Enrique Cobo Jiménez. Diseñador de *hardware* digital en Ericsson, Suecia.
Coordinador del GT Jóvenes Ingenieros del COIT.

Más seguros con el 5G

Las redes 5G ya no son el futuro, ya están aquí, y con ellas viene un cambio de paradigma: todo lo que pueda beneficiarse de una conexión estará conectado. ¿Pone esto en riesgo nuestra seguridad? ¿hasta qué punto se tiene en cuenta la privacidad? ¿**qué mejoras plantea el 5G** con respecto al 4G en este sentido?

La seguridad no deja de ser un compromiso entre lo que se pretende proteger y el coste de esa protección

Hay algo en el 5G que lo hace especial. Es la primera vez que una nueva generación de telefonía móvil nace no solo con la idea de mejorar la calidad de la red en sí, sino con la pretensión de revolucionar la sociedad entera. Son infinitos los casos de uso a los que se les dará cabida: coches conectados, *massive* IoT, industria 4.0 y aplicaciones de telemedicina, entre otras. Además, tu móvil dispondrá de una conexión a Internet más rápida.

Ahí donde hay un dispositivo conectado también hay una amenaza (o una oportunidad, si le preguntas a un *hacker)*, como se ha puesto de manifiesto en diversos artículos [1]. Pero ¿es esto cierto? Después de todo, cada vez que se inicia una conversación por WhatsApp aparece un mensaje que hace saber que "los mensajes y llamadas en este chat están protegidos con cifrado de extremo a extremo". ¿No vale con eso?

No. **El cifrado de extremo a extremo es una medida necesaria** para mantenernos seguros, y sin duda hace que un tercero no sea capaz de leer lo que has escrito, dado que es una conversación privada, pero **no es suficiente**. Otras de los factores que hay que tener en cuenta es la disponibilidad del sistema, que la podríamos definir como la posibilidad de que puedas mandar ese WhatsApp, siguiendo con este ejemplo.

Hay otros tipos de ataque que consisten en precisamente eso: hacer caer un sistema para que quede inoperativo temporalmente. Una caída del sistema en el caso de WhatsApp quizás te moleste un poco, pero, en el caso de la

telemedicina, por ejemplo, un ataque que hiciera caer la red al cirujano que opera a distancia podría ser letal.

Es por todo ello que, dada la gran variedad de casos de uso críticos que usarán la red 5G, ésta debe ser **"resiliente y segura, y preservar nuestra privacidad"** [2]. Resiliente, para que sea capaz de reaccionar con rapidez ante fallos o ataques. Segura, porque la seguridad de la red es nuestra seguridad. Y que preserve nuestra privacidad, porque no debemos ser vistos si no queremos.

Si tomamos el 4G como referencia, el sistema tiene multitud de mecanismos para asegurar su resiliencia y hace uso de criptografía de primer nivel para garantizar su seguridad. Estas características han sido heredadas y mejoradas en 5G. No obstante, respecto a la privacidad, hay algo que quizás no todo el mundo sepa.

Problemas de privacidad en 4G (y anteriores)

Los dispositivos móviles, al igual que sus usuarios, necesitan identificadores que les permitan conocerse y darse a conocer en determinados momentos. Tu móvil tiene infinidad de ellos; desde el IMEI (que identifica al terminal y que más de uno habrá obtenido "llamando" al *#06#) al MSISDN (un 'palabro' para tu número de teléfono). El que nos preocupa es el IMSI (International Mobile Subscriber Identifier), que vendría a ser como el pasaporte de tu tarjeta SIM, y cómo se transmite.

Cuando un dispositivo se conecta a la red, antes incluso de que se establezcan los mecanismos de seguridad, ambos deben identificarse y autenticarse mutuamente. Para ello, el terminal móvil transmite el IMSI en texto plano, esto es sin cifrar, puesto que las claves de cifrado aún no han sido generadas. Al transmitir el IMSI, la red genera una especie de problema que solo puede ser resuelto por la verdadera SIM que corresponde al IMSI. Por último, ahora sí, las claves para cifrar las comunicaciones se generan puesto que ya confían el uno en el otro.

Aquí es donde está el problema. **Si un atacante es capaz de obtener tu IMSI, te puede monitorizar y seguir tus pasos**. Simplemente, lo único que tiene que hacer es esperar a que tu móvil la mande. Estos ataques han proliferado durante los últimos años y se han elegido sitios con gran concurrencia para llevarlos a cabo, como son por ejemplo los aeropuertos. Además, la tendencia es que cada vez llevemos más 'cacharros' conectados, por lo que habrá más IMSI que nos pertenezcan. Adiós privacidad.

COMPARATIVA ENTRE LA SITUACIÓN EN 4G Y LA SOLUCIÓN EN 5G

EXPOSICIÓN DEL IMSI EN 4G Y ANTERIORES

SOLUCIÓN EN 5G CON SUCI

¿Qué es la privacidad?

No es un tema baladí definir la privacidad, puesto que es un concepto que varía entre culturas (tanto es así que en sueco ni siquiera hay palabra para ella). Según el diccionario de la RAE, este es el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

En Europa son muchos los esfuerzos que se están dedicando a mejorar nuestra privacidad. Un ejemplo es la archiconocida GDPR. En el ámbito del 5G, su equivalente sería el proyecto 5G Ensure [6], financiado por la Unión Europea y que trata de asegurar la privacidad de sus usuarios.

Dada la gran variedad de casos de uso críticos que usarán la red 5G, ésta debe ser "resiliente y segura, y preservar nuestra privacidad"

Otra versión más elaborada de este ataque consistiría en que el atacante se hace pasar por una estación base legítima. Por tanto, cuando quisieras conectarte a la red, esta estación base falsa te aparecería como válida, y felizmente le revelarías tu IMSI. Por supuesto, al no ser una base real, el mecanismo no se completa y quedarías expulsado de la red, al menos hasta que el móvil detecte otra estación base. Adiós, privacidad; y, además, adiós disponibilidad.

¿Pero cómo es esto posible? ¿Acaso no se sabía? Pues sí, se sabía. Al final, la seguridad no deja de ser un compromiso entre lo que se pretende proteger y el coste de esa protección. En generaciones anteriores, los dispositivos que permitían hacer todo esto eran muy caros, por lo que en la práctica no se hacía, sencillamente no valía la pena. No obstante, en la actualidad estos dispositivos se han vuelto muy baratos [3] y se pueden desplegar muy fácilmente, por lo que el problema se ha agravado.

¡5G, ayúdanos!

Igual que decimos que la tecnología ha avanzado y a consecuencia de ello los dispositivos para cazar IMSI se han vuelto muy baratos, también lo ha hecho la capacidad de los nuevos terminales móviles para defenderse en estas circunstancias. Esto hace que, por ejemplo, ahora se puedan plantear mecanismos para esconder nuestro IMSI y así mejorar en privacidad.

Es importante resaltar que no transmitir el IMSI no es una opción, ya que de lo contrario la red no tendría forma de autenticarnos y cualquiera podría hacerse pasar por nosotros. Hay que encontrar una forma de enviar esa información, pero escondida. Os presentamos al SUCI (pronunciado suqui), Subscription Concealed Identifier.

El SUCI es como tu IMSI, en el sentido de que te identifica unívocamente en la red, pero con la importante particularidad de que **se genera cada vez que se necesita uno**, de forma que tu IMSI queda oculto en ese identificador aparentemente aleatorio. Acto seguido, la red (legítima) descifra el IMSI de forma que se pueda seguir usando como hasta ahora [4]. Esto hace que, en la práctica, la red haya conseguido tu IMSI pero sin que nadie lo haya interceptado por el camino. ¿Magia? No, criptografía.

Ahora, cada vez que un terminal se conecta a la red, este usa un identificador diferente. Al no haber repetición, no hay forma de trazar una conexión entre el identificador y el usuario, ganando así en privacidad.

En cuanto al ataque por estación base falsa, la red 5G también incorpora mecanismos por los que se el terminal recibe informes sobre qué estaciones base hay en la zona y sus prestaciones. Así, si los datos de una estación base no concuerdan con lo que se espera, simplemente ésta se descarta, por lo que no hay problema de disponibilidad. Y, en el caso peor de que la estación falsa no sea detectada, tampoco revelarás tu identificador, puesto que el SUCI solo puede descifrarlo tu operador. Tu privacidad está garantizada en cualquier caso.

Estas mejoras, al igual que el resto de las características del 5G, ya están implementadas y estandarizadas por el 3GPP en su especificación de seguridad [5].

En definitiva, el 5G viene equipado con un montón de nuevas funciones y casos de uso, y la seguridad no se iba a quedar atrás. En este sentido, ha cogido lo mejor del 4G y ha resuelto problemas del pasado. La mejora de la privacidad es una de las joyas de la corona que ofrece la nueva generación, y ha sido posible gracias a que ésta se ha tenido en cuenta desde las etapas iniciales de diseño del 5G. ■

Lawful Interception o 'pinchazo legal'

Alguno se podrá preguntar si tanta privacidad se nos puede volver en nuestra contra. Al fin y al cabo, como pasa con cualquier herramienta, se puede usar para el bien o para el mal. Las redes móviles son infraestructuras críticas y parte fundamental para resolver crímenes, como por ejemplo siguiendo los pasos que ha realizado algún teléfono móvil.

Ese mecanismo se conoce como *Lawful Interception* y está igualmente estandarizado por el 3GPP e implementado en 5G [7]. Este permite que las autoridades, siempre bajo un pretexto legal, accedan a datos como conversaciones o la localización de dispositivos móviles.

El 5G viene equipado con un montón de nuevas funciones y casos de uso, y la seguridad no se iba a quedar atrás

[1] https://www.finanzas.com/macroeconomia/el-5g-sera-mas-robusto-en-seguridad-y-su-riesgo-vendra-de-la-conexion-masiva_14021397_102.html
[2] https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system
[3] https://www.hackplayers.com/2017/08/como-hacerte-un-imsi-catcher-sencillo.html
[4] E. Cobo Jiménez, P. K. Nakarmi, M. Näslund, y K. Norrman, "Subscription Identifier Privacy in 5G Systems", *2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNet'17)*, 2017.
[5] Security architecture and procedures for 5G systems (2018), 3GPP technical specification, disponible en: http://www.3gpp.org/DynaReport/33501.htm
[6] https://www.5gensure.eu/
[7] Lawful Interception (LI) architecture and functions (2017), 3GPP technical specification, disponible en: http://www.3gpp.org/DynaReport/33127.htm