El papel de la Ciberseguridad en el proceso de la transformación digital en México.[1]

José Luis Cuevas Ruíz

Centro de Estudios

Agosto 2021

A partir del modelo general de la Ciberseguridad, el presente estudio tiene como objeto identificar y analizar las amenazas y vulnerabilidades de los protocolos de señalización usados en las redes de Telecomunicaciones móviles, así como la elaboración de recomendaciones y nuevas prácticas.

[1] El análisis, resultados y recomendaciones expresadas en el presente documento no necesariamente reflejan el punto de vista del Instituto Federal de Telecomunicaciones ni su Centro de Estudios, quedando a cargo del autor la responsabilidad de los mismos.

El papel de la Ciberseguridad en el proceso de la transformación digital en México

Resumen del estudio

El objetivo del presente estudio es el de ***Identificar y analizar las amenazas y vulnerabilidades en materia de Ciberseguridad dentro de las redes de telecomunicaciones del servicio móvil que pudieran inhibir la transformación digital en México, considerando los distintos protocolos de señalización***.

El objetivo previamente señalado se derivó del planteado en la propuesta inicial en incluido en el PAA 2021 del Centro de Estudios, que establece lo siguiente: Analizar y evaluar el papel de la Ciberseguridad en el proceso de la transformación digital en México, considerando el marco regulatorio actual, la evolución de los riesgos y amenazas a la información e infraestructura crítica, la experiencia nacional e internacional, así como el nivel de conocimiento de la sociedad en el tema, con el objeto de identificar áreas de oportunidad que permitan la integración de recomendaciones, buenas prácticas y posibles líneas de acción regulatorias. El estudio aborda el concepto de la ciberseguridad en el marco de los protocolos de señalización en las redes de Telecomunicaciones de servicio móvil.

El estudio presenta un análisis de la Ciberseguridad de lo general a lo particular, partiendo del modelo general de la ITU (*International Telecommunications Union*), identificando los planos, dimensiones y capas de seguridad que lo integran. Dentro de este modelo se detallan los componentes que integran el ciberentorno en el que las redes de telecomunicaciones están inmersas, así como los diferentes elementos que la integran.

Como consecuencia del enfoque planteado para el análisis, algunos aspectos relacionados con la Ciberseguridad no son detallados a profundidad, pretendiendo que esta autolimitación permita una

mayor profundidad del análisis técnico y operativo de los protocolos de señalización usados en las redes de telecomunicaciones móviles dentro del marco de la Ciberseguridad, que es el objeto del presente estudio. Así mismo, el análisis del modelo de ciberseguridad identifica las otras líneas que el análisis de la Ciberseguridad puede ser abordada en trabajos futuros.

Para el caso de la señalización, se proporciona la conceptualización y características técnicas de los protocolos más usados en las redes de datos y de telecomunicaciones móviles. Se detalla la correspondencia y relación existente de estos protocolos con las 7 capas del modelo OSI (*Open System Interconnection*) y el protocolo SS7. La interconexión y convergencia actual de las redes de telecomunicaciones , establece la necesidad de modelos similares de correspondencia para cada uno de los protocolos analizados.

Además de describir e identificar algunos de los riesgos y vulnerabilidades más relevantes de los protocolos de comunicaciones móviles relacionados con la señalización, se identifican algunos de los vectores usados para la ejecución de los ciberataques y ciberamenazas más comunes, así como algunas de recomendaciones para mitigar el riesgo que estas presentan.

Se presentan los conceptos generales de señalización, considerando la señalización IP H.323 y SIP, así como la señalización dentro del núcleo de red, que considera a los protocolos SS7, SIGTRAN, DIAMETER y GTP. Desde el punto de vista de ciberseguridad, estos protocolos son analizados con el objeto de identificar vulnerabilidades de los sistemas de telecomunicaciones móviles, identificando los riesgos que estas vulnerabilidades suponen, así como también se plantean algunas posibles soluciones y consideraciones para enfrentar dichos riesgos.

Los alcances del estudio incluyen el análisis de las funciones y fines que esta señalización ofrece, identificando y describiendo las principales vulnerabilidades y vectores de ataque de las amenazas y ciberataques a las que estas redes pueden estar expuestas.

Las recomendaciones, buenas prácticas y oportunidades que se presentan como resultado del análisis están basadas en los vectores de ataques identificados. Del mismo modo, se plantean algunas recomendaciones relativas a la evaluación que los protocolos de señalización deberán considerar, con el objeto de responder a las exigencias y necesidades surgidas de la convergencia de las redes.

Las recomendaciones y conclusiones mencionadas se profundizan en los siguientes rubros:

- Descripción de las vulnerabilidades de las señalizaciones usadas en las redes de telecomunicaciones móviles.

- Análisis de los principales vectores de ataque usados en los tipos más comunes de ciberataques

- Identificación para el uso de firewalls, así como puntos de detección, control y de intrusos.
- Oportunidades de mejora en los esquemas de ruteo
- Uso de esquemas de encriptación y protocolos de seguridad sobre IP
- Identificación de trabajos futuros

Para cada uno de los aspectos mencionados, se abordan e identifican áreas de oportunidad, buenas prácticas y recomendaciones que pueden servir como soporte para la implementación de estrategias que permitan incrementar la seguridad en las redes.

El presente documento estará integrado por las siguientes secciones: en la Sección I se presenta una Introducción al tema, brindando un panorama de la temática abordada, describiendo el entorno de su aplicación y algunos conceptos que permitirán dimensionar y justificar la problemática descrita. En la sección II se dan algunos conceptos relacionados con la Ciberseguridad, abordando desde un punto de vista técnico, identificando los elementos que la integran. Algunos protocolos de señalización utilizados en las redes de telecomunicaciones móviles son abordados en la sección III. En la sección IV se describen las vulnerabilidades de los protocolos analizados, así como también se identifican y analizan algunos de los perfiles de ataque más comunes. Algunas recomendaciones y líneas de acción son abordadas en la sección V y finalmente en la sección VI se brindan algunas conclusiones. Algunas de las principales referencias usadas en el estudio se enlistan al final.

I. Introducción

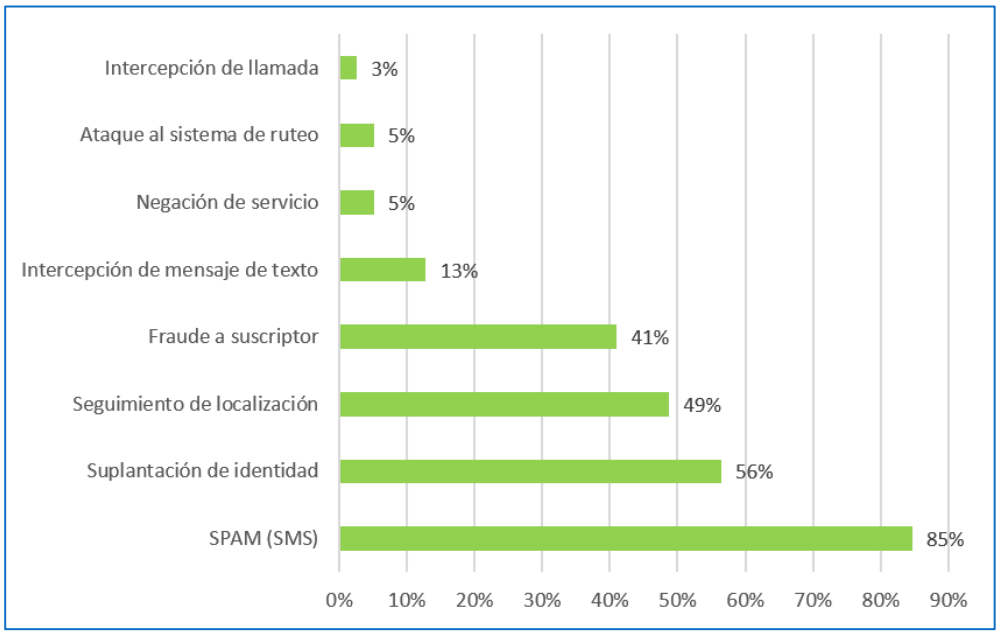
En la actualidad la ciberseguridad representa un elemento fundamental para garantizar una conectividad confiable, que permita el acceso a los servicios digitales de una forma segura. El uso de las Tecnologías de Información y Comunicaciones (TICs) ha permito mejoras sustanciales en la gestión de los sistemas productivos, una mayor calidad en una gran cantidad servicios y productos, así como una mayor variedad de alternativas en sectores como el financiero y el de comercio electrónico. Al mismo tiempo, el uso de la tecnología ha permitido impulsar estrategias que permitan un uso más eficiente de recursos no renovables [OEA, BID (2020)], así como fortalecer acciones encaminadas al logro de los objetivos de desarrollo sostenible propuestos por la ONU [ODS, ONU. (2015)]. Al mismo tiempo, la digitalización e incorporación de los productos y servicios a la nube de las actividades relacionadas a los sectores mencionados, ha generado nuevos riesgos y vulnerabilidades que pueden poner en riesgo su operación y continuidad. De este modo la Ciberseguridad se ha convertido en un tema toral en la promoción y penetración de los servicios y productos ofertados haciendo uso de internet.

De acuerdo con reportes e informes consultados, los ataques a las redes de telecomunicaciones presentan una alta incidencia. En [ENISA. (2018)] se reportan los resultados de una encuesta realizada a proveedores de servicios de comunicaciones respecto a la frecuencia y características de los ataques a las redes de telecomunicaciones en la Unión Europea, y se encontró que más del 80% de los operadores de servicios de telecomunicaciones habían detectado o sufrido algún tipo de ataque, y el 25% de los encuestados reportaron haber sufrido hasta 100 ataques en el año en que se realizó la encuesta. El SIT (*Security, Infrastructure and Trust*), grupo de trabajo de la UIT, informó que el 70% de los operadores de telecomunicaciones no cuentan con información confiable respecto a si sus redes han sido víctimas de algún ataque. Esto dato puede ser indicativo de que estamos en presencia de un problema mucho más grande que lo que se encuentra documentado en reportes e informes.

De acuerdo con la firma Sophos [SOPHOS. (2021)], 1 de cada 4 empresas en México han sufrido algún ataque cibernético ya sea para robo de datos, interrupciones o fallo en la disponibilidad de servicios. En el 2020 en México se reportaron casi el 18 % de las afectaciones por *malware* ocurridos en los países de LATAM y el 12% afectadas por phishing de acuerdo a los resultados publicados del *ESET Security Report 2021* [ESET. (2021)].

Los tipos de ataques que se han detectado en las redes de telecomunicaciones se muestran en la Gráfica 1 [PT. (2016)]. Un ataque puede ser identificado con más de uno de los tipos enlistados. En esta, podemos ver que os ataques que ocupan las 4 primeras posiciones están relacionados directamente con la provisión de servicios financieros.

Gráfica 1. Tipos de ataques a las redes de telecomunicaciones. EEUU, 2018 [PT. (2016)]].



La evolución y diseño de los protocolos de señalización nos ha llevado a contar con protocolos más robustos y con una mayor capacidad para evitar su corrupción. Sin embargo, independientemente del tipo de señalización usada, es casi imposible identificar un protocolo de señalización que garantice una inviolabilidad total.

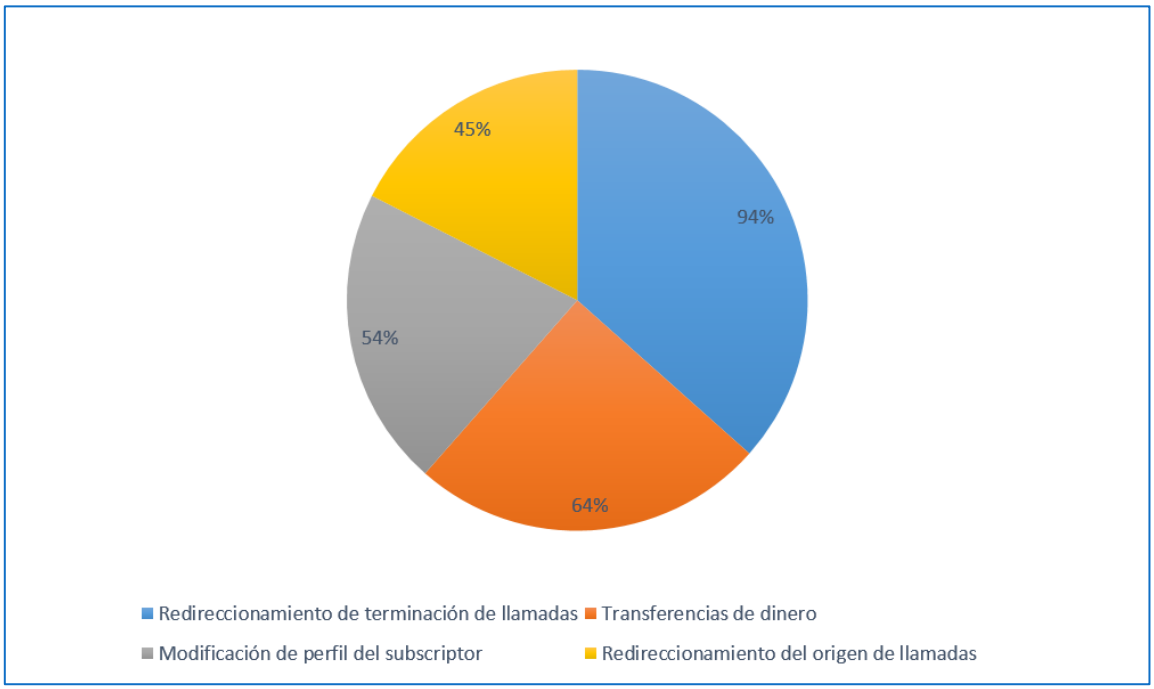
Desde el punto de vista de la seguridad, existe coincidencia en estudios y análisis de campo llevados a cabo que la vulnerabilidad mayor se presenta en los protocolos de las generaciones de telefonía móvil. Así mismo, las redes de telecomunicaciones emergentes están adicionando nuevas amenazas, y al estar interconectadas con las redes previas, también comparten la mayoría de las vulnerabilidades de las redes que ya están operando.

Al respecto de la vulnerabilidad del protocolo SS7, en [PT. (2016)], se reporta que el porcentaje de ataques exitosos dependiendo del tipo de fraude, es mayor en el caso del redireccionamiento de llamadas con un 94%, mientras que en el caso de transferencias de dinero haciendo uso de mecanismos basados en USSD el éxito es del 64%. Grafica 2.

El incremento en la cantidad, complejidad y variedad de los ciberataques y ciberamenazas a los que están expuestos los usuarios y empresas al momento de conectarse a las redes de telecomunicaciones demandan una evolución y mejora en las estrategias y acciones implementadas para combatir estos riesgos. En el marco de sociedades en constante transformación, donde las herramientas, recursos tecnológicos y las redes de telecomunicaciones forman parte importante de

este cambio, los retos de seguridad en la gestión de la información para los empresas, ciudadanos y gobiernos de todos los países alrededor del mundo son cada vez mayores. El diseño e implementación de estrategias que permitan mejorar la seguridad en el acceso a las plataformas que ofrecen servicios, así como garantizar la seguridad de la información y de la infraestructura crítica son esenciales para lograr los objetivos que la transformación digital ofrece.

Gráfica 2. Porcentaje de ataques exitosos en redes que usan el SS7 [PT. (2016)].



Los incidentes relacionados con la ciberseguridad pueden comprometer la disponibilidad, integridad y confidencialidad de la información transmitida por estas redes, así como también la información almacenada en cualquier computador o en la nube, comprometiendo las operaciones y funcionamiento de organizaciones públicas y privadas, incluyendo la infraestructura, tanto virtual como física.

En la actualidad la conectividad permite que prácticamente todas las redes de los operadores de telecomunicaciones estén en condiciones de estar en comunicación. Además de las ventajas que esto trae consigo, no debemos dejar a un lado el riesgo implícito, ya que el acceso a la red para fines maliciosos se presentará, en el mayor de los casos, desde el punto de entrada más débil de la

totalidad de redes conectadas, y este puede estar cientos de kilómetros del lugar donde el ataque se concreta.

Los tipos y perfiles de los ciberataques son diversos y pueden ser abordados y analizados desde diversas ópticas. En una gran cantidad de publicaciones se elaboran y detallan recomendaciones para los usuarios de las redes, encaminadas a concientizar los riesgos y a tomar medidas en consecuencia. Estas acciones son parte de los que se denomina Ingeniería Social, que analiza las condiciones de riesgos generadas por el usuario y que ponen en peligro su información (datos, identidad, recursos, etc.) El análisis abordado en el presente estudio se enfoca principalmente en el aspecto técnico de la operación del SS7, analizando las circunstancias operativas que generan las vulnerabilidades abordadas que conciernen más al operados que al usuario de las redes.

Como consecuencia de lo anterior, estas amenazas pueden comprometer la seguridad de las personas y bienes conectados a estas, así como a la infraestructura que la soporta, pudiendo generar efectos y daños severos en su patrimonio y seguridad. En países con altos niveles de penetración en la digitalización de los servicios financieros y bancarios, la importancia de la operación y seguridad de la infraestructura crítica es un tema de gran relevancia. En el caso particular de los servicios financieros digitales, una gran cantidad de la información generada al momento de la realización de dichas operaciones pasa por las redes y canales de telecomunicaciones, haciendo uso de dispositivos móviles y teléfonos inteligentes. Estos canales de comunicación que enlazan al usuario final con el proveedor de los servicios financieros hacen uso de recursos de señalización como los USSD (*Unstructured Supplementary Service Data)*[2], los SMS (*Short Messaging Service*)[3] y el STK *(Sim Tool Kit*)[4]. Este tipo de señalizaciones presentan vulnerabilidades y riesgos que pueden ser la base de los vectores de ataque de los hackers para la comisión de fraudes y robos en los sistemas y equipos que se interconectan a las redes de telecomunicaciones de servicios móviles. Estos ataques pueden presentar serias consecuencias tanto para el usuario final, como para las empresas proveedoras de servicios. Dentro de los riesgos de mayor relevancia, estas vulnerabilidades permiten al potencial atacante hacer uso de lo que se conoce como suplantación de identidad, algunas veces presentándose al usuario final como la empresa bancaria o financiera proveedora de servicios, o suplantando al usuario para que a su nombre autorizar la realización de operaciones financieras.

Las vulnerabilidades de los protocolos usados en las redes de telecomunicaciones se analizan desde 2 perspectivas: desde la señalización bajo la que opera la comunicación entre terminales y el núcleo

[2] Servicio que permite el envío de datos a través de redes móviles GSM

[3] Señalización que permite el envío de datos en una red celular, haciendo uso de un SMCS (Short Message Service Center) para almacenar el SMS generado de un dispositivo origen hasta que el dispositivo destino se encuentre disponible.

[4] Tecnología que permite una comunicación más eficaz entre la tarjeta SIM y el dispositivo móvil, facilitando programar o personalizar diferentes servicios (principalmente bancarios) sin necesidad de llamar al operador.

de la red, por una parte, y la señalización dentro del núcleo de la red. Para el caso de las señalizaciones usadas dentro de la red, en la actualidad se encuentran interconectados sistemas de comunicaciones móviles que operan con protocolos con diferentes capacidades y niveles de seguridad, desde el SS7 que es un protocolo de señalización desarrollado para las comunicaciones telefónicas fijas existentes en las primeras redes de telecomunicaciones, hasta esquemas más avanzadas y complejos usados en la redes de nueva generación y redes 5G, como el GTP (que es un conjunto de protocolos basados en IP). Estos protocolos de señalización son usados prácticamente en todas las redes telefónicas en funcionamiento alrededor del mundo al momento del establecimiento y terminación de los enlaces de comunicaciones en cada llamada o conexión, permitiendo la ejecución de algunas funcionalidades como identificación de la numeración, portabilidad numérica, servicios de prepago, servicio de mensajería (SMS), entre varios más.

II. Ciberseguridad. Conceptualización y modelo

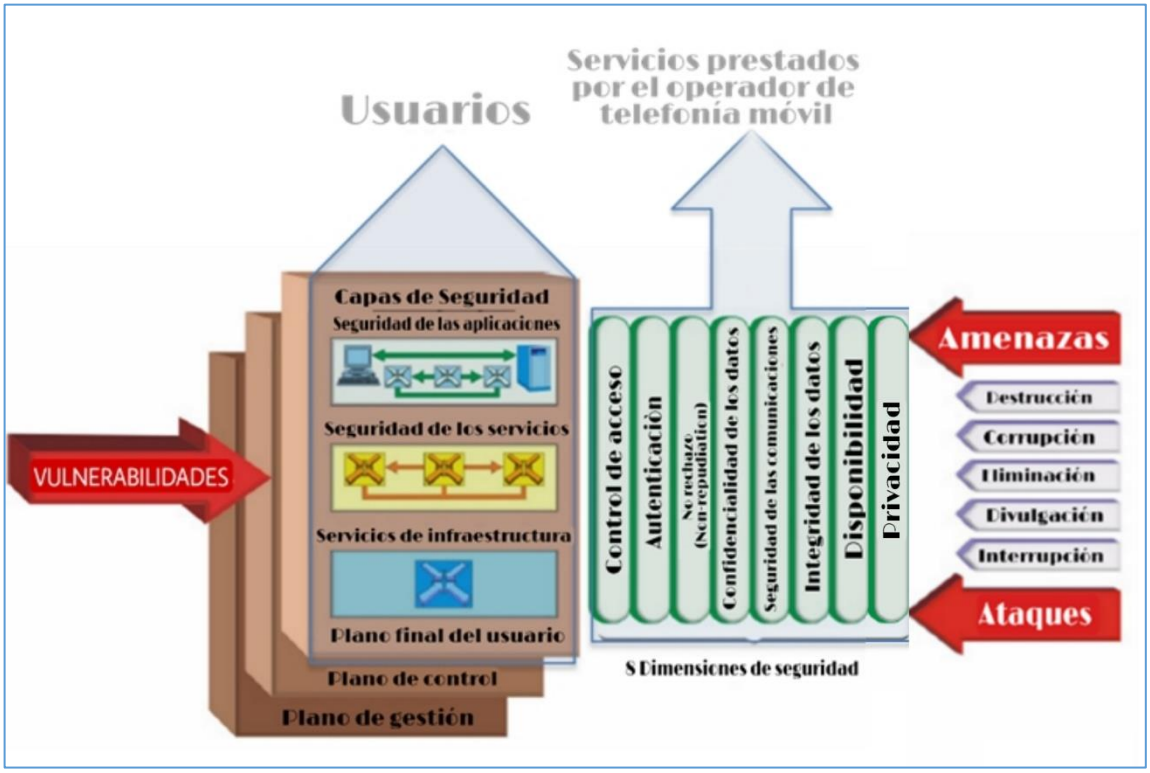
La Ciberseguridad es un concepto amplio que puede ser analizado desde diferentes perspectivas. De acuerdo con la ITU [UIT-T. (2008)], la Ciberseguridad se puede definir como la colección de herramientas, políticas, conceptos y medidas de seguridad, lineamientos, recomendaciones de gestión de riesgos, acciones, entrenamientos, mejores prácticas y tecnologías que pueden ser usadas para proteger el ciberentorno, incluyendo a los usuarios y bienes que lo integran. Los bienes de la organización que integran el ciberentorno así como los usuarios, están integrados por los dispositivos computacionales conectados, personal que hace uso de estos, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones, así como la totalidad de la información enviada y/o almacenada en el ciberentorno. La Ciberseguridad tiene como objeto asegurar la continuidad y mantenimiento de las propiedades de seguridad de la organización, así como proteger los bienes de los usuarios contra riesgos relevantes que pudieran presentarse en el ciberentorno.

Los objetivos de la Ciberseguridad pueden definirse como: Disponibilidad, integridad y confidencialidad de la información e infraestructura que operan en el ciberentorno. En el caso de la ciberseguridad en las redes de telecomunicaciones móviles, el ciberentorno también incluye al software, sistema operativo y aplicaciones que operan desde el dispositivo móvil. El software que opera en el equipo móvil desempeña un papel relevante al momento de evaluar los riesgos a los que la información esta expuesta, ya que es a través de estos programas o aplicaciones que se accede a las diferentes plataformas para la realización de operaciones, entre las que se pueden incluir los servicios financieros o de comercio electrónico.

Los fundamentos relativos a la Ciberseguridad de acuerdo con la ITU están definidos en las recomendaciones X.800 y X.805 [UIT-T. (2003)]. De acuerdo con estas recomendaciones la arquitectura del modelo de ciberseguridad en una conexión punto a punto en una red está definido en función de 3 conceptos fundamentales: Capas de Seguridad, Planos y Dimensiones

En una aproximación jerárquica, los requisitos de seguridad son seccionados a través de la capas y planos, de modo que la seguridad del enlace punto a punto se logra por medio del diseño de acciones de seguridad en cada una de las dimensiones de manera que se identifiquen las amenazas específicas. El modelo propuesto por la ITU se muestra en la Gráfica 3, donde adicionalmente se indican las secciones de relevancia para los operadores y usuarios de las redes de telecomunicaciones móviles.

Gráfica 3. Modelo de Ciberseguridad. ITU



Una dimensión de seguridad es un conjunto de medidas o acciones que permiten la identificación de una amenaza. Estas acciones de seguridad no están limitadas a la red, sino que también se pueden extender a las aplicaciones que utiliza el usuario de la red de telecomunicaciones. De manera específica, las dimensiones de seguridad son aplicables a las empresas que ofrecen los servicios, incluyendo los relacionados con la seguridad a los usuarios.

De acuerdo con lo mostrado en la Gráfica 3, las dimensiones de seguridad se identifican como: A) Control de acceso, B) Proceso de autentificación, C) No repudio (servicio que proporciona pruebas de la integridad y origen de los datos, con altos niveles de autenticación), D) Confidencialidad de los datos, E) Seguridad en las comunicaciones, F) Integridad de los datos, G) Disponibilidad y H) Privacidad. Los procesos e información relacionada con varias de las dimensiones listadas se relaciona de manera directa con la señalización que se utiliza en los enlaces y comunicaciones entre el usuario y los operadores dentro del núcleo de la red de cada operador.

Las amenazas a los sistemas de comunicaciones de datos pueden describirse de acuerdo con las siguientes definiciones [UIT-T. (2003)]:

- Destrucción de la información o de otros recursos

- Corrupción o modificación de la información
- Robo o pérdida de información u otros recursos
- Exposición de información
- Interrupción de servicios

La tendencia actual es pasar de la implementación de los códigos de señalización por medio de hardware hacia una virtualización; de este modo, los protocolos son implementadas por medio de software que opera en los dispositivos de los usuarios y en las plataformas de servicios. Los principales vectores de ataque de los hackers es precisamente romper los candados de seguridad de estos programas de software. La concreción y éxito de las amenazas y vulnerabilidades pasa por la corrupción o violación de los niveles de seguridad que los enlaces y comunicaciones presentan, donde estos niveles de seguridad presentan una dependencia directa con el tipo de protocolo de señalización que usan.

Los protocolos de señalización utilizados en las redes comunicaciones móviles más utilizados alrededor del mundo son el SS7, SIGTRAN, GTP y Diameter [Ullah. (2020)]. Mientras que las tecnologías móviles han presentado una gran evolución en las pasadas décadas para satisfacer la demanda del mercado y los usuarios, proporcionando mayores velocidades y disponibilidad en una mayor cantidad de conexiones, mayor cobertura, incremento en la interconexión de redes alrededor del mundo, intercambio de información, etc., las tecnologías subyacentes a la seguridad de la información para interconectar estas redes no han seguido el mismo ritmo de evolución. Si bien la cantidad de servicios y conexiones, así como la resiliencia de las redes a las demandas por parte del mercado han sido una de las principales preocupaciones, el tema de la seguridad hoy en día se ha convertido en un requerimiento clave. Esta relevancia ha ido en aumento en la medida que el valor de la información que transita por las redes ha incrementado también. La provisión de nuevos servicios y el desarrollo de nuevas aplicaciones que hacen uso de las redes de telecomunicaciones, así como la cantidad e importancia de la información que transita y se almacena en las redes ha enfatizado aún más la problemática expuesta.

En el casos de las comunicaciones dentro del núcleo, las redes 2G/3G hacen uso del protocolo de señalización SS7, para el caso de redes 4G-LTE se Hace uso de Diameter y las redes mejoradas y las de 5G hacen uso de protocolos como el GTP. No obstante que Diameter evoluciona a partir de SS7 para contemplar algunas de las demandas de las redes 4G LTE, ambos protocolos hacen uso de principios de interconexión similares, inherentes a las redes PSTN (*Public Switched Telephone Networks*), donde las conexiones han sido implementadas bajo ciertas condiciones de seguridad y confianza, entre pocos operadores, por lo que muchas de las vulnerabilidades de SS7 no se resuelven en Diameter. La apertura de los mercados y el acceso a un internet abierto ha ocasionado que el

acceso a estas redes sea mucho más sencillo, dando como resultado una gran cantidad de operadores interconectados entre sí alrededor del mundo; una red IP puede estar expuesta a un ataque que provenga de una red 2G.

Una gran cantidad de los ataques a las redes de comunicaciones que hacen uso del protocolo SS7 utilizan funcionalidades provistas por las mismas redes móviles. Al momento de evaluar las vulnerabilidades del SS7 debemos recordar que desde su origen, este no fue diseñado con fines de seguridad o con la idea de controlar el acceso a las redes, de modo que la tarea de enfrentar los retos que en materia de seguridad las redes actuales presentan se visualiza como un reto de grandes dimensiones.

Adicional al reto de integrar las funcionalidades de seguridad y acceso que no fueron abordadas para el SS7 desde su diseño, se debe considerar también que la interconectividad de las redes es un requisito indispensable en la actualidad para aspirar a alcanzar los beneficios de las oportunidades de negocio, recursos y servicios innovadores que la transformación digital trae consigo. Es decir, los operadores requieren abrir sus redes para una gran gama de socios y clientes potenciales; una estrategia de acceso a la red con bajos niveles de control a una gran cantidad de usuarios es la principal razón para redoblar los esfuerzos que permitan incrementar la seguridad y mitigar los riesgos en la señalización usada en estas redes.

Desde el punto de vista de la seguridad de la red, el análisis se enfoca priorizando los puntos de acceso que más vulnerabilidades presentan, que en este caso son las redes que operan con el SS7. Debido a la interoperabilidad de las redes ya mencionada, una vez que el SS7 haya sido vulnerado y el acceso a la red conseguido, el reto de identificar a un usuario ilegal dentro del núcleo de la red es mayor.

Otras de las consideraciones relevantes a tomar en cuenta, es que en los casos de amenazas y ataques que hacen uso de las vulnerabilidades de protocolos como SS7, Diameter y las redes más recientes, el usuario poco puede hacer, debido a que este no cuenta con el nivel de acceso a las capas de señalización, dando como resultado que las potenciales acciones de parte del usuario son limitadas. Las acciones y estrategias de seguridad del sistema se encuentran básicamente a nivel del operador. Sin embargo, como parte de la innovación y desarrollo de nuevos productos y servicios, el papel que el usuario puede jugar en este escenario puede cambiar, accediendo a recursos desde su dispositivo móvil que le permitan monitorear la funcionalidad de su conexión, detectando potenciales anomalías basadas en tráfico inusual, intentos de acceso no autorizado, spam, etc.,

III. Protocolos de señalización en las redes de telecomunicaciones móviles.

La ITU (*International Telecommunications Union*) define a la señalización en su recomendación ITU-T Q.9 como el intercambio de información relacionada específicamente con el establecimiento, liberación y otras formas de control de las comunicaciones, así como con la gestión de la red[5].

Básicamente, el objetivo de los protocolos de señalización es el establecimiento/terminación del canal de comunicación, así como gestionar el intercambio información de control, lo que desde el punto de vista de ciberseguridad resulta de especial relevancia. El acceso de manera ilegal a esta información de control es la que puede traducirse en una vulnerabilidad para todos los sistemas y equipos conectados a la red, ya que además de gestionar el establecimiento de los enlaces, permite el acceso a bases de datos, el intercambio de información de autentificación, autorización y tarificación, además de gestionar, mantener y monitorear los diferentes elementos conectados a la red.

Para fines del presente análisis se consideran las señalizaciones entre los terminales y el núcleo de la red, así como la señalización dentro del núcleo de la red.

Señalización IP H.323.

El H.323 es un protocolo basado en la recomendación de la ITU-T que describe los terminales y dispositivos que proveen servicios de comunicaciones multimedia (video, voz y datos) sobre redes de conmutación de paquetes que no garantizan calidad de servicio (por ejemplo, Ethernet con protocolos TCP/IP). El protocolo VoIP (voz sobre IP) puede hacer uso de este tipo de señalización.

La señalización H.323 extiende los conceptos de señalización ISDN y de transporte a las redes de datos que funcionan sobre IP. En su arquitectura se pueden identificar los siguientes elementos:

- Terminales H.323
- Gateways que permiten interconectar a los sistemas H.323 con el resto de los sistemas de telecomunicaciones a través de la red telefónica.
- Controladores H.323
- Unidades de Control Multipunto. (MCU)

[5] ITU-T Q.9. ile:///D:/Users/jose.cuevas/Downloads/T-REC-Q.9-198811-I!!PDF-S.pdf

Las terminales H.323 soportan comunicaciones de voz, y de manera opcional pueden integrar comunicaciones de datos y video. La recomendación establece los protocolos utilizados en la señalización de llamadas, los mensajes de control, el modo de multiplexación de los mensajes, los codificadores de audio y video (códecs), así como los protocolos utilizados para el intercambio de datos entre terminales.

Las codificaciones de audio que admite la H.323 son: G.711, G.722, G.728, G.723.1 y G729[6]. Cada una de estas presenta diferentes velocidades de muestreo y por ende calidad en la señal, resaltando que de manera obligatoria todas las terminales H.323 deben contar con un códec de audio, y este debe soportar mínimo la codificación G.711. La comunicación de audio entre terminales que hacen uso de codificadores diferentes es gestionada por el H.245, que es un protocolo que tiene la capacidad de transmitir y proporcionar la información necesaria para la comunicación multimedia, tal como la codificación, el control de flujo, la gestión de jitter y las peticiones de preferencia, así como el procedimiento de apertura y cierre de los canales lógicos usados para transmitir los contenidos.

En relación con los codificadores de video, estos son opcionales para el caso del H.323. Si el terminal cuenta con codificación de este tipo, este debe contemplar los codificadores H.261 y el H.263[7]. Existen también otros tipos de codificación que son opcionales. De igual modo que en el caso de los codificadores de audio, la gestión de la comunicación de video entre dos terminales H.323 es gestionada por el H.245. Un mismo terminal puede soportar a la vez varios canales de video, tanto en la transmisión como en la recepción, así como hacer uso de un codificador para la recepción y otro diferente en la transmisión.

Al momento de establecer comunicaciones de datos con otros terminales H.323, se pueden habilitar canales de datos bidireccionales o unidireccionales, y cuando el intercambio de datos es entre terminales H.323 y de otro tipo, el canal se gestiona de acuerdo con la recomendación T.120. Las terminales H.323 también hacen uso de protocolos RTP (*Real-Time Transport Protocol*), que establece los principios de un protocolo de transporte sobre redes que no garantizan calidad de servicio para datos que son transmitidos en tiempo real, como es el caso de las señales de audio y video, e incluyen información sobre números de secuencia, marcas de tiempo y monitoreo de tiempo de entrega. Así mismo, el protocolo RTP soporta transferencia de datos a múltiples destinos (multicast), cuando esto es provisto por la red. Adicionalmente, las terminales H.323 hacen uso del protocolo de control RTCP (*RTP control protocol*), cuyos paquetes son enviados de manera periódica con información relacionada con indicadores de calidad del enlace, y otros datos acerca de la fuente

[6] Son protocolos de voz sobre IP que presentan diferentes velocidades de muestreo y niveles de codificación. http://bibing.us.es/proyectos/abreproy/12088/fichero/4+-+Estado+del+Arte.pdf

[7] Los códecs H.261 y H.263 son básicamente estándares de compresión de video, que definen diferentes capacidades de compresión y niveles de ruido. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10282/102820D/Comparison-of-the-H263-and-H261-video-compression-standards/10.1117/12.227952.short?SSO=1&tab=ArticleLink

y destino de la comunicación, incluyendo la cantidad de paquetes enviados, recibidos y el jitter en el receptor. Para la conexión entre terminales H.323 se hace uso de las funcionalidades definidas en el H.225.0[8], y es abierto por el terminal antes de establecer el canal de control H.245.

Los Gateways realizan la interconexión entre las redes H.323 y otras redes de comunicaciones, como la red pública conmutada. Estos son los responsables de adaptar el audio, video y los datos, así como la señalización de manera transparente para los usuarios. Así mismo, las redes H.323 pueden contar con un elemento que centraliza el control y los servicios telefónicos conocido como Gatekeeper. Si bien en la recomendación se establece como opcional, en la práctica este elemento debe existir. Las funciones que realiza el Gatekeeper son: traducción de direcciones, control de admisión, control de ancho de banda, señalización para el control y autorización de llamadas, entre las más relevantes.

La unidad de control multipunto (MCU) provee soporte para la realización de conferencias entre 3 o más terminales. Esta integrada por las Unidades Controladoras Multipunto (MC) que realizan el intercambio de capacidades entre los terminales de la conferencia haciendo uso del H.245, y los Procesadores Multipunto (MP), que son los que reciben los canales de audio, video y/o datos de los terminales, los procesan y los redistribuyen nuevamente a los terminales, llevando a cabo funciones de conmutación y mezcla de las señales de audio y video

Señalización IP SIP

El protocolo de señalización SIP (*Session Initiation Protocol*) tiene su origen a finales de 1996, como parte de una red experimental que operaba sobre internet y que distribuía contenido multimedia, incluyendo charlas, seminarios y conferencias. Para llevar a cabo la invitación a usuarios a escuchar las sesiones multimedia se hacía uso de este protocolo de iniciación. En las redes de telecomunicaciones la señalización SIP es soportada en el núcleo de la red con una central telefónica SIP, conocida como *softswitch*, que en las redes actuales es solo un componente de software del sistema.

La señalización SIP esta basada en el esquema cliente-servidor usado en HTPP (*Hipertext transfer protocol*), donde los mensajes son de texto, y permite establecer comunicaciones del tipo P2P[9] (*peer to peer*) entre aplicaciones, permitiendo a los usuarios la compartición de información y archivos sin necesidades de protocolos intermedios. En el mensaje SIP se incluye información sobre el codificador

[8] Recomendación ITU-T Q.931. https://www.itu.int/rec/T-REC-Q.931-199805-I/en

[9] Las redes P2P se basan en algoritmos que optimizan los recursos disponibles de los dispositivos, básicamente el ancho de banda. https://www.europapress.es/portaltic/internet/noticia-conexion-p2p-utiliza-pirateria-20170420085940.html

usado o la frecuencia de muestreo, y estos van codificados en un formato conocido como SDP[10] (*Session Description Protocol)*

La arquitectura del protocolo SIP está formada por los siguientes componentes: terminales SIP, servidores SIP y gateways SIP. Las terminales SIP básicamente pueden ser teléfonos IP, que pueden hacer uso de aplicaciones usando las capacidades multimedia del dispositivo, así como iniciar y recibir sesiones SIP. Cada terminal cuenta un UAC (*User Agent Client*) que son los responsables de hacer los requerimientos SIP hacía otros usuarios, contando también con un UAS (*User Agent Server*), que son las unidades encargadas de recibir y atender los requerimientos. Cada uno de estos dispositivos se identifica de manera única por medio de su dirección SIP. Los servidores SIP contiene un registro de usuarios SIP, que se integra por medio de las solicitudes de inclusión de los UAC. También se tiene a los servidores Proxy (*Proxy Server*), que tiene la misión de atender las solicitudes y redirigirlas a su destino correcto, que es consultado en un servidor de ubicaciones, función similar a la de un servidor de redireccionamiento (*redirect server).* Sin embargo, este último no interviene en el establecimiento de la comunicación, solo informa el modo de ubicar el destino final. Por otra parte, el Gateway SIP es responsable de adaptar el audio, video y datos, incluyendo la señalización, entre los formatos propios de SIP y de otras redes de telecomunicación, de manera transparente para los usuarios.

Para llevar a cabo la comunicación entre las diferentes centrales telefónicas se hace uso de un tipo particular de señalización que ha ido evolucionando a medida que la complejidad y composición de las centrales ha aumentado también. Este tipo de señalización se identifica como señalización dentro del núcleo de la red. Inicialmente los protocolos de este tipo de señalización se identificaron como SSX, iniciando con el SS1, y de manera sucesiva hasta el SS7 de las redes 2G y 3G.

El protocolo SS7 fue diseñado cuando la cantidad de operadores de telecomunicaciones que ofrecían los servicios eran escasos y las condiciones y demandas de los servicios eran muy diferentes a las actuales, sobre todo en lo relativo al tema de la seguridad. Con la convergencia de las redes de conmutación de paquetes que operan sobre IP y las redes de conmutación de circuitos de las redes telefónicas, los servicios de telefonía celular incrementaron enormemente su popularidad y con ello, su crecimiento y desarrollo en el mercado. Este crecimiento y expansión ocasionó que otros tipos de redes y tecnologías necesitaran conectarse a las redes que operan con el protocolo SS7, generando a su vez una enorme cantidad de potenciales puntos de entrada a la red. Con el incremento en la penetración y popularización del transporte de datos por IP, se desarrolló un sistema de señalización sobre IP denominado SIGTRAN (*Signalling Transport*), diseñado para transportar de manera confiable la señalización SS7 de las redes ISDN *(Integrated Services Digital Network*), que opera de manera conjunta con el protocolo SIP, heredando prácticamente todas las vulnerabilidades del SS7.

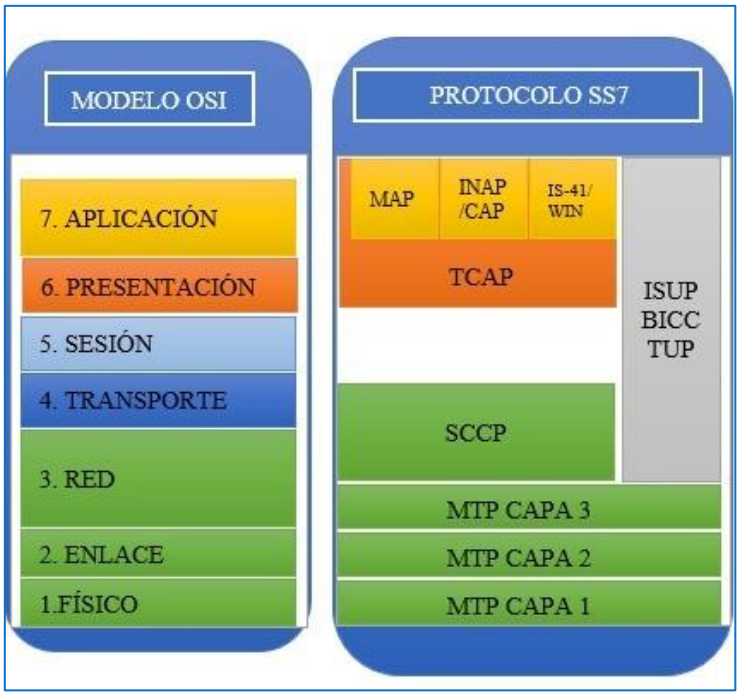
[10] SDP. Session Description Protocol. Network Working Group. https://www.ietf.org/rfc/rfc2327.txt

La proliferación de los terminales móviles y la posibilidad de que un usuario pueda conectarse a la red desde una gran diversidad de puntos, propició el uso de protocolos de autentificación y autorización dentro de las redes de telecomunicaciones, ya que antes de permitir el acceso a la red y de los servicios que esta ofrece, es necesario identificar plenamente al potencial usuario, para correlacionarlo con el perfil de autorizaciones que este posee (permisos y restricciones en relación a los servicios ofertados). Esta necesidad dio origen al desarrollo del protocolo Diameter para su uso dentro del núcleo de la red.

Protocolo SS7

Para que las redes de comunicaciones móviles se conecten a las redes de datos existentes, es necesario que la señalización que utilizan se corresponda con las funciones del modelo OSI bajo el que operan las redes de datos. Cada una de las 7 capas que integran al modelo OSI, lleva a cabo funciones particulares, empaquetando la información específica, permitiendo con esto la estandarización de las comunicaciones entre redes. Para el caso del SS7, la correspondencia de algunas de las funciones de este protocolo de señalización con el modelo OSI se muestran en la Gráfica 4.

Gráfica 4. Correspondencia de algunas de las funciones del protocolo de señalización SS7 con el modelo OSI.



Como puede verse en la Gráfica 4, el protocolo SS7 cuenta una capacidad común con el modelo OSI para el transporte de señalización, llamada MTP (transferencia de mensaje) y la parte de usuario ISUP (*ISDN User Part*). MTP y la parte de control de señalización de conexión (SCCP) forman la parte de los servicios de red, que realiza las funciones correspondientes a las primeras 3 capas del modelo OSI, donde la Capa 1 estandariza las características de compatibilidad física del enlace de transmisión, la Capa 2 está relacionada con la estructura de las tramas de los mensajes enviados por la red, así como la detección y corrección de ciertos tipos de errores. La Capa 3 es donde se identifican los protocolos de señalización para efectuar la transmisión de mensajes entre nodos.

El MTP del SS7, representa un sistema de transferencia de mensajes, que permite transmitir información de señalización a través de la red hacia el punto de destino. El MTP se compone de tres niveles: Nivel 1. Este es el nivel más bajo de este bloque y es análogo a la capa física del modelo OSI. El Nivel 2 es la capa similar al nivel 2 del modelo OSI y tiene como propósito transportar de manera segura los mensajes de punto a punto. Nivel 3 provee la ruta que seguirán los paquetes. La parte de control de la señalización de conexión añadida amplía los servicios de la MTP para alcanzar el equivalente funcional de la capa de red OSI (capa 3), facilitando el transporte de mensajes tanto orientados a conexión (circuito virtual) como aquellos sin conexión (datagramas).

La estructura del nivel SSCP provee 4 funcionalidades: servicio orientado a conexión, de control sin conexión, de gestión y de enrutamiento. De manera funcional junto con los servicios ofrecidos por el bloque TCAP (*Transaction Capabilities Application Part*), esta capa puede definirse de manera similar al nivel de transporte del modelo OSI. TCAP provee un mecanismo para aplicaciones orientadas a transacciones y se refiere al conjunto de protocolos y funciones utilizados por aplicaciones distribuidas en una red. TCAP se compone de dos subcapas: la subcapa de componente y la de transacción. La TCAP es usada para la integración de bases de datos, así como invocar funcionalidades avanzadas de la red o establecer enlaces con el INAP (*Intelligent Network Application Part*) para redes inteligentes o MAP (*Mobile Application Part*) para servicios móviles. El grupo de trabajo 3GPP (*3rd Generation Partnership Project*) ha integrado algunas funcionalidades al TCAP (*TCAPsec*), que proporciona integridad de datos, mecanismos de autentificación de los datos de origen y algunas funcionalidades de confidencialidad.

El bloque TUP (*Telephone User Part*), habilita las conexiones de red y provee servicios asociados con el inicio y terminación de llamadas con las redes telefónicas PSTN (*Public Switched Telephone Transport Network*). El bloque ISUP (*ISDN User Part*) representa la parte clave para el usuario, proveyendo los protocolos para el establecimiento, mantenimiento y terminación de las conexiones para las llamadas.

El bloque de aplicaciones móviles MAP (*Mobile Application Part*) incluye funcionalidades como el handover suave, gestión de la movilidad, servicio de mensajería, y servicios de geolocalización entre otros. Este bloque obtiene su información a través de los elementos que componen al sistema de

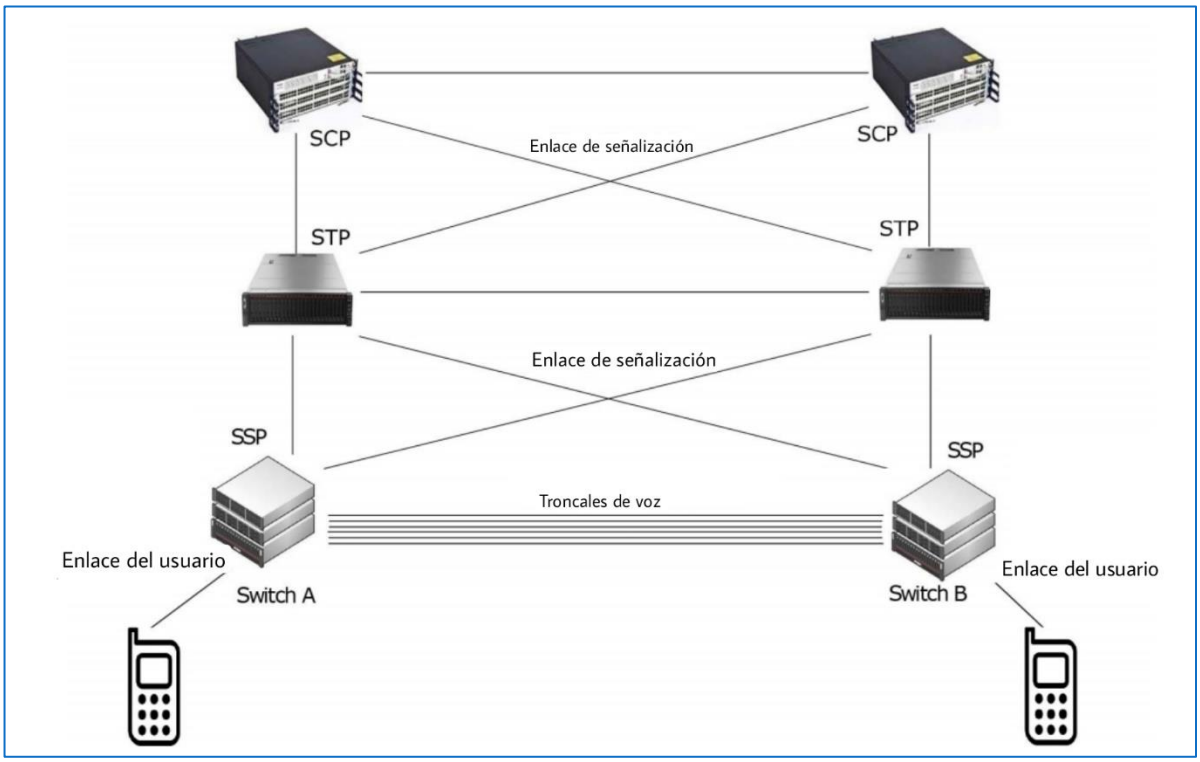
telefonía móvil. El objetivo primordial del MAP es permitir la comunicación entre diferentes bases de datos de los usuarios móviles y centros de conmutación, posibilitando la gestión de los servicios de localización. El 3GPP también ha lanzado actualizaciones para el MAP (*MAPsec*), sobre todo para temas de seguridad y prestaciones en la capa de red para redes IP.

El protocolo de señalización SS7 fue diseñado inicialmente para gestionar el inicio y terminación de las llamadas. La evolución de las redes de telecomunicaciones y la interconectividad con redes que operan bajo diferentes señalizaciones y prestaciones, ha ocasionado que las funcionalidades definidas inicialmente para el SS7 hayan evolucionado también. Entre estas podemos mencionar las siguientes:

- Posibilita la comunicación entre diferentes núcleos de red para el ruteo de las llamadas
- Soporta el mecanismo de *handover*, permitiendo el cambio del usuario móvil entre diferentes radio bases
- Provee prestaciones y facilidad para la ejecución del roaming
- Es usado para la generación de información para servicios de facturación
- Permite la generación y distribución de SMS (*Short Message Service*)
- Provee facilidades que permiten la geolocalización para servicios de emergencia
- Permite la implementación de servicios de llamadas sin costo para entidades gubernamentales y organizaciones privadas
- Permite algunos servicios adicionales como enlaces de llamadas y el despliegue del número telefónico en una llamada entrante

Los elementos funcionales que integran el protocolo SS7 se muestran en la Gráfica 5 [Ullah. (2020)].

Gráfica 5. Bloques funcionales de protocolo SS7 [Ullah. (2020)].

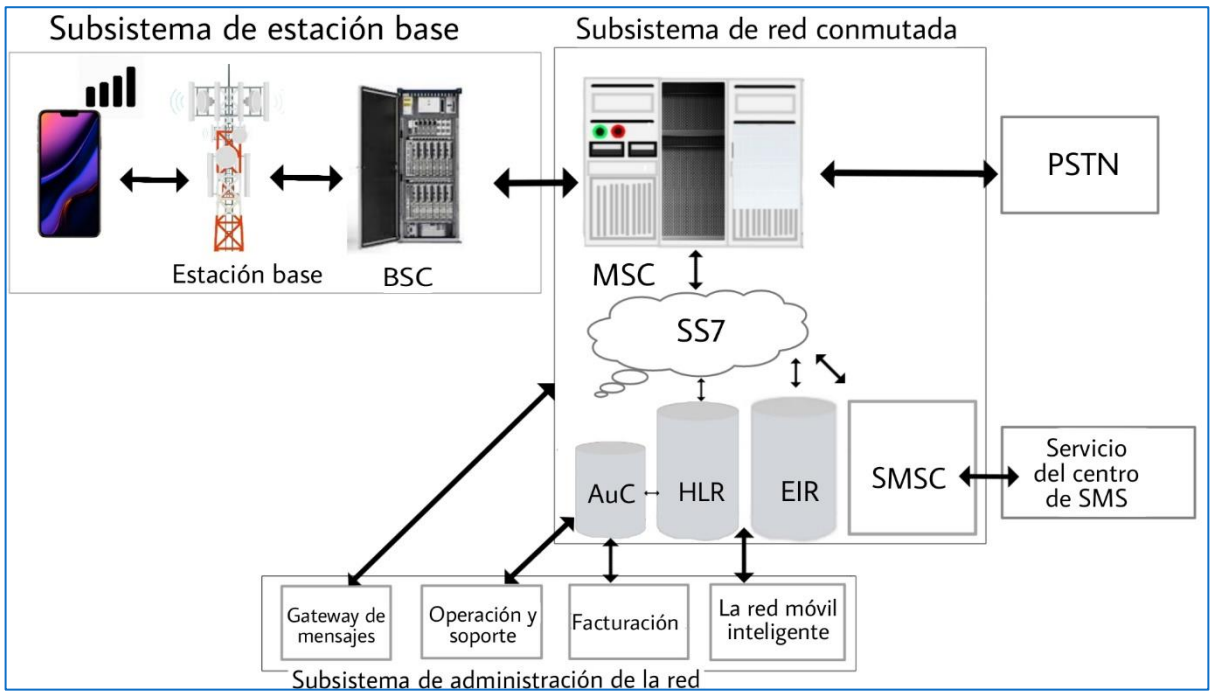


La Gráfica 5 muestra los componentes funcionales, así como el flujo de información en el núcleo de una red de telecomunicaciones móviles que hace uso del protocolo SS7. Al inicio de una llamada, por medio del enlace del suscriptor el dispositivo móvil se comunica con el *switch*, que es el punto de entrada a la red, donde los enlaces de señalización son usados para transportar información de los enlaces y de los usuarios entre los diferentes elementos que integran la red. Los enlaces troncales de voz son los que transportan la información de los servicios de voz de los usuarios, una vez que la llamada ha sido establecida.

El protocolo SS7posee puntos de señalización básicos que permiten la gestión de la señalización en la red. Los SSP (*Service Switching Points*) tiene como función principal iniciar una llamada cuando el usuario realiza la marcación desde su equipo, así como también gestionar la finalización de esta. También provee el tono de disponibilidad de la red (*dialling*) y convierte los números marcados en códigos que son compartidos con los otros elementos de la red. Los puntos de transferencia STP (*Signal Transfer Points*) gestionan el ruteo de las llamadas recibidas por los SSPs hacia todos los STPs, lo que permite enlazar la llamada hasta su destino final. Los puntos de control de la señalización SCP, (*Signal Control Points*), insertan algoritmos de decisión a la red SS7 y proveen algunas funcionalidades adicionales, indicando a los SSPs el mecanismo de ruteo de las llamadas, decidiendo si estas proceden o no.

En la Gráfica 6 se muestra el esquema general de una red GSM, indicando algunos de los elementos que la integran, los sistemas y subsistemas más relevantes, así como un indicativo de la función de enlace y comunicación que desempeña el SS7 dentro del sistema.

Gráfica 6. Bloques funcionales de una red GSM. [Ullah. (2020)].



Para el caso de una red GSM que hace uso del SS7, uno de los componentes más relevantes que hace uso del SS7 para gestionar su operación se puede identificar al Centro de Conmutación Móvil MSC, (*Mobile Switching Center*) que comunica la red móvil con la red fija, proporcionando el ruteo de las llamadas, servicios de mensajería, así como la gestión para el cambio de conexión del usuario entre diferentes MSCs (definido como handover suave). Otro elemento de la red GSM que es parte importe en la gestión de la información que usa el SS7 es el HLR (*Home Location Register*), que almacena la información relativa a la posición geográfica de un usuario, de modo que las llamadas puedan ser direccionadas directamente al destino solicitado. Así mismo, incluye información del suscriptor relativa a las llamadas realizadas y las prestaciones, facilidades y servicios a los que tiene acceso. El HLR es una base de datos que administra mucha de la información sensible de los subscriptores, así como también provee los datos necesarios para la realización de funciones y operaciones fundamentales dentro de la red.

El AuC es el centro de identificación y verificación del usuario, que es consultado y validado previo a otorgarle los permisos de acceso a la red. Esta unidad almacena claves y configuraciones personales del usuario. Así mismo, genera llaves y algoritmos usados para la encriptación del tráfico durante una

conexión. Por otro parte, el VLR (*Visitor Location Register*) posee una copia de la información almacenada por el HLR de los usuarios que están conectados a una particular MSC, de modo que esta no necesita realizar requerimiento al HLR cada vez que un determinado usuario solicite un servicio.

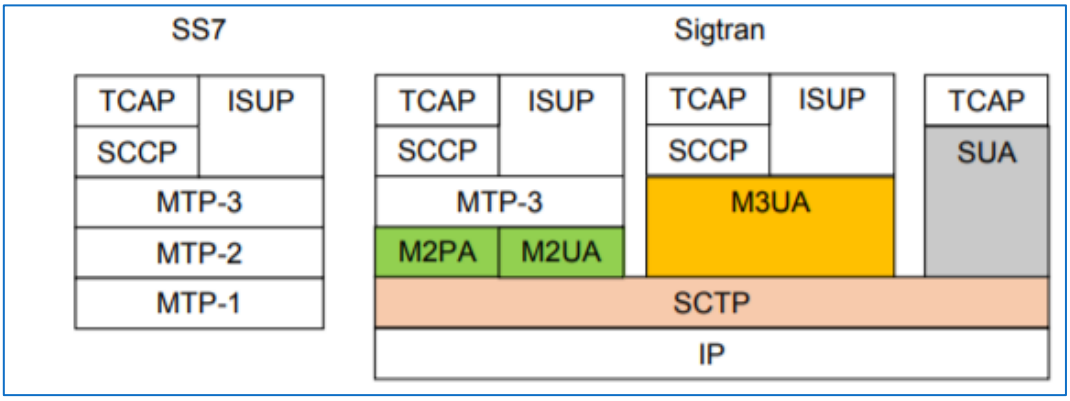
Cada dispositivo conectado a la red es identificado por un código definido como IMEI (*International Mobile Equipment Identity*). En una red GSM, el EIR (*Equipment Identity Register*) es el encargado de almacenar aquellos IMEIs que pueden acceder a la red y las condiciones para ello. Cuando un dispositivo es reportado como robado, este se integrará a lo que se conoce como la lista negra de modo que el IMEI correspondiente no podrá acceder a la red. El SMSC (*Short Message Service Center*) se encarga de llevar a cabo el ruteo de los SMS hacia su destinatario, comunicándose con el HLR para solicitarle la posición de este.

Como se ha descrito, la información relativa a la identificación, posición y prestaciones de un subscriptor conectado a una red GSM es gestionado por medio del SS7. La vulnerabilidad de este protocolo incrementa el riego de exponer la información necesaria para la ejecución de ataques y fraudes no solo a los sistemas GSM, sino a cualquier dispositivo, servidor o equipo, conectado a internet, incluidas las redes IP.

SIGTRAN

Como ya se mencionó, este protocolo se introdujo para soportar el transporte de datos por IP, y permite traducir o transportar mensajes MTP del SS7 en mensajes IP. Esto se lleva a cabo en los gateways de señalización, que permiten comunicar sistemas digitales TDM de SS7 con sistemas que hacen uso de paquetes IP. El modelo de capas de SIGTRAN se corresponde con las capas del SS7, brindando a las capas superiores los mismos servicios que se brindan en SS7. Gráfica 7.

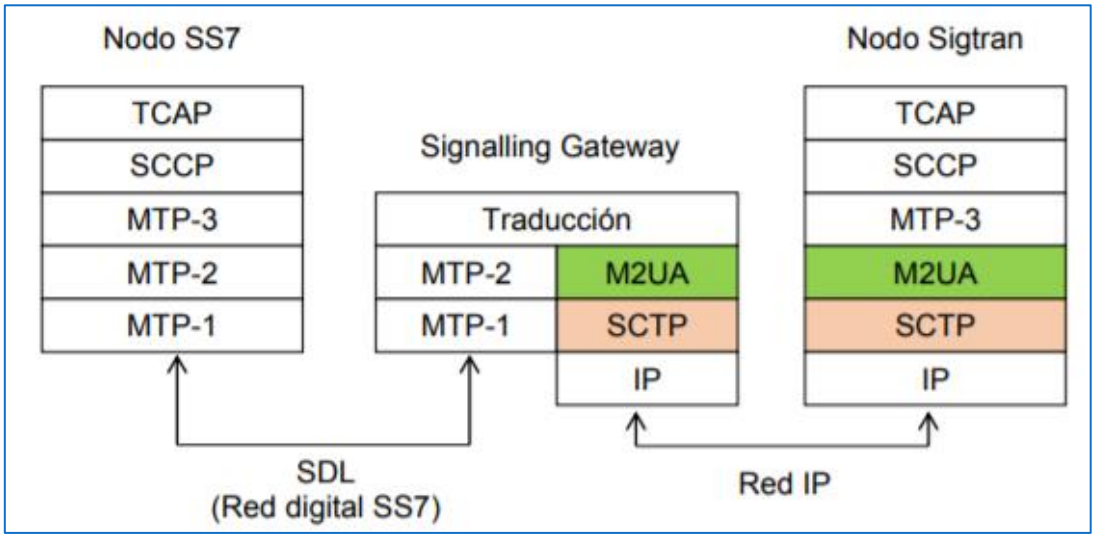
Gráfica 7. Modelo de SIGTRAN en correspondencia con SS7 (tomado de Joscowicz(2017))



El nivel 1 de MTP se reemplaza en SIGTRAN por el protocolo SCTP/IP (*Stream Control Transmission Protocol*), que oferta cierta ventajas sobre los protocolos tradicionales como TCP y UDP, haciéndolo

mas adecuado para transportar mensajes de señalización SS7. El nivel 2 de MTP se reemplaza en SIGTRAN por las capas M2UA (*MTP-2 User Adaptation*) o por el M2PA (*MTP-2 Peer to peer Adaptation Layer*). M2UA adapta la capa superior (MTP-3) directamente al protocolo SCTP, y permite el intercambio de mensajes punto a punto entre pares MTP-3 que pueden estar en nodos SS7 o SIGTRAN. La interconexión del Gateway de señalización que permite la interconexión entre la red digital TDM y la red IP se muestra en la Gráfica 8.

Gráfica 8. Interconexión SS7-SIGTRAN (tomado de Joscowicz(2017))



Así mismo, la capa M2UA es un Gateway a nivel MTP-2, entre un nodo SS7 y otro SIGTRAN y no cuenta con una dirección SS7 ya que no implementa las funciones completas de MTP-3, contrario al caso de la capa M2PA que constituye un nodo SS7, y por lo tanto si cuenta con una dirección SS7. El nivel 3 de MTP se reemplaza en SIGTRAN por la capa M3UA (*MTP-3 User Adaption*), que posee una dirección SS7 y su función es la de rutear los mensajes hacia nodos SIGTRAN que están conectados a la red.

DIAMETER

En lo que respecta al protocolo Diameter, este es usado para establecer la comunicación entre los componentes de la SAE (*System Architecture Evolution*), que se constituye como la parte medular de las redes que operan bajo el estándar LTE (*Long Term Evolution*). Dentro de la estructura del SAE, el componente principal es el EPC (*Evolved Packet Core*).

Los protocolos NAS (*Non Access Stratum*) constituyen el nivel más alto del plano de control entre el equipo del usuario final (*UE*) y el MME (*Mobility Management Entity*), soportando la movilidad del UE y los procedimientos de gestión de las sesiones para establecer y mantener conectividad IP entre

el usuario y el gateway de la red digital de paquetes, PND. Así mismo, define las reglas durante los escenarios de movilidad entre redes 3G y redes de otro tipo, proporcionan esquemas y medidas de seguridad y cifrado a la información transferida. Adicional al protocolo MME, las transacciones del protocolo NAS consisten en la integración y desarrollo de procedimientos basadas en los protocolos específicos para la operación de los gateway de los servidores (*SGW, Serving Gateway*) y los gateways de la red de paquetes de datos (*PGW, Packet Data Network Gateway*) [FIGI, (2020)].

Diameter es un protocolo diseñado para suministrar servicios conocidos como AAA (*Authentication, Authorization, Accounting*) para aplicaciones que involucran acceso a redes o aplicaciones con usuarios móviles. El acceso se lleva a cabo mediante un nombre de usuario y contraseña, y la validación del mismo se realiza con un servidor, donde se comprueba que la información es correcta por medio del uso de esquemas de autentificación como PAP (*Password Authentication Protocol*, CHAO (*Challenge Handshake Authentication Protocol*) o EAP (*Extensible Authentication Protocol*) [11].

DIAMETER ofrece mejoras sustanciales a su predecesor RADIUS[12], donde se pueden destacar las siguientes: una mayor confiabilidad en la capa de transporte haciendo uso de TCP o SCTP, ofrece mecanismos de fail-over, por medio del manejo de acuses de recibo (ACKs) a nivel de capa de aplicación, uso de agentes para enrutar los mensajes de otros nodos hacia su destino, en función de la información que contiene el mensaje y las tablas de enrutamiento, para modificar los mensajes con el objeto de implementar la aplicación de ciertas políticas y para su uso en escenarios donde la configuración de enrutamiento esta centralizada, entre otras funcionalidades.

Como ya se mencionó, DIAMETER es un protocolo basado en mensajes, donde la información se intercambia con base a transacciones del tipo cliente-servidor entre cliente y servidor. La definición base del protocolo tiene pocos comandos (*Command codes*), pero permite extenderlos según las necesidades de cada aplicación.

Protocolo GTP

Para el caso de las redes 4G y 5G se hace uso de un conjunto de protocolos basados sobre IP, que se utiliza para transportar servicios generales de radio por paquetes GPRS (*General Packet Radio Services*) dentro de las redes GSM, UMTS y LTE. Este protocolo se conoce como GTP (*GPRS Tunnelling Protocol*) de túnel GPRS. No obstante que presenta mejoras sustanciales respecto a sus predecesores que operan en redes previas, también presenta algunas vulnerabilidades sobre todo en lo relativo a la información sobre la localización del usuario.

[11] Protocolos de autentificación. https://workos.com/blog/authentication-protocols-your-guide-to-the-basics

[12] How Does RADIUS Work? Cisco. https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Los protocolos que contempla el GTP son el GTP-C, GTP-U y GTP'. El primero se utiliza dentro de la red central GPRS para la señalización entre los nodos de soporte GPRS de puerta de enlace de GGSN y los nodos de soporte GPRS (SGSN). Esto permite al SGSN activar una sesión en nombre de un usuario mediante la activación de contexto PDP (*Packet Data Protocol*), desactivar o actualizar una sesión para un usuario de recién ingreso. El GTP-U se utiliza para transportar datos de usuario dentro de la red central GPRS y entre la red de acceso de radio y la red central. Los datos de los usuarios pueden ser transportados en formatos IPv4, IPv6 o PPP[13]. Para la GTP' se utiliza la misma estructura de mensaje que el GTP-C Y GTP-U, y se puede utilizar para transportar datos de carga desde la función de datos de carga CDF[14] (*Charging Data Function*) de la red GSM o UMTS a la función de puerta de enlace de carga o CGF (*Charging Gateway Funtion*).

En la actualidad no existen planes o acciones encaminadas a dejar de usar el SS7 en las redes 2G y 3G, o sustituirlo por algún otro protocolo más eficiente en términos de seguridad y protección de la información. Adicionalmente, y no obstante que las redes 5G y las de nueva generación pudieran ofrecer nuevas y mejores herramientas para combatir las vulnerabilidades de las redes, el punto más débil al parecer se encuentra en las redes que operan con el protocolo SS7, significándose como el punto de entrada más usado y con mayor éxito por parte de los atacantes, de acuerdo con las estadísticas mostradas en el Capítulo I.

Considerando el proceso de evolución de las redes móviles operando con los primeros estándares digitales como GSM/UMTS hacia estándares como LTE y redes 5G, se plantea una primer interrogante, ¿es conveniente transformar/modificar/actualizar protocolos como el SS7, o lo mejor será diseñar un protocolo nuevo basado en las nuevas tecnologías (Inteligencia Artificial, Machine Learning, etc.) que este en mejores condiciones de responder a las demandas planteadas por las necesidades de las redes actuales y futuras? El problema no es menor, ya que, de acuerdo con la ITU en el 2020 en el mundo había un promedio de poco más 900 mil millones de personas que aún hacían uso del protocolo SS7, aproximadamente el 15% de la población con acceso a una red de banda ancha móvil, habiendo regiones como África donde el porcentaje de usuarios puede alcanzar el 55% [(ITU. (2021)). Mientras los operadores no migren sus redes 2G/3G a redes 4G/5G, el uso del SS7 continuará, y las redes 4G/5G que implementen nuevos mecanismos de señalización deberán también considerar la compatibilidad con el SS7 debido a la coexistencia con redes previas. De acuerdo con [Ullah. (2020)], hasta el 2020, los usuarios de telefonía 2G era más del 60% en países del sur de Asia, más del 40% en África, más del 50% en el oeste de Asia y en Europa del este. De este

[13] PPP es un protocolo creado por la IETF para transmitir datos que contengan más de un protocolo de red sobre mismo enlace punto a punto. https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/ppp_feature_overview_guide.pdf

[14] CDF y CGT son especificaciones técnicas que especifica funcionalidades para la trasferencia de datos en redes 3GPP (GSM, UMTS,EPS). https://www.etsi.org/deliver/etsi_TS/132200_132299/132297/15.01.00_60/ts_132297v150100p.pdf

modo, es de esperarse que el SS7 permanecerá presente por varios años más, lo que plantea la necesidad de acciones que permitan reducir los riegos de su uso.

IV. Vulnerabilidades. Perfil de ataques

En las redes que operan haciendo uso de H.323 y protocolos similares que operan sobre IP una de las principales vulnerabilidades se identifica en las fallas de configuración en algunos teléfonos IP, lo que permite que por medio de algunas herramientas de software disponibles en el mercado sea viable la extracción del tráfico de una conversación que cursa por la red, posibilitando que el archivo de audio extraído pueda grabarse, escucharse y manipularse. Estas escuchas o intervenciones ilegales puede presentarse cuando el protocolo de transmisión que lleva a cabo la transmisión de voz carece de cifrado o codificación, que se presenta cuando solo se usa RTP como capa de transmisión multimedia. Existe una alternativa que es una versión mejorada conocida como SRTP[15] que incluye estrategias de cifrado y autentificación que mejoran sustancialmente la seguridad de las llamadas. Sin embargo, vulnerabilidades adicionales se puede presentar en algunos dispositivos móviles con algún puerto abierto, que varias aplicaciones instaladas en el equipo pueden usar con el fin de recabar estadísticas, información o llevar a cabo configuraciones o mantenimiento remoto. Esto puerto pueden ser una entrada para potenciales ataques.

Uno de los ataques más comunes en redes IP es la que se conoce como de repetición, y su fin es el de secuestrar la información de registro del usuario. El protocolo SIP emplea un comando de registro para indicar al software de gestión de llamadas dónde se encuentra un usuario en función de su dirección IP. El atacante puede reproducir esta solicitud y sustituir la dirección IP original por otra, para desviar todas las llamadas a esta. Muchos de los ataques de repetición se producen porque hay partes del protocolo SIP que se comunican en texto normal. Existen protocolos SIP que operan sobre TLS[16] (SIPS), proporcionando una mayor integridad y procesos de autentificación.

La denegación de servicio se puede presentar en redes IP por medio de la orquestación del envío de una enorme cantidad de tráfico (lo que se conoce como flooding), enviando masivas invitaciones para iniciar una conversación. Esto se hace muchas veces con fines de extorsión.

Existen algunas otras vulnerabilidades de los equipos que operan sobre IP que están relacionadas con otros factores diferentes al protocolo (como el acceso a páginas web, fraudes telefónicos, etc.), que no son el objeto de este análisis.

Para el caso de redes 4G y 5G, una de las principales vulnerabilidades se presenta en el protocolo GTP usado. Por medio de la corrupción de este, el usuario puede interferir el equipo de red (un nodo

[15] The Secure Real-time Transport Protocol (SRTP). (SRTP: el protocolo seguro de transmisión en tiempo real), ETF. http://tools.ietf.org/html/rfc3711

[16] Seguridad en capas de transporte. Protocolo que incluye métodos de criptografía. https://datatracker.ietf.org/doc/html/rfc5246

de soporte) y deshabilitar el acceso a una zona geográfica determinada, o en el caso de un ataque a un usuario, puede suplantar su identidad y acceder a diversos recursos y hacer uso los servicios de la red con cargo al usuario o burlando el cargo por parte del operador. Este ataque puede gestarse desde un equipo terminal móvil. Esto se debe a que la parte central de las plataformas de red 5G (*core network*) define su evolución e interconexión desde 4G EPC[17], por lo que varias de las vulnerabilidades de 4G se pueden transferir a las redes 5G. De este modo, los operadores móviles están expuestos a las vulnerabilidades de GTP, posibilitando ataques como denegación de servicio, suplantaciones y fraudes.

Una de las principales fallas reportadas para el protocolo GTP es el proceso para la verificación de la ubicación del usuario, de modo que un atacante puede enviar tráfico gestionando un ataque y el operador pudiera tener problemas para identificar su legitimidad. Un atacante puede robar también el perfil de identificación de un usuario accediendo al Gateway de interconexión.

De acuerdo con lo expuesto, podemos inferir que los protocolos diseñados para las redes más recientes sean más seguros y con mayores capacidades y recursos para mitigar ataques, disminuir las vulnerabilidades, así como brindar una mayor seguridad a la información. De este modo, el análisis se centra en lo que consideramos el punto de acceso a la red más expuesto a un ataque: redes operando con el SS7.

Para el caso de las redes 2G/3G el primer obstáculo para materializar los riesgos que una red de telecomunicaciones que opera bajo el protocolo SS7, es precisamente lograr el acceso a la red. Esta aparente obviedad también brinda una primera oportunidad para la implementación de acciones preventivas para futuros ataques. Se han identificado varios vectores de ataque que pueden ser utilizados por los ciberdelincuentes para lograr este acceso. Las condiciones descritas aplican de igual manera a Diameter, ya que en términos de seguridad presenta prácticamente las mismas condiciones generales que el SS7.

Algunos de los potenciales puntos de entrada a una red SS7 (y con ello estar en condiciones de acceder a cualquier otro punto conectado a internet) pueden ser los siguientes.

- Mercado negro. Desafortunadamente existe un mercado ilegal donde el acceso a redes SS7 puede ser adquirido. Estas empresas en su mayoría están integradas por hackers experimentados.
- Aprovechando la interconexión de las redes a nivel mundial, si un operador sufre un ataque exitoso que comprometa la integridad de su red, automáticamente el hipotético atacante,

[17] 4G EPC es una red 4G LTE que cuenta con la capacidad de gestionar paquetes de voz y datos sobre el protocolo IP. https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core

con una solo tarjeta SIM, puede tener acceso a cualquier otra red en el mundo que se encuentre conectada a internet.

- Fallas en la configuración de los equipos de una red. Por medio del uso de protocolo como SIGTRAN (*Signaling Transport*), SCTP (*Session Control Transmmision Protocol*) y *Session Initiating* es viable el envío masivo de mensajes SS7 por medio de internet, con el objeto de detectar posibles entradas en las redes debido a fallas en la configuración de estas.
- Aprovechar las vulnerabilidades que algunos dispositivos conectados a una femtocelda presentan. Si el operador despliega este tipo de redes, desde cualquier dispositivo conectado a este tipo de redes se puede acceder a la red SS7.
- Bloques funcionales de redes implementadas de manera distribuida en diferentes localizaciones. La comunicación remota entre estas entidades, combinado con bajos niveles de seguridad en el transporte de la información entre estas, puede elevar la vulnerabilidad de la red.
- Uso de Sistemas de Soporte de Operaciones (OSS) automático. El sistema OSS normalmente esta integrado por computadoras que de manera automática realizan tareas de gestión, resolución de problemas y la implementación de soluciones innovadoras. Estas computadoras podrían ser atacadas y/o vulneradas por medio de algún virus, o por el uso de puertas traseras de los dispositivos, envío de troyanos, etc., afectando la operación y seguridad de la red.
- Aprovechar la señalización de los gateways. Los gateways pueden interconectar diferentes protocolos (SS7, conexiones IP). Las redes IP presentan varias vulnerabilidades que pueden ser aprovechadas para comprometer la operación de los gateways.
- Portabilidad de números locales. Esta portabilidad es provista por medio de alguna interface de aplicación (API), que podría presentar poca resistencia ciertos ataques. Estas APIs poseen información relevante del suscriptor.

Adicionalmente, no debe dejarse de lado escenarios donde el acceso a las redes SS7 pueden ser ocasionadas por fugas de información del personal mismo de las empresas, fortuitas, por malas prácticas o en ocasiones por acciones mal intencionadas.

Una vez que un intruso se encuentra dentro de la red SS7, este puede aprovechar las vulnerabilidades del protocolo para realizar diferentes tipos de ataques, sobre todo considerando que internamente una red SS7 prácticamente no contempla mecanismos de autentificación para el intercambio de información entre los bloques funcionales del núcleo de la red. Estos ataques pueden estar basados en la capacidad de acceso a cada uno de los bloques del núcleo de red que almacenan y manejan la información de los suscriptores, y se llevan a cabo enviando mensajes falsos de acceso o solicitud a dichos bloques. Así mismo, el intruso puede suplantar la identidad de algunos de los bloques de la red y con esto obtener el perfil del suscriptor del suscriptor, los identificadores que usan los operadores para identificar destinos de las llamadas (y con esto hacer cargos por roaming cuando aplica), localización del suscriptor, autorizaciones para iniciar procedimientos, etc.

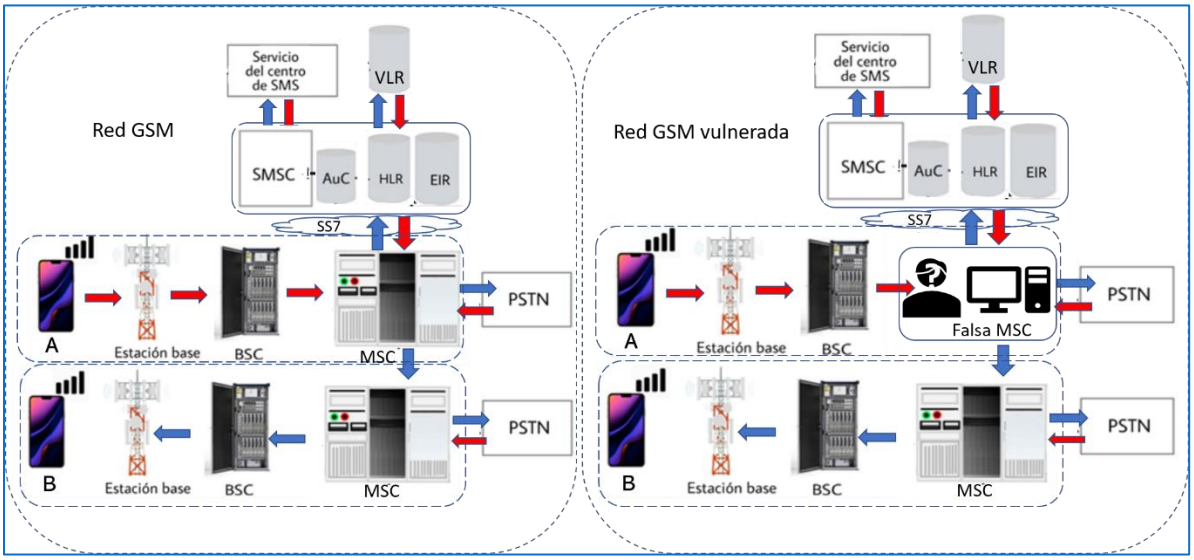
De este modo, una vez que un atacante se ha introducido al sistema, obtener información de algún subscriptor se puede limitar a suplantar a alguno de lo elementos que forman el núcleo de la red, y haciendo uso de los comandos y parámetros adecuados, hacer la solicitud de la información a la base de datos del sistema, normalmente el HLR o VLR. La falta de mecanismos de validación/verificación interna hace que operaciones como la descrita puede realizarse con altas probabilidades de éxito. De este modo, las vulnerabilidades del SS7 pueden materializarse en ataques que pueden seguir algunas de las vertientes siguientes:

Seguimiento de la geolocalización del usuario.

La geolocalización de los subscriptores es información que los operadores utilizan para que el sistema pueda enrutar cualquier mensaje o llamada al destinatario correcto. El usuario puede estar conectado a la red de la cual es subscriptor (red doméstica) o haciendo uso de cualquier otra con la que su operador tenga acuerdos de roaming (red visitada). En ambos casos, el intercambio de información y datos entre el dispositivo y los componentes de la red incluyen el perfil del usuario. Esta es información de interés para un hacker.

En la Gráfica 9 se muestra el flujo de datos en el núcleo de una red GSM cuando un usuario A desea comunicarse con el usuario B, así como el escenario cuando un intruso suplanta la identidad de la MSC. Bajo condiciones de operación normal, el fujo de la información es el siguiente: el suscriptor A se comunica con la Central de Conmutación Móvil (MSC) a través de la radio base (BSC) que brinda cobertura en su posición geográfica. La MSC requiere la dirección hacia donde la llamada o mensaje debe ser ruteado. Para ello, solicita al Registro Local de Localización del operador HLR la identificación GT (*Globlal Title*) de la MSC que corresponde al usuario B; así mismo el HLR puede proporcionarle el IMSI (*International Mobile Subscriber Identity*) del usuario B. Si el suscriptor B esta fuera de la red doméstica (condición de roaming), el HLR solicita al VLR el número de roaming (un número temporal que se proporciona al usuario cuando se encuentra conectado fuera la red de su operador). De este modo el VLR le proporciona al HLR el número de roaming de la estación móvil (MSRN, *mobile station roaming number*), así como la IMSI del suscriptor. El HLR le envía esta información a la MSC y entonces la llamada puede ser cursada a través de la radio base que brinda la cobertura al usuario B. La comunicación entre los elementos anteriormente descritos se lleva a cabo usando el SS7. Cuando un intruso ha penetrado a la red del operador, puede suplantar a la MSC y solicitarle la información directamente al HLR, teniendo acceso al perfil completo del subscriptor, así como información relativa a los códigos de roaming que el operador utiliza para realizar los cobros, los códigos móviles del país (MCC, *Mobile Country Code*), así como los códigos de área con los que se incrementa la precisión de la localización del suscriptor. Un flujo similar de información y el esquema de intrusión mostrado es similar cuando se hace el envío de SMS por la red, ya que la información relativa a estos es procesada y reenviada también por la MSC, dando como resultado que el intruso también pueda acceder a los mensajes enviados.

Gráfica 9. Proceso de llamada en el núcleo de una red GSM.

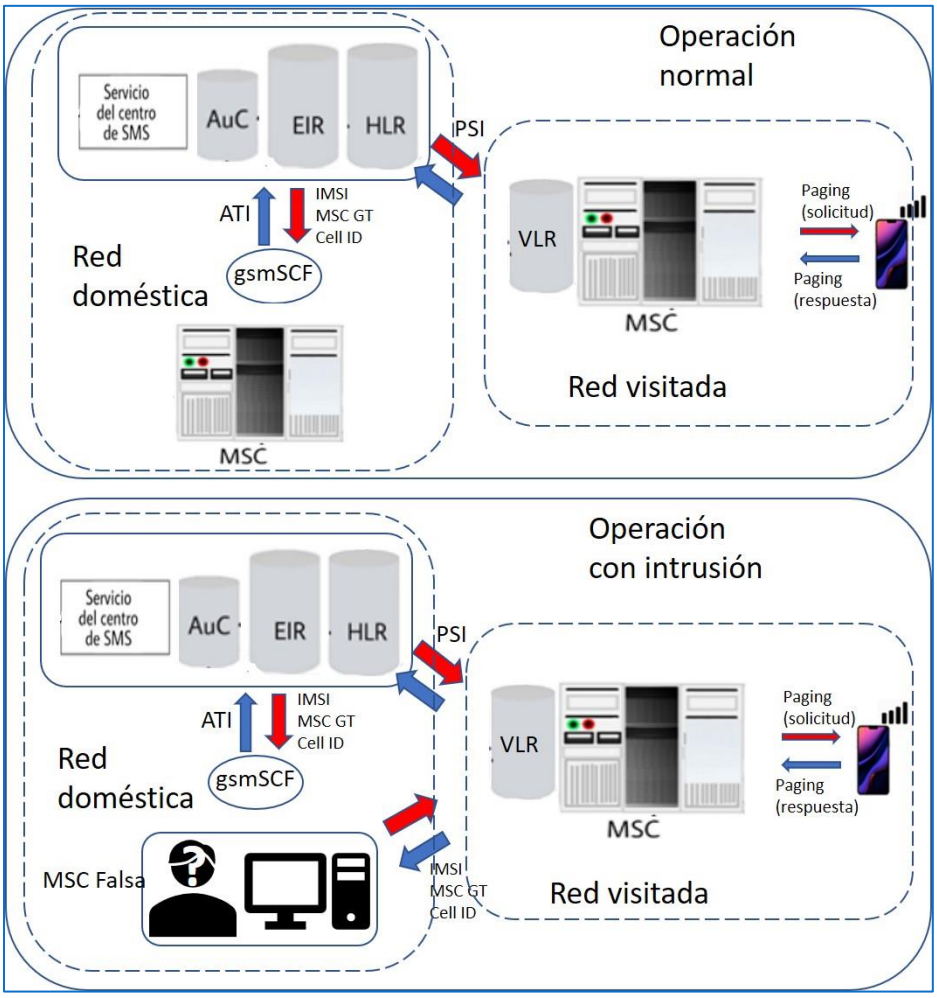


Una de las condiciones relevantes de las situaciones descritas es el hecho de que el SS7 no posee un proceso de autentificación de acceso interno que permita, para el caso particular de las llamadas y servicio SMS, llevar algún proceso de validación de la información que el HLR recibe del MSC.

Cuando se combinan las prestaciones que el sistema de SMS brinda, con los servicios de localización que algunas aplicaciones instaladas en los equipos móviles utilizan, un hacker puede acceder a la localización precisa del usuario en cualquier momento. Algunos servicios de los operadores pueden hacer uso de mensajes CAMEL (*Customized Application for Mobile Networks Enhanced Logic*) para conocer la localización de un subscriptor para fines de gestión interna y proveer esta localización a ciertas aplicaciones que hacen uso de esta. Para ello se hace uso de mensajes conocidos como MAP ATI (*Mobile Application Part, Any Time Interrogation*). Como se indica en la Gráfica 10 Inicialmente el gsmSCF (*GSM Service Control Function*) envía un mensaje del tipo ATI al HLR conteniendo el MSISDN (*Mobile Subscriber ISDN*) de un subscriptor. Sin proceso de autentificación, el HLR recibe el mensaje y envía el MAP PSI (*MAP Provide Subscriber Information*) al VLR/MSC. El equipo responde el mensaje de paging con un mensaje PSI que contiene el IMSI y el ID de la celda donde el subscriptor esta localizado; de este modo el HLR ya cuenta con la información deseada, respondiendo por medio de un MAP ATI al gsmSCF con esta. El escenario donde esta funcionalidad es hackeada básicamente se conforma por medio de la suplantación de identidad del gsmSCF y establecer la comunicación con el HLR para acceder a la información. A partir de la obtención de la posición de un subscriptor el hacker puede iniciar diversos tipos de ataques, como se verá más adelante.

Debido a preocupaciones relativas a la seguridad y privacidad de la información, algunos operadores han prohibido el uso de comandos del tipo ATI. Sin embargo, si este tipo de comandos se encuentra bloqueado, el hacker procede a realizar la petición de manera directamente al HLR/MSC.

Gráfica 10. Obtención de la geolocalización.



Existen servicios de emergencia ofertados como parte fundamental del servicio otorgado, para los que es fundamental contar con información precisa de la localización de un usuario que realiza una llamada solicitando un servicio de este tipo, con el objeto de iniciar con la mayor celeridad posible las acciones de ayuda y atención. Básicamente esta geolocalización se lleva a cabo por medio de triangulación y/o señales GPS. En este proceso, los servicios de emergencia hacen uso de comandos tipo MAP LBS (MAP *Location Based Services*) desde el Gateway del Centro de Localización Móvil

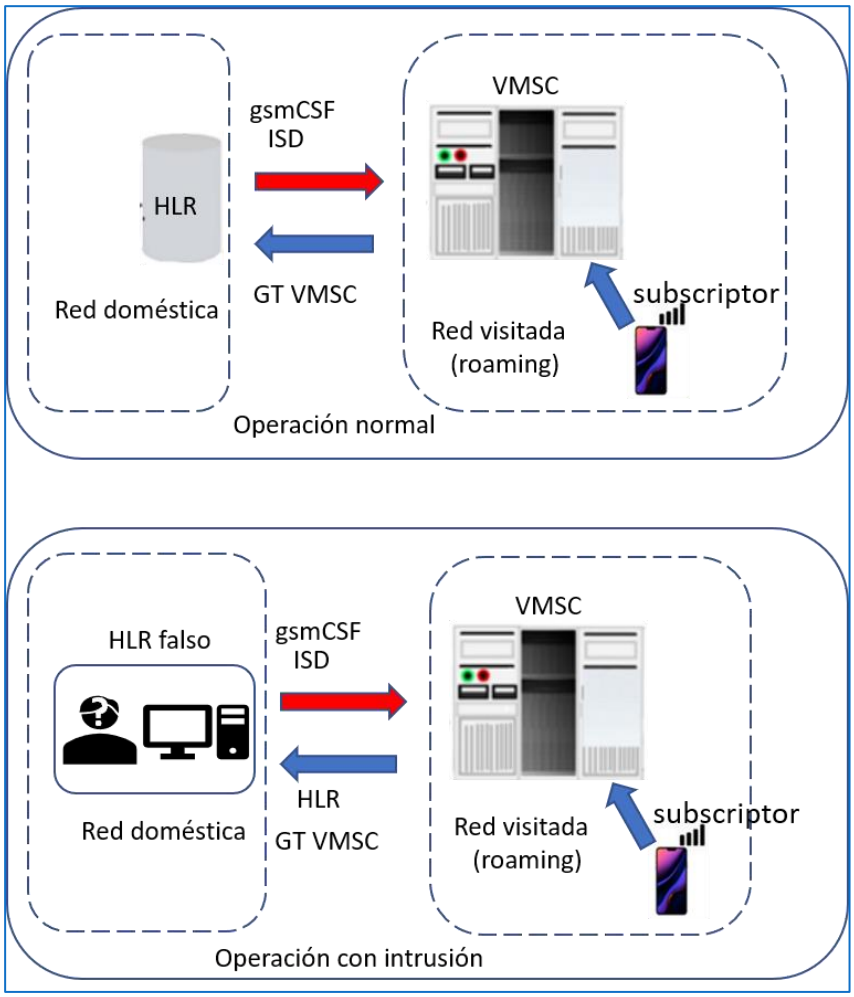
(GMLC). El proceso es similar a los procesos ya señalados, donde una de las principales diferencias es que el GMLC hace uso de un proceso de autentificación. Sin embargo, el proceso de evadir este mecanismo de validación se puede realizar solicitando previamente el MSISDN del usuario suplantando al SMSC (*SMS Center*), obteniendo con ello el IMSI y la dirección del MSC que proporciona el servicio al subscriptor de interés. Con esta información, el atacante puede suplantar al GMLC y de este modo obtener la información.

Modificación e intervención de llamadas

Los requerimientos de conectividad para un usuario en cualquier lugar del mundo haciendo uso de un único SIM (*Subscriber Identity Module*) ha impulsado el establecimiento de acuerdos de roaming entre diferentes operadores.

Cuando un usuario se encuentra fuera de su red doméstica, la continuidad de su conexión se basa en la correcta ejecución de los comandos y funcionalidades de los servicios de roaming. Este proceso se detalla en la Gráfica 9 (operación normal). En esta, el usuario se registra en el MSC para visitantes (VMSC). El VMSC envía un mensaje de solicitud de actualización de localización ULR (*Update Location Request*) al HLR, que contiene el GT de la VMSC además de algunos otros parámetros. Con esta información, las llamadas y mensajes pueden ser ruteados a través del VMSC identificada. Para ello, el HLR envía un mensaje ISD (*Insert Subscriber Data*) al VMSC, que contiene el perfil de información del subscriptor, detalles de seguridad y la dirección de su gmsCSF con una lista de eventos que serán reportados a la red de suscripción. Cuando el subscriptor realiza una llamada a su país de origen el VMSC solicita al gsmCFS del usuario en la red doméstica información referente a la llamada. Entonces el gsmCSF convierte el número local marcado a un formato internacional insertando el código del país e informando al VMSC que procese la llamada con el número modificado. Con esto el servicio de roaming ha sido completado. Sin embargo, La funcionalidad de roaming puede también ser aprovechada por un intruso presente dentro de la red y usarla para intervenir una llamada, entre otras cosas. Esto se muestra en la misma Gráfica 11 en la que se detalla la operación del servicio con intrusión. Una vez que el intruso ha obtenido tanto la dirección del MSC donde se encuentra el usuario, como su IMSI y el MSRN *(Mobile Station Roaming Number*), el atacante puede suplantar la identidad del HLR y enviar un mensaje ISD (*Insert Subscriber Data*) al VMSC con una lista de eventos y agregar direcciones de gsmCSF maliciosas a la que los eventos deberán ser reportados. Cuando el subscriptor hace una llamada sin hacer uso del código del país, este envía un mensaje IAM (*Initial Address Message*) al VMSC, que pasa esta solicitud al gsmCSF malicioso y el intruso cambia el número marcado por otro de su elección y regresa este número modificado al VMSC para que realice la llamada a este nuevo número. Este número controlado por el intruso puede permitirle intervenir la llamada, permitiéndole escuchar/grabar la llamada, entre otras posibilidades.

Gráfica 11. Intervención de llamadas.



Los servicios adicionales relacionados con las llamadas que el usuario recibe y que son ofrecidos por los operadores, como el redireccionamiento de llamadas a otro número o el despliegue del número del equipo donde se origina la llamada, contienen información que también puede ser usada por los hackers para redireccionar las llamadas a números de su elección.

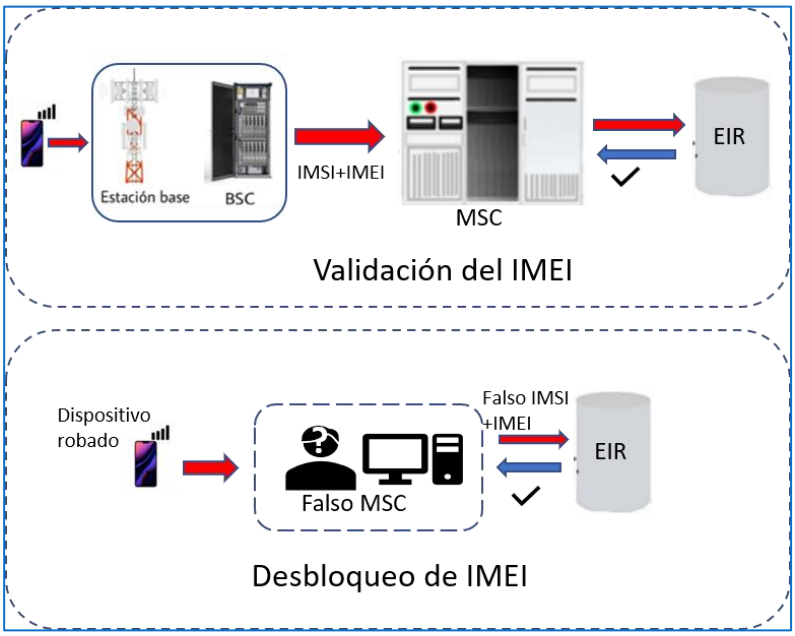
Aunque con un poco más de dificultad, un hacker puede interceptar llamadas a partir del tráfico de radio que se establece entre un usuario móvil y la antena de la radio base. Para ello, el intruso deberá estar en la vecindad del subscriptor. Esto se puede llevar a cabo cuando el equipo del usuario en movimiento, como consecuencia de su cambio de posición, inicia un proceso de solicitud de cambio de MSC. En este proceso de actualización, en la señal radio enviada y recibida desde la estación base están contenidas las instrucciones y direcciones para la nueva conexión. Esta información puede ser útil para intervenir la llamada.

Modificación e intervención de mensajes (SMS)

Los SMS son un recurso comúnmente usado como parte de los mecanismos de fortalecimiento de la seguridad de muchos servicios, incluidos los bancarios. La intercepción/modificación de estos mensajes aprovechando las vulnerabilidades del SS7 es uno de los principales vectores de ataque hoy en día.

Normalmente la intercepción de los SMS se lleva a cabo por medio de la suplantación de la identidad de un MSC, que gracias a la comunicación directa (y sin verificación) que puede tener con el HLR, puede acceder a la información necesaria para tomar el control del envío de estos mensajes. Esto permite, entre otras cosas, el envío masivo de mensajes de spam con fines comerciales, o la orquestación del envío masivo de mensajes cortos a un usuario, con el objeto de inhabilitar su operación. Uno de los usos más comunes y redituables para los delincuentes es el desbloqueo de equipos móviles reportados como robados. Esta práctica ilegal lamentablemente es común en muchos países, ofertando el desbloqueo de los equipos móviles de manera abierta y sin control. Como es sabido, los dispositivos móviles cuentan con un IMEI (*International Mobile Equipment Identity*) único, y los equipos reportados como robados se integran en lo que se conoce como la lista negra, con el objeto de que todos los operadores puedan verificar si los equipos que están accediendo a sus redes fueron adquiridos de manera legal por el usuario. Si el operador identifica que un dispositivo móvil con un IMEI que se encuentra en dicha lista intenta acceder a su red, inmediatamente quedará bloqueado su acceso. En la Gráfica 12 se muestra el proceso de identificación de los dispositivos móviles una vez que se conectan a la red y el mecanismo de desbloqueo ilegal basado en la suplantación del MSC.

Gráfica 12. Desbloqueo de un equipo móvil.

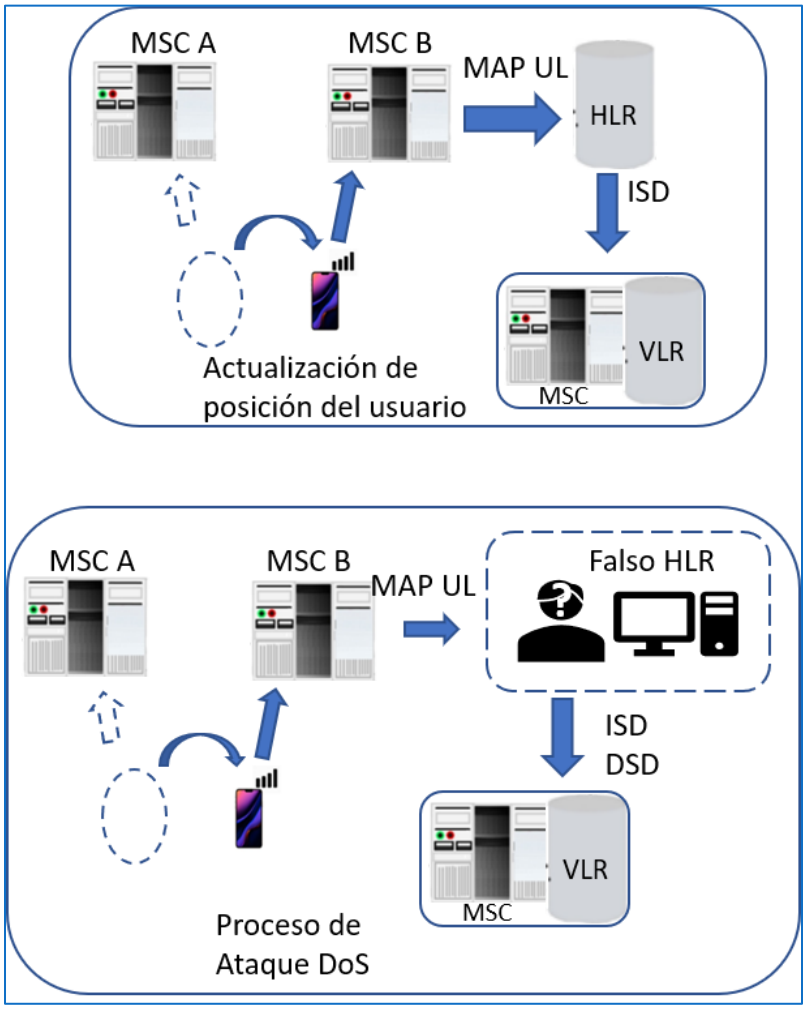


Cuando un equipo móvil se intenta conectar a la red, este se comunica por medio de una radio base a la MSC, enviando el identificador del equipo (IMEI), junto con el identificador del número telefónico (IMSI) del usuario que realiza la conexión. Como parte del proceso de validación y autorización del acceso a la red, el MSC envía esta información al EIR (*Equipment Indentity Register*) para verificar si el equipo (IMEI) tiene reporte de robo (lista negra). Si el IMEI no se encuentra en la lista negra, el EIR registra el IMEI y su IMSI asociado y lo valida para su acceso a la red, enviando este mensaje a la MSC. Cuando un equipo se intenta conectar haciendo uso de un nuevo número (IMSI), pero posee un IMEI que cuenta con un reporte de reporte de robo y que por lo tanto se encuentra en la lista negra, el HLR le envía la negativa de acceso al MSC y el operador de la red deshabilita su acceso a la red, de modo que el equipo con reporte de robo quedaría imposibilitado de conectarse a la red. No obstante, si el hacker suplanta la identidad de una MSC y envía una solicitud de verificación del IMEI con reporte de robo haciendo uso del número de identificación (IMSI) del usuario original (información falsa), el EIR detectará que el IMSI y el IMEI están nuevamente accediendo juntos a la red, y asume que el reporte de robo pudo haber sido un error o que el usuario original solo había extraviado su equipo y ya cuenta nuevamente con este, de modo que procede a sacar de la lista negra el IMEI reportado. Gráfica 10. Una vez conseguido esto, el hacker puede colocar otra tarjeta SIM al dispositivo (nuevo IMSI) y este accederá a la red sin inconvenientes.

Denegación de servicios (DoS)

Una de las vulnerabilidades más conocidas es la Denegación de Servicio DoS (*Denial of Service*). El objetivo de este tipo de ataques es bloquear el acceso a los servicios contratados por un subscriptor en particular. Este ataque hace uso de las señalizaciones que se envían por la red cuando un usuario cambia de una MCS a otra, como se indica en la Gráfica 13. Cuando esta funcionalidad se activa, la nueva MSC deberá enviar un mensaje de actualización de ubicación MAP UL, (*MAP Update Location*) al HLR. Una vez recibido el mensaje, el HLR comparte esta actualización con el MSC/VLR, enviando un mensaje ISD (*Insert Subscriber Data*); este mensaje, junto con el DSD (*Delete Subscriber Data*) son enviados también al MSC/VLR cuando el subscriptor cambia las condiciones de su paquete de servicios contratados. Estos mensajes contienen los detalles de las actividades y servicios a los que un usuario tiene acceso o no. Un potencial atacante puede alterar la información de estos mensajes para inhibir el acceso a casi cualquier servicio, suplantado la identidad del HLR y enviando información alterada al MSC/VLR. Cuando el atacante deshabilita todas las funcionalidades de comunicación del subscriptor queda imposibilitado de enviar/recibir notificaciones (DoS).

Gráfica 13. Denegación de servicio.



Gestión de mensajes en la red.

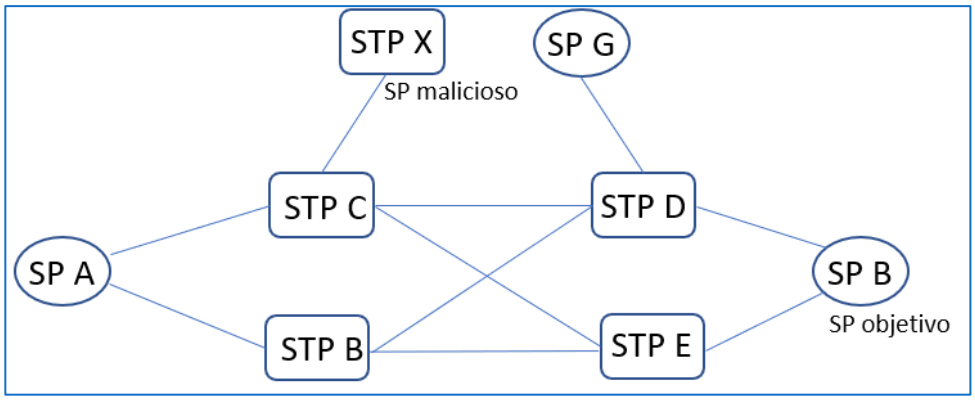
Como se mostró en la estructura del SS7, en la capa MTP 3 se gestiona el intercambio de mensajes entre dos puntos STP (*Service Transfer Point*). El objetivo es determinar el estado de una ruta determinada respecto a la no-disponibilidad/congestión que pudiera presentar. De los procedimientos usados para gestionar el tráfico de los mensajes, se destacan las vulnerabilidades de 2 en particular. Uno de ellos es el conocido como Procedimiento de Cambio (*Changeover Procedure)*. Este procedimiento se usa cuando alguno de los enlaces de señalización falla o no está disponible para señalización de tráfico, y es necesario redireccionar el tráfico hacia rutas alternas disponibles que permitan alcanzar el destino final. Los indicadores que permiten detectar estas fallas son: altas tasas de errores, retardos en la recepción de la confirmación de recepción de mensajes, congestión e indisponibilidad del equipo terminal. Cuando alguna de estas condiciones es detectada por uno de los SP conectados este procedimiento es activado, enviando un mensaje de este cambio a los otros

SP. El procedimiento de cómo esta funcionalidad puede ser aprovechada por un atacante se muestra en el esquema de la Gráfica 14. Suponiendo que un STP ha sido controlado por el atacante, este se encuentra en condiciones de enviar mensajes alterados al resto de los nodos. Suponiendo que hace el envío de un mensaje indicando el cambio de procedimiento al STP B suplantando a SP A utilizando la etiqueta de su ruta (esto es lo único que verificará el SP A para validar el mensaje), STP B asume que el mensaje es válido y detiene los mensajes de señalización por el link reportado como no disponible en el Procedimiento de Cambio. Si el atacante puede hacer el envío masivo a STP B en coordinación con otros nodos puede inhabilitar una gran cantidad de enlaces, ocasionando que los STPs busquen rutas alternas, ocasionando una degradación del rendimiento de la red y un mayor consumo de recursos.

Otro procedimiento es el conocido como TFP (*Transfer Prohibited Procedure*). Este se activa cuando un determinado destino no puede ser alcanzado por un STP, entonces este inicia un procedimiento de prohibición TFP, informando a SP adyacentes acerca de la no disponibilidad del mencionado destino, para que estos a su vez ya no hagan envíos a este. En la Gráfica 12 se muestra como un atacante puede hacer uso de este procedimiento para gestar ataques. En operación normal, el STP D tiene dos rutas para transferir mensajes a SP B. Si ambas rutas estuvieran inhabilitadas STD no podría enviar mensajes a SP B, de modo que STP D iniciaría un procedimiento TFP para notificar a STP adyacentes que SP B no esta disponible y que los mensajes ya no sean ruteados por él hacia SP B.

Si el atacante hace uso de este procedimiento para centrar su acción hace SP B podría proceder de la siguiente manera: el atacante controla el SPT X y envía un TFP falso a STP B suplantado a STP D, para que contenga la dirección de SP B como no disponible. Si el atacante puede enviar mensajes masivos e iniciar el mismo procedimiento con STP E, SP B quedará incomunicado, generando un *DoS* para SP B. Todo esto a partir de la suplantación de STP D.

Gráfica 14. Gestión del envío de mensajes.



Por medio de lo anteriormente descrito, un atacante puede tomar control de las bases de datos y el núcleo de la red, pudiendo comprometer personas, bienes e infraestructura. Por ejemplo, puede

alterar una base de datos y generar el envío masivo de mensajes de emergencia o notificación de desastres, pudiendo generar caos y confusión entre la población.

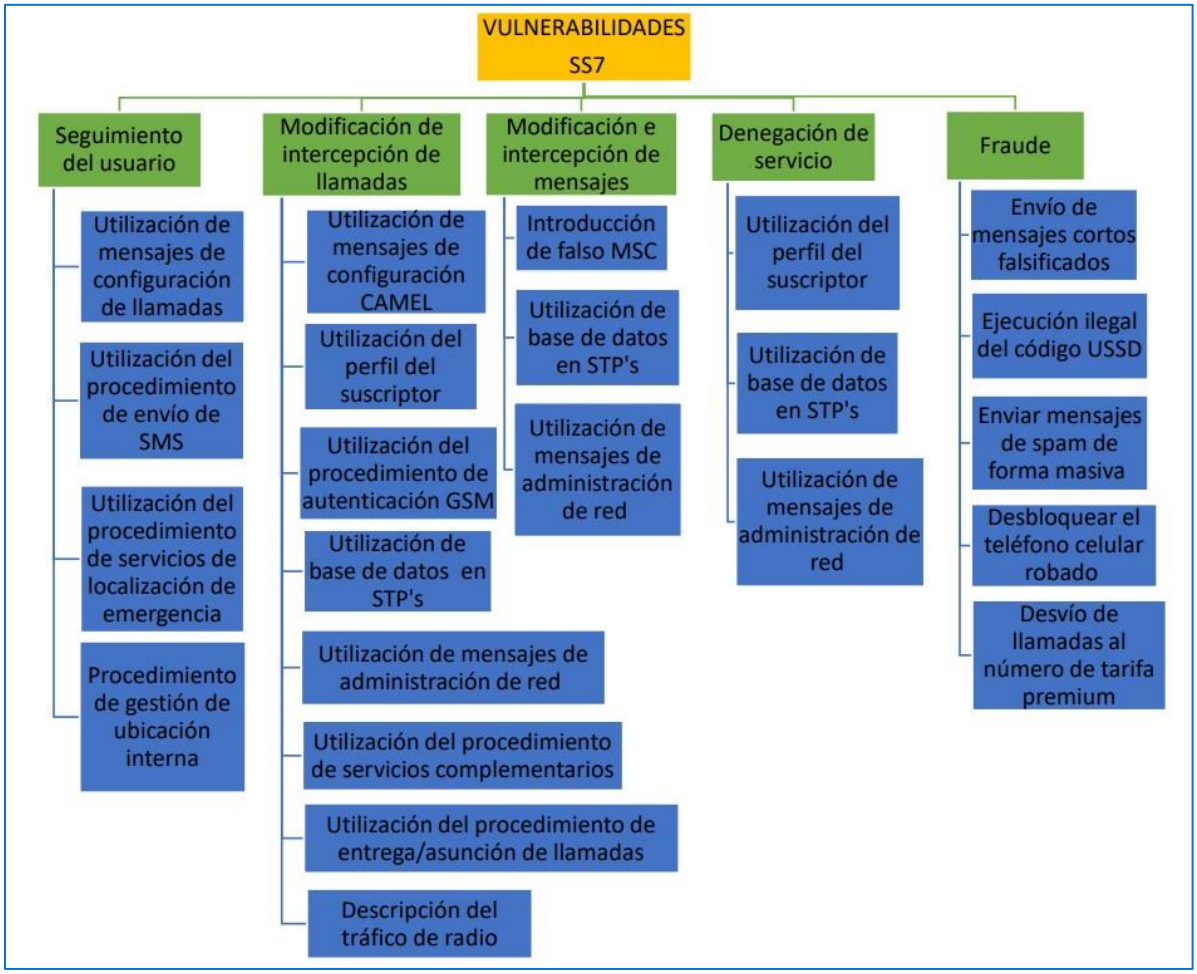
En la Gráfica 15 se muestra un esquema que resume las vulnerabilidades descritas para el SS7, así como las estrategias que pueden implementar los atacantes para aprovechar estas vulnerabilidades. Cada uno de estos casos presenta particularidades, retos y potencial para generar nuevos modos de aprovechar las vulnerabilidades mencionadas.

El concepto de los ataques descritos es aplicable casi para todas las redes, sin importar el protocolo de señalización, ya que finalmente el fin es el mismo. Es claro que las vulnerabilidades son menores en el caso de protocolos recientes, sin embargo, como ya se ha hecho mención se recomienda iniciar el análisis partiendo de los puntos de acceso que pudieran presentar una mayor vulnerabilidad.

De acuerdo con lo anteriormente expuesto, atender y resolver las vulnerabilidades, riesgos a la diversidad de ataques a los que los usuarios y operadores de las redes de telecomunicaciones móviles están expuestos se presenta como un reto de grandes dimensiones y de mucha relevancia. La descripción de cada uno de los casos considerados pudiera dar la impresión de que estamos ante una inmensidad de problemas, donde cada uno de estos requerirá de acciones y estrategias particulares. Sin pretender restar importancia a la magnitud de lo anteriormente mencionado, el presente estudio pretende recabar información de casos de estudios y experiencias previas, analizar las evidencias de los hechos descritos para proponer acciones que permitan avanzar en la solución de esta problemática.

Con esta idea en mente se integran algunas recomendaciones y líneas de acción.

Gráfica 15. Vulnerabilidades del protocolo SS7.



V. Recomendaciones

Como ya se ha comentado a lo largo del estudio, en el proceso de identificación y descripción de las vulnerabilidades de los sistemas operando con los diferentes protocolos existen factores comunes en las causas para varios de los casos particulares presentados. Entre otros, se debe considerar que para que estas vulnerabilidades se materialicen en ataques es necesario que el atacante haya penetrado la red y que, con solo este hecho, encuentre prácticamente las puertas abiertas para comunicarse y acceder a casi la totalidad de los elementos y recursos de la red.

Así mismo, la interconexión con redes IP hace extensivos muchos de los riesgos de los accesos vía web, a los equipos telefónicos que ofrecen la posibilidad de navegación y acceso a internet.

Con el fin de contribuir en la integración de algunas propuestas que permitieran avanzar en la solución de lo hasta aquí presentado, alternativas como una mayor seguridad para el acceso y la implementación de mecanismos internos de seguridad y validación surgen como ideas preliminares. En la bibliografía se encuentras estudios que han abordado estas líneas de solución, integrando una gran cantidad de propuestas, de una gran diversidad [RAO. (2015)].

Como una recomendación inicial, el autor propone la integración de grupos de trabajo principalmente de los operadores y fabricantes de equipos, con el fin de evaluar y analizar la factibilidad de las ideas expuestas en este trabajo, y las que el mismo grupo identifique, basados en su experiencia e información disponible.

De manera puntual, y como resultado de lo expuesto en la sección IV se enlistan algunas de las recomendaciones y líneas de acción sugeridas, viabilidad de las mismas, análisis de ventajas/desventajas, impacto, etc. Estas ideas también pueden sugerir líneas de acción para trabajos futuros.

- Para el caso de las llamadas sobre IP (VoIP), verificar que en la configuración del equipo se incluya la versión mejorada del protocolo RTP (SRTP).

- Para el caso de las redes 5G, se recomienda establecer recomendaciones, lineamientos y recomendaciones para que los operadores tomen acciones respecto al protocolo GTP, como pueden ser las recomendaciones de seguridad del GSMA FS.20 GPRS, incluida la implementación de monitoreo y análisis continuo del tráfico de señalización para detectar posibles amenazas de seguridad.

- Dada la relevancia de la información que se gestiona en el núcleo de las redes que operan bajo el SS7, se recomienda la integración de controles y filtros de verificación de la señalización que entra y sale de la red. El uso de firewalls, de sistemas de detección de intrusos (ISD) y de Sistemas de Prevención de Intrusión (IPS) son recomendables.

- Como se ha descrito, los eventos y actividades que se realizan dentro del núcleo de la red se llevan a cabo prácticamente sin mecanismos de autentificación. Se recomienda que para la ejecución de los mismos se implementen estrategias de autorización, así como que una vez que estas sean acciones se ejecuten, se implemente un esquema de seguimiento y auditoría de las mismas, con fines de evaluación.

- Desarrollo y puesta en marcha de mecanismos de estrés[18] que permitan probar la seguridad y funcionalidad de la red, sobre todo después de eventos relevantes como actualización y configuraciones de equipos, altas/bajas de IMEIs, etc.

- Integración de equipos especializados en sistemas SS7, que permitan monitorear las amenazas que la red recibe, así como el diseño de estrategias de mitigación y delimitación de los efectos, en caso de la presencia de un ataque exitoso.

- En el caso de los procesos de configuración y actualizaciones de equipos, la adopción y seguimiento de lineamientos de buenas prácticas es muy recomendable. Las acciones de este tipo consideradas de alto impacto deberán ejecutarse de manera local, o en su caso haciendo uso de canales seguros.

- La señalización que envían las redes visitadas a las redes domésticas (sobre todo los mensajes del tipo MAP ISD que contiene datos de los subscriptores) deberán ser sometidos a mecanismos de autentificación, verificando por canales alternos que el mensaje es enviado efectivamente por una VMSC válida.

- Las solicitudes de información al HLR deberán ser procesadas por mecanismos de validación y estar sujetas a algoritmos de encriptación, dada la relevancia de la información que almacena (IMSI, entre otras).

- Integración a la capa de aplicación de firewalls que controlen el acceso a mensajes MAP y CAP.

[18] Pruebas experimentales de la seguridad llevadas a cabo por el propio gestor de la red.

- Promover el desarrollo y uso de aplicaciones para los equipos móviles que permitan al usuario evaluar el tráfico de su conexión y detectar tráfico inusual. En el mercado existen algunas, y el trabajo pudiera ser de familiarización y uso de parte de los usuarios.

- Prohibir el uso de mensajes MAP ATI en la gestión de las redes. En el estudio han sido abordado las condiciones de riesgo generadas a partir de su uso. La Unión Europea ha bloqueado su uso en los operadores que operan en esa región, pero en muchos países del mundo es una práctica común su uso.

- Adicionar esquemas de validación a los mensajes MAP SRI SM. Una alternativa es el uso de SMS como respaldo para este proceso de validación.

- Como se ha descrito, en la mayoría de los casos la obtención del IMSI y el GT de la MSC es relativamente sencilla una vez que el intruso se encuentra dentro de la red valiéndose de mensajes MAP SRI SM. Se recomienda analizar y en su caso verificar que las recomendaciones hechas por el 3GPP para la resolución de este problema sean cumplidas.

- Establecer mecanismos de seguridad y autentificación en SPs adyacentes dentro de una red SS7. Existen recomendaciones que plantean el uso de MTPsec.

- En [Ullah. (2020).] se propone un modelo conceptual que propone la adición de componentes y medidas de seguridad a la red SS7, como mecanismos de control de acceso, encriptación de mensajes, uso de protocolos de seguridad para SS7 sobre IP (IPsec), integración de sistemas de detección de introducción de intrusos, entre otras cosas. Gráfica 16.

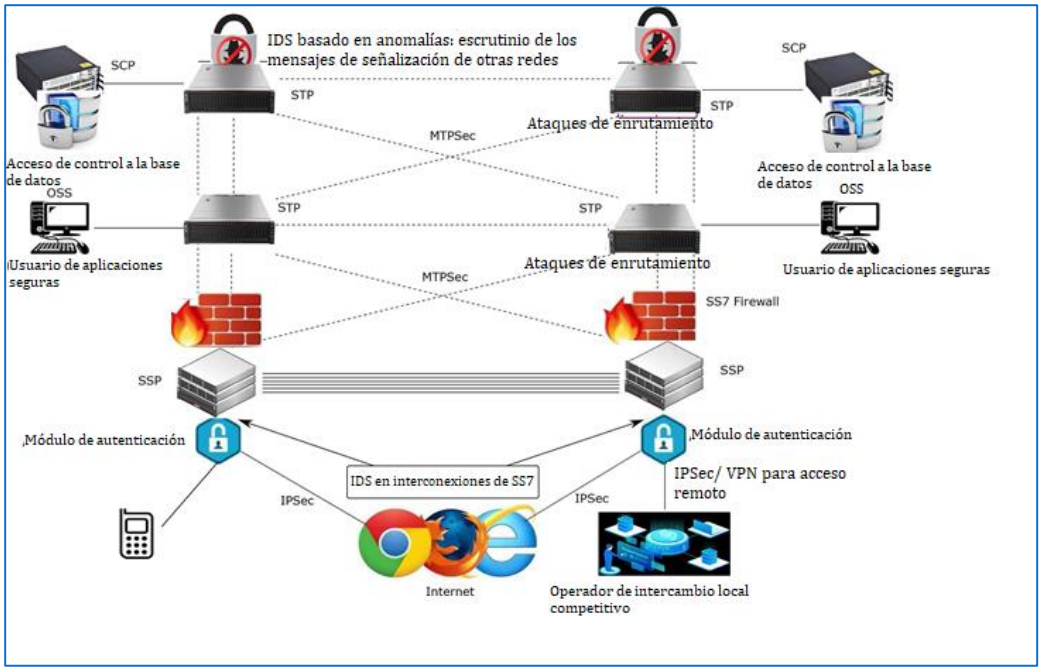
- Analizar esquemas y configuraciones adicionales que pudieran integrar herramientas de machine learning para la detección de las amenazas. Las referencias sobre investigaciones y experiencias al respecto son variadas.

- Revisión y evaluación de la implementación de la integración y uso del IER, con el objeto de encontrar propuestas de solución al problema no menor, del robo de equipos de telefonía celular. El autor considera que una vigilancia mas estricta de los IMEIs reportados como robados pudiera dar frutos. Un seguimiento mas puntual de los IMEIs que entran y salen de la lista negra podría dar elementos para emprender acciones de prevención y mitigación de la problemática. Un usuario que hace uso de un equipo robado que fue desbloqueado de manera ilegal pudiera considerar volver a usarlo si de parte del operador recibiera un

mensaje de que en el pasado el equipo tuvo reporte de robo. Repito, se recomienda una revisión más profunda.

- La transformación digital de una sociedad se fundamenta, entre múltiples factores, en la confianza de los usuarios para utilizar redes de telecomunicaciones seguras y confiables. Estrategias de seguridad que mitiguen las amenazas y vulnerabilidades expuestas, se espera contribuyan a la integración de redes mas resilientes, que estén en mejores condiciones de ofertar servicios y productos a los usuarios y empresas en un marco de ciberseguridad más robusto.

Gráfica 16. Modelo de redes SS7 propuesto. Tomado de [Ullah. (2020).].



VI. Conclusiones

La problemática de la Ciberseguridad en las redes de telecomunicaciones es un problema con muchas aristas. El enfoque del presente se llevó a cabo de manera particular los protocolos de señalización de las redes de telecomunicaciones móviles. La recomendación respecto a considerar potenciales acciones y recomendaciones que incluyan primordialmente los puntos de acceso con más vulnerabilidad se propone como una primera acción, que puede incluir acciones conjuntas para otros aspectos y redes.

Respecto a la pertinencia de considerar como solución la eliminación del estándar SS7 y aprovechar las funcionales que los protocolos de señalización de 4G y 5G presenta, la enorme cantidad de equipos operando con el SS7 y la complejidad de la adaptación de los sistemas en funcionamiento a un nuevo protocolo son temas a considerar para estar en condiciones de tomar una decisión al respecto. Sin embargo, el tiempo avanza, actualmente los casos de ataques a redes SS7 se siguen presentando y es necesario abordar la problemática, con el fin de contribuir en la solución de esta. No obstante, la paulatina salida de sistemas 2G y 3G, las estadísticas muestran que estaremos en convivencia con estas durante algunos años más.

Una vez detalladas y analizadas las vulnerabilidades, las propuestas presentadas son de diversa índole, tratando de no solo enfocarse en el tema absolutamente técnico; sin embargo, se hace énfasis en el mismo.

Como complemento a lo mencionado, el autor considera de relevancia la integración de mesas de trabajo, así como la implementación de estrategias de seguimiento y vigilancia basadas en tecnologías como inteligencia artificial y ciencias de datos como base para la integración de nuevas estrategias.

La ciberseguridad de las redes es un concepto amplio y con una gran cantidad de dimensiones y aspectos. Los protocolos de señalización son uno de ellos, considerándolos de especial relevancia ya que, a partir de su corrupción las redes pueden quedar expuestas.

Así mismo, la garantía de redes de telecomunicaciones más seguras y confiables se constituyen como un elemento fundamental en la confianza de uso por parte de empresas y ciudadanos, contribuyendo de esta manera una mayor demanda y desarrollo de los servicios y productos ofertados por estas redes.

Referencias

[ODS, ONU. 2015]. Objetivos de desarrollo sostenible. ONU. 2015. https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

[OEA, BID. (2020). CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINAY EL CARIBE. Reporte Ciberseguridad 2020. 29-02-2021.

UIT-T. (2008). Recomendación UIT-T X.1205 Aspectos generales de la ciberseguridad. SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD Seguridad en el ciberespacio – Ciberseguridad, I, 1-66. 28/jun/2021, De SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD.

UIT-T. (2003). Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo. SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS Seguridad, I, 1-28. 28/jun/2021,

ENISA. (2018). Signalling Security in Telecom SS7/Diameter/5G EU level assessment of the current situation. 29/Jun/2021, de ENISA Sitio web: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

Ullah. (2020). K. Ullah, I. Rashid, H. Afzal, M. M. W. Iqbal, Y. A. Bangash and H. Abbas, "SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1337-1371, Secondquarter 2020, doi: 10.1109/COMST.2020.2971757.

PT. (2016). PRIMARY SECURITY THREATS FOR SS7 CELLULAR NETWORKS. 30/06/2021, de Positive Technologies Sitio web: https://www.ptsecurity.com/upload/ptcom/SS7-VULNERABILITY-2016-eng.pdf

FIGI. (2020). Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions. Jul 2020, de Financial Inclusion Global Initiative Sitio web: https://figi.itu.int/wp-content/uploads/2021/04/Technical-report-on-the-SS7-vulnerabilities-and-their-impact-on-DFS-transactions_f-1-1.pdf

SOPHOS. (2021). El estado del ransomware 2021. Agoto, 2021, de Sophos Cibersegurity evolved Sitio web: https://www.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

ESET. (2021). Security Report. Latinoamérica 2021. Agosto, 2021, de ESET Sitio web: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

ITU. (2021). Measuring digital development Facts and figures 2020. Agosto 2021, de InternationalTelecommunications Union Sitio web: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

RAO. (2015) S. P. Rao, S. Holtmanns, I. Oliver, and T. Aura, “Unblocking stolen mobile devices using SS7-map vulnerabilities: Exploiting the relationship between IMEI and IMSI for EIR access,” in Proc. IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 1171–1176

Rao2. (2015)S. P. Rao, S. Holtmanns, I. Oliver and T. Aura, "Unblocking Stolen Mobile Devices Using SS7-MAP Vulnerabilities: Exploiting the Relationship between IMEI and IMSI for EIR Access," 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 2015, pp. 1171-1176, doi: 10.1109/Trustcom.2015.500

Jensen. (2016) K. Jensen, T. V. Do, H. T. Nguyen and A. Arnes, "Better Protection of SS7 Networks with Machine Learning," 2016 6th International Conference on IT Convergence and Security (ICITCS), Prague, Czech Republic, 2016, pp. 1-7, doi: 10.1109/ICITCS.2016.7740315.

Thru (202). B. Thuraisingham, "Cyber Security and Artificial Intelligence for Cloud-based Internet of Transportation Systems," 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 2020, pp. 8-10, doi: 10.1109/CSCloud-EdgeCom49738.2020.00011.

Mat (2019) W. Matsuda, M. Fujimoto, T. Aoyama and T. Mitsunaga, "Cyber Security Risk Assessment on Industry 4.0 using ICS testbed with AI and Cloud," 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia, 2019, pp. 54-59, doi: 10.1109/AINS47559.2019.8968698.

Mbel (2016) T. M. Mbelli and B. Dwolatzky, "Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security," 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Beijing, China, 2016, pp. 1-6, doi: 10.1109/CSCloud.2016.18.

Alh (2017)A. K. Alharam and W. El-madany, "Complexity of Cyber Security Architecture for IoT Healthcare Industry: A Comparative Study," 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Prague, 2017, pp. 246-250, doi: 10.1109/FiCloudW.2017.100.

Jose Joskowicz. (2017). Introducción a Sistemas de Señalización. Montevideo, Uruguay: Universidad de la República.