Biblioteca del Congreso Nacional de Chile

Desafíos de seguridad del 5G

Serie Minutas Nº 57-21, 24/06/2021

por Marek Hoehn

Resumen

La presente Minuta introduce la tecnología de telecomunicaciones conocida como 5G, presenta las vulnerabilidades descubiertas por investigadores especializados y entrega recomendaciones generales para la seguridad cibernética.

Esta Minuta fue elaborada para apoyar la participación de las parlamentarias chilenas y los parlamentarios chilenos en el 18o Foro Parlamentario de Inteligencia y Seguridad del Parlamento Latinoamericano y Caribeño que se llevará a cabo en la Ciudad de Panamá durante los días 29 y 30 de Junio de 2021.

Departamento de Estudios, Extensión y Publicaciones - Biblioteca del Congreso Nacional
eMail: mhoehn@bcn.cl, Anexo: 1868

Tabla de contenido

1. Antecedentes generales

El 5G ya no es una tecnología del futuro, sino una realidad actual. Economías nacionales enteras ya han empezado a adoptar el 5G. Sin exagerar se pueda hablar del inicio de una nueva era. Se trata de la única tecnología creada hasta ahora con un enorme potencial para elevar el uso del Internet de las Cosas (*Internet of Things* - IoT), fomentar un entorno de interconectividad y sostener el crecimiento económico. La tecnología 5G traerá consigo un sin fin de beneficios, como una mayor velocidad de los datos, una menor latencia en el tiempo de respuesta de la red y una mayor fiabilidad. Sin embargo, al mismo tiempo y por ello mismo, es probable que surjan nuevas amenazas de ciberseguridad.

Los datos personales sensibles almacenados por empresa e instituciones podrían verse comprometidos por ciberataques en un mundo 5G. Esto no es nuevo ni constituye una particularidad de la tecnología 5G, pero más dispositivos IoT conectados implican más objetivos y vulnerabilidades que pueden ser aprovechados por atacantes. Es probable que todos y cada uno de ellos planteen riesgos de seguridad para toda la red de la que son parte[1], sea del hogar, de empresas o de instituciones públicas. Y una vez que los dispositivos IoT son vulnerados por los ciberdelincuentes, pueden causar daños en las respectivas organizaciones e incluso provocar daños físicos.

2. 5G – Una definición conceptual

En telecomunicaciones 5G significa "quinta generación", es decir, se refiere a la quinta generación de comunicaciones móviles y como tal a un un estándar de comunicaciones móviles que se está generalizando desde 2019. La tecnología denominada 5G se basa en la norma *Long Term Evolution* (LTE=4G) existente. Se espera que las células de radio (antenas) se desplieguen de forma más densa en las ciudades con el 5G que con las tecnologías predecesoras. De esta forma la conexión a Internet será de mayor velocidad y de menor la latencia.

Resumimos aquí brevemente la evolución de las generaciones tecnológicas para las telecomunicaciones:

- En los años 1980s fue introducido el estándar análogo que posteriormente fue llamado 1G. Su ancho de banda fue de 2 kbps (2 kilobits o 2 mil bits por segundo).
- Este estándar análogo fue reemplazado por uno digital, llamado 2G, que permitió enviar SMS (*Short Message Service*) y MMS (*Multimedia Messaging Service*). Su ancho de banda fue de 150 a 384 kbps, es decir, entre 100 y 200 veces más rápido que el estándar anterior.
- En el año 2000 fue introducido el estándar UMTS (*Universal Mobile Telecommunications System*), llamado comúnmente 3G. Su servicio fue denominado "banda ancha" por alcanzar hasta 2 Mbps (2 megabits o 2 millones de bits por segundo), es decir 5 a 10 veces más que la tecnología anterior, lo que ya permitió la navegación web, envío de correo electrónico y video llamadas en el teléfono celular.

1 Para más detalles sobre estos riesgos, véase: https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/, consultado el 23 de junio de 2021.

- Desde 2010 está disponible el estándar LTE (*Long-Term-Evolution*), llamado 3.9G y poco después el estándar LTE+ (*Long-Term-Evolution-Advanced*), el verdadero 4G. Este estándar permite conexiones inalámbricas de banda ancha, con velocidades entre 100 Mbps y 1 Gbps (entre 100 megabits y 1 gigabit por segundo), es decir, los datos son transmitidos entre 50 y 500 veces más rápido que con la tecnología anterior.
- Desde 2019 se está implementando el estándar 5G, basado en tecnología LTE pero con velocidades de datos de hasta 10 Gbps (10 gigabits por segundo; 10 a 100 veces más rápido que la tecnología anterior). El estándar usará rangos de frecuencia más altos y permitirá 100 mil millones de dispositivos móviles en todo el mundo direccionables simultáneamente. Por esta última característica, esta tecnología permitirá el desarrollo del Internet de las cosas IoT.

En algún momento, lo más probable es que la 5G sustituya a las actuales redes 4G. Según el Informe de Movilidad de Ericsson[2] publicado en junio de 2019, las suscripciones al 5G alcanzarán los 1,9 mil millones a finales de 2024, lo que supondrá más del 20% de todas las suscripciones móviles en ese momento. Así que, aunque todavía falta tiempo antes de que 5G se masifique, no es demasiado pronto para empezar a pensar en las implicaciones del 5G, tanto positivas como negativas.

3. Beneficios del 5G

Con la transición a la tecnología 5G, sepuede esperar un mejor uso de los recursos y una mejora de las comunicaciones diarias. Más concretamente, estas son las principales áreas en las que se mostrarán los beneficios del 5G.

- Mayor velocidad de conexión a redes: Como hemos señalado, la primera ventaja es la alta velocidad soportada por la red, que aumentará el volumen datos transmitidos.
- Mejor comunicación: La comunicación y la colaboración virtuales también mejorarán. Además, los métodos de comunicación de vanguardia que implican la realidad virtual y la realidad aumentada se sustentarán con éxito en la potente red 5G.
- Desarrollo de la red IoT: El 5G conectará todos los dispositivos que componen la red IoT. Este aspecto permitirá oportunidades para los usos del IoT, que van desde los drones, los autos autodirigidos, equipos de realidad virtual y realidad aumentada, así como otras tecnologías emergentes.
- Más innovación: Es muy probable que la tecnología 5G se convierta en un catalizador de la innovación. En los principales sectores verticales de la industria, como la sanidad, la automoción y la fabricación, observaremos avances tecnológicos nunca antes vistos.
- Reducción de consumo de energía: La tecnología 5G reducirá el consumo de la red principal en un 90% y ampliará la vida de la batería de sus dispositivos.

2 https://www.ericsson.com/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf

4. Vulnerabilidades de seguridad de la tecnología 5G

Durante la Conferencia "Black Hat 2019", investigadores de ciber-seguridad señalaron un fallo de seguridad en el 5G[3] que permite ataques de tipo "hombre en el medio" (*Man-in-the-Middle* - MiTM). Al parecer, los protocolos y algoritmos de seguridad para el 5G se están portando desde el estándar 4G y los expertos han descubierto que esto puede permitir la toma de huellas dactilares de los dispositivos para realizar ataques dirigidos y ataques tipo MiTM.

Lo anterior es posible porque la red 5G se compone de estaciones base, o células, que cubren un área determinada. Se conectan a la nube, y ésta se conecta a la red base. Para que la conexión sea posible, los dispositivos 5G envían información a la estación base. A continuación, la estación la envía a la cadena para que se autentique en la red central. La información entregada incluye detalles de configuración como si se habilitan o no las llamadas de voz, la capacidad de los SMS, la compatibilidad con la comunicación vehículo a vehículo (V2V), qué bandas de frecuencia se utilizan, la categoría del dispositivo, [...] los requisitos de radio.

Durante la misma conferencia "Black Hat 2019", los investigadores revelaron que en el 5G, al igual que en 4G, la información sobre las capacidades del dispositivo se envía a la estación base antes de aplicar cualquier medida de seguridad a la conexión. Básicamente, el tráfico está cifrado desde el punto final hasta la estación base, pero como las capacidades del dispositivo se envían antes de aplicar el cifrado, aún pueden leerse en texto plano (sin estar encriptado). Y esto permite múltiples tipos de ataque, como el mapeo de la red móvil (MNmap)[4], el *bidding down* (o degradación del servicio)[5] y el agotamiento de la batería en los dispositivos de banda estrecha del Internet de las cosas.

5. Interceptación de llamadas y rastreo de ubicación

Los investigadores también han descubierto tres fallos de seguridad tanto en el 4G como en el 5G, que pueden ser explotados para interceptar las llamadas telefónicas y rastrear la ubicación de los usuarios de teléfonos móviles. Lo realmente peligroso es que este tipo de ataque es poco complejo y que cualquiera con un poco de conocimiento de los protocolos de localización celular podrá llevarlo a cabo.[6]

---

3 Véase: https://threatpost.com/5g-security-flaw-mitm-targeted-attacks/147073/

4 El equipo de investigación que desveló esta amenaza fue capaz de crear un mapa de dispositivos conectados a una determinada red y enumerar detalles muy específicos como el fabricante del dispositivo, el sistema operativo, la versión, el modelo, lo que les permitió categorizar con precisión un dispositivo como Android o iOS, IoT o un teléfono, módem del vehículo, router, etc. Y este fallo abre la puerta a ataques dirigidos contra dispositivos específicos.

5 Los hackers pueden utilizar dispositivos que se hacen pasar por IMSI para ejecutar ataques de denegación de servicio (DoS). También pueden utilizar su condición de nodos de red de confianza para llevar a cabo ataques de "hombre en el medio", en los que envían comandos maliciosos a los dispositivos conectados. Uno de estos ataques hace que los dispositivos "pujen" (*bid down*, lenguaje de remates) por protocolos de red de menor calidad, provocando una degradación de la calidad de su servicio. Esto podría ser un ataque sutil pero muy dañino contra las redes de empresas.

6 Véase: https://techcrunch.com/2019/02/24/new-4g-5g-security-flaws/

7. Conclusiones

En primer lugar, la tecnología 5G sin duda permitirá más puntos de entrada para los ciberataques, no porque presentaría más o mayores vulnerabilidades que las tecnologías anteriores, sino que justamente porque es mejor y más rápida, por lo que aumentará e número y la variedad de dispositivos que la usen (desde refrigeradores a ampolletas o comederos para mascotas). Y mientras el nivel de conectividad y velocidad entre sus dispositivos IoT interconectados aumentará, se desplegarán múltiples oportunidades para que los actores maliciosos irrumpan en sus sistemas. Por lo tanto, podríams ser testigos de ataques a una escala nunca antes vista.

El masivo uso de la tecnología 5G también podría dar lugar a ataques de *botnets* (redes de algoritmos que suplantan identidades), que se extenderán a una velocidad mucho mayor de la que permiten las redes actuales. Los atacantes también podrían utilizar las *botnets* para iniciar ataques de denegación de servicio distribuidos (DdoS).

Con el rápido desarrollo de IoT y 5G, es crucial disponer de una estrategia de seguridad general antes de que comenzar a adoptar la tecnología 5G. Como ocurre con cualquier tecnología emergente, el 5G generará nuevos casos de uso que necesitarán medidas de ciberseguridad adecuadas. Por lo tanto, es recomendable antes de desplegar las redes 5G tener en cuenta las medidas de seguridad.

Es probable que se produzcan violaciones de la seguridad debido a los fallos de seguridad de la 5G. Es por ello que las redes 5G deben tener medidas de seguridad incorporadas. El primer paso importante seguirá siendo identificar las normas de seguridad que la tecnología 5G realmente necesita, junto con las estrictas normas y regulaciones de ciberseguridad impuestas a los proveedores de redes 5G.