puede ver la configuración ya mencionada, la cual permite navegar sin costo en ciertos operadores.

Figura 28: Configuración de YourFreedom para navegar gratis sobre el protocolo DNS.

3.2.2.3. TroidVPN

TroidVPN es una aplicación de VPN que en complejidad se podría considerar como intermedia entre YourFreedom y DroidVPN. Esto es porque permite al usuario configurar ciertas cosas, pero no al nivel de YourFreedom. TroidVPN ofrece 100 megabytes diarios gratis para navegar por sus servidores y luego es necesario pagar para seguir utilizándolo.

Este cliente VPN permite hacer túnel de datos sobre UDP, TCP e ICMP. Particularmente, uno de los protocolos preferidos de los atacantes (además de DNS) es el ICMP, ya que también se suele dejar afuera de las políticas de cobro por las mismas razones que DNS. ICMP es imprescindible para Internet y TroidVPN permite utilizarlo. A diferencia de los otros protocolos, ICMP no tiene un puerto establecido, ya que consta de tipos de mensajes y el puerto es irrelevante. En la Figura 29 se ve cómo se establece un túnel de datos sobre ICMP.

Figura 29: Menú principal de TroidVPN.

En la Figura 29 también se puede ver el menú principal de TroidVPN. En este menú basta seleccionar el protocolo ICMP para utilizarlo en el túnel. Cuando se presiona "Connect", TroidVPN empaquetará todo el tráfico como si fueran mensajes ICMP e intentará conectarse con uno de sus servidores VPN externos. Si los mensajes ICMP no son cobrados por el operador móvil en cuestión, entonces se establecerá la conexión y estos llegarán al servidor externo. Este último desempaquetará el tráfico y los enviará al servidor web o a donde sea que vayan dirigidos. Al recibir la respuesta, el servidor VPN la empaquetará como ICMP y la enviará de vuelta a TroidVPN. Por último, TroidVPN la desempaquetará y permitirá al host recibir la información sin cobro alguno.

En la Figura 30 se puede ver cuando ya se estableció la conexión con el servidor externo y se ha traficado un gran cantidad de datos gratis.

Figura 30: TroidVPN conectado y navegando gratis.

3.2.3. Mal Uso de Proxies Internos

La red de un operador móvil es una red realmente compleja y normalmente ofrece múltiples servicios a los clientes. Usualmente se tienen múltiples portales para ofrecer estos servicios. Si alguno de esos servicios o servidores está mal configurado y permite el acceso a Internet, podría ser utilizado como proxy por los atacantes.

Durante el estudio se pudo confirmar que esto ocurre y se encontraron formas de navegar a través de servidores proxy mal configurados. En el "Operador 1" se podía navegar por el proxy 10.99.0.10:8080, el cual era un proxy interno y permitía el acceso libre a Internet. Sin embargo, la vulnerabilidad fue reparada en el transcurso de este trabajo. En el "Operador 2" aún se puede navegar por dos proxies internos, estos son 172.17.8.28:80 o 172.17.8.11:80.

Otro de los sistemas utilizados para este tipo de ataques es la plataforma WAP. Esta plataforma es utilizada para soportar el protocolo WAP para acceder a Internet. Funciona como proxy para aquellos usuarios que aún utilizan esta tecnología. Otro uso muy común es para el servicio de mensajería multimedia (MMS, *Multimedia Messaging Service*). La plataforma WAP también actúa como proxy para el transporte de los MMS al centro de mensajería multimedia

(MMSC, *Multimedia Messaging Center*). El tráfico MMS es enviado usualmente por otro nombre de punto de acceso (APN, *Access Point Name*) que ya viene configurado por defecto en los equipos móviles. Como el trafico MMS es pequeño, la mayoría de los operadores lo cobran por evento y no por volumen. El menú donde el usuario puede modificar el APN de su dispositivo se muestra en la Figura 31.

¿Qué ocurre si un atacante usa el APN destinado a los MMS y la plataforma WAP como proxy para salir a Internet en vez de usarlo para enviar MMS? Esto es posible, ya que la plataforma WAP tiene acceso a Internet. Y como no se mide el volumen, entonces no es fácil para el operador detectar este fraude. Durante este estudio, fue posible utilizar el APN MMS del "Operador 1" y del "Operador 2" para navegar gratuitamente por Internet. En el "Operador 1" la vulnerabilidad fue solucionada en el transcurso de este trabajo.

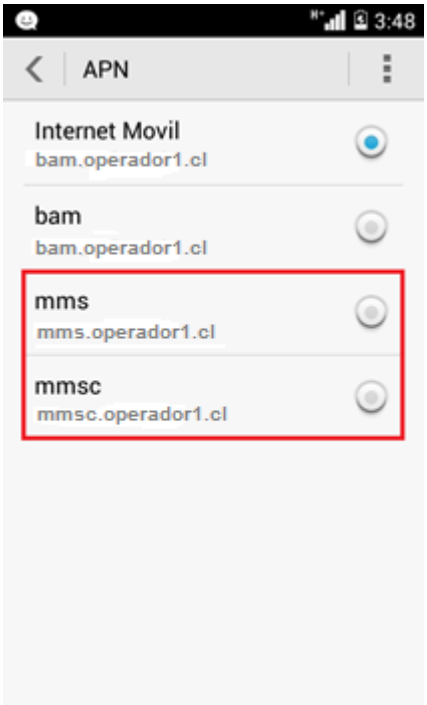

Figura 31: APN's del Operador 1.

3.2.4. Problemas de "Accounting"

Para cobrarle a un cliente es necesario que este tenga un identificador único en la red. Este identificador es normalmente el MSISDN, conocido como el número de teléfono. Cuando se activan los datos móviles, al cliente se le asigna una IP. Esta asignación es dinámica. Por lo tanto, ¿cómo puede el sistema cobrarle a un MSISDN que cambia constantemente de IP?.

Las plataformas de cobro están constantemente sincronizando la IP que le asigna el GGSN al MSISDN correspondiente. Cuando el usuario activa los datos móviles, se envía un mensaje de inicio de "accounting" al sistema de cobros, especificando que a un determinado MSISDN se le ha asignado cierta IP. De esta manera, el PCRF mantiene una base de datos con el mapeo y cobrará lo que navegue cierta IP al MSISDN especificado. Cuando el usuario se desconecta, se envía un mensaje de termino de "accounting" al sistema de cobros indicando que la IP ya no está asignada al MSISDN y que podría ser utilizado por otros clientes.

Dado lo anterior, es evidente que los mensajes de accounting son imprescindibles para el proceso de cobro de cada usuario. Si un usuario se desconecta y el mensaje no se envía, entonces ningún otro usuario podría usar esa IP. Lo que es peor, si un usuario se conecta y el mensaje no se envía, este podría navegar gratis anónimamente dependiendo de la configuración del operador móvil.

Un ataque común a este proceso es cuando un usuario se conecta y desconecta de la red constantemente, enviando una gran cantidad de mensajes de inicio y término de "accounting". Si esto se hace a una hora punta y existiera una gran cantidad de usuarios haciendo lo mismo, existe la posibilidad de que una de las veces se produzca un error y el mensaje no se envíe, permitiendo al usuario navegar libremente por Internet.

Pareciera que es necesario que muchos factores se cumplan al mismo tiempo para que este ataque sea exitoso, pero no es así. Durante este estudio se ha comprobado que es posible efectuar este ataque a cualquier hora y sin la necesidad de otros usuarios atacando al mismo tiempo al operador móvil. Dada la enorme cantidad de usuarios que tienen, hay muchas plataformas que funcionan al máximo de su capacidad. Este ataque fue realizado con éxito al operador móvil "Operador 1", sin embargo la vulnerabilidad fue solucionada en el transcurso de este trabajo. En el "Operador 2" y "Operador 3" no se suele utilizar esta vulnerabilidad por los atacantes, ya que tienen otras vulnerabilidades que son más simples de sacar provecho (como un túnel de datos).

Capítulo 4: ANÁLISIS DE RESULTADOS

En este capítulo se expondrán y discutirán los resultados obtenidos en la realización del estudio. Se revisarán dos escenarios principales: la realización de fraudes en Chile y en modalidad Roaming en el extranjero.

4.1. Revisión de Fraudes en Chile

Los distintos tipos de fraudes presentados en el capítulo anterior se realizaron (o intentaron realizar) en los operadores móviles más grandes del país. Estos son el "Operador 1", "Operador 2" y "Operador 3".

Últimamente, el tema de fraudes se ha convertido en un tópico muy importante dentro de las empresas de telecomunicaciones y, a raíz de esto, los operadores móviles han ido solucionando sus vulnerabilidades. En consecuencia, este estudio considera el escenario de fraudes hasta Abril 2015.

4.1.1. Operador 1

En el "Operador 1" se hicieron pruebas en un prepago común con saldo para hacer llamadas, con bolsa de megabytes y sin bolsa de megabytes para navegar. Es importante mencionar que el saldo es necesario para que se establezca la conexión de datos o PDP con el operador móvil. En el caso contrario, si no se tiene saldo no hay conexión de datos y como sea no se puede hacer fraude. Por otro lado, pueden existir diferencias en los resultados de las pruebas en este operador si el móvil tiene o no una bolsa de megabytes y esta fue una variable muy importante a considerar. Esto es porque el fraude igual se puede hacer con bolsa de megabytes, solo que en ese caso la cuota no disminuye. Se obtuvieron los siguientes resultados.

Operador 1		
TIPO DE FRAUDE (Vulnerabilidad Usada)		**ESTADO**
VPN + Header de página gratis		**No conecta**
VPN Tunneling	**TCP O UDP**	**Sí conecta**
	ICMP (PING)	**Con bolsa conecta**
	DNS (Domain Name Server)	**No conecta**
Mal-uso de proxies internos		**No conecta**

Figura 32: Resultados en "Operador 1".

Durante el estudio, esta tabla ha cambiado mucho. En un principio, todos los métodos para conectarse gratis servían. Esto muestra el gran interés que tiene la empresa para finalizar con los fraudes y solucionar las vulnerabilidades. De hecho, esta empresa de telecomunicaciones es considerada por los usuarios una de las menos vulnerables. Esto produjo que muchos usuarios que intentan navegar gratis en prepago hayan migrado a otras empresas mediante la portabilidad, ya que es mucho más fácil navegar sin costo.

En la actualidad, es posible conectar un túnel de datos mediante el protocolo TCP 80 y el puerto local 8090. Estos parámetros, por ejemplo, se

pueden colocar fácilmente en TroidVPN, presionar "Connect" para conectarse y navegar libremente.

La vulnerabilidad que el túnel de datos sobre el protocolo ICMP explota fue solucionada en el transcurso de este trabajo, sin embargo con bolsa todavía funciona. En otras palabras, cuando se tiene saldo y no se tiene bolsa, el túnel no se puede conectar. Esto es porque el protocolo ICMP se cobra en esa condición. Pero si se tiene saldo y sí se tiene bolsa, el sistema lo considera una situación distinta y el protocolo ICMP no se cobra. De esta manera, se puede establecer el túnel de datos y se puede evitar el consumo de la cuota de la bolsa.

Hay que notar que las bolsas tienen dos condiciones de expiración: una es la cuota de navegación y la otra es un límite temporal. Por lo tanto, si se compra una bolsa de 100 megabytes que dura 30 días, con el túnel de datos sobre ICMP se puede evitar el consumo de la cuota de navegación y se puede navegar hasta que ésta expire por tiempo.

Si un usuario común que navega en promedio 100 megabytes diarios hiciera este fraude, llegaría a navegar 3 gigabytes en lo que demora la bolsa en expirar (30 días) y solo pagaría 100 megabytes de su consumo. La bolsa con más cuota de navegación y vigencia en el "Operador 1" cuesta $3.990 pesos chilenos e incluye 250 MB y 30 días de duración. Esto significa que podría llegar a consumir doce bolsas de $3.990 y en vez de pagar $3.990 x 12 = $47.880, pagaría $3.990. En consecuencia, se perderían $43.890 pesos chilenos mensuales por usuario. Si solo 1.000 usuarios promedio navegaran de la misma forma, la empresa dejaría de ganar $43.890.000 pesos chilenos mensuales.

4.1.2. Operador 2

En el "Operador 2" se hicieron pruebas en un prepago común con saldo para hacer llamadas, con bolsa de megabytes y sin bolsa de megabytes para navegar. En este operador, al igual que en el "Operador 1", el saldo es necesario para que se establezca la conexión de datos o PDP. Por lo tanto, si no se tiene saldo no hay conexión de datos y no se puede hacer fraude. En el "Operador 2" se obtuvieron los siguientes resultados:

Operador 2		
TIPO DE FRAUDE (Vulnerabilidad Usada)		**ESTADO**
VPN + Header de página gratis		**Sí conecta**
VPN Tunneling	**TCP O UDP**	**No conecta**
	ICMP (PING)	**No conecta**
	DNS (Domain Name Server)	**No conecta**
Mal-uso de proxies internos		**Sí conecta**

Figura 33: Resultados en "Operador 2".

En el "Operador 2", es posible conectarse aprovechando la vulnerabilidad de las páginas gratis. En particular, se utiliza el programa SimpleServer y se ingresa "www.operador2.cl" en "Inject Query" y en "Header Value 0". Luego se redirecciona todo el tráfico del host hacia Simple Server con una aplicación de VPN y se puede navegar gratis.

También es posible navegar a través de los proxies destinados al servicio de MMS. Estos proxies son 172.17.8.28:80 y 172.17.8.11:80. Para navegar sin costo, se tiene que establecer una conexión VPN a un servidor externo y definir como proxy uno los dos que recién se mencionaron.

Si un usuario promedio (que consume 100 MB diarios) hiciera fraude durante un mes, llegaría a utilizar 3 GB. En este operador, la bolsa de navegación con más cuota cuesta $7.490 pesos chilenos e incluye 1 GB. Por lo tanto, dejaría de pagar $7.490 x 3 = $22.470 pesos chilenos mensuales.

4.1.3. Operador 3

En el "Operador 3" se hicieron pruebas en un prepago común con saldo para hacer llamadas, con bolsa de megabytes y sin bolsa de megabytes para navegar. En este operador, al igual que en los anteriores, el saldo es necesario para que se establezca la conexión de datos o PDP. Por lo tanto, si no se tiene saldo no hay conexión de datos y no se puede hacer fraude. En este operador, a diferencia de los anteriores, se ofrece unas bolsas llamadas "redes sociales gratis", las cuales permiten utilizar Facebook, Whatsapp y Twitter sin costo. No se ha podido demostrar que esta oferta comercial agrega nuevas vulnerabilidades a la red, porque se ha intentado conectar túneles VPN sobre los protocolos que utilizan estas aplicaciones sin éxito. En el "Operador 3" se obtuvieron los siguientes resultados:

Operador 3		
TIPO DE FRAUDE (Vulnerabilidad Usada)		**ESTADO**
VPN + Header de página gratis		**Sí conecta**
VPN Tunneling	**TCP O UDP**	**Sí conecta**
	ICMP (PING)	**No conecta**
	DNS (Domain Name Server)	**No conecta**
Mal-uso de proxies internos		**No conecta**

Figura 34: Resultados en "Operador 3".

En el "Operador 3" se puede navegar aprovechando las páginas gratis y con un túnel de datos sobre TCP.

Para aprovecharse de las paginas gratis se debe utilizar "miportal.operador3.cl" en los campos "Inject Query" y "Header Value 0" de Simple Server. Luego, se debe redireccionar toda el tráfico del host a Simple Server con un programa VPN y se tiene Internet gratis.

La configuración del túnel de datos es protocolo TCP con puerto remoto 443 y puerto local 1024 y también protocolo TCP con puerto remoto 80 y puerto local 9090. Estas configuraciones pueden ingresarse fácilmente en los

campos de TroidVPN. Luego, al presionar "Connect", el túnel de datos establece la conexión y se puede navegar sin costo.

Si se analizan las pérdidas tal como en los operadores anteriores, la bolsa de navegación con más cuota cuesta $7.500 pesos chilenos e incluye 1 GB. Por lo tanto, si un usuario promedio hiciera fraude durante un mes, dejaría de pagar $7.500 x 3 = $22.500 pesos chilenos mensuales.

4.2. Revisión de Fraudes en el Extranjero (Roaming)

Los fraudes presentados en el capítulo anterior se probaron en los operadores móviles más grandes del país estando en el extranjero, es decir, en modo roaming. Estos son "Operador 1", "Operador 2" y "Operador 3".

El estar en modo roaming significa una condición distinta para el sistema de cobro y de navegación, por lo tanto los resultados pueden llegar a ser completamente distintos. Además, hacer fraude en el extranjero significa una pérdida aún mayor para los operadores móviles.

Hay que tener claro que las vulnerabilidades que se explotan dependen del operador que hace el cobro y no del operador del país extranjero. Por ejemplo, si se lleva una SIM Card Prepago del "Operador 1" a un país extranjero y allá se conecta a un "Operador Extranjero" en modo roaming, las vulnerabilidades que se pueden explotar dependen de "Operador 1" y no del "Operador Extranjero".

4.2.1. Operador 1

En el "Operador 1" se hicieron pruebas en modo roaming en un prepago común con saldo para hacer llamadas, con bolsa de megabytes y sin bolsa de megabytes para navegar. Al igual que cuando se está en Chile, el saldo es necesario para que se establezca la conexión de datos o PDP con el operador móvil. Sin embargo, no es relevante tener la bolsa de megabytes, ya que al navegar disminuye el saldo y no la bolsa. En el extranjero se obtuvieron los siguientes resultados.

Operador 1 (R)		
TIPO DE FRAUDE (Vulnerabilidad Usada)		**ESTADO**
VPN + Header de página gratis		**No conecta**
VPN Tunneling	**TCP O UDP**	**No conecta**
	ICMP (PING)	**No conecta**
	DNS (Domain Name Server)	**Sí conecta**
Mal-uso de proxies internos		**No conecta**

Figura 35: Resultados en "Operador 1" en Modo Roaming.

El túnel de datos sobre el protocolo DNS se puede utilizar para navegar sin costo. Con el programa YourFreedom y la configuración que se proporciona en el capítulo anterior se puede establecer una conexión VPN sin problemas.

En este operador se sabe que cada megabyte en modo roaming cuesta $6.500 pesos chilenos, los cuales se descuentan del saldo al navegar. Si solo un usuario traficara 100 MB con fraude en modo roaming, dejaría de pagar $650.000 pesos chilenos.

4.2.2. Operador 2

En el "Operador 2" se hicieron pruebas en roaming con un prepago común con saldo para hacer llamadas, con bolsa de megabytes y sin bolsa de

megabytes para navegar. En este operador, al igual que en el "Operador 1" en modo roaming, el saldo es necesario para que se establezca la conexión de datos o PDP. Además, también es irrelevante tener una bolsa de megabytes, ya que al navegar disminuye el saldo y no la cuota de la bolsa. En el "Operador 2" se obtuvieron los siguientes resultados:

Operador 2 (R)		
TIPO DE FRAUDE (Vulnerabilidad Usada)		**ESTADO**
VPN + Header de página gratis		**Sí conecta**
VPN Tunneling	**TCP O UDP**	**No conecta**
	ICMP (PING)	**No conecta**
	DNS (Domain Name Server)	**Sí conecta**
Mal-uso de proxies internos		**No conecta**

Figura 36: Resultados en "Operador 2" en Modo Roaming.

En el "Operador 2", al igual que estando en Chile, es posible conectarse aprovechando la vulnerabilidad de las páginas gratis. En particular, se utiliza el programa Simple Server y se ingresa "www.operador2.cl" en "Inject Query"

y en "Header Value 0". Luego se redirecciona todo el tráfico del host hacia Simple Server con una aplicación de VPN y se puede navegar gratis.

También es posible navegar a través de un túnel de datos sobre el protocolo DNS. Con el programa YourFreedom y la configuración que se proporciona en el capítulo anterior se puede establecer una conexión VPN sin problemas.

En el "Operador 2" se sabe que cada MB en modo roaming cuesta $4 USD. Si nuevamente se considera a un usuario que trafica 100 MB con fraude en modo roaming, las pérdidas alcanzarían los $400 USD, lo cual equivale a $250.632 pesos chilenos ($1 USD = $626,58 pesos chilenos con fecha 01-04-2015).

4.2.3. Operador 3

En el "Operador 3" se hicieron pruebas en modo roaming en un prepago común con saldo para hacer llamadas, con bolsa de megabytes y sin bolsa de megabytes para navegar. En este operador, al igual que en los anteriores en modo roaming, el saldo es necesario para que se establezca la conexión de datos o PDP. Tal como en "Operador 1" y "Operador 2", es irrelevante tener una bolsa de megabytes, ya que al navegar disminuye el saldo y no la cuota de la bolsa. La bolsa de redes sociales también es irrelevante, ya que la oferta comercial no se aplica en el extranjero. En el "Operador 3" en modo roaming se obtuvieron los siguientes resultados:

Operador 3 (R)		
TIPO DE FRAUDE (Vulnerabilidad Usada)		**ESTADO**
VPN + Header de página gratis		**Sí conecta**
VPN Tunneling	**TCP O UDP**	**No conecta**
	ICMP (PING)	**No conecta**
	DNS (Domain Name Server)	**Sí conecta**
Mal-uso de proxies internos		**No conecta**

Figura 37: Resultados en "Operador 3" en Modo Roaming.

En el "Operador 3" en modo roaming se pueden explotar las mismas vulnerabilidades que en el "Operador 2" en modo roaming.

En el "Operador 3" es posible conectarse en modo roaming a través de las páginas gratis. Se debe utilizar el programa Simple Server e ingresar "miportal.operador3.cl" en "Inject Query" y en "Header Value 0". Luego, se debe redireccionar todo el tráfico del host a Simple Server con cualquier cliente VPN y se podrá navegar sin costo.

También es posible navegar en modo roaming con un túnel de datos sobre el protocolo DNS. Con YourFreedom y la configuración que se muestra

en el capítulo anterior se puede establecer una conexión VPN para navegar gratis.

En este operador, el MB en modo roaming cuesta $2.000 pesos chilenos. Si nuevamente se supone a un usuario que navega 100 MB con fraude, las perdidas alcanzarían los $200.000 pesos chilenos.

4.3. Velocidad y Estabilidad de los Fraudes

Sobre la velocidad y estabilidad de los fraudes se puede señalar lo siguiente:

I. La navegación a través de las paginas gratis es sumamente estable. La velocidad que se alcanza es cercana a 2 Mbps de descarga y 0,5 Mbps de subida. El ping es cercano a 500 ms.
II. La navegación por un túnel de datos TCP es estable. La velocidad que alcanza es aproximadamente 1 Mbps de descarga y 0,4 Mbps de subida. El ping es cercano a 500 ms.
III. La navegación por un túnel de datos UDP es relativamente inestable. Suele desconectarse cada cierto periodo de tiempo. La velocidad que alcanza es aproximadamente 1,8 Mbps de descarga y 0,5 Mbps de subida. El ping es cercano a 500 ms.
IV. La navegación por un túnel de datos ICMP es estable. La velocidad que alcanza es cercana a 2 Mbps de descarga y 0,5 Mbps de subida. El ping es cercano a 600 ms.
V. La navegación por un túnel de datos DNS es muy inestable. La velocidad máxima que se alcanza es 0,05 Mbps de descarga y 0,01 Mbps de subida. El ping es cercano a 800 ms.
VI. La navegación a través de un proxy interno de la red es muy estable. La velocidad que se alcanza es cercana a 2 Mbps de descarga y 1 Mbps de subida. El ping es cercano a 400 ms.

Método	Velocidad de Subida	Velocidad de Bajada	Ping	Comentarios
Páginas Gratis	1,8 – 2,0 Mbps	0,4 – 0,5 Mbps	~ 500 ms	Estable y rápido.
TCP	1 Mbps	0,4 Mbps	~ 500 ms	Estable.
UDP	1,5 – 1,8 Mbps	0,4 – 0,5 Mbps	~ 500 ms	Inestable.
ICMP	1,8 – 2,0 Mbps	0,4 – 0,5 Mbps	~ 600 ms	Estable y rápido.
DNS	0,01 Mbps - 0,05 Mbps	0,01 Mbps	~ 800 ms	Muy inestable y lento.
Proxy Interno	1,8 – 2,0 Mbps	0,9 – 1 Mbps	~ 400 ms	Muy estable y rapido.

Figura 38: Tabla resumen del rendimiento de los distintos fraudes.

La pruebas de velocidad y ping se realizaron con la aplicación "Speedtest" de "Ookla" como se ejemplifica en la Figura 39. En ella se puede ver uno de todos los test de velocidad que se realizaron para los distintos fraudes.

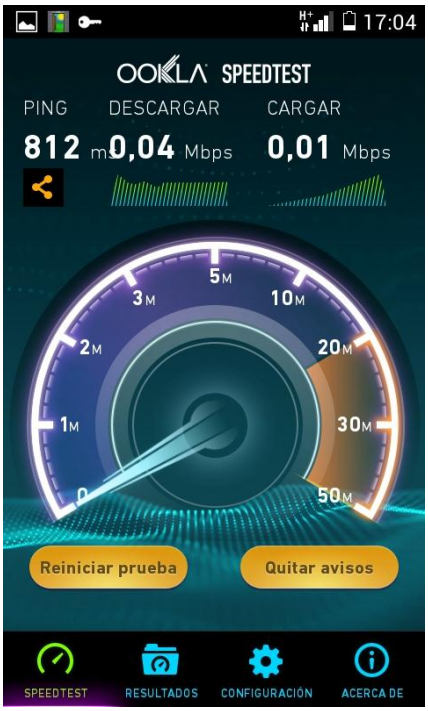

Figura 39: Test de velocidad para un túnel de datos DNS.

Capítulo 5: CONCLUSIONES

En el presente trabajo de título se han discutido las distintas formas de fraudes que hacen los usuarios en el servicio móvil de Internet y sus respectivos rendimientos.

Quedó demostrado que para todas las redes de los operadores aquí estudiados existe al menos una forma de navegar de forma fraudulenta, sin costo y sin mucho esfuerzo. Las velocidades y estabilidad para algunos métodos son suficientes como para preferir conectarse mediante fraude, en vez de gastar saldo en una bolsa de navegación. Esto convierte al fraude en una opción viable para un usuario promedio. A eso se le suma la rapidez con la que se propaga la información y la impunidad por hacer este tipo de acciones, haciendo tentadora la oferta de navegar gratis a una velocidad parecida a la que se navega pagando. Por lo tanto, para los operadores móviles es un tema que inminentemente tendrán que enfrentar.

Por otra parte, los ingresos que dejan de recibir los operadores móviles son millonarios. Sin incluir el tráfico de roaming, el "Operador 1" perdería $43.890 pesos chilenos mensuales aproximadamente por usuario promedio, el "Operador 2" perdería $22.480 pesos chilenos mensuales aproximadamente por usuario promedio y el "Operador 3" perdería $22.500 pesos chilenos mensuales aproximadamente por usuario promedio. Si tan solo 1.000 usuarios decidieran hacer fraude, las perdidas serían enormes. Pero se sabe que si está información se difunde serían mucho más de 1.000 usuarios los que empezarían a navegar con fraude. En ese caso, el impacto sería catastrófico. Es importante señalar que las consecuencias económicas son distintas para cada operador debido al valor del MB. Por ejemplo, es mucho peor que los usuarios exploten una vulnerabilidad en el "Operador 1", ya que el MB es más caro que en los demás operadores.

El panorama se ve mucho más complicado si se incluye el fraude en modo roaming en la ecuación. Cuando un prepago está en el extranjero, cada megabyte que usa se le descuenta del saldo a precios altísimos. Si bien el modo roaming es una condición que rara vez es utilizada por los usuarios, las pérdidas que se generan al hacer fraude con roaming en un solo día equivalen a las pérdidas que produce un usuario en todo un año sin roaming. Por lo tanto, es mucho más preocupante el panorama en esta modalidad. Además, si se compara el costo del MB de los tres operadores estudiados, se concluye nuevamente que hace más daño explotar una vulnerabilidad en el "Operador 1" que en los demás operadores.

En otro ámbito, los fraudes son una externalidad negativa importante para los demás usuarios, ya que quienes hacen fraude abusan de la navegación gratuita y eso repercute en la calidad de servicio y de experiencia de la red. Quienes navegan con herramientas fraudulentas generalmente navegan muchos GB por no tener límites, lo cual satura el acceso a la red y otras plataformas internas. Otra consecuencia de la navegación desmesurada por parte de estos individuos son los errores que se podrían cometer al calcular cuánto se debe invertir en capacidad de red para periodos siguientes. En otras palabras, se producen graves errores al hacer una planificación de la red.

En conclusión, este es un tema que no puede ignorarse bajo ninguna circunstancia y los operadores móviles lo tienen claro. En un futuro no muy lejano, la gran fuente de ingresos provendrá de servicio de datos móviles y no del servicio de voz, por lo cual se tiene que atacar este problema lo antes posible. El caso del "Operador 1" llama la atención, ya que las vulnerabilidades son muy dinámicas. Luego de aproximadamente dos semanas después de que se viraliza un método para hacer fraude, este es solucionado. El caso contrario es el "Operador 2", que mantiene las mismas vulnerabilidades por meses.

Por último, estudios como el que se desarrolla en estas páginas son sumamente importantes, ya que identifican donde están los problemas en cada operador. De esta forma, se pueden tomar decisiones y llevar a cabo trabajos que permitan ir solucionando las vulnerabilidades más costosas (como el roaming por ejemplo). Además, en este estudio no solo se entrega información de los protocolos con fallas, sino que se entrega también información de las aplicaciones y sus respectivas configuraciones. Eso permite la reproducción de los fraudes por parte de los operadores, para así poder estudiarlos más a fondo con herramientas como el traceroute.

Glosario

- APN: *Access Point Name / Nombre de punto de acceso.*
- Authoritative DNS Server: *Servidores DNS autoritativos*.
- BS: *Base Station / Estación base*.
- CA: *Certificate Authority*.
- CN: *Core Network / Red core.*
- DHCP: *Dynamic Host Configuration Protocol / Protocolo de configuración dinámica de host.*
- DNS: *Domain Name System / Sistema de nombres de dominio.*
- DOCSIS Protocol: *Data Over Cable Service Interface Specification Protocol / Protocolo de especificación de interfaz para servicios de datos por cable.*
- DoS: *Denial of Service attack / Ataques de denegación del servicio.*
- DPI: *Deep Packet Inspection / Inspección profunda de paquetes.*
- EDGE: *Enhanced Data Rates for GSM Evolution / Tasa de datos mejoradas para la evolución de GSM.*
- EGP: *Exterior Gateway Protocols / Protocolos de paso exteriores*.
- FTP: *File Transfer Protocol / Protocolo de transferencia de archivos.*
- GGSN: *Gateway GPRS Support Node / Nodo de compuerta GPRS*.
- GPRS: *General Packet Radio Service / Servicio general de paquetes vía radio.*
- GSM: *Global System for Mobile Communications / Sistema global para las comunicaciones móviles.*
- GTP-C: *GPRS Tunneling Protocol – Control / Protocolo de túnel GPRS de control*.
- GTP-U: *GPRS Tunneling Protocol – User / Protocolo de túnel GPRS del usuario*.

- HTTP: *HyperText Transfer Protocol / Protocolo de transferencia de hipertexto*.
- HLR: *Home Location Register / Registro de ubicación base*.
- ICMP: *Internet Control Message Protocol / Protocolo de mensajes de control de Internet.*
- IDS: *Intrusion Detection System / Sistema de detección de intrusos.*
- IGP: *Interior Gateway Protocols / Protocolos de paso interiores.*
- IMSI: *International Mobile Suscriber Identity / Identidad internacional del suscriptor móvil*.
- IP: *Internet Protocol / Protocolo de Internet.*
- IPS: *Intrusion Prevention System / Sistema de prevención de intrusos.*
- IPsec: *IP Security / Protocolo de seguridad IP*.
- IPv4: *Internet Protocol Version 4 / Protocolo de Internet versión 4.*
- IPv6: *Internet Protocol Version 6 / Protocolo de Internet versión 6.*
- ISO: *International Organization for Standardization / Organización internacional de estandarización.*
- ISP: *Internet Service Provide / Proveedores de servicios de Internet.*
- LAN: *Local Area Network / Acceso de red de área local*.
- MME: *Mobility Management Entity | Entidad encargada de la movilidad*.
- MMS: *Multimedia Messaging Service / Servicio de mensajería multimedia.*
- MMSC: *Multimedia Messaging Center / Centro de mensajería multimedia*.
- MSISDN: *Mobile Station International Suscriber Directory Number*.
- MSK: *Master Secret Key / Llave maestra secreta.*
- MSS: *Maximum Segment Size / Tamaño Máximo del Segmento.*
- MTU: *Maximum Transmission Unit / Unidad Máxima de Transmisión*.
- OCS: *Online Charging System / Sistema de cobros en línea*.
- OFCS: *Offline Charging System / Sistema de cobros fuera de línea*.

- OSI Model: *Open Systems Interconnection Model / Modelo de interconexión de sistemas abiertos.*
- PCEF: *Policy and Charging Enforcement Function / Función de políticas y de realización de cobros.*
- PCRF: *Policy and Charging Rules Function / Función de políticas y reglas de cargos.*
- PDN: *Public Data Network / Red pública de datos*.
- PDP: *Packet Data Protocol / Protocolo de paquetes de datos.*
- PGW: *Public Data Network Gateway / Paso de red de datos públicos*.
- PPP: *Point-to-Point Protocol / Protocolo punto a punto.*
- RNC: *Radio Network Controller / Controlador de red de radio.*
- Root DNS Server: *Servidores DNS raíz.*
- SGSN: *Serving GPRS Support Node / Nodo de servicio GPRS.*
- SGW: *Serving Gateway / Paso de servicio*.
- SMS: *Short Message Service / Servicio de mensaje corto.*
- SMTP: *Simple Mail Transfer Protocol / Protocolo para transferencia simple de correo.*
- SNMP: *Simple Network Management Protocol / Protocolo simple de administración de red.*
- SSH: *Secure Shell / Intérprete de órdenes segura.*
- SSL: *Secure Socket Layer.*
- TCP: *Transmission Control Protocol / Protocolo de control de transmisión.*
- TELNET: *Teletype Network / Protocolo de terminal virtual.*
- TLD DNS Server: *Top Level Domain DNS Server / servidores DNS de dominio de nivel superior.*
- TLS: *Transport Layer Security.*
- TTL: *Time To Live / Tiempo de vida.*
- UDP: *User Datagram Protocol / Protocolo de datagramas de usuario.*

- UE: *User Equipment / Equipo del usuario*.
- UMTS: *Universal Mobile Telecommunications System / Sistema universal de telecomunicaciones móviles.*
- UTRAN: *UMTS Terrestrial Radio Access Network / Red UMTS terrestre de radio acceso*.
- VoIP: *Voice over IP / Telefonía por Internet.*
- VPNs: *Virtual Private Networks / Redes privadas virtuales.*
- WAP: *Wireless Application Protocol / Protocolo de aplicaciones inalámbricas.*

Bibliografía

[1] Cisco VNI Mobile 2015 http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

[2] Chetan Sharma Consulting, US Wireless Market Update 4/4 of 2014 http://www.chetansharma.com/US_Wireless_Market_Q4_2014_Update_Feb_2015_Chetan_Sharma_Consulting.pdf.

[3] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 1, page 3.

[4] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 1, page 34.

[5] Networkplanet88 Blog http://networkplanet88.blogspot.com/2013/07/a-comparison-of-network-models.html.

[6] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 2, page 134.

[7] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 2, page 137.

[8] 2.2 Dissecting a Network Package http://books.gigatux.nl/

[9] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 3, page 251.

[10] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 8, page 732.

[11] 3rd Generation Partnership project (2014, September 26), TS 32.240 Charging Architecture and Principles, Release 12, p18. http://www.3gpp.org/ftp/Specs/archive/32_series/32.240/32240-c50.zip

[12] 3rd Generation Partnership project (2014, June 24), TS 23.002 Network Architecture, Release 12. http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/23002-c50.zip

[13] FOROUZAN, B.A. Transmisión de datos y redes de comunicaciones. McGraw Hill, 2007.

[14] COMER, D. Internetworking with TCP/IP, Vol I. Prentice-Hall, 2006.

[15] PETERSON, L.L., DAVIE, B.S. Computer Networks: A Systems Approach. Cuarta Edición. Morgan Kaufmann, 2007.

[16] Página principal de Your Freedom. http://your-freedom.net/

[17] Patricio Valenzuela C., Sistemas de Acceso Móvil Inalámbrico, Universidad de Chile, Octubre 2014.

[18] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 1, Section 5.

[19] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 2, Section 5.

[20] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 3, Section 3.

[21] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 3, Section 5.

[22] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 4, Section 4.

[23] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 8, Section 2.

[24] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 8, Section 9.

[25] OZEKI VoIP SIP SDK http://www.voip-sip-sdk.com/attachments/231/voip-udp-packet-125.png.

[26] TCP/IP Tutorial http://www.yaldex.com/tcp_ip/FILES/06fig08.gif.

[27] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 3, page 201.

[28] Computer Networking: A top-down approach 6th Edition. Kurose. Chapter 4, page 354.

Nota

Los fraudes no pueden ser encontrados en libros o algo parecido, ya que son nuevos, dinámicos y constantemente aparecen más. Por lo tanto, la indagación de los mismos fue en redes sociales, foros y grupos organizados, donde se divulga la información, ya sea por ayudar a los demás o por lucrar.

Los lugares que más información tienen son los más masivos, como Facebook o Twitter. Hay agrupaciones privadas que se dedican a divulgar la información y otras a venderla. Día a día, las restricciones para pertenecer a estos círculos son mayores, ya que se sabe que las empresas están trabajando para acabar con esto.

Figura 41: Grupos que se dedican a vulnerar el sistema.

Figura 40: Grupo cerrado donde se comparte información.

Sin embargo, ninguno de estos grupos o red social entrega la información de qué realmente está pasando con cada uno de los programas, protocolos y puertos que se utilizan. Por lo tanto, el estudio que permite entender la base de la red, su funcionamiento y eventuales vulnerabilidades proviene de los siguientes sitios y libros.