ARTÍCULO DE INVESTIGACIÓN / RESEARCH ARTICLE
http://dx.doi.org/10.14482/inde.38.2.006.31

Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos

Cybersecurity in Mobile Telecommunication Networks and Management Risk

Miguel Ángel Roldán Álvarez[1]
Héctor Fernando Vargas Montoya[2]

1 Instituto Tecnológico Metropolitano, Colombia.
Orcid: https://orcid.org/0000-0002-6160-0021.
Correspondencia: miguelroldan@itm.edu.co

2 Instituto Tecnológico Metropolitano, Colombia.
Orcid: https://orcid.org/0000-0002-0861-2883

Resumen

La tecnología de redes 3.5G y 4G son actualmente las más usadas en Colombia dado el gran despliegue que han realizado los proveedores de servicios de internet, lo que supone un reto de seguridad con respecto a los diferentes ataques a dichas redes. La interceptación de datos a través de ataques de tipo hombre en el medio (MitM, por sus siglas en inglés) y la negación de servicio (DoS, por sus siglas en inglés) (en el *smartphone* o en la red móvil) son muy factibles. En este artículo de investigación aplicada tiene como objetivo establecer algunos riesgos y posibles impactos asociados a las redes de telecomunicaciones y cómo un atacante con poco recurso computacional puede eventualmente vulnerar el sistema, se muestran algunas vulnerabilidades de seguridad en las redes móviles, los riesgos que esto tiene y su posibilidad de explotación, así como las recomendaciones generales para la reducción de dichos riesgos. Para lograr lo anterior, se realizó una investigación de diferentes vulnerabilidades en estas redes de telecomunicaciones, se elaboró un mapa de riesgos para visualizar los posibles impactos, se desarrolló una prueba técnica que consolida un ataque MitM con una captura de tráfico siendo exitoso dicho ataque. Finalmente, se entregan recomendaciones de seguridad en el caso que se logren ejecutar ciberataques, con ello, poder contar con una base para el aseguramiento de redes y sistemas de telecomunicaciones, permitiendo a diferentes personas reconocer las vulnerabilidades poco exploradas en este tipo de sistemas.

Palabras clave: 3.5G, 4G, ataque informático, ciberseguridad, gestión de riesgos.

Abstract

The 3.5G and 4G network technologies are, currently, the most used in Colombia, given the great deployment that Internet service providers have made, which represents a security challenge with respect to the different attacks on these networks. The interception of data with "Man in the middle attacks" (MiTM) and denial of service - DoS (in the smartphone or in the mobile network) are very feasible. In this article of applied research aims to establish some risks and possible impacts associated with telecommunications networks and how an attacker with little computational resource can eventually compromise the system, some risk and security vulnerabilities in mobile networks and their possibility of exploitation, as well as the general recommendations for risk reduction are studied. To achieve the above, an investigation of different vulnerabilities in these telecommunications networks was carried out, a risk map, in order to visualize the possible impacts, was made. Then, a technical test was run to capture traffic during the MiTM attack (which was successful), and as a final result, deliver recommendations in the event that they can execute cyber-attacks, with this, to be able to have a basis for the assurance of telecommunications networks and systems, allowing different people to recognize the vulnerabilities little explored in this type of systems.

Keywords: 3.5G, 4G, computer attack, cybersecurity, risk management.

Fecha de recepción: 6 de febrero de 2020
Fecha de aceptación: 2 de agosto de 2020

1. INTRODUCCIÓN

En Colombia [1], para el tercer trimestre de 2019 los accesos a internet móvil ascendían a 28,9 millones de suscriptores, en que 1,4 millones usan las redes 2G, 8,2 millones las 3G y 19,4 millones las 4G. Asimismo, para el primer trimestre de ese año [2], los accesos fueron de 28,2 millones de suscriptores, en que 1,5 fueron a través del uso de 2G, 9,5 de 3G y 17,2 de 4G, lo que supone una disminución para 2G y 3G, pero un aumento en el uso de 4G, sin embargo, es claro que aún se tiene el 39 % de los suscriptores que emplean redes por debajo de 4G.

Desde el punto de vista de los proveedores de tecnología y de los fabricantes de teléfonos móviles [4], para el tercer trimestre de 2019, se vendieron aproximadamente (en el mundo) 2139 millones de *smartphone* y se proyectaron 2155 millones para 2020. En atención al alto volumen previsto en el uso de este tipo de dispositivos, es claro que se están usando algunas de las redes para la conexión hacia y desde internet, lo que incrementa la preocupación tanto de las empresas como de las personas en temas de ciberseguridad y protección de las redes. En ese sentido, en 2019 [5], el 40 % de las empresas en América Latina tuvieron una infección por *malware*, mientras que el 57 % están preocupadas por el aumento en robo de información y el 61 % por el acceso indebido a sistemas. Asimismo, el 13 % de las empresas sufrieron ataques de negación de servicio (DoS, por sus siglas en inglés), y en Colombia, el 58 % de las empresas participantes en el muestreo indicaron haber tenido algún incidente de seguridad.

Por otro lado, la inseguridad en las redes de telecomunicaciones y las tecnologías de la información y la comunicación (TIC), en general, siempre será latente, acorde con la Asociación Colombiana de Ingenieros de Sistemas (ACIS) [6]. Ataques como el *phishing*, caballos de Troya y ataques de negación de servicio ocuparon el 49 % de los eventos de seguridad en Colombia y parte de América Latina entre 2018 y 2019. Lo anterior, sumado a las múltiples dificultades en los dispositivos móviles con respecto a la seguridad en *software* (Android es el sistema más usado y atacado en los últimos años [7], [9]), daría como resultado un aumento en los riesgos potenciales en el uso y la utilización de *smartphone* con Android en una red de telecomunicaciones. Bajo ese panorama, en Colombia, se tiene un alto volumen de teléfonos en el mercado con sistema Android que son conectados a las diferentes redes de telecomunicaciones, lo que puede implicar que diferentes vulnerabilidades pueden ser explotadas en algún momento. En ese sentido, se tiene un aumento en las preocupaciones en torno a la seguridad (por el alto uso de las redes) y se crea la necesidad de contar con un proceso de identificación de posibles riesgos potenciales como la debida protección y controles de seguridad a desarrollar.

En este artículo, se tiene como hipótesis que, con la identificación y prevención de los riesgos de ciberseguridad en el uso de las tecnologías de telecomunicaciones a

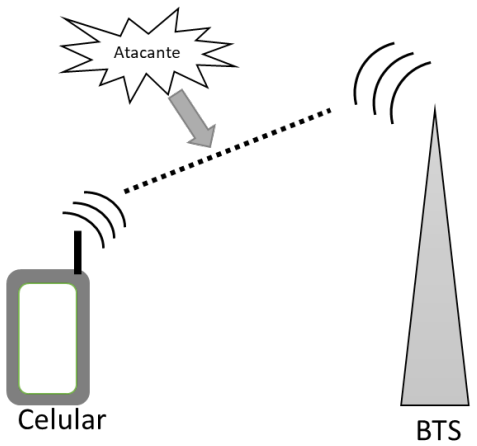
través de dispositivos móviles, se mitigan los posibles impactos que los ciberataques puedan generar. Asimismo, se expone un marco referencial sobre ataques informáticos y tecnologías de telecomunicaciones y sus vulnerabilidades, que evidencia la posibilidad de que, a través de una breve gestión de riesgos, dichas vulnerabilidades puedan ser explotadas y se ejecute un ataque de hombre en el medio (MitM, por sus siglas en inglés) sobre una red de telecomunicaciones, para demostrar lo frágil que puede ser este tipo de redes y la consolidación de los posibles riesgos. Finalmente, se proponen algunos mecanismos para la reducción de los riesgos de exposición.

2. Marco teórico

Entender los ataques informáticos supone conocer los diferentes riesgos e impactos que tiene una tecnología determinada, para establecer mecanismos de control que ayuden a la reducción de los impactos. De igual manera, cuando ocurre un evento de seguridad, es necesario darle un adecuado manejo, lo cual implica identificar posibles fuentes de riesgos, vulnerabilidades, impactos y un proceso para la gestión de los incidentes.

2.1. MitM

Se define [10] como un ataque que se realiza fijando una interceptación en medio de dos puntos que intentan comunicarse y captura la información (figura 1). Esta interceptación es posible realizarla a través de programas de tipo *sniffer* sobre las frecuencias de radios de transmisión, para lo cual, en redes de telecomunicaciones, es necesario usar una celda falsa o algún *software* que permite la captura de la señal con su respectiva antena receptora (tal es el caso de GNU Radio).



Fuente: elaboración propia.

Figura 1. Modelo de conexión de una red de telecomunicaciones.

El concepto de MitM es antiguo, aun así, ha sido uno de los vectores de ataque más exitosos en el transcurso de su historia. A lo largo del tiempo y del desarrollo de nuevas tecnologías, los métodos de ataque han variado para ser más efectivos, sin embargo, en el fondo continúa siendo la misma base para interceptar la información entre dos puntos para sustraerla (principio de confidencialidad), cambiarla o modificarla (principio de integridad) o negar el acceso a dicha información (principio de disponibilidad), según el fin que el atacante busque [11]. Una de las características más importante de este ataque, y que lo hace peligroso, es su versatilidad para explotar diferentes vulnerabilidades en diferentes escenarios, por ejemplo, en sistemas operativos, en *routers*, servicios web, red de telecomunicaciones, entre otros.

Algunas de las técnicas o variantes del MitM son conocidos como *monkey-in-the-middle*, *bucket-brigade attack* y *session hijacking* [12]. Por otro lado, se tiene una descripción de al menos tres formas de categorizar los ataques MitM más comunes [13], son estos: a) MitM basado en técnicas de suplantación, b) MitM basado en el canal de comunicación donde se ejecuta el ataque y c) MitM basado en la ubicación del atacante y el objetivo en la red.

2.2. Vulnerabilidades en sistemas operativos

Las vulnerabilidades [14] son errores, fallos o huecos de seguridad que están contenidos en un desarrollo de un *software*, plataforma o programa informático, y que en algunas ocasiones pasan desapercibidos al programador o administrador del sistema, pero que los atacantes o cibercriminales tienen la capacidad de identificar y detectar, quienes a través de diferentes ataques generan múltiples actividades que crean riesgos en los sistemas e impactos negativos a estos, tales como ingresar al sistema operativo y de archivos, modificar el comportamiento del sistema, implantar *malware* y, en casos extremos, controlar el dispositivo comprometido de forma remota. Pero las vulnerabilidades se manifiestan a veces desde el diseño mismo de programas o servicios informáticos. En algunas ocasiones, no se considera la verificación de datos o archivos de entrada, que, al ser recibidos por el sistema, generan un comportamiento no esperado cuando se explota una vulnerabilidad, la cual termina siendo un alto riesgo en la tecnología usada.

2.3. Tecnología 3.5G

El término 3.5G se emplea para referirse a las versiones del estándar UMTS (por sus siglas en inglés) que ofrecen mejoras en la capacidad, el rendimiento y la eficiencia con respecto a la primera versión. Una de las versiones UMTS se conoce como HSDPA (por sus siglas en inglés), la cual permite alcanzar velocidades de descarga de información desde los 2.0 Mbps en condiciones ideales de funcionamiento (como en una

oficina) y velocidades promedio de 800 Kbps [15], tecnología que en funcionamiento permite alcanzar velocidades de 7,2 Mbps y 14 Mbps en condiciones ideales; posteriormente, la UMTS toma una evolución hacia 4G (denominada LTE, por sus siglas en inglés). El modelo de cobertura global que ofrece GSM (por sus siglas en inglés) ha servido de base para que UMTS/HSDPA logre mayor aceptación [15].

Una red 3.5G está basada en la tecnología HSDPA (por sus siglas en inglés) que ofrece tasas de transferencias de datos muy alta y una mejora de velocidad en el *downlink* (bajada de datos), mas no en el *uplink* (subida de datos).

Para mejorar la velocidad de *uplink*, existe la tecnología HSUPA (por sus siglas en inglés) que puede brindar servicios de descarga de contenido, videos y *streaming*. Esta red 3.5G se complementa con la red GSM en varios sentidos, por ejemplo, en el uso de un mismo chip y número de línea tanto para el servicio de GSM como para los servicios de 3G y 3.5G [16]. También tiene una generación intermedia conocida como 3G+ denominada HSPA (por sus siglas en inglés) con capacidades de transmisión de datos que podrían alcanzar velocidades de hasta 14,4 Mbps en el enlace descendente y 5,8 Mbps en el enlace ascendente.

Otra característica muy importante y visible, especialmente para los usuarios, fue la introducción del SIM card (por sus siglas en inglés), donde se almacena la información de subscripción de los usuarios, que es independiente del terminal telefónico móvil. Aunque esta característica se introdujo en la tercera generación, la SIM card también fue adoptada por la tecnología 2G.

En atención a los problemas de seguridad en telecomunicaciones, y acorde con el portal de búsquedas de vulnerabilidades National Vulnerability Database (NVD), en 2019 se publicaron al menos dos vulnerabilidades consideradas críticas en el protocolo HSPA, así como otras en 2018 y 2017. Estas son:

1. CVE-2018-11422. Publicada el 3 de julio de 2019, es una vulnerabilidad en G3100-HSPA Series, en que la información es enviada en texto plano, lo que implica poder interceptar esta (a través de un MitM) y realizar modificaciones, tales como subir o bajar configuraciones o actualizar *firmware* [17].

2. CVE-2018-11421. Publicada el 3 de julio de 2019, afecta a G3100-HSPA Series y se encontró que la información va en texto plano, un atacante puede interceptarlo (con un MitM) y obtener información sensible, incluso, las contraseñas de los administradores [18].

3. CVE-2018-5455. Publicada el 5 de marzo de 2018, los investigadores descubrieron un problema de integridad en el componente Moxa OnCell G3100-HSPA, lo que permite que se pueden ejecutar ataques de fuerza bruta saltando la autenticación y obtenien-

do acceso al dispositivo [19]. Este problema de seguridad es similar a la CVE-2017-7915, en el cual un atacante puede hacer uso del problema de autenticación para comprometer el sistema a través de la instalación no consentida de un componente *software*, y permitir con este *software* un ataques de tipo MitM.

4. CVE-2017-7913. El 29 de mayo de 2017, sobre el componente Moxa OnCell G3110-HSPA, fue publicada una vulnerabilidad en el almacenamiento del archivo de configuración, el cual expone sin protección parámetros que representan contraseñas, y permite que un atacante puede ingresar y extraer información [20].

2.4. Sistema de radio definido por *software*

Las plataformas físicas de radio son complejas y requieren un alto costo y mantenimiento si se necesita realizar algunas pruebas funcionales. Los sistemas de radio definidos por *software*-SDR fueron desarrollados para la facilidad académica y conceptual [21], lo cual permite una simulación y comprobación de errores, y con ello poder tomar decisiones e implementaciones reales. La tecnología de telecomunicaciones que puede ser simulada a través del *software* permite recrear escenarios con diferentes funcionalidades y frecuencias, así como modular, demodular y sintonizar diferentes frecuencias de radio [22].

De las plataformas SDR (por sus siglas en inglés), GNU Radio es una herramienta de código libre que permite la creación (simulación) de frecuencias de radio a través de bloques de procesamiento, igualmente puede interactuar con componentes *hardware* externos como antenas de diferentes frecuencias [23].

2.5. Ciberataques

Como se ha indicado, algunas de las técnicas usadas son los ataques por suplantación que involucra una o varias víctimas (estos son los extremos finales, celulares y antenas repetidoras o estaciones base) y el atacante. Algunas de las técnicas [24] usadas son el ARP *spoofing*, DNS *spoofing*, IP *spoofing* y ataque de estación base falsa (FBS, por sus siglas en inglés). Estos ataques permiten, a través de la interceptación de las comunicaciones, obtener la información suficiente y necesaria para suplantar, lo que conlleva vulnerar el sistema. Los ciberataques en estaciones base y las interceptaciones de GSM, a través de implementación de redes definidas por *software*, pueden ser ejecutadas de manera simple. Es posible establecer, al menos, dos tipos de ataques [25] que pueden realizar sobre la estación transceptora base (BTS, por sus siglas en inglés) falsa, igualmente se pueden crear estaciones base para fines de captura maliciosa del tráfico en tránsito; con ello, cuando un dispositivo hace una conexión GSM, es posible la captura de datos como el IMSI o IMEI (por sus siglas en inglés).

Desde el punto de vista de la detección, y tratándose de un ataque que se ejecuta desde la interceptación de las ondas, es difícil su identificación para un posterior control. Sin embargo [26], se han presentado algunas técnicas (a modo de propuesta) que puedan dar solución a la identificación y control de ataques MitM, una de ellas es lograr identificar si el ataque hace parte de una suplantación (falsa radio base). El método consiste en identificar la cantidad de celdas (que se tiene por topología en una cobertura determinada) comparadas con los resultados después de hacer un escaneo de celdas disponibles reales; en caso de existir alguna diferencia, se tendría el supuesto de que existe una celda falsa.

Otro mecanismo usado por los atacantes es a través de mensajes de texto, los cuales han tenido una gran repercusión en los temas de seguridad, tal es el caso de *malware* por SMS (por sus siglas en inglés), secuestro de archivos, bombardeo y *spoofing* de SMS y otros ataques [27].

En ese sentido, los investigadores encontraron una vulnerabilidad en los dispositivos móviles conocido como Simjacker, que permite a los atacantes, a través de mensajes de texto, inyectar *software* espía (*spyware*) y tomar posesión del dispositivo (forma remota) mediante el uso malicioso de la SIM card. Algunos dispositivos como Samsum y Motorola son susceptibles de dichos ataques, registrados a través de los CVE-2019-16257 y CVE-2019-16256 [28], a lo que se suma, en particular, que Colombia es uno de los países afectados por esa vulnerabilidad. Asimismo, el uso de técnicas de ingeniería social, para que atacantes puedan obtener información relevante de clientes o personas, son muy eficientes, dado que este tipo de ataques aprovecha el desconocimiento, la desinformación de los usuarios finales y el alto uso de las redes sociales.

Otro caso del ataque es SIM *swapping* [29], [30], en que un atacante con información básica puede obtener datos desde el operador de telefonía y, con ello, lograr realizar ataques de intercambio de SIM o negar el servicio (DoS, por sus siglas en inglés) a través de la red.

2.6. Gestión de riesgos

La gestión de riesgos es un proceso interactivo que permite la obtención de posibles impactos sobre diferentes activos de información, para lo cual un riesgo es la posibilidad que una amenaza explote una vulnerabilidad en un activo determinado y genere un impacto negativo al sistema [31]. Las diferentes normas establecen procedimientos capaces de identificar, analizar, evaluar y entregar los riesgos sobre un proceso o sistema a través de una matriz de aceptabilidad o mapa de riesgos y, con ello, lograr crear un plan de tratamiento que permita la reducción de posibles riesgos de exposición [32].

3. METODOLOGÍA

Conscientes de la necesidad de fortalecer los procesos de seguridad sobre las diferentes redes y recursos informáticos, se plantea una alternativa de cómo identificar y mitigar distintos ciberataques en las redes y los dispositivos móviles. Esta metodología se desglosa en tres fases. En una primera fase, se analizan las posibles vulnerabilidades con sus impactos (gestión de riesgos) acorde con las posibles fuentes de amenazas, se consulta en la CVE, se calculan los riesgos a través de una metodología ajustada y se obtiene un mapa de riesgos de 3 × 3 donde el proceso está dado por levantamiento de activos, obtención de amenazas y vulnerabilidades, así como calificación de los escenarios de riesgos.

En una segunda fase, se hace una prueba práctica de cómo obtener información del tráfico de red (captura de datos de una llamada móvil en curso) para establecer posibles ataques de tipo MitM, se comprueba parte de los riesgos obtenidos, se configura una arquitectura (figura 6) básica, se hace uso de GNU Radio y *software* para captura de paquetes Wireshark y, finalmente, se entregan propuestas de mitigación de posibles impactos.

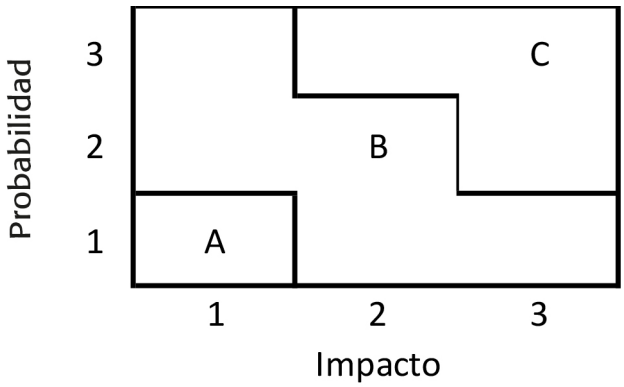
4. RESULTADOS Y DISCUSIÓN

4.1. Análisis de riesgos y sus impactos

Como se indicó en la conceptualización, existen diferentes vulnerabilidades en las redes de telecomunicaciones y en los dispositivos móviles, debilidades que pueden ser explotadas por diversos actores según su objetivo a perseguir. Uno de los mecanismos para calcular los posibles impactos sobre la información que puedan generarse con diferentes ataques informáticos es la gestión de riesgos, la cual, a través de una serie de pasos secuenciales, permite establecer un nivel de impacto relativo acorde con la organización y su nivel de tolerancia [31]. Dentro del proceso de gestión de riesgos, se establece una identificación de activos, una identificación de amenazas y vulnerabilidades, posibles impactos y unos resultados consolidados en un mapa de riesgos [33].

Para calcular los posibles impactos en las redes de telecomunicaciones, se siguió el proceso dado en la norma ISO 27005:2018 [31], pero con una matriz de 3 × 3 a efectos prácticos (la norma indica una matriz de 5 × 5), para lo cual la probabilidad de ocurrencia en la norma ISO (muy bajo, bajo, medio, alto, muy alto) queda con tres valores: bajo (valor de 1), medio (valor de 2) y muy alto (valor de 3). Asimismo, para el impacto, en la norma ISO, se definen los valores muy bajo, bajo, medio, alto, muy alto; para este artículo, queda definido un impacto muy a (valor de 3), medio (valor de 2) y bajo (valor de 1), de modo que son estos los valores claves para su medición.

En consecuencia, se hace levantamiento de activos, identificación de amenazas para los activos y creación de escenarios de riesgos y calificación. Para obtener el mapa de riesgos, al escenario de riesgos se le da un valor en probabilidad (siendo 3 el valor máximo, muy alto) e impacto (siendo 3 el valor máximo, muy alto) si esa amenaza se consolida. Se usó una matriz de 3 × 3 (figura 2) con las siguientes distribuciones acorde con la zona o el nivel de aceptabilidad: riesgo bajo (A), riesgo medio (B) y riesgo alto (C).



Fuente: elaboración propia.

Figura 2. Mapa de riesgos.

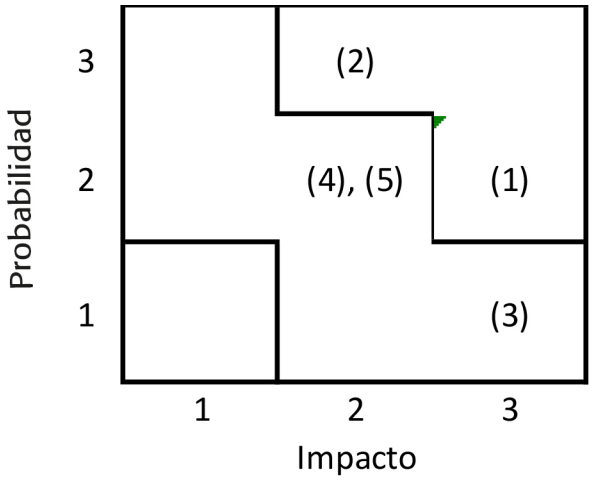
Los activos evaluados son las redes de telecomunicaciones y los dispositivos móviles. Entre las amenazas se consideraron *malware*, ataque SMS, DoS/DDoS y la interceptación o el robo de información. Los escenarios de riesgos tienen la siguiente valoración (tabla 1):

Tabla 1. Escenarios de riesgos

Escenario de riesgo	Probabilidad	Impacto
1) Probabilidad de ejecución de malware en dispositivos móviles.	2	3
2) Probabilidad de ataques a través de SMS en dispositivos móviles.	3	2
3) Probabilidad DoS y DDoS en las redes.	1	3
4) Probabilidad DoS y DDoS en dispositivos móviles.	2	2
5) Probabilidad de interceptación o robo de información en las redes y dispositivos móviles.	2	2

Fuente: elaboración propia.

Como se muestra en la tabla 1, y luego de realizar la valoración, estamos frente a cinco escenarios posibles de riesgos, los cuales fueron calificados en probabilidad e impacto, tras lo cual se obtuvo el siguiente mapa (figura 3):



Fuente: elaboración propia.

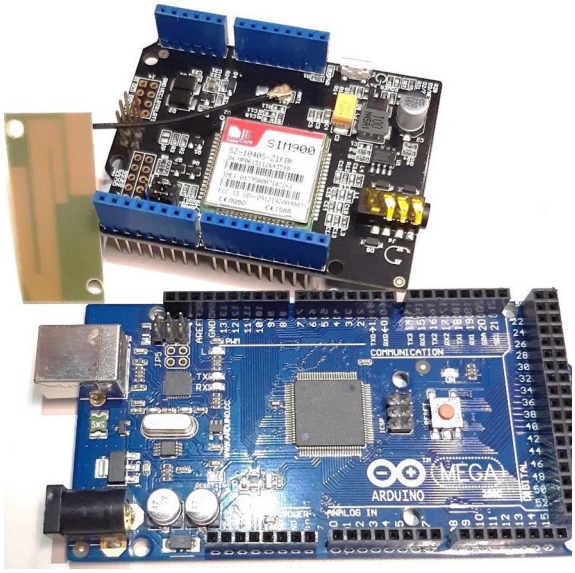
Figura 3. Mapa de riesgos que calcula la probabilidad por el impacto.

Acorde con el mapa de riesgos, existen dos riesgos altos y tres medios, para lo cual es necesario establecer mecanismos de mitigación que ayuden a conservar la información y evitar que los riesgos se consoliden. Cuando tenemos redes de telecomunicaciones, es muy probable, como se evidencia, que los ataques informáticos pueden generar grandes problemas y repercusiones en la disponibilidad por causa de *malware* o SMS.

Por otro lado, los riesgos que están en la zona de riesgo medio (B) son de especial cuidado, dado que estos deben ser revisados periódicamente para no aumente su probabilidad de ocurrencia y se generan impactos negativos mayores.

4.2. Laboratorio de análisis del riesgo de interceptación o robo de información

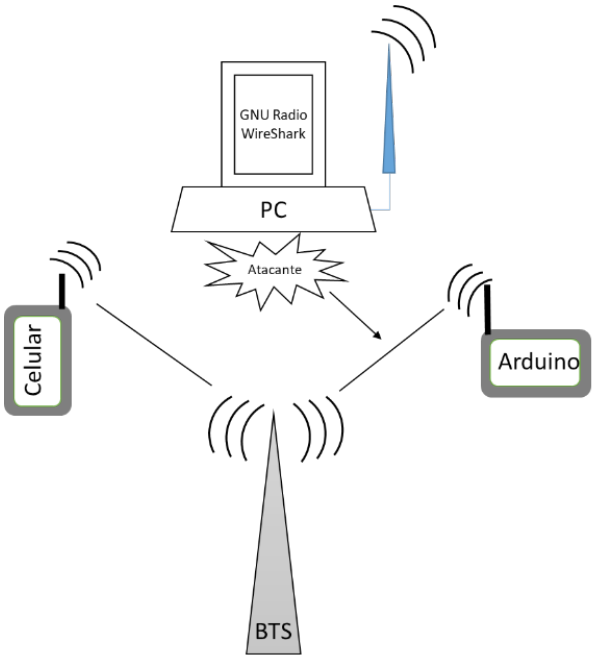
Como evidencia de la posible consolidación de los riesgos ya identificados, se realizó una prueba práctica de interceptación y robo de información en una red de telecomunicaciones (riesgo 5, figura 3). Para el montaje de la red de prueba (realizando llamadas a través del operador respectivo), se usó un programa desarrollado en Arduino Mega con su módulo GSM-SIM900 (figura 4) para la interceptación de dichas llamadas, se empleó una antena para 3.5G + GNU Radio y se realizaron capturas con Wireshark.



Fuente: elaboración propia.

Figura 4. Arduino usado para las pruebas.

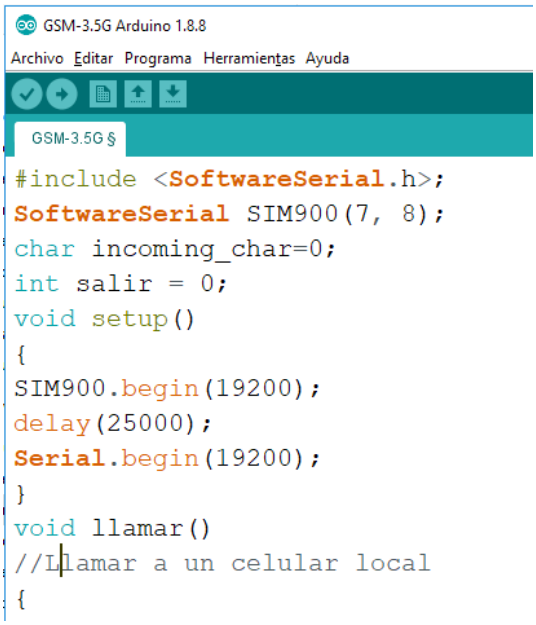
En la figura 5, se puede observar el montaje realizado con todos los componentes.



Fuente: elaboración propia.

Figura 5. Diseño del montaje para la interceptación de tráfico 3.5G.

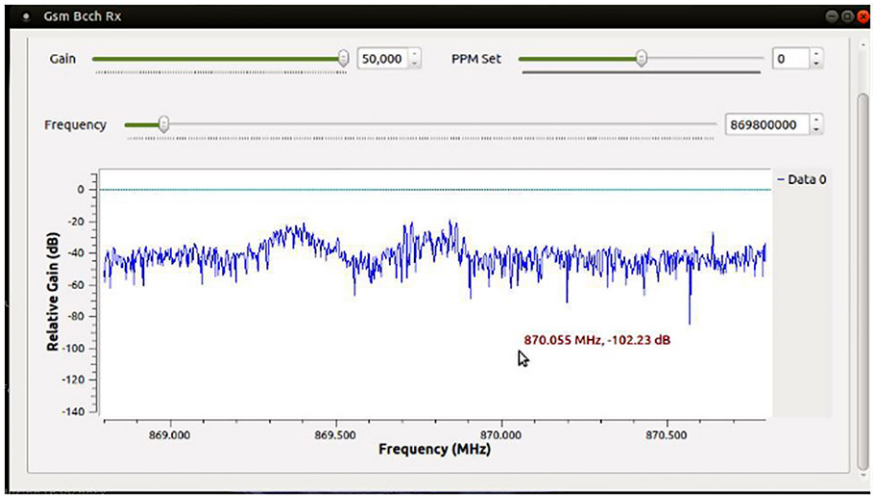
En el proceso de ensamble de los componentes, se consideró la conexión del Arduino hacia cualquiera de las antenas (BTS, por sus siglas en inglés) disponibles por el proveedor de servicios. De mismo modo, se conectó la antena 2000 MHz a un Linux con GNU Radio para la escucha del tráfico en tránsito (como antena atacante); dicho tráfico es capturado a través de Wireshark y, con ello, se logró la extracción de la información relevante de las conexiones. Para el siguiente paso, se implementó un programa para Arduino con una conexión hacia las redes GSM (figura 6); una vez compilado el programa, se ejecutó la llamada, la cual es capturada por la antena del atacante.



Fuente: elaboración propia.

Figura 6. Código fuente de Arduino para la ejecución de las llamadas de pruebas.

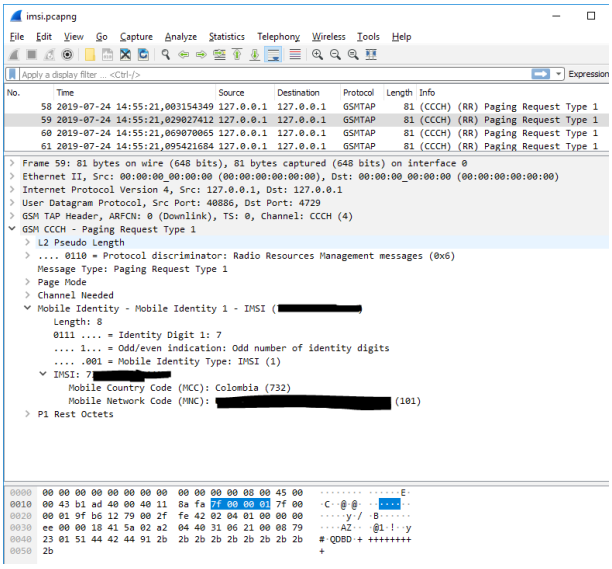
Antes de la ejecución de la llamada, se tiene activo el programa en GNU Radio que localiza en un rango de frecuencias (entre 870 MHz y 1900 MHz, frecuencia ya establecida por el proveedor de servicio) capaz de escuchar la transmisión de *broadcast* de todas las posibles llamadas cursantes (figura 7).



Fuente: elaboración propia.

Figura 7. Captura de frecuencia a través de GNU Radio.

Con la captura de la señal, se activa Wireshark (figura 8) para la visualización de datos cursantes por la antena del atacante:



Fuente: elaboración propia.

Figura 8. Información desplegada desde Wireshark una vez se ejecuta la captura de información.

Como se puede apreciar (figura 9), parte de la información que se logra capturar (de forma simple) es el IMSI (por sus siglas en inglés) y otros datos y, con ello, se demuestra la posibilidad de que el riesgo de interceptación y robo de información se consolide y sea real. En consecuencia, con herramientas básicas, un atacante puede, eventualmente, obtener información relevante en una llamada telefónica y, con ello, poder actuar en diferentes frentes de la seguridad: robo de información sensible, ataques a las redes y dispositivos móviles, inyección de códigos maliciosos (*malware*), entre otros. Además, estas acciones técnicas se pueden potencializar con el uso de ingeniería social [29] y aumentar la probabilidad de ocurrencia, efectividad y niveles de impacto.

4.3. Posibles impactos y recomendaciones de seguridad

En atención a que los diferentes ataques técnicos que pueden generar, o desde la red de telecomunicaciones, o en Android directamente, es claro que un ataque MitM afectaría la disponibilidad, integridad y confidencialidad de la información. Algunos de los impactos podrían ser:

1. En la pérdida de disponibilidad, no se tendría conexión con las antenas o torres de comunicación desde los celulares, igualmente se podría desconectar la llamada.

2. El lograr interceptar información (figura 9) permite a un atacante robar datos que pueden ser técnicos o personales, en consideración a que se podrían visualizar las tramas y los datos enviados, lo que supone una clara violación a la intimidad si los datos obtenidos representan a las personas (principio de *habeas data*).

3. Para el caso de la integridad de datos, si se logra obtener copia de la información, se podría modificar esta o ingresar al sistema desde la red de telecomunicaciones (por fuerza bruta, ingeniería social o haciendo uso de una explotación de la vulnerabilidad en Android); en cualquier situación, se modificarían datos para obtener acceso y ganar privilegios.

En general, los impactos, en atención a la cantidad de celulares y tipo de tecnología que es usada en Colombia, supone un estado crítico a la hora de ejecutar este tipo de ataques y una alta probabilidad de éxito. Para reducir posibles impactos, se sugiere revisar normas como ISO27001:2013 [34], ITU serie X500 [35] o NIST 800-53 [36], entre otras.

Por otro lado, y a fin de reducir otros riesgos de exposición, para el caso de infección por *malware* en el *smartphone*, es necesario que los usuarios finales tengan configuradas las protecciones de los proveedores de los móviles o la instalación de un *software* antivirus que tenga aplicabilidad. Para los riesgos de negación de servicio (DoS/DDoS), y en consideración a que la consolidación de estos se puede presentar en la

red de telecomunicaciones (del lado del proveedor de servicio [ISP, por sus siglas en inglés), es necesario que el ISP implemente mecanismos de tipo DPI (por sus siglas en inglés) o mecanismos de continuidad de negocio que permitan la operación continua. Un programa de sensibilización y cultura hacia los usuarios finales es importante, lo que permitirá la reducción de ataques de tipo ingeniería social o ejecución remota a través de SMS, por lo cual la capacitación es fundamental para el entendimiento de la seguridad, así como conocer los riesgos de las redes sociales y su uso cotidiano.

5. CONCLUSIONES

Conocer el funcionamiento de la tecnología de telecomunicaciones en relación con el uso y las amenazas de seguridad permite, con las herramientas adecuadas (administrativas y técnicas), vulnerar el sistema y obtener información valiosa, o en tránsito o local de los sistemas, dado que un atacante con pocos recursos podría eventualmente hacer una captura de tráfico en las redes móviles y hacer uso de esta para fines maliciosos.

Se hace necesario, dada la cobertura actual de las redes móviles de telecomunicaciones en Colombia, pensar cómo identificar y proteger o controlar los diferentes ataques en dichas redes (en el uso de la tecnología actual o futura), en que los proveedores de telecomunicaciones desempeñan un papel muy importante en ese sentido. Asimismo, se plantea la necesidad de encontrar controles alternos que puedan ser propuestos por los diferentes proveedores de tecnología cuando no se puede actuar directamente sobre los riesgos, no se cuenta con un control específico o dicho control es costoso de implementar. También contar con medidas preventivas enfocados a las personas es fundamental, en atención a que los riesgos deben ser tratados (evitar, transferir, reducir o aceptar) independiente de la solución técnica o administrativa que pueda darse.

La gestión de riesgos es un mecanismo clave para la identificación de posibles amenazas e impactos en los sistemas, con lo cual usar un *framework* o norma para ello es fundamental a la hora de establecer los niveles de consecuencia a que se enfrenta una organización. En ese sentido, es necesario establecer un mecanismo de búsqueda continua de nuevas vulnerabilidades en los sistemas, consultado con los proveedores de servicio, fabricantes o fuentes como la CVE, así como establecer procesos de actualización permanente.

6. TRABAJO FUTURO

Se proyecta como trabajado futuro el desarrollo o el uso de otras herramientas que logren consolidar cualquiera de los ataques a los que se encuentran expuestas permanentemente las redes móviles de telecomunicaciones.

REFERENCIAS

[1] Ministerio de Tecnologías de la Información y las Comunicaciones. (31 en. 2020). *Boletín trimestral de las TIC, enero de 2020* [En línea]. Disponible en: https://colombiatic.mintic.gov.co/679/w3-article-125648.html

[2] Ministerio de Tecnologías de la Información y las Comunicaciones. (24 abr. 2020). *Boletín trimestral de las TIC: cifras primer trimestre de 2019* [En línea]. Disponible en: https://colombiatic.mintic.gov.co/679/w3-article-135691.html

[3] Ministerio de Tecnologías de la Información y las Comunicaciones. (5 mzo. 2019). *Boletín trimestral de las TIC: cifras tercer trimestre 2018* [En línea]. Disponible en: https://colombiatic.mintic.gov.co/679/w3-article-82350.html

[4] Gartner Group. (26 sep. 2019). *Gartner says global device shipments will decline 3.7 % in 2019* [En línea]. Disponible en: https://www.gartner.com/en/newsroom/press-releases/2019-09-26-gartner-says-global-device-shipments-will-decline-1-percent-in-2019

[5] ESET. (2019). *ESET Security Report América Latina 2019* [En línea]. Disponible en: https://es.readkong.com/page/eset-security-report-latinoamerica-2019-4355431

[6] A. Almanza. XIX Encuesta Nacional de Seguridad Informática. *Sistemas*, no. 151, pp. 12-41, 2019. https://doi.org/10.29236/sistemas.n151a3

[7] *Dinero*. (1 en. 2018). Sistemas operativos iOS y Android se volvieron menos confiables en el 2017 [En línea]. Disponible en: https://www.dinero.com/empresas/artículo/ios-y-android-tuvieron-mas-vulnerabilidades-durante-el-2017/253771

[8] J. Domenech. (2 en. 2018). *2017 registró un aumento de las vulnerabilidades en plataformas móviles* [En línea]. Disponible en: https://www.silicon.es/2017-registro-aumento-las-vulnerabilidades-plataformas-moviles-2368302?inf_by=5a6a2fb8671db8a70c8b4692

[9] National Vulnerability Database. (2019). *Statistics results of android* [En línea]. Disponible en: https://nvd.nist.gov/vuln/search/statistics?adv_search=false&form_type=basic&results_type=statistics&search_type=last3years&query=android

[10] Kaspersky Labs. (10 abr. 2013). *¿Qué es un ataque Man-in-the-Middle?* [En línea]. Disponible en: https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/

[11] D. Pérez y J. Pico. (2011). *A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communi-cations* [En línea]. Disponible en: http://www.cic.ipn.mx/~pescamilla/MS/papers_2014/PerezandPico2011.pdf

[12] S. Prowell, R. Kraus y M. Borkin, "Man-in-the-Middle", en *Seven deadliest network attacks*, C. Grimes, Ed. Syngress: Elsevier, 2010, pp. 101-120.

[13] M. Conti, N. Dragoni y V. Lesyk, "A survey of man in the middle attacks", *IEEE Journal*, vol. 18, no. 3, 2016, pp. 2027-2051. Doi: 10.1109/COMST.2016.2548426

[14] Instituto Nacional de Ciberseguridad. (20 mzo. 2017). *Amenaza vs. vulnerabilidad, ¿sabes en qué se diferencian?* [En línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[15] A. Kumar1, Y. Liu y J. Sengupta. (2010, ag.). Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation communication network. *IJECT* [En línea]. *1 (1)*, pp. 68-72. Disponible en: http://chenweixiang.github.io/docs/Evolution_of_Mobile_Wireless_Communication_Networks.pdf

[16] O. Rodríguez, R. Hernández, L. Torno, L. García y R. Rodríguez. (2005, en.-mzo.). Telefonía móvil celular: origen, evolución, perspectivas. *Ciencias Holguín* [En línea]. *11 (1)*, pp. 1-8. Disponible en: https://www.redalyc.org/artículo.oa?id=181517913002

[17] National Vulnerability Database. (7 mzo. 2019). *CVE-2018-11422 details* [En línea]. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2018-11422

[18] National Vulnerability Database. (7 mzo. 2019). *CVE-2018-11421 detail* [En línea]. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2018-11421

[19] National Vulnerability Database. (3 my. 2018). *CVE-2018-5455 detail* [En línea]. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2018-5455

[20] National Vulnerability Database. (29 my. 2017). *CVE-2017-7913 detail* [En línea]. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2017-7913

[21] A. L. García Reis, A. F. Barros, K. Gusso Lenzi, L. G. Pedroso Meloni y S. E. Barbin, "Introduction to the *software*-defined radio approach", *IEEE Latin America Transactions*, vol. 10, no. 1, pp. 1156-1161, en. 2012. Doi: 10.1109/TLA.2012.6142453

[22] R. Díaz y Y. García. (2017, nov. 10). *Desarrollo de un sistema receptor de FM utilizando radio definida por software* [En línea]. Disponible en: https://www.academia.edu/download/57598047/Ciencias_economicas-aportaciones_de_las_tecnologias_de_neuroimagen_p._127-129.pdf#page=295

[23] GNU Radio Foundation. (2020). *About GNU Radio* [En línea]. Disponible en: https://www.gnuradio.org/about/

[24] B. Bhushan, G. Sahoo y A. K. Rai, "Man-in-the-middle attack in wireless and computer networking: a review", en *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall)*, IEEE, Dehradun, 2017, pp. 1-6. Doi: 10.1109/ICACCAF.2017.8344724

[25] S. Yubo, K. Zhou y X. Chen, "Fake BTS attacks of GSM system on *software* radio platform", *Journal of Networks*, vol. 7, no. 2, 2012. Doi: 10.4304/jnw.7.2.275-281

[26] H. Alrashede y R. A. Shaikh, "IMSI Catcher Detection Method for Cellular Networks", *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, IEEE, Riyadh, 2019, pp. 1-6. Doi: 10.1109/CAIS.2019.8769507

[27] Kaspersky Labs. (2019). *Amenazas de seguridad móvil dirigidas a dispositivos Android* [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/threats/mobile

[28] National Vulnerability Database. (12 sep. 2019). *CVE-2019 detail* [En línea]. Disponible en: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Simjacker&search_type=all

[29] K. Lee, B. Kaiser, J. Mayer y A. Narayanan. (2020). *An Empirical study of wireless carrier authentication for SIM Swaps* [En línea]. Disponible en: https://www.usenix.org/conference/soups2020/presentation/lee

[30] Portal IsSMS2FASecure.com. (2020). *Security analysis of SMS-enabled websites* [En línea]. Disponible en: https://www.issms2fasecure.com/dataset

[31] International Organization for Standardization. *ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management*. Suiza: International Organization for Standardization, 2018.

[35] Municipio de Viterbo Carlas. (2019). *Plan de tratamiento de riesgos de seguridad y privacidad de la información* [En línea]. Disponible en: http://www.viterbo-caldas.gov.co/planes/plan-de-tratamiento-de-riesgos-de-seguridad-y-privacidad

[33] National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments - NIST 800-30* [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[34] International Organization for Standardization. *Norma técnica ISO/IEC 27001:2013*, 2.ª ed. Suiza: International Organization for Standardization, 2013.

[35] Unión Internacional de Telecomunicaciones. (2019). *X.500: Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services* [En línea]. Disponible en: https://www.itu.int/rec/T-REC-X.500/e

[36] National Institute of Standards and Technology. (2013). *800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organization*. [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf