Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Título: Geolocalización de dispositivos móviles mediante el Protocolo SS7

Autor: Lic. Ricardo Rubén Rocha

Tutor: Ing. Hugo Pagola

Cohorte 2018
Año de presentación: 2020

DECLARACIÓN JURADA

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

FIRMADO
Ricardo Rubén Rocha
DNI 20.890.486

RESUMEN

El sistema de señalización SS7 es un conjunto de protocolos utilizado en telefonía pública que describe una forma de comunicación entre diferentes elementos de una red telefónica. Su uso fue implementado originalmente en las redes clásicas PSTN de telefonía fija, permitiendo la interconexión de redes nacionales e incluso internacionales.

Con el advenimiento de la telefonía móvil, las redes de telefonía celular debieron interconectarse con las redes de telefonía fija y lo hicieron también mediante señalización SS7.

Las redes nacionales de telefonía celular, conformadas por diversos operadores de telecomunicaciones debieron también interconectarse y éstas a su vez debieron interactuar con otras redes nacionales en otros países de manera que un terminal móvil de un operador determinado pudiera comunicarse en redes de otros operadores, incluso en redes de telefonía móvil en países diferentes al país de origen.

En sus inicios, el sistema de señalización SS7 no fue pensado para proveer seguridad en las comunicaciones. Por el contrario, debía asegurar una alta disponibilidad, facilidad y agilidad del servicio telefónico. Este protocolo, heredado de la telefonía fija fue entonces el que permitió la integración de las diferentes redes de telefonía celular desde las primeras generaciones, la analógica 1G y luego las digitales 2G y 2,5G, actualmente en uso en la mayoría de los países, conviviendo incluso con generaciones posteriores, 3G, 4G y 5G.

La falta de seguridad en el protocolo permite explotar muchas vulnerabilidades, entre ellas, las que posibilitan la localización de un terminal, cuyo análisis, es el objeto del presente trabajo.

PALABREAS CLAVES: BTS, 5G, GEOLOCALIZACIÓN, SS7, ROAMING.

ÍNDICE DE CONTENIDOS

INDICES DE ILUSTRACIONES

AGRADECIMIENTOS

A mi esposa Verónica y a mis hijos Ana Laura, Matías y Federico, quienes fueron mi apoyo incondicional y motivador durante mi carrera y estudios.

A las autoridades de la Policía Federal Argentina donde presto servicios, quienes permitieron y alentaron mi continuidad académica.

Al Ingeniero Hugo Pagola y al Dr. Pedro Hecht por los conocimientos que con humildad y paciencia brindaron y por la confianza depositada.

GLOSARIO

3GPP 3RD GENERATION PARTNERSHIP PROJECT

A5 ALGORITMO DE CIFRADO 5

A8 ALGORITMO DE CIFRADO 8

AES ADVANCED ENCRYPTION ESTÁNDAR

AKA AUTHENTICATION AND KEY AGREEMENT

AMF ACCESS AND MOBILITY MANAGEMENT

ARPF AUTHENTICATION CREDENTIAL REPOSITORY AND PROCESSING FUNCTIOIN

AUC CENTRO DE AUTENTICACIÓN

AUSF AUTHENTICATION SERVER FUNCTION

AUTN AUTHENTICATION TOKEN

AVP ATRIBUTE VALUE PAIRS

BSC ESTACIÓN DE CONTROL

BSS SUBSISTEMA DE ESTACIÓN BASE

BTS ESTACIÓN BASE

DEA DIAMETER EDGE AGENT

DNS DOMAIN NAME SYSTEM

EDGE ENHANCED DATA RATES FOR GSM

EIR REGISTRO DE IDENTIDAD DE EQUIPO

EMBB ENHANCED MOBILE BROADBAND

eUTRAN ENVOLVED ULTRA TERRESTRIAL RADIO ACCESS

GMLC GATEWAY MOBILE LOCATION CENTER

GMSC GATEWAY MSC

GPRS GENERAL PACKET RADIO SERVICE

GSM GLOBAL SYSTEM MOBILE

GT GLOBAL TITLE

GUAMI GLOBAL UNIQUE AMF IDENTIFIER

HLR REGISTRO LOCAL DE LOCALIZACIÓN

hPCRF HOME POLICY CHARGING AND RULE FUNCION

IAM INITIAL ADDRESS MESSAGE

IMEI IDENTIDAD INTERNACIONAL DE EQUIPO MÓVIL

IOT INTERNET OF THINGS

IPSEC INTERNET PROTOCOL SECURITY

ISUP ISDN USER PART

IWF INTERWORKING FUNCION

KC CLAVE DE CIFRADO

KI CLAVE DE IDENTIFICACIÓN

KN CLAVE DE CIFRADO COMPARTIDA

KSI KEY SET IDENTIFIER

LAC LOCATION AREA CODE

LAI IDENTIFICADOR DE ÁREA LOCAL

LTE LONG TERM EVOLUTION

M2M MACHINE TO MACHINE COMMUNICATION

MAC MESSAGE AUHTNTICATION CODE

MAP MOBILE APPLICATION PART

MCC MOBILE COUNTRY CODE

MIMO MULTIPLE IMPUT MULTIPLE OUTPUT

MioT Massive Internet of Things

MME MOBILITY MANAGEMENT ENTITY

MNO MOBILE NETWORK OPERATORS

MS ESTACIÓN MÓVIL

MSC CENTRO DE CONMUTACIÓN

MSU MESSAGE SIGNAL UNIT

MTP MESSAGE TRANSFER PART

NDS NETWORK DOMAIN SECURITY

NMS SUBSISTEMA DE GESTIÓN DE RED

NSS SUBSISTEMA DE RED

OFDMMULTIPLEX POR DIVISIÓN DE FRECUENCIAS ORTOGONALES

OMC CENTRO DE OPERACIÓN DE MANTENIMIENTO

PDU PROTOCOL DATA UNIT

PLMN PUBLIC LAND MOBILE NETWORK

PO PAGING OCASSION

PRN PROVIDE ROAMING NUMBER

PSL PROVIDE SUBSCRIBER LOCATION
PSTN RED DE TELEFONÍA PÚBLICA
RDSI RED DIGITAL DE SERVICIOS INTEGRADOS
SBI SERVICE-BASED INTERFACES
SCCP SIGNALLING CONNETION CONTROL PART
SD SLICE DIFERENCIATOR
SEAF SECURITY ANCHOR FUNCTION
SEP SIGNAL END POINT
SEPP SECURITY EDGE PROTECCION PROXY
SGSN SERVING GPRS SUPPORT NODE
SIDF SUBSCRIBER IDENTITY DE-CONCEALING FUNCTION
SIM SUBSCRIBER IDENTITY MODULE
SIM SUBSCRIBER IDENTITY MODULE
SIO SERVICE INFORMATION OCTECT
SMS SHORT MESSAGE SYSTEM
SNOW CIFRADOR DE FLUJO PARA 4G
SON SELF ORGANIZED NETWORK
SPC SIGNAL POINT CODE
SPI SUBCRIPTION PERMANENT IDENTIFIER
SQN SEQUENCE NUMBERE
SS7 SISTEMA DE SEÑALIZACIÓN NRO. 7
SST SLICE SERVICE TYPE
STP SIGNAL TRANSFER POINT
SUCI SUBSCRIPTION CONCEALED IDENTIFIER
SUPI SUBSCRIPTION PERMANENT IDENTIFIER
TCAP TRANSACTION CAPABILITIES APPLICATION PART
TIMSI IDENTIFICACIÓN TEMPORAL DE
TLS TRANSPORT LAYER SECURITY
TUP TELEPHONE USER PART
UDM UNIFIED DATA MANAGEMENT
UDP USER DATAGRAM PROTOCOL
UDR UNIFIED DATA REPOSITORY

URLLC ULTRA-RELIABLE AND LOW LATENCY COMMUNICATION

VLR REGISTRO VISITANTE DE LOCALIZACIÓN

vPCRF VISITED POLICY CHARGED AND RULE FUNCTION

XOR OR EXCLUSIVA

ZUC ALGORITMO 3GPP DE INTEGRIDAD Y CONFIDENCIALIDAD

CAPITULO 1: INTRODUCCIÓN

Según el informe Mobile Economy que publica cada año la Asociación de Operadores Móviles GSM y quien organiza anualmente el MWC (Mobile World Congress), 1.000 millones de suscriptores de telefonía móvil se han sumado en los últimos cinco años a nivel mundial, lo que lleva a un número de 5.100 millones el número de personas que utilizaban un dispositivo móvil hasta el año 2018, lo que representa 2/3 de la población mundial. El informe también menciona que en los próximos siete años se incorporarán 700 millones más. Adicionalmente, 1,4 millones de personas comenzarán a usar internet móvil en dicho período, lo que lleva a un número de 5.000 millones para el año 2025. Si a eso le sumamos las tarjetas SIM que las operadoras entregan para uso en dispositivos industriales e internet de las cosas (IoT), la cifra superará el 100 % de la población para esa fecha.

El presente trabajo se iniciará con una explicación de las diferentes generaciones de telefonía móvil para entender así su evolución, también se incluirá un desarrollo de las distintas arquitecturas y protocolos, en particular el SS7 por ser la plataforma heredada de la telefonía fija en donde se apoyó durante mucho tiempo la telefonía celular, y lo sigue haciendo en algunos casos, como sistema de señalización para interconectar distintas redes a nivel local y global.

Se hará hincapié en la seguridad de las distintas generaciones y en las diferentes vulnerabilidades halladas e informadas y su explotación, para cada generación, reforzándose aquellas que permitan conocer la localización de los dispositivos móviles.

Finalmente se mencionarán algunas herramientas, aplicaciones y soluciones que existen en el mercado para lograr la localización de los dispositivos móviles, terminando con las conclusiones y recomendaciones a consideración del autor.

CAPITULO 2: EVOLUCIÓN DE LAS TECNOLOGÍAS MÓVILES

En el año 1946, la compañía Bell Telephone Labs presenta el primer sistema de telefonía móvil conocido. Se implementó en la ciudad de St. Luis USA y fue nombrado MTS (Mobile Telephone Service). El servicio era bastante limitado en principio ya que el número de canales y el ancho de banda eran reducidos. En 1970 AT&T diseña y prueba un sistema que hace un uso más eficiente del espectro de radiofrecuencia útil. En 1975 la FCC (*Federal Communication Committe*) concede a la firma la primera licencia par operar un servicio de radio celular en la ciudad de Chicago USA; el sistema conocido como AMPS (*Advanced Mobile Phone Service*). [1]

Así como en Estados Unidos surgió este sistema, otros países hicieron lo propio, apareciendo entonces varios sistemas de telefonía móvil, sin embargo, pronto se dieron cuenta que aparecía una creciente demanda de servicio por lo cual debieron optimizar la tecnología para hacer un uso eficiente de recurso natural limitado del espectro radioeléctrico y además, debieron mejorar la compatibilidad para que los sistemas pudieran interoperar. Así entonces aparece la primera generación, 1G la cual nació con tecnología analógica y carente de seguridad ya que lo que se pretendía era lograr una gran capacidad de usuarios, el uso eficiente del espectro y una amplia cobertura.

Respecto de la cobertura, la red celular fue diseñada teniendo en cuenta la reutilización de las frecuencias asignadas y para ellos se dividió el área en pequeñas celdas de forma hexagonal en la teoría, las cuales eran atendidas por una estación de radio. Cada estación de radio funcionaba con un grupo de canales de radio teniendo en cuenta la distribución en las diferentes celdas de modo de no causar interferencias entre celdas próximas.

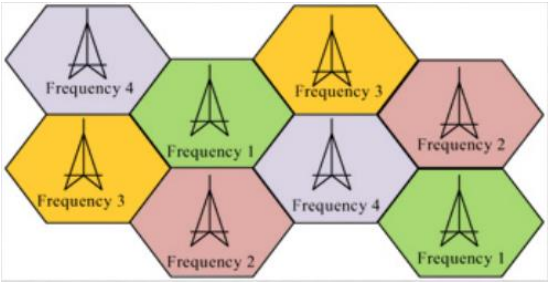

Ilustración 1 Red Básica de Telefonía Móvil.

Fte: "1ª Generación Móvil (1G)". Pag.10. Rosas Serrano Edson

"Los estándares más exitosos de esta generación fueron: NMT (*Nordic Mobile Telephone*), TACS (*Total Access Communications System*), y AMPS (*Advanced Mobile Phone Service*). NMT, creado en Escandinavia tuvo dos variantes, usando las bandas de 450 Mhz (*Megahertz*) y 900 Mhz, ofrecía el servicio de Roaming (*Itinerancia*) internacional lo cual significó una gran ventaja respecto de la competencia. El Reino Unido creó el estándar TACS en la banda de 900 MHz, el cual se basa en el protocolo AMPS, original de USA donde utilizaba la banda de 800 MHz. Japón también creó sus propios estándares, como el NTT y MCS". [1]"

El sistema de esta generación originalmente fue concebido para la transmisión de voz y en cuanto a la movilidad del usuario permitía la traspaso entre celdas o *handover* con tiempos de conmutación menores a los 500 milisegundos. Este mecanismo era manejado por el MSC (*Mobile Switching Center*) controlado por la red NCHO (*Network Control Handover*). La facilidad del mecanismo de registración permite conocer fácilmente la ubicación del terminal móvil dentro del área de cobertura. Finalmente, la tecnología de esta generación no permite la interconexión entre sistemas de diferentes proveedores lo que representa una limitación en la movilidad por no contar con el roaming internacional. [2, p.27]

2.1 SEGUNDA GENERACIÓN 2G

La primera tecnología digital fue la segunda generación (2G). Se trataba de aquellos sistemas que utilizaron las técnicas digitales para realizar las transmisiones. Uno de los sistemas más representativos de esta

generación fue sin dudas GSM (*Global System Mobile*) o sistema global para comunicaciones móviles. El gran cambio que introdujo esta generación fue la digitalización que posibilitó la oferta de nuevos servicios como ser el SMS (*Short Message System*) o sistema de mensajes cortos; además se introdujo la tarjeta SIM (*Suscriber Identity Module*) que independizó el terminal móvil del usuario.

Los elementos básicos de una red de telefonía celular para los sistemas de 2G son:

a) Estaciones Móviles (MS)
b) Estaciones Bases (BTS)
c) Estaciones de Control (BSC)
d) Centros de Conmutación (MSC)

Las MS son los equipos que suministran el servicio de voz, datos e imágenes a los usuarios. Pueden ser desde teléfonos celulares simples hasta smartphone, tabletas, pc, etc. Cuando solicita una comunicación utiliza la máxima potencia para conectarse a la red y una vez que obtiene el acceso acuerdan con la BTS, entre otras cosas la potencia óptima, reajustando los valores mínimos necesarios para mantener la comunicación.

Las BTS establecen el enlace radioeléctrico entre los MS y las Estaciones de Control (BSC), también se la conoce como interfaz de aire. Atiende una o varias MS y en base a la cantidad de éstas y el tipo de servicio se calcula la cantidad de BTS para dar cobertura en un área geográfica determinada.

Las BSC realizan la función de gestión y mantenimiento del servicio. También son las encargadas de asignar las BTS a las MS que se encuentran en un sector. Permite realizar la función de “handover o handoff” por la cual cambian de canal de comunicación de la estación base anterior por otro canal libre en la BTS próxima cuando se encuentra en desplazamiento (función de conmutación de las comunicaciones entre estaciones bases). Otra función importante es la de localización de una MS que se encuentra fuera de su sector habitual, esto implica que deben conocerse las MS residentes y las MS

visitantes para que las BSC puedan conocer la ubicación en cualquier instante.

Los MSC son los Centros de Conmutación de Servicios Móviles son los encargados de interconectar los usuarios de la red móvil con la red fija o usuarios de redes móviles entre sí. También mantienen las bases de datos para tratar las peticiones de llamadas de los abonados. Forman parte del Subsistema de Conmutación de Red (NSS-Network Switching Subsystem). Además de las tareas de conmutación, los MSC cuentan con un registro denominado VLR (Visitor Location Register) que guarda información de los MS que se encuentran fuera de la zona de su servicio central.

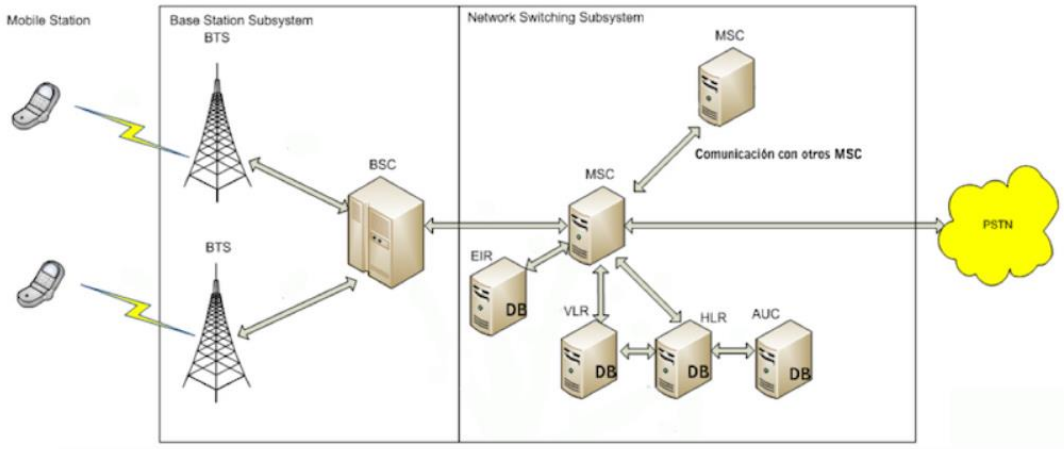

Ilustración 2 Elementos de una Arquitectura

Fte: "Sistemas de Telefonía y Comunicaciones Móviles.

".

La red GSM está conformada por entidades funcionales físicas y lógicas de acuerdo con el siguiente diagrama.

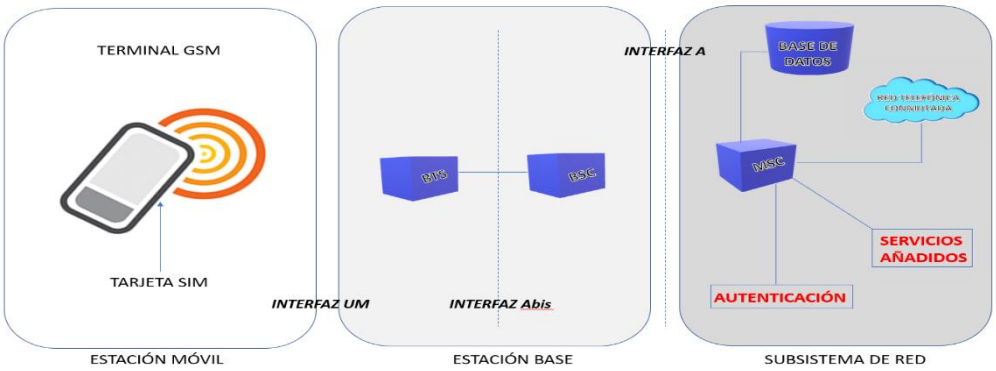

Ilustración 3 Arquitectura de una red GSM

Fte: "Comunicaciones Móviles", pág. 124, José Manuel Huidobro

A su vez se pueden distinguir tres subsistemas, a saber:

1- BSS o Subsistema de Estación Base
2- NSS o Subsistema de Red
3- NMS o Subsistema de Gestión de Red [2, p.124]

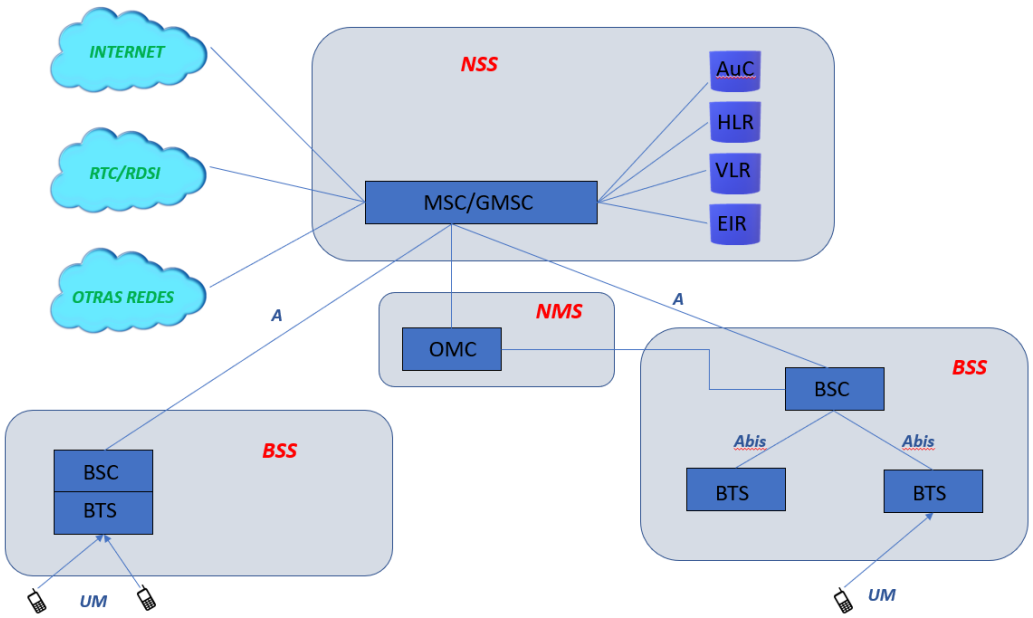

Ilustración 4. Diagrama en Bloques de una red GSM.

Fte: "Comunicaciones Móviles", pág. 125, José Manuel Huidobro

“El Subsistema de Estaciones Bases (BSS) está compuesto de los siguientes elementos:

BSC o Controlador de Estación Base: Es un centro de conmutación de canales de radio de alta capacidad. Controla la asignación de frecuencias y coordina la transferencia de llamadas entre distintas BTS (handover), con el objeto de mantener la comunicación evitando interferencias. Cada BSC controla varias estaciones bases (BTS) y a su vez, una MSC controla varias BSC. La interfaz entre la MSC y la BSC se denomina “Interfaz A”.

BTS o Estación Base Transceptora: Contiene los transmisores, receptores, amplificadores, antenas, duplexores, multiacopladores, combinadores y todo el procesamiento de las señales en la interfaz de radio para cubrir un área determinada con una o más celdas. La interfaz entre la BTS y la BSC se denomina “Interfaz Abis. Suele ser un enlace MIC (Modulación por Impulsos Codificados o PCM).

TC o Unidad de Adaptación de Velocidad y Transcodificación: Es la responsable de la transcodificación de la voz y adaptación de velocidad de 16 Kbs a 64 Kbs. Este componente algunas veces se encuentra integrado al conjunto BTS/BSC. Tanto si se encuentra integrado o no, el canal de 2 Mbps con el MSC puede transportar 120 canales de tráfico” [2, p.125].

“Las interfaces A y Abis permiten que los elementos constitutivos puedan ser provistos por diferentes fabricantes, siempre que respeten la norma.

La función principal de la BSS es conectar a los usuarios con la red móvil (NSS) por medio de la interfaz de aire” [2, p.126].

“El Subsistema de Red (NSS) está compuesto por los siguientes elementos:

MSC o Centro de Conmutación de Servicios Móviles: Es el equivalente a una central Pública de Conmutación Digital, pero con el agregado de capacidades para la red móvil. Realiza la función de conmutación telefónica y el control de llamadas entre abonados. Controla las llamadas provenientes o dirigidas a otras redes de telefonía o datos, como la red de telefonía pública (PSTN), a red digital de servicios integrados (RDSI), las redes de datos públicas y privadas o las redes móviles no propias del operador. También se

ocupa de las llamadas que se producen dentro de la red del operador y para ello necesita comunicarse con otros MSC dentro de su propia red y con el HLR dentro de su nodo. En todas las acciones que realiza se comporta como una pasarela para encaminar o enrutar los distintos tipos de llamadas por ello también se lo puede ver como un Gateway y comúnmente se lo suele denominar como GMSC o Gateway MSC. Por otro lado, también se ocupa de almacenar información para la facturación [5].

"La interfaz de señalización entre el MSC y la Red Pública Conmutada utiliza el Sistema de Señalización Nro. 7 (SS7)" [2, p.125].

"GMSC o Gateway Mobile Service Center: Sirve como puerta de acceso a otras redes. Se encarga de interconectar la Red de Telefonía Pública con la red GSM" [2, p.129].

"HLR o Registro Local de Localización: Es una base de datos local donde se almacena información de suscripción de los abonados. Almacena información sobre el perfil del servicio, localización y estado de actividad del abonado. Contiene la información de los usuarios que se han dado de alta dentro de la zona geográfica que abarca el nodo en el que se encuentra ubicado. En general posee los siguientes datos:

a) Identificación del abonado
b) Servicios adicionales contratados por el abonado
c) Información para su localización
d) Información para la autenticación del abonado" [5]

El HLR está vinculado al MSC y al VLR.

"VLR o Registro de Localización de Visitantes: Es una base de datos que contiene información del abonado que, en un momento determinado, se encuentran localizados en el área de acción de un nodo que no se corresponde con el nodo donde fueron dados de alta. El MSC es el que se percata de esta situación e incluye al abonado en el VLR. Además, contacta con el MSC de origen para que actualice la información de localización en su HLR. De esta manera, las llamadas dirigidas a este abonado pueden ser enrutadas correctamente" [5]. "Contiene información del abonado importante

para el Roaming de un abonado entre distintas redes. Se encuentra integrada al MSC. Cuando un abonado se encuentra en una red que no es la red local, la información sobre el mismo es transferida desde el HLR (Home Location Register) usando el procedimiento de actualización de la localización.

AuC o Centro de Autenticación: Autentica al usuario a fin de permitir el acceso del abonado a la red. También proporciona información de encriptación para cifrar los datos en la interfaz de aire.

EIR o Registro de Identidad de Equipo: Es una base de datos que contiene información para evitar llamadas desde estaciones móviles no autorizadas o robadas. Se basa en la información de identificación del teléfono IMEI (International Mobile Equipment Identity)" [2, p.130]. "Es un componente opcional dentro de la red GSM" [5].

"GIWI o GSM Interworking Unit: Sirve de interfaz de comunicación entre distintas redes de telecomunicaciones.

El MSC es responsable de controlar las llamadas en la red móvil y del encaminamiento de estas. Identifica el destino y origen de la llamada y el tipo de llamada. Cada Central MSC suele tener integrado un VLR que mantiene actualizada la información de los abonados.

El VLR es el encargado de mantener los registros de localización. Esta información es siempre temporal es decir que se conserva hasta que sale de su área de servicio.

El HLR mantiene la información de los abonados en forma permanente y además de los datos básicos almacena la localización actual de cada uno de los abonados, información que se utiliza para encaminar las llamadas [2].

Para la comunicación entre los distintos elementos de la red como ser MSC, HLR, VLR, AuC y EIR se utiliza el protocolo MAP (Mobile Application Part). Asimismo, utiliza el Sistema de Señalización Nro. 7 (SS7) para la transferencia de información.

El MSC cuenta con un centro de autenticación AuC asociado al HLR para proteger la información contra intrusión y fraude. También un EIR para controlar el acceso a la red y evitar el empleo de equipos móviles no autorizados" [2, p.130].

“El Subsistema de Gestión de Red (NMS) se ocupa de controlar y monitorear toda la red GSM. Para ello se encuentra vinculada al BSS y NSS. Su componente principal es el OMC o Centro de Operación y Mantenimiento. El OMC en un centro de monitoreo que está conectado a distintos componentes de la red como el BSC o el MSC, generalmente a través de conexiones X.25. El OMC recibe información de la red que le permite el estado de esta (tráfico, caída de enlaces, etc.) y actuar en consecuencia modificando distintos parámetros. Suele existir un OMC por cada Nodo” [5].

2.2 TERMINALES MOVILES (MS)

“El MS es el terminal móvil que se conecta con la red GSM a través de la interfaz de aire. Esta interfaz se denomina “Um”. El MS o terminal móvil está compuesto por el equipo móvil ME (*Mobile Equipment*) y una tarjeta inteligente denominada SIM (*Suscriber Identity Module*). El MS posee las características necesarias para soportar el canal de aire entre el MS y la BTS. El estudio complejo de la interfaz de aire, la codificación, modulación, etc. no son objeto de estudio en el presente trabajo.

El módulo de identificación del abonado (tarjeta SIM) provee la movilidad personal ya que el usuario puede acceder a los servicios que tiene suscripto con independencia del terminal telefónico. Posee capacidad para almacenar números telefónicos (de 100 a 250 registros) y cualquier otra información sobre perfiles, servicios, etc. La tarjeta SIM tradicional debe contener al menos la siguiente información:

a) Número de Serie, Estado (bloqueado o desbloqueado),
b) Clave del algoritmo de autenticación,
c) Algoritmo de Autenticación (A3),
d) Identificación Internacional del usuario móvil (IMSI),
e) Identificación temporal del usuario móvil (TMSI),
f) Algoritmo de generación de clave de cifrado (A8),
g) Clave del Algoritmo de Cifrado (A5),
h) Número de Secuencia de la Clave del Algoritmo de Cifrado y
i) Clase de Control de Acceso del Usuario

Además, se encuentra protegida por un número de cuatro dígitos llamado PIN (*Personal Identificaction Number*)" [2, p.131].

"La tarjeta SIM almacena información específica de la red usada para autentificar e identificar al cliente, entre otros parámetros:

- IMSI (*International Mobile Suscriber Identity*), que sirve para identificar al abonado en todo el mundo. Este número es el que permite el roaming.
- ICCID (*Integrated Circuit Card ID*), que es el número de serie de la tarjeta. Haciendo una analogía con redes TCP/IP, este número sería equivalente a la dirección MAC de una tarjeta de red de un dispositivo.
- KI o Clave de autentificación única que se asigna por el operador en el momento de personalización de la tarjeta.
- LAI o Identificador de área local (*Location Area Identity*). Este identificador está relacionado con las celdas y la ubicación geográfica en la que se encuentra el dispositivo móvil y su la tarjeta en ese momento. Cuando el terminal móvil cambia de ubicación de un área local a otra almacena su nuevo LAI en la tarjeta SIM y la envía al operador para informar a la red de esta nueva localización" [4].

Ilustración 5 Número ICCID de una tarjeta SIM

Fte: "Sistemas de Telefonía y Comunicaciones Móviles

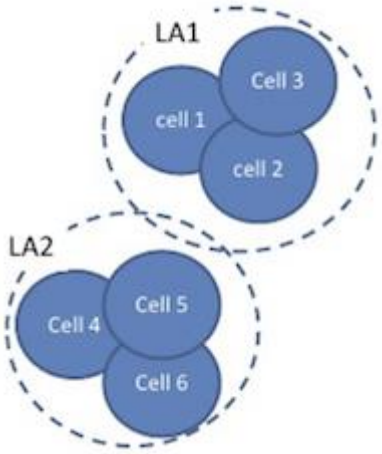

Ilustración 6. Conjunto de Estaciones Bases dentro de un Código Local de Área

Fte: "Sistemas de Telefonía y Comunicaciones Móviles

"El número IMSI, de acuerdo con el estándar ITU E.212 está formado por:

- MCC: Código del país (3 dígitos).
- MNC: Código de la red móvil (2 o 3 dígitos).
- MSIN: Número de 9 ó 10 dígitos como máximo que contiene la identificación de la estación móvil (*MS o Mobile Station*).

Siguiendo con la analogía con redes TCP/IP, el número ICCID sería el equivalente a la dirección IP asociada a un dispositivo cuando entra en una red de datos.

Por último, asociado a la compañía telefónica nos encontramos con la numeración MSISDN (*Mobile Station Integrated Services Digital Network*) que es nuestro número de teléfono móvil que fácilmente recordamos. Está compuesto por 15 dígitos como máximo (recomendación de la ITU-T, norma E.164) divididos en CC (*Country Code*), NDC (*National Destination Code*) y SN (*Subscriber Number*). En el caso de Argentina tenemos CC = 54, NDC vendría determinado por operador y dentro de éstos habría varios.

El IMSI se usa para registra al usuario en la red móvil del país (PLMN). Cuando un abonado se quiere registrar en la red, el HLR debe asociar el MSISDN con el IMSI.

El terminal móvil (equipo telefónico o aparato) se identifica ante la red a través de su número IMEI (*International Mobile Equipment Identity*). Este número es incorporado al equipo por el fabricante durante la manufacturación. El prestador de servicio de telefonía móvil guarda este número en un registro del EIR" [2, p,133].

"El IMEI está normalizado por la 3GPP y el documento TS 23.003, tiene 15 cifras (en algunos teléfonos 14, se omite el último dígito SPARE, normalmente un 0). Los IMEI que contengan la secuencia «17», sus 2 últimos dígitos no se emplean «00». El IMEI se subdivide en varios campos TAC, FAC, SNR y SPARE. El código de IMEI consta de cuatro partes y sigue el siguiente esquema: XXXXXX YY ZZZZZZ W.

Los seis primero caracteres en la primera parte (XXXXXX), conforman el TAC (*Type Allocation Code*), en donde los primeros dos dígitos indican el país de fabricación del equipo.

La segunda parte (YY) es el FAC (*Final Assembly Code*) e indica el fabricante del equipo.

La tercera parte (ZZZZZZ), compuesta de seis caracteres, es el número de serie del teléfono (SNR).

El último dígito (W), es el dígito verificador o (*Spare*), usado para verificar que el IMEI es correcto" [6].

2.3 ESTRUCTURA DE LA RED GSM

DIAGRAMA CELULAR: Las redes móviles tienen un identificador denominado LAI (*Location Area Identity*) o Identificador de Área de Localización. Este identificador es de carácter internacional y se utiliza para actualizar la posición de los suscriptores móviles. Se compone de tres códigos decimales, un código de tres dígitos que identifica el país de la red denominado MCC (*Mobile Country Code*), un código de tres o dos dígitos (según el continente) que identifica la red móvil denominado MNC (*Mobile*

Network Code) y un código de hasta cinco dígitos de área de ubicación denominado LAC (Location Area Code).

En base a lo anterior el LAI es la suma de tres códigos: LAI = MCC + MNC + LAC.

El LAC está constituido por un conjunto de celdas. Cada celda está identificada por un CELLID o Identificador de Celda. Dentro de la red la ubicación de un terminal móvil se conoce por el LAC donde se encuentra. Este código se almacena en el VLR y en el HLR. Cuando un terminal móvil pasa de un LAC a otro su localización se actualiza (esto no pasa cuando pasamos de un CELLID a otro dentro de un mismo LAC o si se cambia de LAC mientras se cursa una llamada) [5].

Cuando se cursa una llamada a un terminal móvil se transmite un mensaje a todas las celdas perteneciente al LAC para localizarlo.

Un MSC está formado por varios LAC y representa un nodo o zona geográfica controlado por éste. En su VLR se almacena el LAC de los abonados que se encuentran en su zona pero que no fueron dados de alta en su nodo. En el HLR se almacenan el LAC de los abonados que fueron dados de alta en ese nodo, sea cual fuera su posición [5].

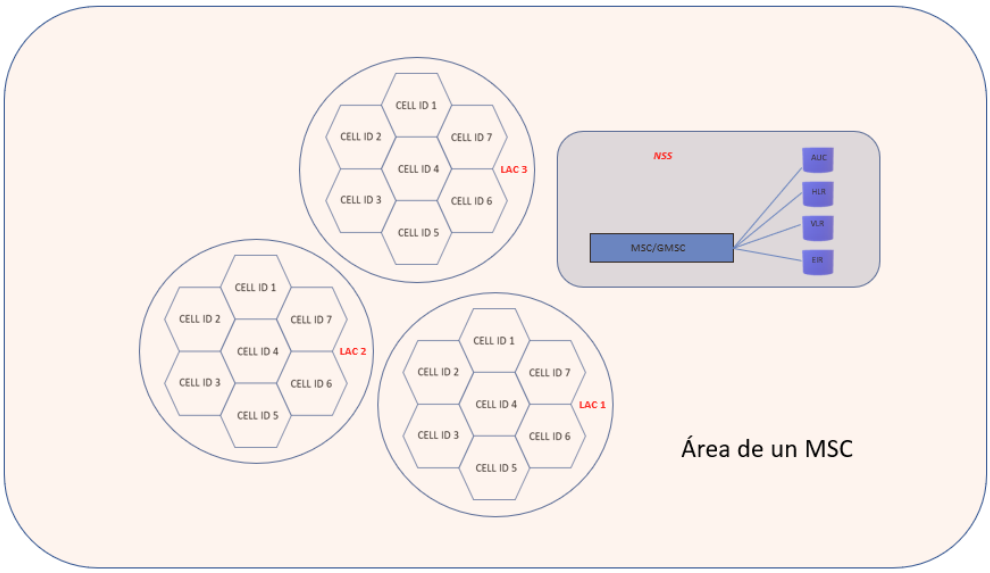

Ilustración 6. Área de un MSC.

Fte: Propia

Al conjunto de celdas controladas por un operador se lo denomina PLMN (*Public Land Mobile Network*)

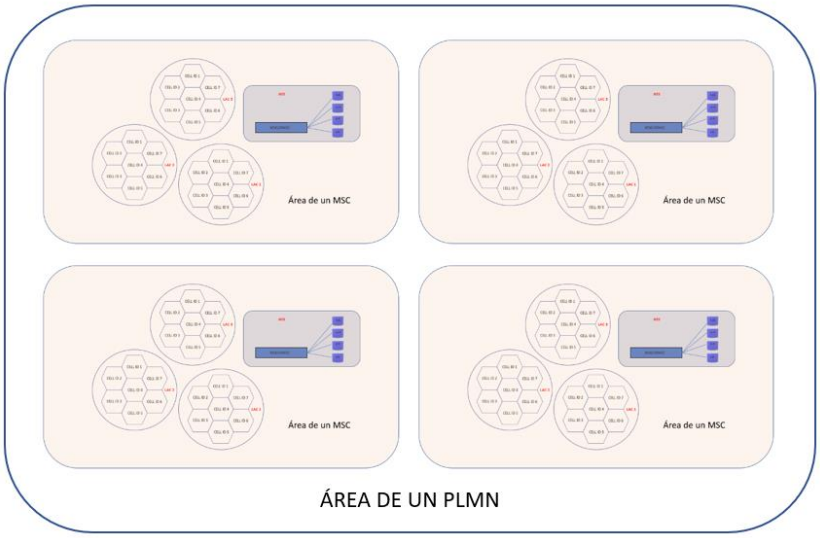

Ilustración 7 PLMN

Fte: Propia

El Área GSM es aquella donde se puede tener acceso a la Red GSM. El término “ROAMING” tiene que ver con la PLMN. Es decir que un abonado está en ROAMING cuando la red GSM en la que se encuentra no pertenece al operador con la que se dio de alta.

2.4 REALIZACIÓN DE UNA LLAMADA

“El escenario está conformado por un terminal móvil registrado en la red de telefonía móvil como visitante el cual marca un número de abonado con el cual se quiere comunicar.

Una vez enviada la petición la red analiza los datos del abonado que inicia la llamada para realizar tres operaciones:

- Autorizar el uso de la red
- Activar el servicio solicitado
- Encaminar la llamada

La llamada puede tener como destino un teléfono fijo u otro terminal móvil.

En el primero de los casos la llamada es encaminada hacia una red de telefonía fija pasando primero por la RTC.

En el segundo caso, si el terminal móvil se encuentra en la misma red, el MSC comienza un procedimiento de “Enquiry” hacia el HLR que será procesado del mismo modo que si la llamada tuviera su origen en la red PSTN.

Para lograr la comunicación se necesita cumplir con dos condiciones: Identificar y localizar al terminal móvil destino.

El MSISDN proporciona el servicio de identificación, pero para la localización la red GSM se vale de un procedimiento denominado “*Location Update*”.” [2, p. 143]

2.5 ACTUALIZACIÓN DE POSICIÓN

“En la práctica hay tres tipos de actualización de posición:

- Registro de posición.
- Registro de actualizaciones genéricas.
- Registro de actualizaciones periódicas.

El primero se lleva a cabo cuando se enciende el terminal móvil. A este procedimiento se denomina IMSI Attach. Tan pronto como el terminal es encendido, informa al VLR su nuevo estado. Como resultado de un registro correcto, la red envía al terminal móvil dos números que éste guardará en su tarjeta SIM. El primero de estos números es el Código de Área de Localización LAC (*Location Area Code*), y es enviado por la red mediante los canales de control de la interfaz de radio. El otro número es el TMSI (*Temporary Mobile Subscriber Identity*) y es utilizado por motivos de seguridad para que el IMSI de un abonado no tenga que ser transmitido por la interfaz de aire. Se trata de una identidad temporal que es cambiada periódicamente.

Cada vez que el terminal recibe datos a través de los canales de control, lee el LAC y lo compara con el que tiene almacenado en la tarjeta SIM. En caso de que sea diferente, se produce una actualización de posición genérica. El terminal comienza un proceso de actualización de posición consultando al MSC/VLR que envió los datos de posición. Se establece así una conexión de señalización entre los dos MSC/VLR, y el IMSI del abonado es transferido desde el viejo MSC hacia el nuevo. Usando este IMSI, el nuevo MSC solicita datos del abonado al HLR y actualiza el VLR y el HLR luego de la autenticación.

La actualización periódica de posición se lleva a cabo cuando la red no recibe ninguna petición de actualización desde el móvil en un cierto periodo. Esta situación se presenta cuando un móvil es encendido, pero no se origina ningún tráfico, ya que en este caso el móvil se limita a leer y sopesar la información enviada por la red. En caso de que el abonado se esté moviendo dentro de una misma área de localización, no es necesario que envíe ninguna petición de actualización de posición.

Las actualizaciones periódicas están controladas por contadores cuyo valor es establecido por el operador en el VLR. Este valor, además, es difundido por la red para que lo conozcan las estaciones móviles. Así, pues, cuando el valor temporal es establecido, la estación móvil comienza un proceso de registro mediante el envió de una señal de petición de actualización (*Location Update Request Signal*). El HLR recibe la petición y confirma el registro del móvil dentro del área de localización. Si la estación móvil no sigue este procedimiento, es posible que se deba a un agotamiento súbito de la batería o a que se encuentre fuera de cobertura En ese caso, el VLR cambia los datos de localización del móvil a desconocido". [2, p.143]

2.6 MECANISMOS DE SEGURIDAD

"La interfaz de radio es la más vulnerable ya que se encuentra a la mano de cualquier persona. Para evitar que un atacante pueda aprovechar esta debilidad se adoptaron varias medidas de seguridad, entre ellas el cifrado del enlace y la autenticación del abonado, mediante el uso de la tarjeta SIM. Esta tarjeta guarda información relativa al suscriptor y un código de

identificación persona (*PIN*) de cuatro cifras, el cual es empleado cuando el terminal es activado. Luego que el usuario se identifica ante el SIM mediante su PIN, la red verifica el SIM mediante un protocolo de autenticación. En cada nueva operación del sistema consulta el registro de posiciones (local o visitante) en la central de conmutación y se cerciora de que el usuario tiene derechos de acceso a la red mediante un breve diálogo con la tarjeta SIM. La protección de la identidad del terminal, para evitar el seguimiento de su localización por terceros, ser realiza mediante la asignación por parte de la red de un alias temporal (TIMSI), al menos en cada actualización de posición". [2, p.153]

2.7 PROCESO DE CIFRADO

"La seguridad en GSM reside en la tarjeta SIM del suscriptor, cual contiene entre otras cosas, un PIN o número de identificación personal, la identidad internacional móvil del usuario (IMSI), la clave individual de autenticación del usuario (Ki) y el algoritmo de autenticación A3.

Cuando se inicia una comunicación, el suscriptor se identifica en la red y recibe un número aleatorio R que junto con la clave Ki se usan para calcular la respuesta S (*Signed*), invocando el algoritmo A3.

$$S = [Ki\ (A3)\ R]$$

El resultado S se envía a la red y se compara con la versión local almacenada en la AuC del sistema para autorizar el acceso. A su vez, la red envía al suscriptor un mensaje con una clave Kn que se usa como clave de cifrado por el emisor y el transmisor. Esta clave Kn lo guarda el suscriptor y se envía en el primer mensaje a la red. El suscriptor usa la clave de cifrado Kc empleando el algoritmo confidencial A8, de generación de clave de cifrado, almacenado en la tarjeta SIM del suscriptor y los parámetros R y Ki.

$$Kc = [Ki\ (A8)\ R]$$

La clave de cifrado Kc se procesa en la red y así no se envía ninguna información confidencial desprotegida en la interfaz de radio. [2, p.153]

"A esta altura tanto el suscriptor como la red conocen Kc.

La red codifica y decodifica los mensajes con el algoritmo A5 para asegurar la confidencialidad.

Del lado del usuario, la confidencialidad se puede mejorar aun protegiendo la identidad del usuario a través de la identidad temporal lograda con el TIMSI asignada al suscriptor por la red en áreas específicas. El TIMSI identifica al IMSI en un área específica. Fuera de esta área la identificación debe ser asociada a una identificación de área local (LAI). El registro VLR que forma parte de la red controla las asociaciones TIMSI-IMSI como así también el proceso de localización de cada TIMSI en cada nueva área.

Este proceso es activado a voluntad por los distintos operadores de la red de telefonía celular. De acuerdo con el estado de la red el operador puede habilitar o deshabilitar esta función ya que la misma reduce el rendimiento del sistema en general, es decir que el uso de cifrado es inversamente proporcional a la calidad del servicio en cuanto a la disponibilidad de recursos necesarios para brindar servicios y los suscriptores no tienen noción de ello". [2, p.154]

Como se mencionó anteriormente, la red 2G fue la primera red de telefonía móvil digital. La misma posee entonces tres partes bien diferenciadas.

1- Infraestructura de usuario
2- Red de Acceso
3- Red Core (Heredada de la telefonía clásica previa)

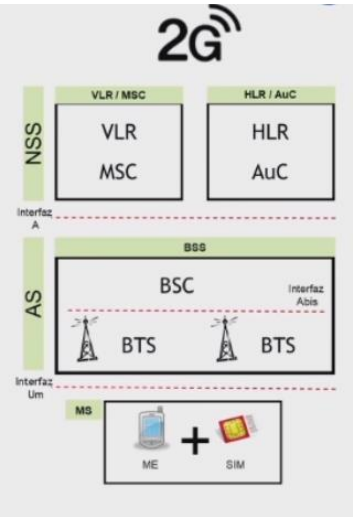

Ilustración 8. Arquitectura de la red 2G.
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Dentro de sus características principales podemos citar que la Red Core es una red de conmutación de circuitos que inicialmente estaba pensada para transportar comunicaciones de voz. Incorporaba algunas características de datos muy básicas.

Posteriormente sobre esta infraestructura se incorporaron capacidades de transmisión de datos GPRS y luego se mejoraron la tecnología EDGE llegando a dar una tasa de transferencia de 470 Kbps.

Esta generación nació con un problema de seguridad bastante grande: Los usuarios se autenticaban ante la red, pero la red no lo hacía ante los usuarios. Esto posibilitó un gran número de ataques basados en BTS (estaciones de radiobase falsas) que se intentó solucionar en la siguiente generación, 3G [7].

2.8 TERCEREA GENERACIÓN (3G)

En esta generación se agregó el dominio de datos en la Red Core como un dominio de conmutación de paquetes sobre el dominio existente de conmutación de circuitos.

A nivel de arquitectura general no hubo cambios, aunque sí hubo cambios a nivel de la red de acceso, en cuanto a las velocidades de acceso de transmisión de datos llegando a una tasa de transferencia de 42 Mbps.

La novedad fue la incorporación de un procedimiento de intercambio de claves denominado ACA que garantizaba que tano el usuario como la red se autenticaran mutuamente. Esto solucionó gran parte de los ataques de estaciones bases falsas.

El gran cambio de infraestructura se da en la cuarta generación (4G) aunque esta también hereda ACA de la generación anterior.[7]

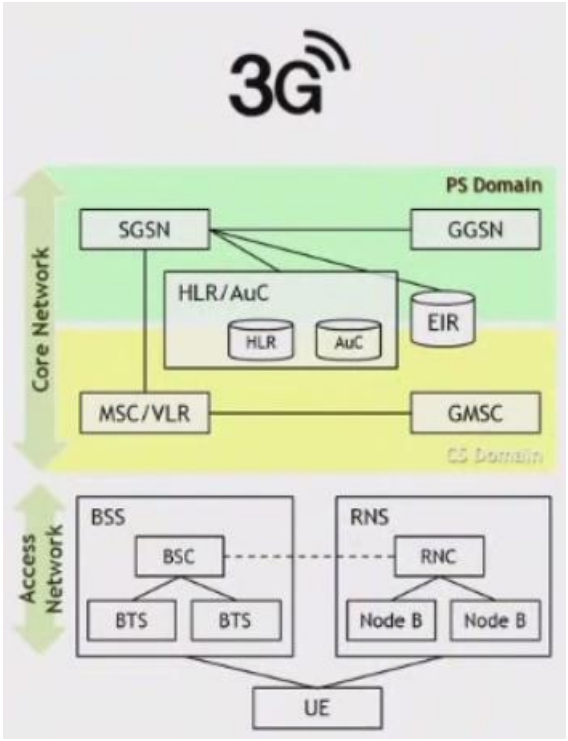

Ilustración 9. Arquitectura de la red 3G

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

2.9 CUARTA GENERACIÓN (4G)

El cambio fundamental es en la arquitectura de red (ahora la arquitectura es de una red totalmente IP, salvo en la interfaz de radio), aparte de las capacidades de radio en la red de acceso consiguiendo llegar aproximadamente a 1 Gbps en la especificación ADVANCE y 3 Gbps en la especificación ADVANCE PRO.

En esta generación se comenzó a pensar en dar soporte a dispositivos que no fueran los terminales de usuarios, los denominados dispositivos IOT (internet de las cosas). Estos requerían acceso a la red de lugares puntuales y con poca capacidad de datos, pero con requerimientos de ahorro de baterías bastante grandes y dispositivos industriales. [7]

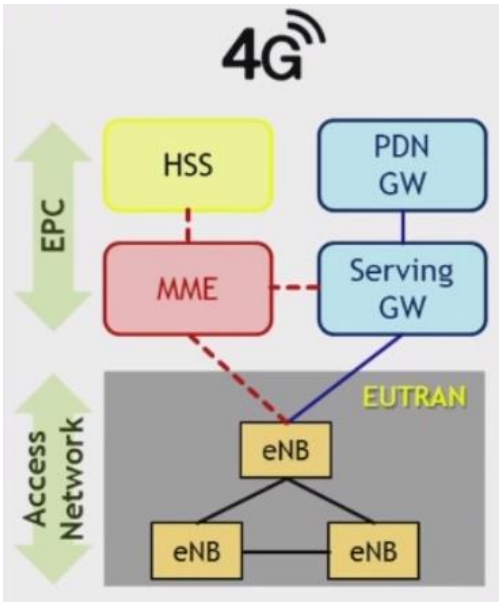

Ilustración 10. Arquitectura de la red 3G.

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

CAPITULO 3: SITUACIÓN ACTUAL DE LOS PROTOCOLOS 5G

"Si bien en nuestro país esta red no se encuentra todavía desplegada, a nivel teórico la Release 15, denominada fase 1, ya se encuentra publicada desde finales del año 2018 y está orientada al despliegue mínimo de la tecnología, donde se ha diseñado la arquitectura de seguridad, de la red core y se han definido los requisitos mínimos de los mecanismos de gestión y tarifación. También se ha definido un soporte en tres grupos de dispositivos. Uno de ellos se relaciona con los dispositivos IoT, el otro es un grupo de dispositivos que requiere comunicaciones extremadamente fiables con una latencia muy baja para permitir el funcionamiento de equipos industriales de alta disponibilidad, M2M (*Machine to Machine Communication*) y dispositivos similares; finalmente, dispositivos móviles con alta tasa de transferencia para permitir servicios como realidad aumentada, realidad virtual, etc.

La Release 16, denominada fase 2, va a ser publicada a principios del año 2020 y lo que pretende es solucionar algunas de las fallas de seguridad que se han detectado en la Release 15 y mejorar la definición de capacidades de soportes a los dispositivos mencionados. También se tratará de mejorar

los servicios de geolocalización y de comunicación de móviles que circulan a grandes velocidades (trenes de alta velocidad, vehículos militares, etc.)” [7]

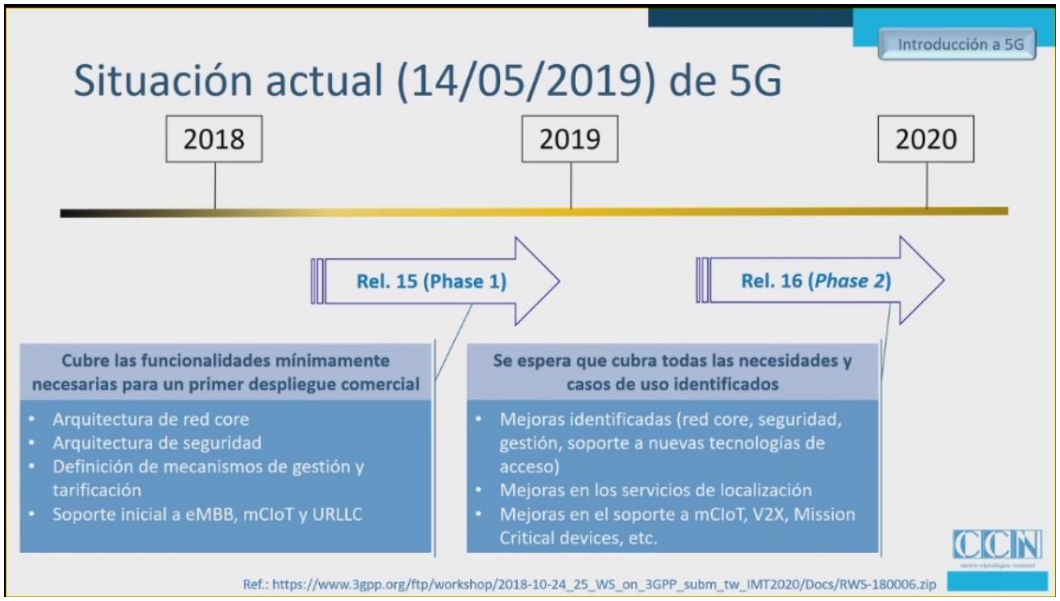

Ilustración 11. Situación actual de la Red 5G.

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

La motivación principal para la implementación de la 5ª Generación es agregar capacidades a la tecnología ya existente, para el soporte de los tres grandes grupos de dispositivos mencionados

- EmBB (*Enhanced Mobile Broadband*)
- MioT *(Massive Internet of Things*)
- URLLC (*Ultra-reliable and Low Latency Communications*)

Los dispositivos EmBB requieren ancho de banda aumentado y más velocidad de transmisión para conseguir servicios como transmisión (*streaming*) de video de ultra alta definición, realidad aumentada y realidad virtual.

Luego también se requiere mejorar la movilidad de los usuarios, para proporcionar mejor cobertura y mejores servicios en el salto entre celdas y mejorar también la velocidad de despliegue para los operadores.

En el caso de MioT, lo que se pretende es brindar un soporte adecuado a dispositivos, ya sean domésticos o industriales, que exigen por ejemplo un gran ahorro de batería y el uso en múltiples entornos (industriales, salud, misión crítica, etc.).

Con relación a los dispositivos URLLC, se necesita alta fiabilidad y muy baja latencia; sobre todo para dispositivos industriales y también en atención médica remota, todos ellos son servicios críticos que requieren muy alta disponibilidad. [7]

La pretensión de brindar servicio a la totalidad de los dispositivos abarcados en los tres grandes grupos representa un gran desafío, debido a que cada uno de ellos tiene una parametrización o unas necesidades muy diferentes, en cuanto a fiabilidad, disponibilidad, latencia, localización, capacidad de tráfico, velocidad y densidad de la interfaz de aire, aislamiento y tarifación.

Esto es lo que ha motivado el cambio de arquitectura en la infraestructura de 5G.

3.1 ARQUITECTURA

Podría decirse que el gran motivador para este cambio ha sido la virtualización de las funciones de red y por otro lado lo que se ha llamado fragmentación de la red (*Network Slicing*).

La virtualización de la red posibilita que con una infraestructura razonablemente eficiente se pueda dar servicio a los diferentes tipos de dispositivos mencionados [7].

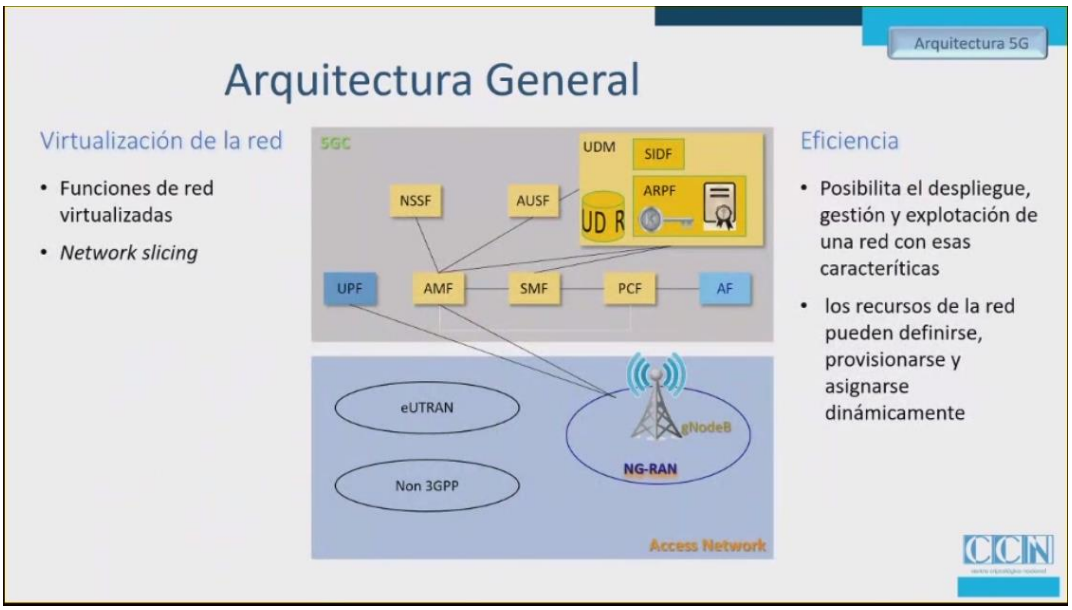

Ilustración 12 Arquitectura de la Red 5G.

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

3.2 RED DE ACCESO

La idea es mejorar las tecnologías empleadas en la interfaz de aire o acceso de radio para mejorar las capacidades de transmisión.

Esta mejora está basada en la técnica llamada OFDM ESCALABLE, antenas MIMO masivas, técnicas de compartición del espectro radioeléctrico, todo ello para que la transferencia de datos pueda llegar a 20 Gbps y una latencia máxima en los servicios más críticos de 1 milisegundo, de extremo a extremo. Esta evolución de la tecnología de radio en 5G es denominada NG-RAN. [7]

En cuanto al resto de tecnologías soportadas, se mantiene la tecnología eUTRAN ya que se pretende compatibilidad con la tecnología 4G y además el acceso a la red a través de cualquier tecnología de red de acceso conectada a internet. Esto último si bien es un servicio que se brindaba en la

generación anterior, las especificaciones se encuentran definidas en forma mucho más precisa en 5G.

Entonces, los tres tipos de acceso que se soportan son los nativos 3GPP, que son el 5G (NG-RAN), el eUTRAN de 4G, y acceso desde internet [7].

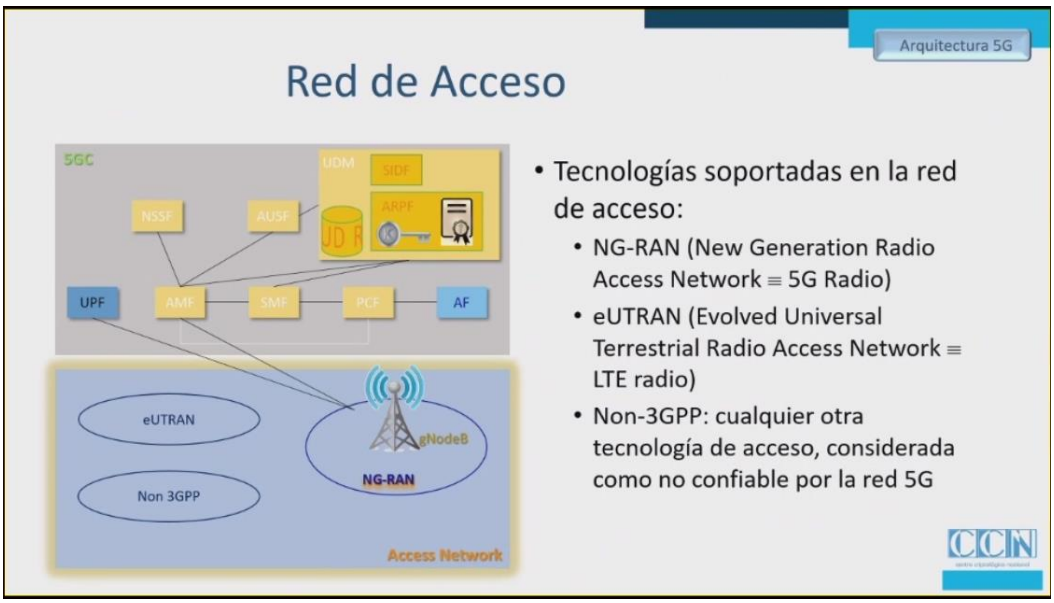

Ilustración 13 Red de Acceso 5G.

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

3.3 ARQUITECTURA DE RED DE ACCESO

En la red CORE se han definido funciones de red basados en el servicio que proporcionan, dinámicamente configurables, parametrizables, etc. Estas funciones tienen definidos los servicios que brindan mediante dos fases que se llaman SBI (*Service-Based Interfaces*). Otra característica es que se definen sin estado el cual es delegado en el almacenamiento de datos de usuarios, que guarda no solo datos de usuarios sino también aquellos que varían con el tiempo, como por ejemplo los datos de su conexión o los datos de la celdas en que se encuentran los suscriptores.

Esta forma de virtualizar las funciones de red es lo que permite que se puedan ofrecer servicios parametrizables para un tipo específico de dispositivo, junto con el network Slicing.

Otra característica es que se soporta la exposición dinámica de sus capacidades. Esto permite también que la interconexión entre redes sea más eficiente e incluso que se puedan delegar ciertas capacidades de la red en terceros que no pertenecen a la propia red [7].

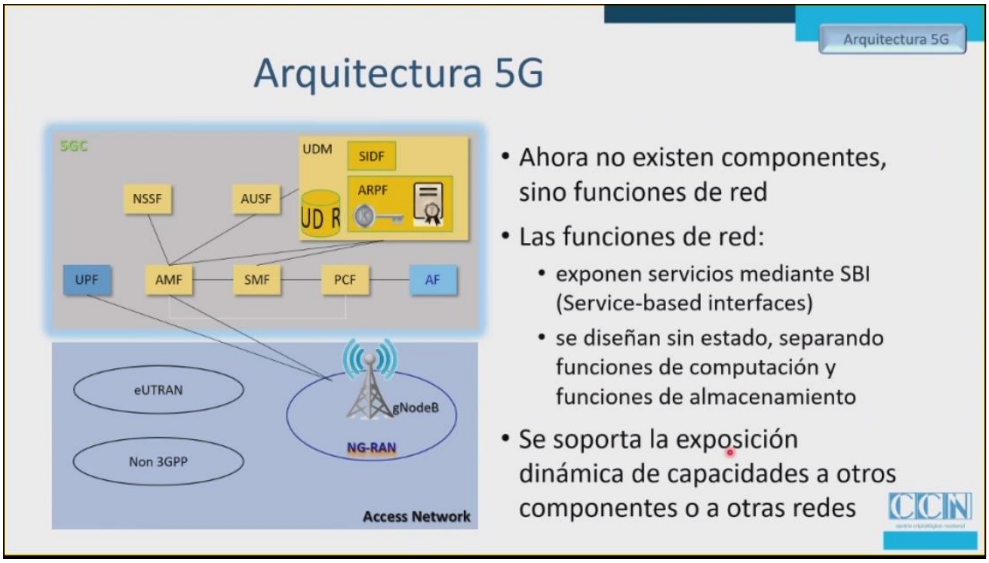

Ilustración 14 Arquitectura 5G.
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"La cuestión de la seguridad forma parte del diseño de las comunicaciones móviles en 5G por lo cual se ha pensado también en la seguridad de estas interfaces.

Las principales funciones de red core son, a saber:

AMF: Access and Mobility Management Function
SMF: Session Management Function
AUSF: Authentication Server Function
UDM: Unified Data Management
SIDF: Subscription Identifier De-Concealing Function
ARPF: Authentication credential Repository and Processing Function

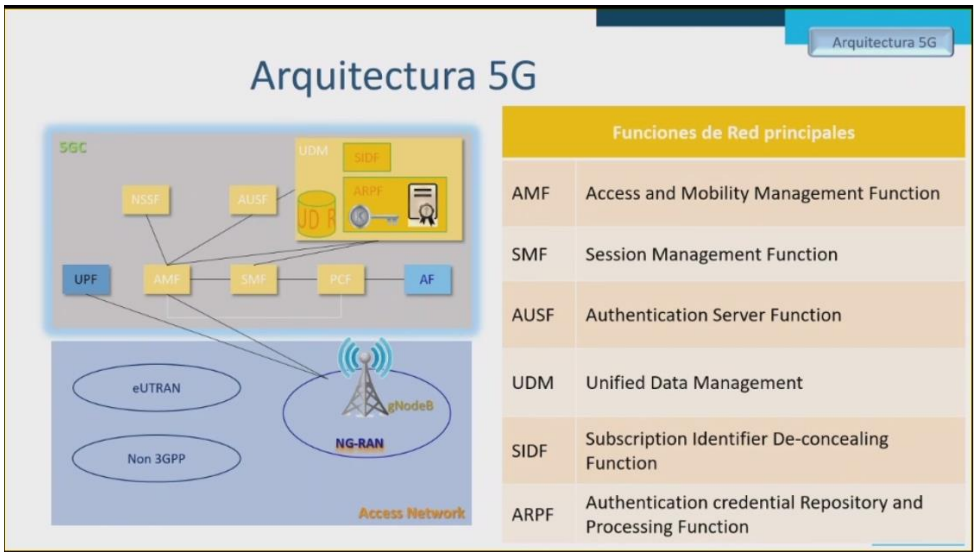

Ilustración 15. Arquitectura 5G (Funciones de Red Principales).

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"En cuanto a las comunicaciones entre los propios elementos de la red core, también hubo un cambio importante en 5G.

A partir de 3G, las comunicaciones entre elementos de la red core se basaba en la pila de protocolos SS7. Este protocolo nació en 1975 para las redes de telefonía clásicas cableadas, por lo tanto, su definición no incluía nada de seguridad porque se consideraba que era seguro de por sí. La seguridad era proporcionada por los accesos físicos a la red que estaban o se suponía que estaban protegidos" [7].

En 3G se heredan las infraestructuras y también la presunción de que los entornos de comunicación entre elementos de la red core estaban inherentemente protegidos, como así también las comunicaciones entre diferentes redes, las cuales se realizaban mediante canales dedicados. La realidad fue cambiando con el tiempo debido a que aparecieron un gran número de operadores y de empresas que dan otros tipos de servicios que son capaces de conectarse a las redes core de los operadores.

El uso del protocolo SS7 y luego DIAMETER que es la evolución del protocolo para 4G condujo a que hayan aparecido un gran número de vulnerabilidades explotables y de gran impacto dado que permiten desde el secuestro de las comunicaciones hasta la suplantación de usuarios o la geolocalización de estos. [7]

DIAMETER es un protocolo de red, diseñado para suministrar un marco de trabajo que ofrezca servicios triple A (*Authentication, Authorization, Accounting*) para aplicaciones que involucran acceso a redes o aplicaciones IP Móvil. Es un estándar cuyo desarrollo se ha basado en el protocolo RADIUS y esta estandarizado de acuerdo con el RFC 6733. [8]

Ilustración 16. Protocolo DIAMETER

Fte: DIAMETER

Respecto del Protocolo SS7, dado que es un vector de ataque muy explotado se desarrollará el contenido en una sección aparte.

En 5G el paradigma de la seguridad ha cambiado con la incorporación de los SBI (*Service-Based Interfaces*) ya que es una interface unificado y definido que incorpora la seguridad.

La pila de protocolo que se utiliza para este acceso se encuentra predefinida e incorpora TLS como capa de seguridad para la autenticación mutua, extremo a extremo y que son dos funciones de red como así también la confidencialidad en las comunicaciones entre estos dos extremos. De esta forma cualquier comunicación entre cualquier elemento de la red core está protegida por TLS.

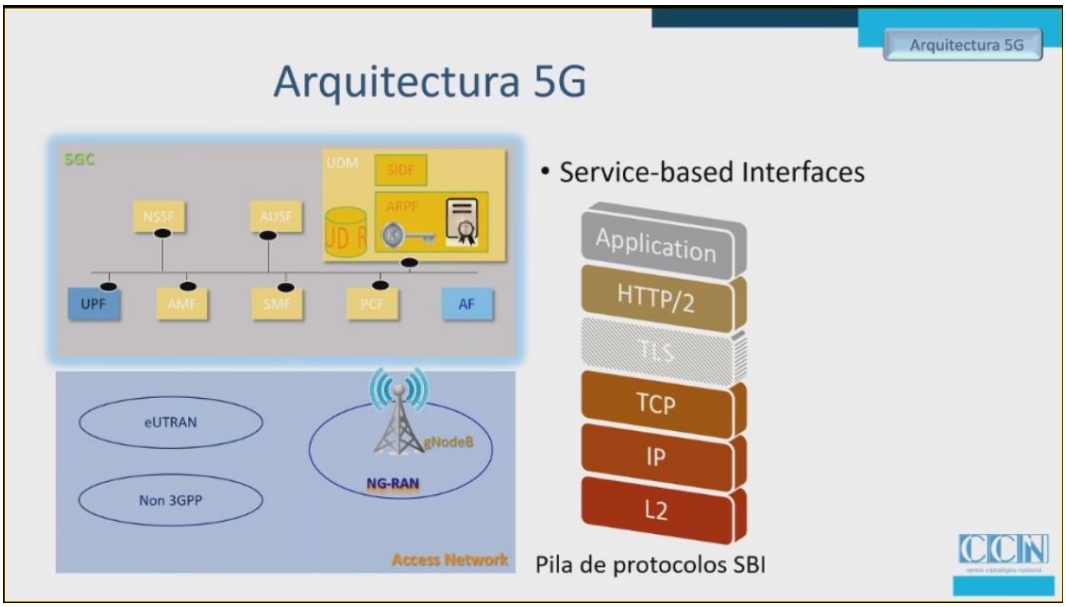

Ilustración 17. Arquitectura 5G (Protocolo SBI)

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G.

Además de las SBI, se definen los "*References Point*". Así como las interfaces definen las capacidades que se ofrece y cómo acceder a ellas para cada función de red, los *References Point* definen las interacciones entre dos funciones de red concretas, es decir, qué operaciones dentro de las permitidas por las interfaces de ambos son utilizadas para las comunicaciones entre estos dos elementos de red. [7]

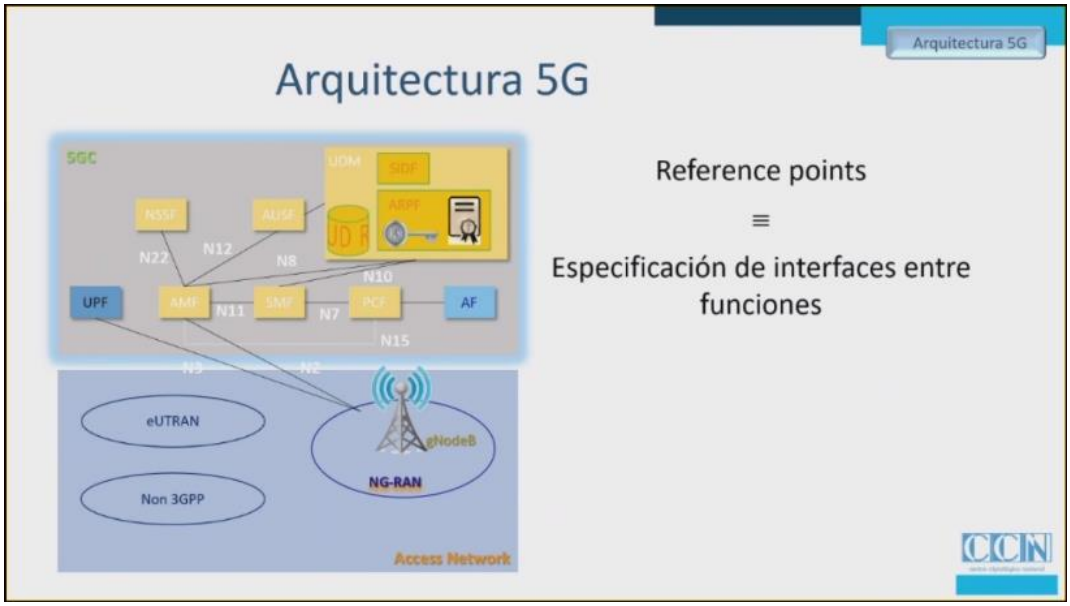

Ilustración 18. Arquitectura 5G (References Point).

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Para los casos de comunicaciones de funciones red entre diferentes redes, se ha definido un elemento específico para realizar la función de proxy, tanto directo como inverso. Esto se hace por ejemplo cuando nos encontramos en un entorno de roaming. Si estamos en el extranjero, la red que nos está dando servicio tiene que hablar con la red core que ha emitido nuestra tarjeta SIM. Estas comunicaciones se producen siempre a través de estos proxys SEPP (*Security Edge Protection Proxy*).

Ilustración 19. Arquitectura 5G (SEPP).

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Los proxys SEPP son “no transparentes”, es decir, las funciones de red que hablan con otras redes saben de su existencia y las comunicaciones están protegidas también con TLS, lo que también proporciona autenticación mutua y protección de la información en tránsito. [7]

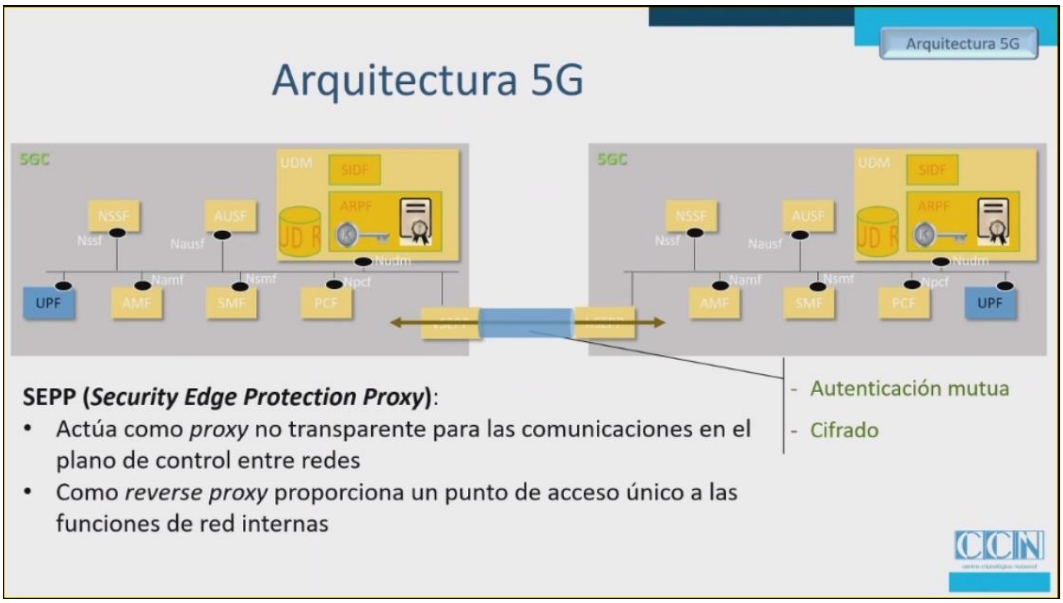

Ilustración 20. Arquitectura 5G (SEPP con TLS).

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

3.4 NETWORK SLICING

Es la segunda funcionalidad principal que aportó un cambio significativo en la red 5G.

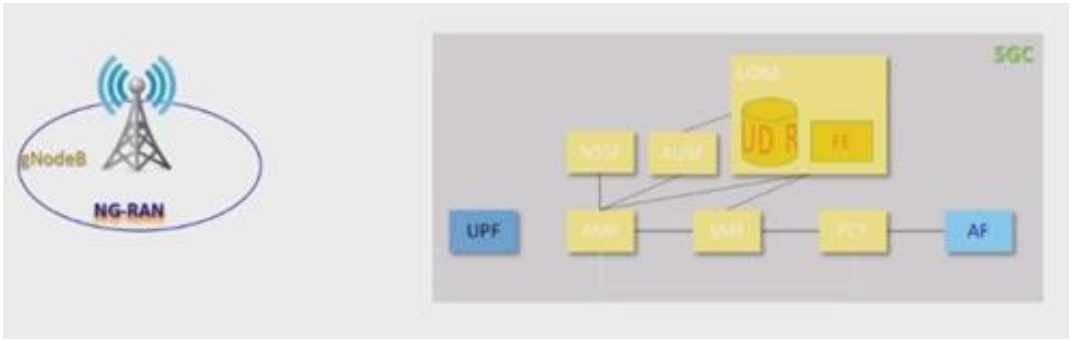

Ilustración 21. Arquitectura 5G (SLICING).

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

El Network Slicing es una virtualización completa del conjunto de funciones que forma una red core, de manera tal que no existe una sola red core, sino que existen un número indeterminado de redes core virtualizadas que las podemos ver como un conjunto de funciones de red.

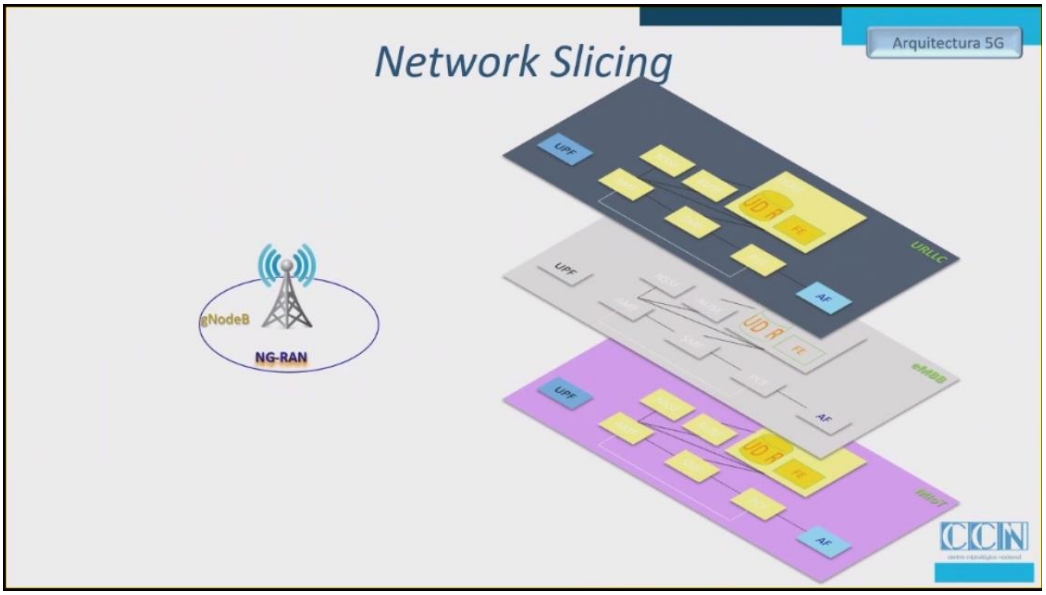

Ilustración 22. Arquitectura 5G (SLICING-VIRTUALIZACIÓN).

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Cada una de estas funciones de redes que llamamos "*Slices*" están parametrizadas y provistas de los recursos necesarios para dar servicio a un tipo específico de dispositivo.

La norma define como Slices estándar las tres que se muestran en la figura. Ella son la *URLLC*, asociada con las comunicaciones de muy alta fiabilidad y muy baja latencia, la *ENHANCED MOBILE BROADBAND* relacionado con los dispositivos de usuarios que requieren un gran ancho de banda a fin de brindar altas velocidades de transmisión por ejemplo en transmisión de video; y, por último, el Internet de las cosas Masivo (MioT). Estos tres grandes grupos están definidos como Slices estándar en las normas, sin embargo, esta también permite que cualquier operador en cualquier red pueda crear un Slice ad-hoc para cualquier tipo de servicio, con una parametrización o con un provisionamiento tan específico como la red

quiera. Luego, si bien existen tres tipos de estándar la red puede definir cualquier tipo de Slice y cualquier número de ellas. [7]

“Ahora, ¿qué sucede con la red de acceso? La red de acceso no se puede virtualizar de la misma forma que la red core, puesto que la red de acceso obligatoriamente tiene elementos físicos.

La red de acceso se encuentra relacionada con estos nuevos Slices. Para ello establece, en las comunicaciones que pasan a través de los nodos de acceso, de la NG-RAN, que cada sesión de usuario esté asociada a una PDU Session y a su vez con una de las Slices. De forma que la red de acceso es consciente en cuanto a las capacidades de acceso que tiene que dar a cada uno de los usuarios.

En base a diferentes técnicas como ser calidad de servicio, políticas de asignación de recursos, aislamientos de recursos o gestiones de acceso a los Slices, gestiona estos accesos de forma tal que cada una de las comunicaciones que pasan a través de ellas mantengan los requerimientos exigidos por los propios Slices.

Así, cualquier dispositivo que se quiera conectar a la red 5G, en realidad se conecta a uno de los Slices que le van a dar el servicio más adecuado a los requerimientos que está solicitando. Si estamos hablando de un dispositivo industrial, probablemente se conecte aun Slice del tipo URLLC, mientras que si es un dispositivo de usuario posiblemente se conecta a un Slice tipo EmBB, o un dispositivo IoT se conecte a un Slice MIoT. Cada dispositivo se conecta al Slice que le corresponde. La red de acceso gestiona esa conexión de forma que los requerimientos se mantienen también en el nivel de radio.

Es importante destacar que un dispositivo se conecta no solo a un Slice. Un dispositivo puede requerir distintos tipos de servicios y puede estar conectado simultáneamente a más de un Slice, lo cual le posibilita que pueda recibir servicios de distintos tipos [7].

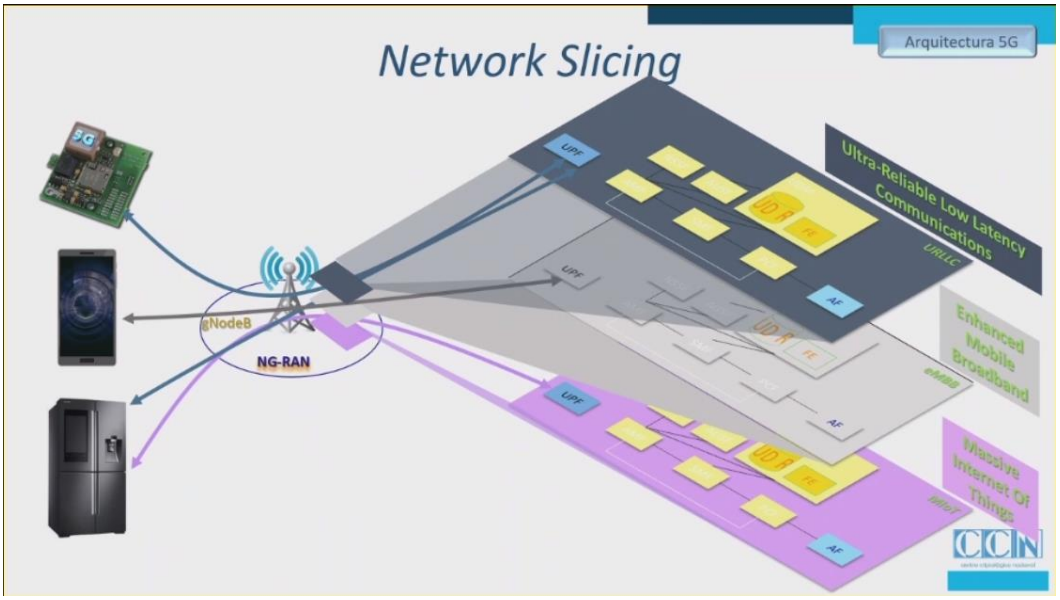

Ilustración 23. Network Slicing

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Ahora bien, ¿cómo se identifican las Slices? La norma define un identificador para cada uno de los Slices. Este identificador tiene dos partes, el SST (*Slice Service Type*) que define el tipo de servicio y puede ser alguno de los números que se encuentran en la norma, por el ejemplo el MBB es el uno, el URLLC es el dos, el MioT es el tres y estos números definen qué tipo de servicios están brindando estos Slices. Luego tiene un SD (*Slice Diferenciator*), una información opcional, para definir Slices dentro de ese tipo, de un subtipo especial que está reservado para que sea definido por el operador. Cada uno de estos números identifica de manera unívoca a los Slices del operador" [7].

Ilustración 24. Identificación de los Slices

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Uno de los elementos claves en cada uno de estos Slices es el elemento de gestión de movilidad AMF (*Access and Mobility Management Función*).

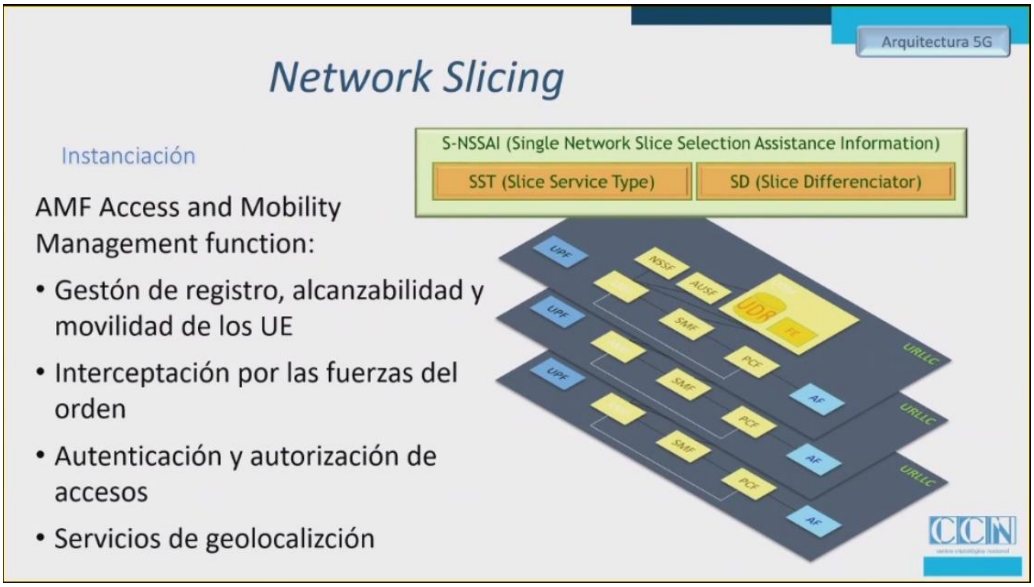

Ilustración 25. Instanciación de los Slices. AMF

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

La gestión de movilidad se encuentra en todas las versiones de protocolos móviles y se ocupa la gestión de los registros de los usuarios, si el usuario está registrado o no, dónde es alcanzado, cuál es la parte de la red de acceso que puede dar servicio al dispositivo, etc.

También se ocupa de la gestión de la movilidad de los dispositivos, es decir, si un dispositivo se está moviendo y pasa de una parte de la red core a otra parte de la red core.

5G implementa (en otras versiones se encontraba separado) las funciones de interceptación por las fuerzas del orden; esta definición es obligatoria en la norma.

Gestiona la Autenticación y la Autorización inicial de los accesos de los dispositivos a la red core como así también la geolocalización de los dispositivos, tanto a nivel macro (celda o grupo de celdas) como así también, geolocalización precisa [7].

Este gestor de movilidad es la única de las funciones de red que puede definirse de manera común a varios Slices al ser un tipo de servicio muy

específico, es decir que un mismo AMF puede ser compartido por varios Slices.

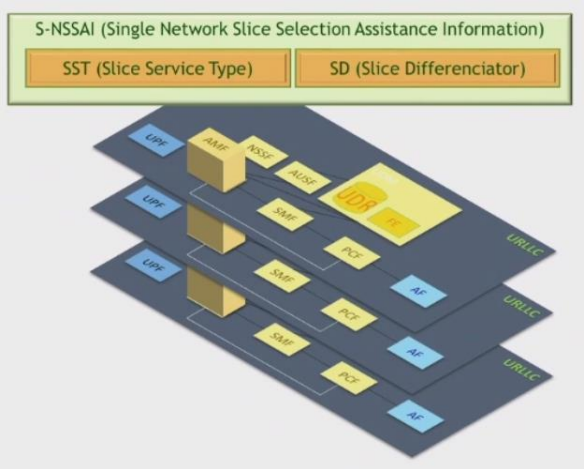

Ilustración 26. AMF

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Luego, ¿Cómo se asocia un dispositivo a un nuevo Slice cuando se registra en la red? Para ello el dispositivo tiene un conjunto de Network Slices a los que le solicita conexión. [7]

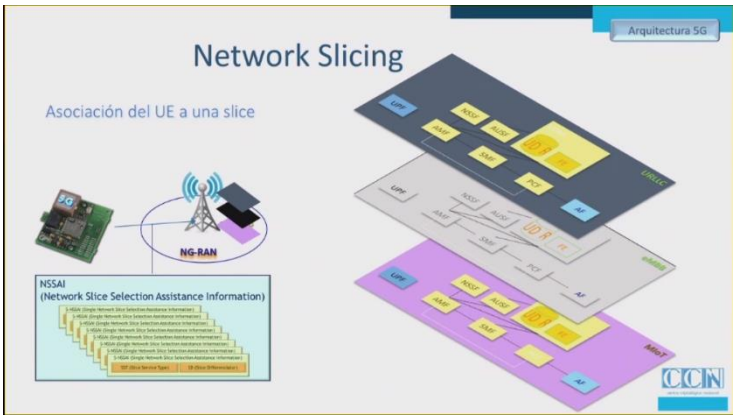

Ilustración 27. Asociación de un dispositivo a un Slice

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“Este conjunto tiene una definición estática toda vez que se encuentra almacenada en la SIM del dispositivo y por otra parte se define también

dinámicamente y esta definición se puede realizar en el plano de control de las comunicaciones móviles. Por lo tanto, el dispositivo dispone de esta información y además solicita un conjunto de Slices a los que se podría conectar.

En función de varios parámetros como puede ser la disponibilidad de los Slices en la red de acceso donde el dispositivo se está conectando o políticas de la red core que le permite o no el acceso al Slice en función de ciertos parámetros, la red de acceso accede a la red core para solicitar el Slice al que se quiere conectar el dispositivo.

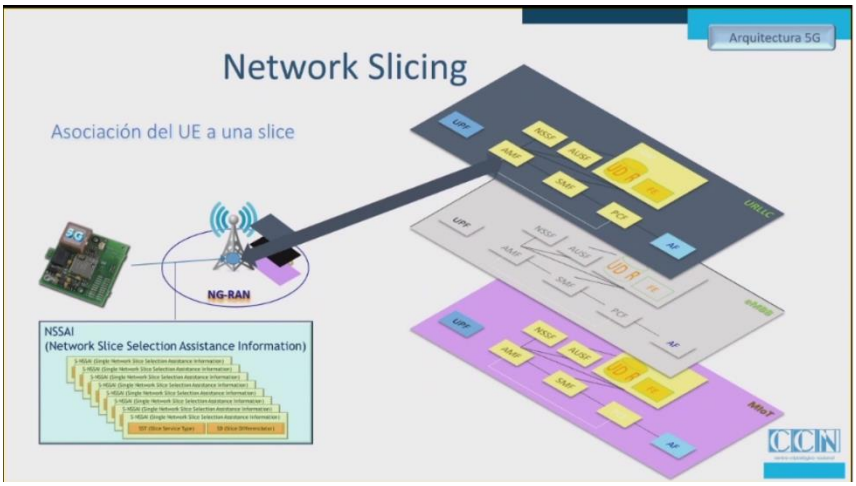

Ilustración 28. Asociación de un dispositivo a un Slice Fig.

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

A partir de ese momento la red de acceso redirige el tráfico al gestor de movilidad AMF correspondiente y por lo tanto al Slice correspondiente. A partir de ese momento se genera una PDU sesión, que va asociada a ese Slice y que ya tiene los requerimientos de servicios o parametrización necesaria para dar el servicio adecuado a ese tipo de dispositivo en concreto.

Este proceso mencionado se da en el registro inicial del dispositivo. Es posible que el dispositivo, cuando se registre nuevamente en la red, ya disponga de la información necesaria; en ese caso el dispositivo ya no negocia y se conecta directamente al Slice correspondiente" [7].

3.5 DEFINICIONES

"En cuanto a las definiciones, las funciones soportadas son totalmente dinámicas, es decir que se pueden almacenar dinámicamente.

La red core puede crear Slices nuevos dinámicamente, parametrizarlas, puede definir dinámicamente los recursos que están asociados a ella y puede monitorearlas.

Se definen dos tipos de gestión, como servicio y como parte de la infraestructura del operador ya que estas funciones de red están preparadas para ser accesibles desde redes externas hacia la red core propia del operador. Esto hace que la gestión de esta red pueda externalizarse de manera más sencilla.

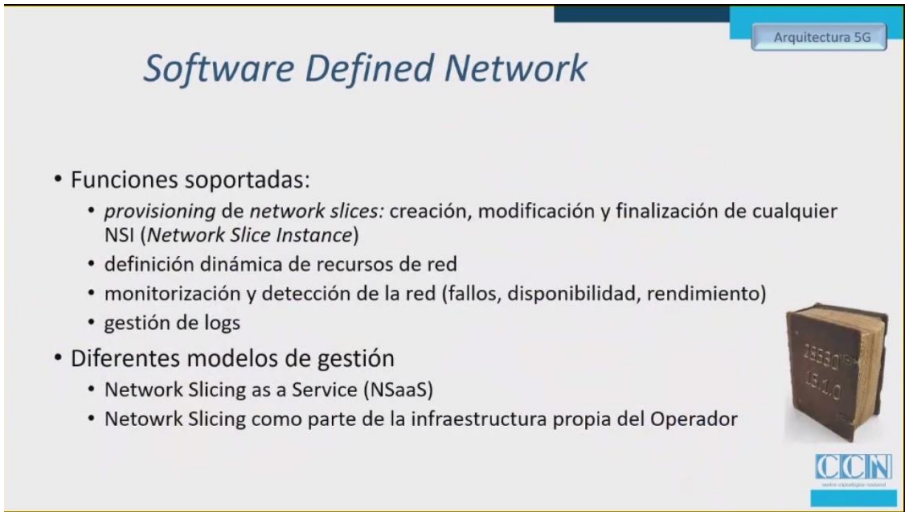

Ilustración 29. Definiciones

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones

La arquitectura descripta para la 5ª Generación de telefonía móvil muestra cuáles son las funcionalidades nuevas que permiten que a una serie nueva de dispositivos con unos requerimientos tan dispares se les pueda dar servicios con un costo razonable dentro de la infraestructura de red. Estas funcionalidades son, la virtualización de la red (*Network Slicing*) y las Funciones de Red, es decir la transformación de elementos de red en funciones de red y el soporte desde la red de acceso a las *Network Slices*. Este conjunto de funciones es lo que ha permitido que se le pueda dar este conjunto de servicios tan dispares a diferentes tipos de dispositivos. [7]

3.6 NUEVAS FUNCIONALIDADES DE SEGURIDAD 5G

1- Protección de Identidad
2- Autenticación
3- Control de la Home Network
4- Protección de las comunicaciones
5- Accesos desde redes externas.

La protección de la identidad ha sido un problema tradicional desde el inicio de las comunicaciones móviles. Cuando un usuario adquiere una tarjeta SIM, la misma es configurada por la red y esa configuración consiste en la grabación de un número que la identifica unívocamente, denominado IMSI o por lo menos se llamaba así hasta esta generación (5G), además de una clave precompartida tanto por la red core como por la tarjeta SIM (en el momento de su configuración es cuando se graba en la tarjeta y nunca más vuelve a salir de allí. Este proceso de asignación tiene una implicación y es que esta tarjeta se identifica y se asocia de forma unívoca al usuario que la adquiere, por lo tanto, identificar este número sería algo equivalente a identificar al usuario, lo cual tiene implicancias a nivel seguridad ya que identifica al suscriptor, puede geolocalizarlo, se pueden realizar ciertos ataques como suplantación de identidad, denegación de servicio, secuestro de las comunicaciones, etc. La información de usuario se considera en general, información sensible.

En 5G, además del IMSI, que es el número de identificación permanente de usuario que se soportaba hasta versiones anteriores, también se soporta otro tipo de identificadores basados en la RFC 7542 que están pensados para cuando se implementa una red 5G en un entorno privado, no conectado a internet, por ejemplo en plataformas petrolíferas, barcos o entornos industriales en los que se quiera hacer uso de la tecnología 5G pero en un entorno privado, es decir, aislado de un operador que brinda servicios de telecomunicaciones. Estas dos posibilidades de identificador permanente de usuario en 5G se llama SUPI (*Subcription Permanent Identifier*). [7]

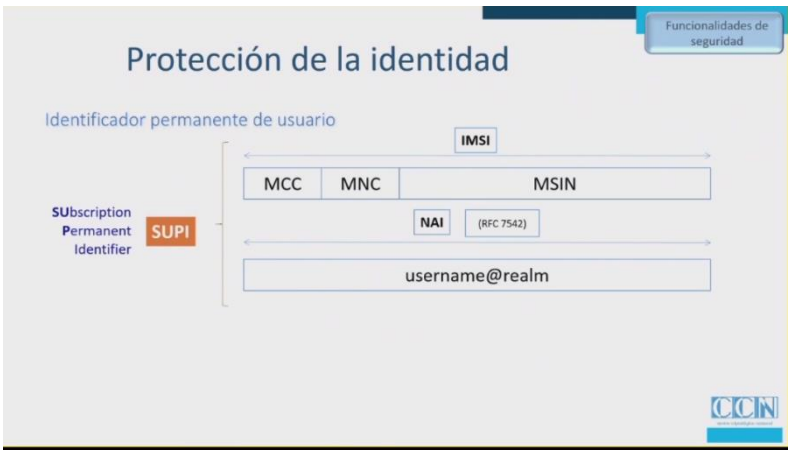

Ilustración 30. Protección de Identidad

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Hasta 4G la identidad del usuario se ha protegido utilizando identificadores temporales, para no tener que enviar por el aire el identificador permanente de usuario. 5G incorpora además el identificador de Slice al que el dispositivo de usuario está conectado. Este identificador de Slice se denomina GUAMI (*Global Unique AMF Identifier*)

Al identificar el GUAMI se identifica el Slice con el cual el usuario está conectado. Esto no existía en las versiones anteriores de los protocolos de comunicaciones móviles [7].

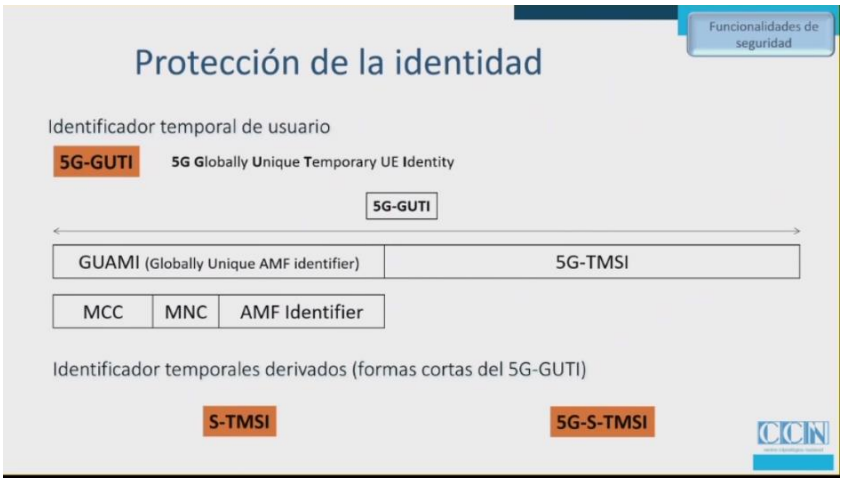

Ilustración 31. Protección de Identidad - GUAMI

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Entonces, ¿Cuál era el problema de seguridad de esta técnica hasta 5G? En principio el problema consistía en que es imposible que el identificador temporal se use siempre. Imaginemos el caso de un dispositivo que es adquirido por el usuario y en ese momento, por primera vez se conecta a la red. Obviamente el dispositivo no va a tener ningún identificador temporal asignado por la propia red porque este se asigna tras la registración inicial. En estos casos, en el primer momento de las comunicaciones, el identificador permanente se envía por el aire sin protección. En 4G ya se reconocía que esto era una deficiencia de seguridad de la norma y en 5G se ha diseñado una solución. [7]

La solución a este problema consiste en que cuando se tiene que enviar el identificador permanente de usuario por la interfaz de radio ya no se envía en claro. En su lugar se envía ese identificador en modo cifrado. Este se cifra con una clave pública que es suministrada por el operador en el momento de la finalización o configuración de las tarjetas SIM y que utiliza uno de los varios esquemas de protección que especifican los protocolos. De esta forma, cuando hay que enviar el identificador permanente se envía este siempre protegido, resolviendo de esta forma el problema de confidencialidad de información sensible [7].

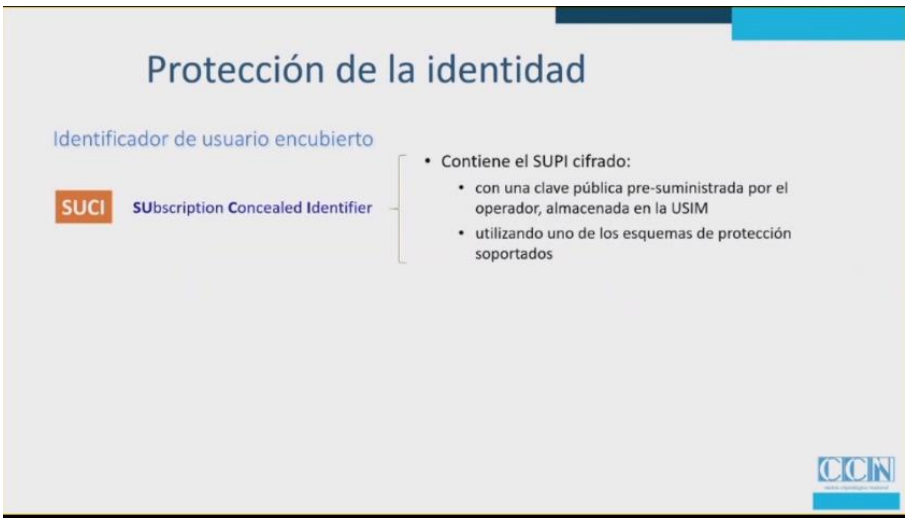

Ilustración 32. Protección de Identidad - SUCI

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Hay que tener en cuenta que la norma permite un esquema sin protección en los siguientes casos.

- Cuando se tienen que realizar llamadas de emergencias, lo cual es adecuado porque cuando se da esta circunstancia de emergencia lo prioritario es que la llamada se curse independientemente de que se consiga o no la autenticación. En este caso no se exige el cifrado del identificador permanente, sino que lo que se hace es permitir el esquema de protección nulo.
- Cuando la Home Network se ha configurado para que no se use el esquema de protección. Es el operador el que define si se debe utilizar este esquema de protección. Además, la Home Network debe haber proporcionado esta clave pública necesaria para cifrar el identificador de usuario. Ni no lo ha hecho, no se podrá cifrar.
- Cuando la Home Network no ha proporcionado la clave pública necesaria para el cifrado.

Finalmente, el mecanismo de protección de la identidad del usuario solo es efectivo en tanto el operador haya activado el mecanismo y haya configurado la tarjeta SIM con la clave pública necesaria para proteger este identificador [7].

3.7 AUTENTICACIÓN

"En el proceso de autenticación participan varios agentes.

El primer agente que participa es el UE (*User Equipment*) o equipo de usuario o dispositivo final que se quiere conectar a la red móvil. La mayor parte del proceso de autenticación dentro del terminal lo realiza la tarjeta SIM, la cual hoy en día tiene que ser una tarjeta física, aunque en la definición de la norma se propuso utilizar tarjetas software o incluso delegar la autenticación en tarjetas remotas o definidas por software. A la fecha las únicas tarjetas permitidas de acuerdo con la Release 15 son las tarjetas SIM CARDS, que pueden ser extraíbles como las de cualquier terminal móvil o embebidas. En

el caso de las tarjetas embebidas la finalización o configuración no se hace en el momento de la venta de la tarjeta al usuario, sino que se realiza antes de la venta del dispositivo y eso lo tiene que hacer el fabricante. La norma define mecanismos de interconexión entre los fabricantes y los operadores para poder realizar el proceso de finalización de las tarjetas SIM, que proporciona la identificación del propio dispositivo o del usuario y de la clave precompartida para la autenticación como así también la clave pública para la protección de la identificación del usuario. Es importante saber que cuando la tarjeta SIM se encuentra embebida en el dispositivo, la finalización es coordinada entre el operador y el fabricante del dispositivo. En el otro caso es el propio operador el que finaliza la tarjeta SIM antes de venderla al usuario final.

Existen tres tipos de tarjetas predefinidas en la norma (Release 15), que son las tarjetas transicionales, las tarjetas 5G con la funcionalidad completa y las tarjetas de bajo consumo, diseñadas para dispositivo IoT o industriales" [7].

Ilustración 33. Tipos de SIM card

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"El primer agente de autenticación es el propio dispositivo de usuario que es quien se quiere autenticar. El segundo agente que interviene en la autenticación es la red que brinda el servicio, es decir la *Service Network*. En un entorno de movilidad, la red que nos da servicio para poder comunicarnos no siempre es la que nos ha proporcionado la tarjeta SIM, sino que podemos estar en otro país o en otro entorno y nos está brindando servicios de telefonía

móvil otra red que no es la que nos ha proporcionado la tarjeta SIM. A esta red que brinda el servicio la denominamos red de servicios o service network.

En esta red de servicio es donde se establece el canal de radio entre el equipo de usuario y la red 5G, es decir el canal de radio se establece con la red de servicio y no con la red core.

El tercer actor que interviene en el mecanismo de autenticación es la Home Network que es la red que nos ha dado servicio, sin esta no se puede obtener el acceso a la red, por lo tanto, sin tener el acceso a la red home no podremos tener servicio en ningún país del mundo. Es decir que todas las Home Network de las naciones se encuentran interconectadas entre ellas" [7].

3.8 MECANISMOS DE AUTENTICACIÓN

"Los mecanismos de autenticación que actualmente se soportan son:

1- 5G-AKA: Es una ampliación del mecanismo AKA que se desarrolló en 3G que es de obligado soporte para todos los dispositivos 5G.
2- EAP-AKA´: Está básicamente pensado para redes que soporten el método EAP como método de autenticación. Es una mejora que introduce algunas funcionalidades adicionales, por ejemplo, se utiliza SHA256 en lugar de SHA1 y hay algunas protecciones a ataques a los algoritmos de protección.
3- EAP ADICIONALES: Pensado para el uso de redes privadas, que utilizan la tecnología 5G pero que no están conectadas al exterior.

La Release 15 solo acepta el EAP-TLS y se supone que más mecanismos van a estar soportados en el futuro.

La protección de las comunicaciones no está basada en una única clave, sino que se basa en toda una jerarquía de claves. Estas claves se van adquiriendo y generando durante el proceso de autenticación y establecimiento de claves. Este proceso cumple esas dos funciones, por un lado, la autenticación bidireccional entre el usuario y la red, por otro lado, cumple la función de que las claves usadas para la protección de la información del usuario, en todos los tramos que pasa y especialmente en el

canal de radio entre el propio equipo de usuario y la red de acceso, el lugar menos seguro, estén disponibles” [7].

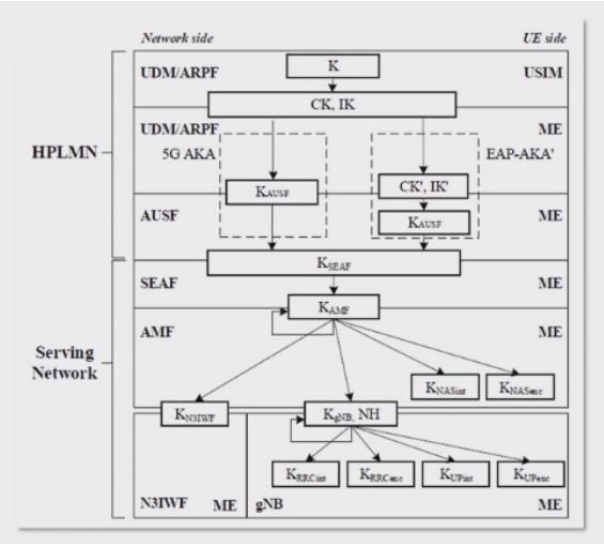

Ilustración 34. Set de Claves

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“Varios son los actores que intervienen en el proceso de autenticación.

Tenemos en primer lugar el equipo de usuario (UE) que es el dispositivo del suscriptor que solicita la autenticación.

Luego tenemos el SEAF (*Security Anchor Function*) que es la función de la red de servicio que va a estar involucrada en el proceso de autenticación.

También encontramos el AUSF (*Authentication Server Function*) en la network home, siendo este el equivalente del SEAF de la red de servicio. Es quien gestiona toda la autenticación en esta red.

Dentro de la Home Network se encuentra la función de gestión de claves que se realiza en el UDM que es el lugar donde se almacena los datos de usuarios incluyendo las claves y que también hace la traducción entre el identificador permanente de usuario, a través del SIDF, y el identificador cifrado de usuario. El SIDF proporciona la función de obtención del SUPI a partir del SUCI” [7].

“El ARPF (*Authentication Credential Repository and Processing Function*) es el repositorio de claves que contiene la clave precompartida para cada usuario. Esta clave precompartida es la clave K en el diagrama, y de esta clave se derivan la clave base de protección de integridad que es la IK y la clave base de protección de la confidencialidad que es la CK. La clave K es precompartida, entre la red y la tarjeta SIM y de ella se derivan CK e IK” [7].

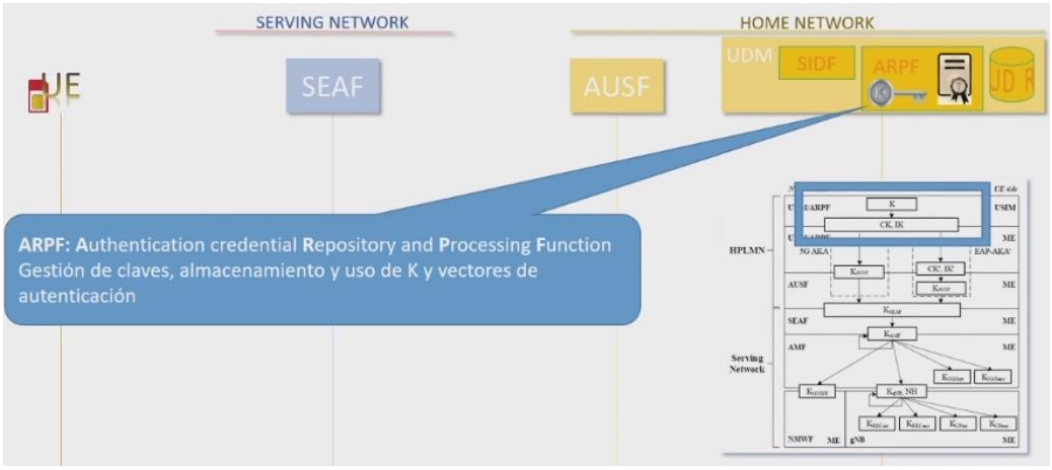

Ilustración 35. ARF

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Los datos de usuarios se almacenan en un repositorio al efecto de la red core que es el UDR y almacena además algún otro tipo de datos de usuarios

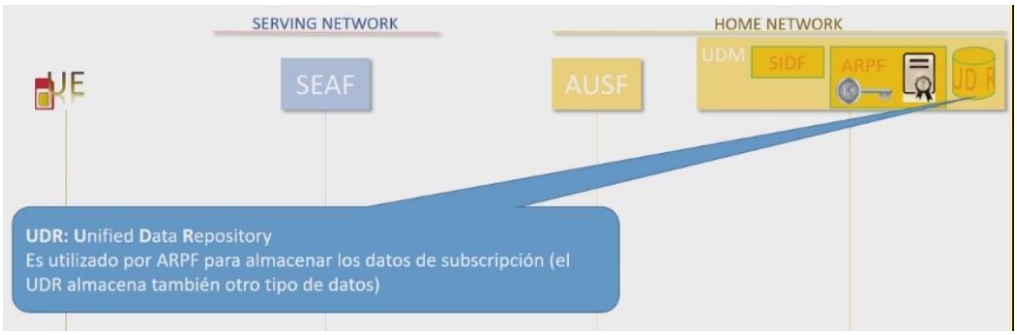

Ilustración 36. UDR

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

3.9 PROCEDIMIENTO DE AUTENTICACIÓN

Comienza con un mensaje inicial de un móvil en el que proporciona su identidad. En este punto el UE ya ha establecido un canal de radio con la red que le da servicio. Ese canal de radio se establece sin autenticación para poder comunicar el mensaje y sucede antes del mensaje inicial. En el mensaje se envía el identificador tanto temporal si es que el usuario ya lo ha obtenido de la red en una comunicación anterior (esto lo hace el sistema para evitar gestionar ese identificador y de las claves asociadas). En el caso de que no disponga del identificador temporal se iniciará entonces el proceso de autenticación.

En la red de acceso el SEAF toma esta petición y comunica la network home con el servidor de autenticación de la network home y le añade el nombre de la red de acceso (muy importante). Este nombre se construye de una forma estandarizada para que tanto el UE como la red de servicio (Service Network) y la network home, conozcan el nombre de la red que está dando servicio al terminal móvil. Es una novedad de 5G y la finalidad que persigue es autenticar a la red que está dando servicio, cosa que no se hacía en las generaciones. Hasta 4G solo se exigía que tuviera comunicación con la network home. Esto evita ataques en los cuales la propia red de servicios en forma maliciosa intente hacer ver al terminal que se trata de otro tipo de red.

El nombre de la red se añade a la petición de autenticación desde la red de servicio a la network home.

La network home verifica que el nombre que la función le envía en la petición se corresponde con el que tiene almacenado para la función a la cual le está llegando, por lo tanto, verifica que el nombre es correcto desde la función de red que le está llegando la petición y una vez hecha la verificación envía esta petición al ARPF que es el gestor de claves [7].

“El gestor de claves en función del identificador de claves que recibe del dispositivo que requiere servicio elige un método de autenticación para ese dispositivo y genera un vector de autenticación denominado 5G HE AV.

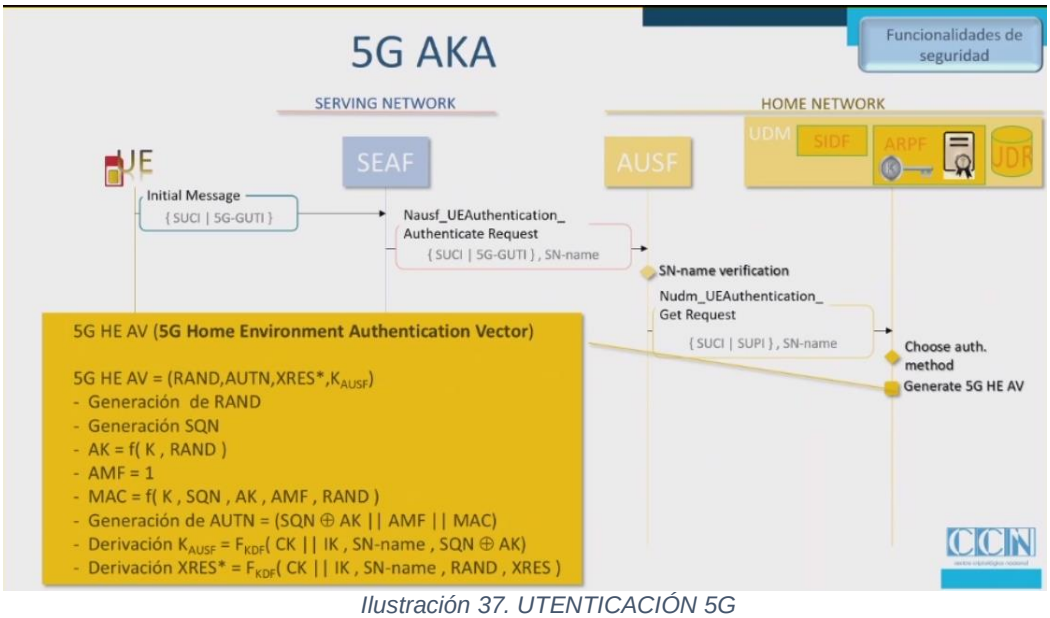

Ilustración 37. UTENTICACIÓN 5G

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

El Vector de Autenticación consiste en los siguientes elementos. Por un lado, tenemos el elemento RAND que es un desafío puesto que la autenticación de ambos extremos que va a estar basado en un mecanismo de *Challege-Respose* o desafío que se va a satisfacer porque ambos extremos tienen la clave precompartida mencionada anteriormente. Este RAND es generado por el ARPF en el momento que recibe el pedido de autenticación. Luego se va a generar un vector de autenticación llamado AUTN que es el vector de autenticación de la red hacia el dispositivo móvil.

El AUTN está compuesto por los siguientes elementos:

SQN: Es un número de secuencia asociado al vector de autenticación que se va a enviar. Este número de secuencia protege contra el uso del mismo vector de autenticación más de una vez o de un vector de autenticación antiguo. El terminal móvil sabe qué número de secuencia le va a llegar y si recibe un numero de secuencia antiguo no va a aceptar el vector de

autenticación. El número de secuencia va a viajar por la interfaz de radio por lo cual debe ir enmascarado o anonimizado con una clave llamada AK (*Anonymization Key*).

La clave AK es una función criptográfica del Challenge (RAND) y la clave precompartida K. Por lo que se puede ver, tanto el emisor de la clave K, que es la network home como el receptor final que es el UE, ambos son capaces de generarlas a partir del RAND y de la K. Este RAND le va a llegar durante el proceso de autenticación al UE, y lo que es importante; el UE puede obtener también la clave K.

El siguiente dato es el AMF. Este es un campo que hasta la 4ª Generación se lo reservaba para uso interno del operador, pero ahora en la 5ª Generación se usa para definir al usuario y definir el proceso del vector de autenticación como del tipo 5G-AKA.

Luego tenemos el MAC (*Message Authentication Code*) que es una especie de hash firmado. Es una función criptográfica de todo el contenido de la AUTN, el cual garantiza que el AUTN ha sido emitido por el emisor que es la red. Lo garantiza toda vez que es una función criptográfica basada en la clave que tienen precompartida tanto el UT como la network home. La función es calculable también, al tener la clave precompartida, por el dispositivo móvil.

El otro elemento del vector de autenticación es el XRES*. Ese asterisco, en la nomenclatura 5G significa que se ha añadido el nombre de la red. Este elemento es una función de claves precompartidas derivadas; es una función del RAN, es una función del response al challenge que sería XRES y también se le ha añadido el nombre de la red que da servicio. Esto se hace para poder autenticar a la red que da servicio” [7].

5G HE AV (**5G Home Environment Authentication Vector**)

5G HE AV = (RAND,AUTN,XRES*,K_{AUSF})
- Generación de RAND
- Generación SQN
- AK = f(K , RAND)
- AMF = 1
- MAC = f(K , SQN , AK , AMF , RAND)
- Generación de AUTN = (SQN ⊕ AK || AMF || MAC)
- Derivación K_{AUSF} = F_{KDF}(CK || IK , SN-name , SQN ⊕ AK)
- Derivación XRES* = F_{KDF}(CK || IK , SN-name , RAND , XRES)

Ilustración 38. VECTOR DE AUTENTICACIÓN

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"En este punto la red es capaz de generar la clave asociada al servidor de autenticación en la parte de la red. Esta clave es la K_{AUSF} que es una función criptográfica del nombre de la red, el número de secuencia y las claves que se han compartido" [7].

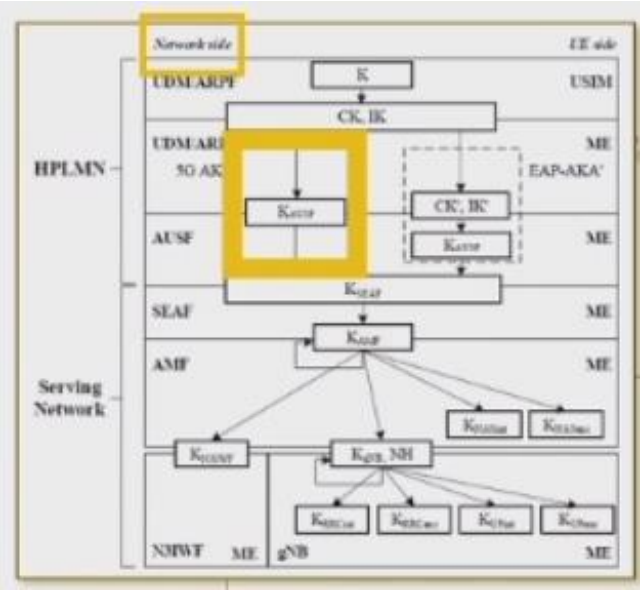

Ilustración 39. GENERACIÓN DE CLAVES
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“Todo esto constituye el vector de autenticación de 5G, que es generado en el ARPF de la network home.

$$5G\ HE\ AV = (RAND, AUTN, XRES^*, K_{AUSF})$$

Este vector de autenticación es enviado al servidor de autenticación, todavía adentro de la red core, el cual almacena la XRES* porque va a recibir una respuesta y necesita guardarlo para comprobar si esa respuesta es correcta o no y poder autenticar al dispositivo.

A continuación, se calcula el HXRES* que es un hash de la combinación del challenge y la respuesta XRES* esperada” [7].

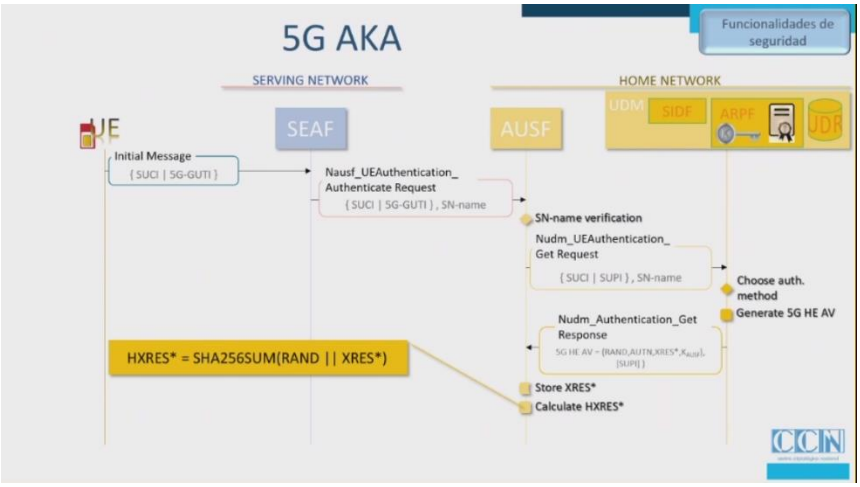

*Ilustración 40. HXRES**
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Luego se calcula la K_{SEAF} que es una clave que tanto el UE como la red van a poder deducir, y es la clave que va a utilizar el SEAF (que es el elemento de la red que da servicio) para poder derivar todas las claves que se utilizan para la protección en confidencialidad e integridad de los diferentes planos de comunicación que hay entre el dispositivo móvil y la propia Service Network, en el interfaz de radio. Estas claves son las que se van a necesitar para proteger las comunicaciones y son derivadas directamente de la K_{SEAF} [7].

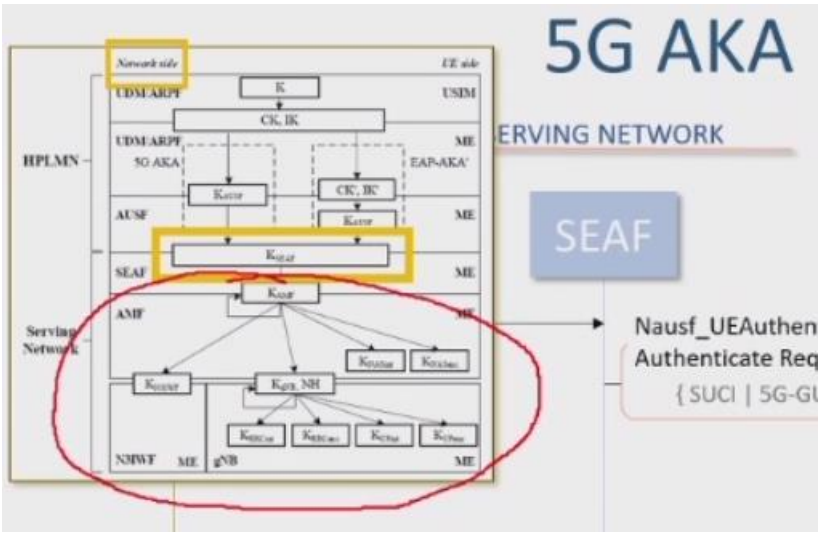

Ilustración 41. KSEAF
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Esta clave K_{SEAF} es calculada en este momento por la network home. Todos los elementos que se encuentran en el cálculo de esta clave son también deducibles por el UE, pero no por la red de servicios [7].

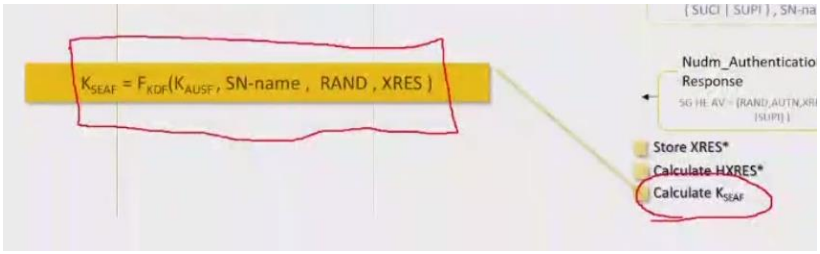

Ilustración 42. CALCULO DE KSEA
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

La red de servicio no va a poder comunicar con el UE hasta que no reciba esta clave.

El vector de autenticación contiene ese vector de autenticación 5G-SE, asociado a la comunicación entre la Service Network y el UE y contiene estos parámetros que son enviados junto con el resto de los parámetros de la AUTN al SEAF. [7]

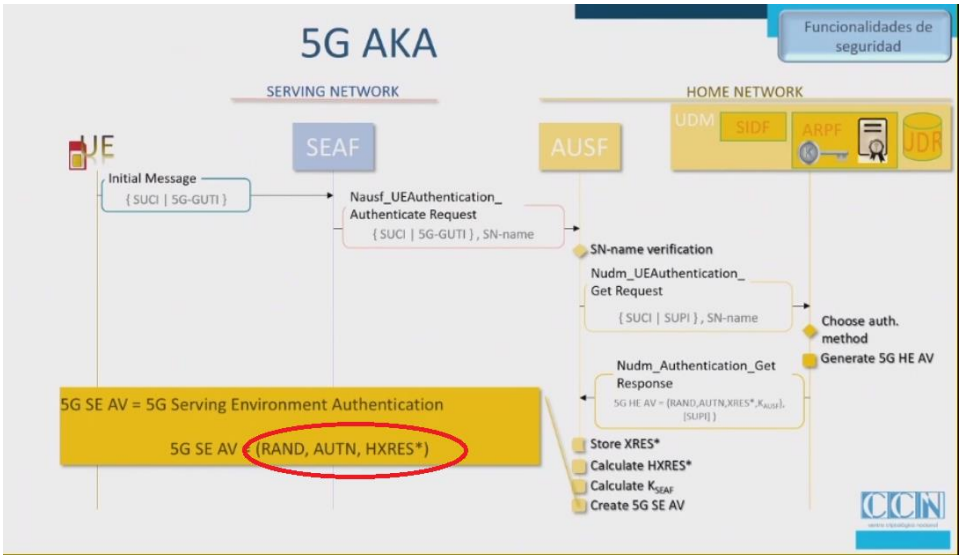

Ilustración 43. CALCULO DE KSEAF
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

El SEAF recibe el challenge de la AUTN y la respuesta esperada [7].

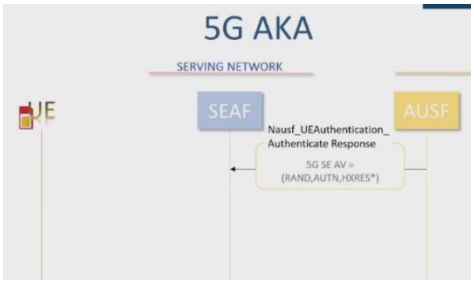

Ilustración 44. SEAF
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

El SEAF le envía al UE el RAN del challenge, el AUTN y algunos parámetros más con lo cual el equipo móvil puede comprobar la AUTN puesto que todos los parámetros son calculables también por el móvil. De esta forma, el suscriptor está autenticando tanto a la red de servicio como a la red home. El AUTN, que lleva los parámetros también de servicio, calcula la respuesta la cual añade a la red de servicio, deriva la clave K_{SEAF} y la envía. La clave K_{SEAF} es calculada también por el terminal móvil. [7]

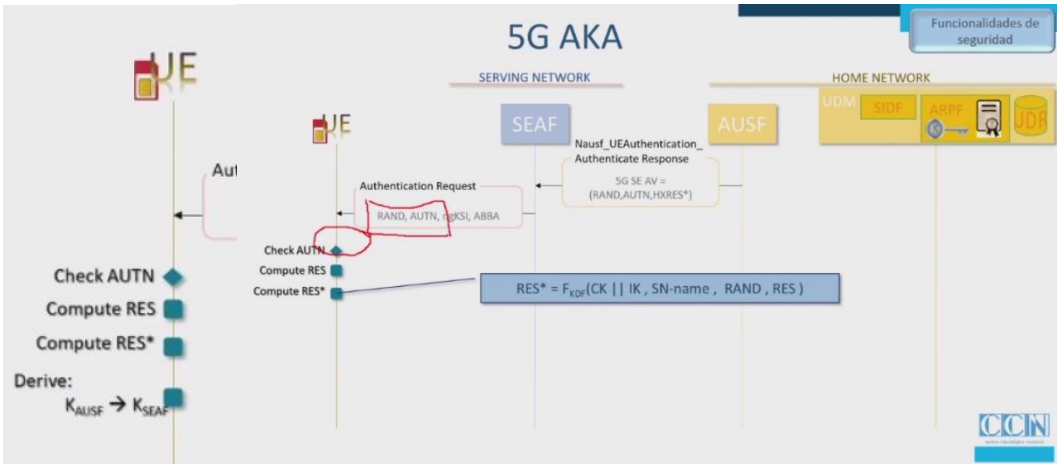

Ilustración 45. RESPUESTA DEL SEAF AL UE
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

El EU envía la respuesta de autenticación (RES*) al SEAF el cual realiza un proceso de verificación.

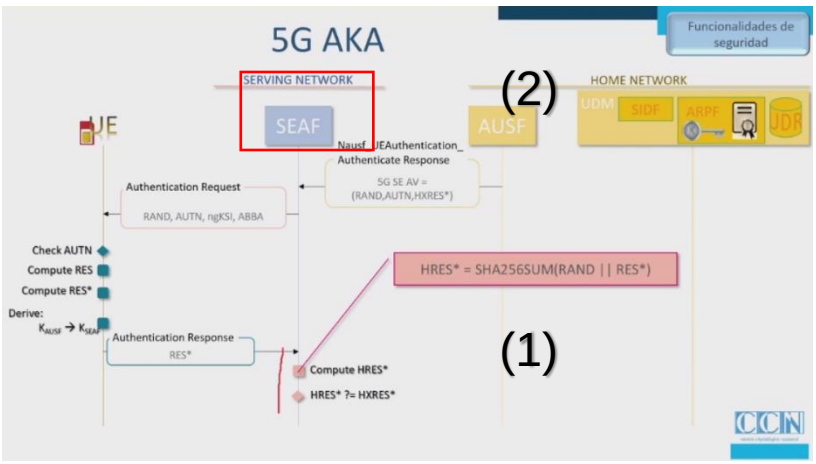

Ilustración 46. AUTENTICACIÓN

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"En este punto (1) la red de servicio está autenticando al móvil, puesto que su respuesta coincide con la que le ha llegado de la network home (2), pero todavía no puede comunicarse con él porque todavía no tiene la K_{SEAF}. Este hecho se produce cuando la network home comprueba si se ha producido la expiración del vector de autenticación y si no es así comprueba el challenge frente a la response, que incluye la información de la red de servicio y solo

suministra la K_{SEAF} al SEAF, para que este pueda derivar al resto de claves y pueda al fin comunicar con el UE” [7].

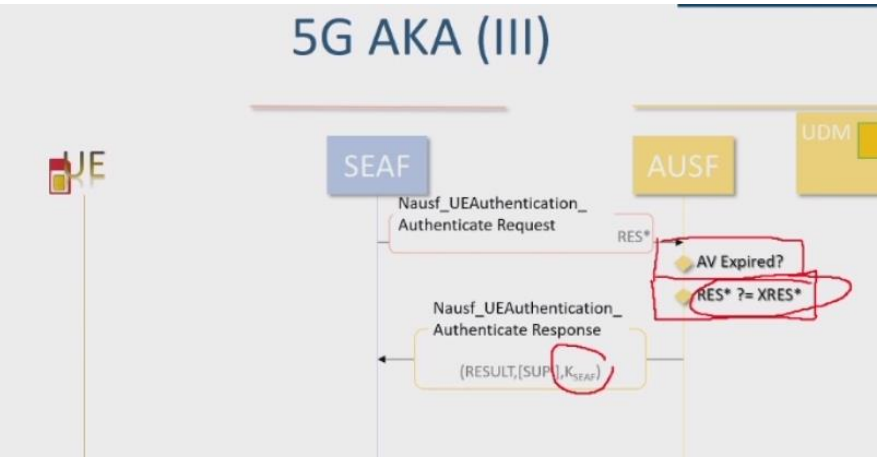

Ilustración 47. Verificación de Expiración del V.A.
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

3.10 PROCEDIMIENTO DE AUTENTICACIÓN EAP

El procedimiento de autenticación EAP-AKA es un método clásico de autenticación. La función de PEER la realiza el UE, la función de Authenticator (*Pass Through*) la realiza el SEAF y la función de Backend Authentication Server la realiza el AUSF.

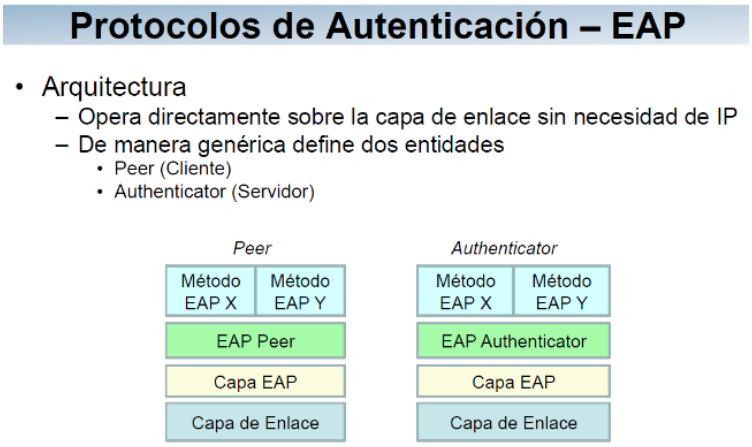

Ilustración 48. PROTOCOLO EAP
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

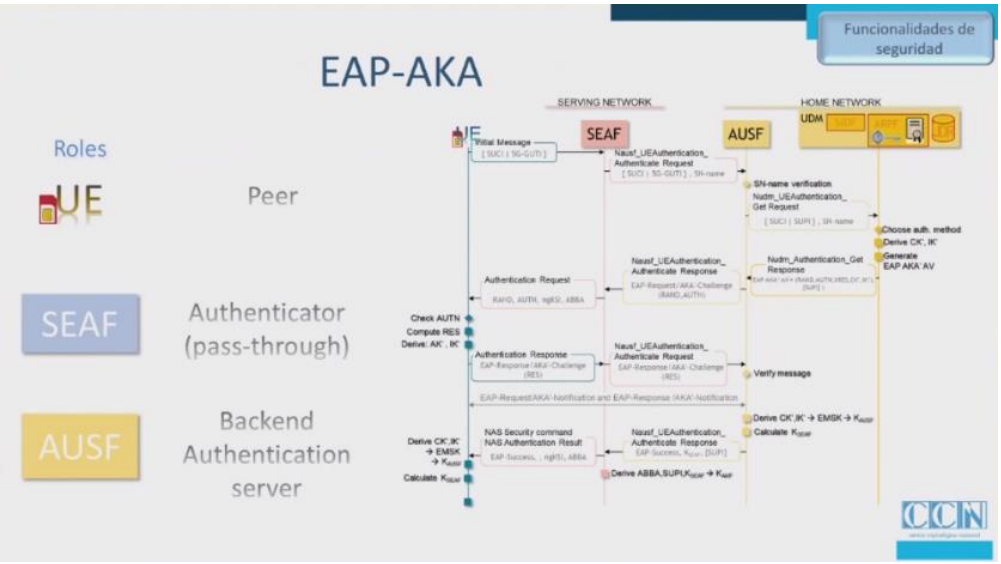

Ilustración 49. AUTENTICACIÓN EAP-AKA
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

3.11 PRINCIPALES MEJORAS EN EL PROCESO DE AUTENTICACIÓN INTRODUCIDAS EN 5G

Hasta la 4ª Generación, quien daba el visto bueno en la autenticación de un usuario era la red de servicio. La network home solo generaba los vectores de autenticación, pero no tenía ningún control sobre la autenticación del usuario. Era la red de servicio quien, usando los vectores de autenticación, autenticaba al usuario. [7]

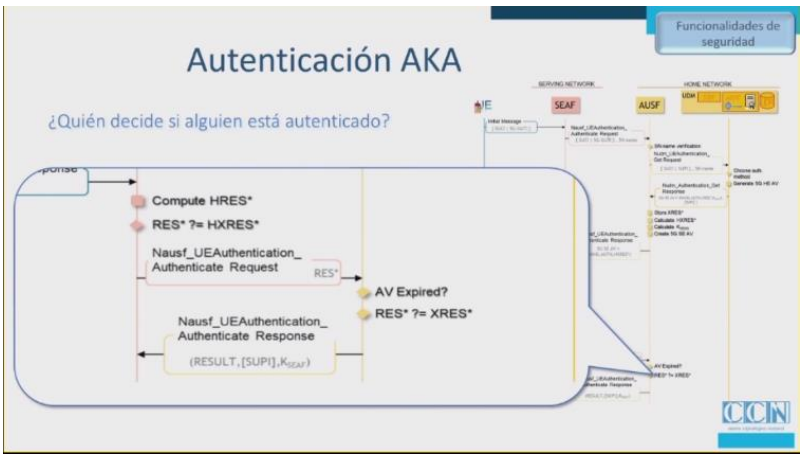

Ilustración 50. AUTENTICACIÓN AKA
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

En cambio, en 5G, hasta que no se produce la comprobación en la network home de que la respuesta que ha enviado el móvil, que incluye el

nombre de la red de servicio, es la misma que se ha generado en la red core, la comunicación no se establece. La K_{SEAF} es el elemento que puede utilizar la red de servicio para generar el resto de las claves que protegen las comunicaciones en integridad y confidencialidad del usuario.

Hasta que no se produce la autenticación por parte de la red home, la K_{SEAF} no se envía a la red de servicio, por lo tanto, la red de servicio no puede comunicar con el dispositivo. Esta es la principal diferencia y mejora que presenta el procedimiento de autenticación AKA respecto de las generaciones anteriores. Mediante este procedimiento es la propia network home, además de la red de servicios quien autentica al usuario y hasta que eso no se produce las comunicaciones no se pueden realizar [7].

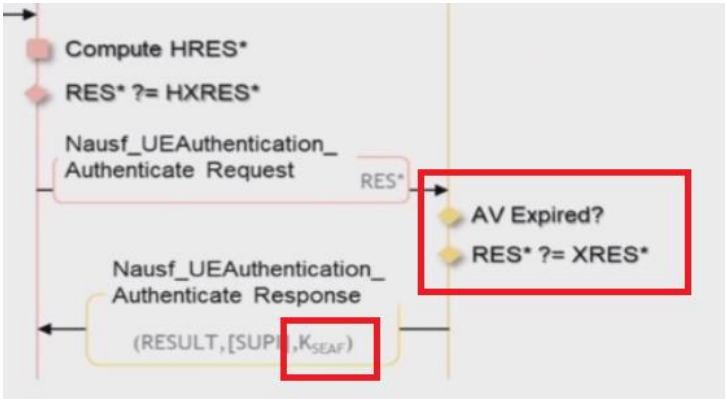

Ilustración 51. Autenticación de la Home Network
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

3.12 CONTROL DE LA HOME NETWORK

Otras de las funcionalidades de seguridad que incorpora 5G es que la network home tiene mucho más control. Por ejemplo, puede impedir que un AMF de un operador que está controlado por un agente malicioso le proporcione información de un registro falso de un UE que podría utilizarse para intentar ubicar a un usuario en una localización en la que no se encuentra. Este tipo de situaciones se contemplan en la norma, pero lo que no se define es como implementarla, dejándolo a criterio de cada uno de los operadores que quieran hacerlo. Sin embargo, el la Release 15 se sugieren mecanismos para ejercer ese tipo de control como por ejemplo que el UDM autorice las operaciones cada nuevo procedimiento de red, el registro, el

cambio de localización, la actualización del registro, etc. Esto posibilita mayor control de la network home sobre la información que recibe de la red de servicio.

Otras de las funcionalidades es que la red de servicios también autentica. El nombre de la red de servicio viaja desde el contacto inicial desde la red de servicio a la network home en el procedimiento de autenticación de cada usuario y además es verificado por la network home que el nombre sea correcto [7].

Ilustración 52. Autenticación de la Service Network
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Además, en el cálculo de las respuestas al challenge se incluye este nombre de red, por lo tanto, se comprueba la autenticación de la red de servicio [7].

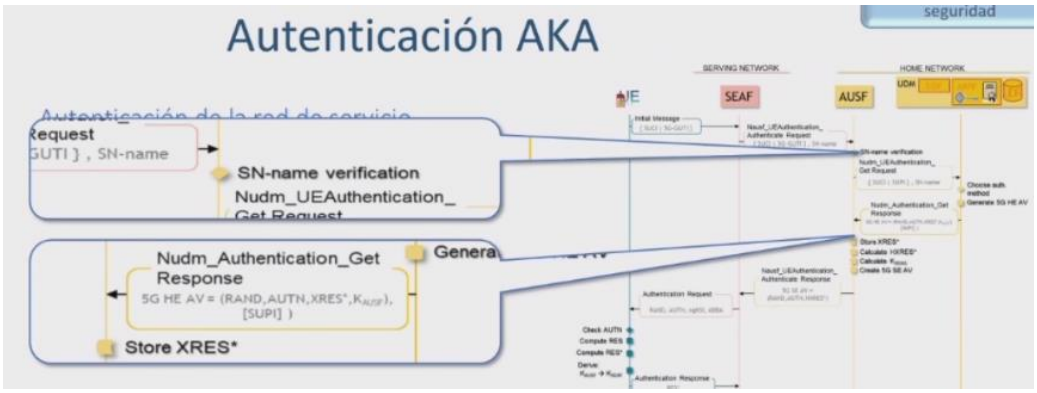

Ilustración 53. Comprobación de autenticación de la SN
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Finalmente, no se proporciona una clave para derivar las claves de protección a la red de servicio, hasta que la autenticación ha sido verificada

por la network home. Así se garantiza la autenticación de la red de servicio [7].

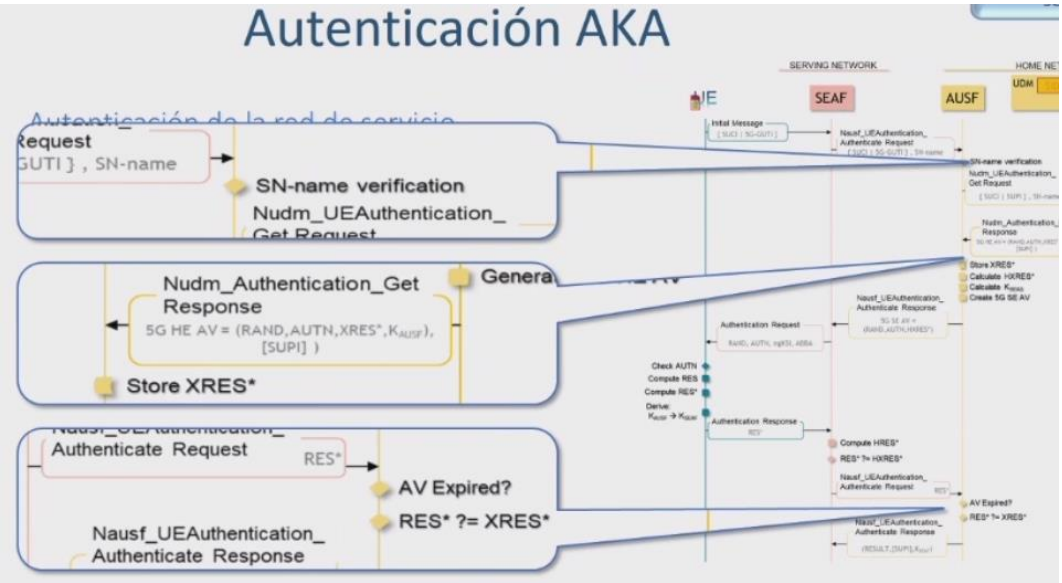

Ilustración 54. Comprobación de autenticación de la HN
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

¿Por qué se han dedicado recursos a incorporar estas funciones al procedimiento de autenticación? Imaginemos el caso en el que nos encontramos en un país en el que tenemos varios operadores que nos pueden dar servicio, un país que no ha sido el que nos ha emitido nuestra tarjeta SIM o sea que no es nuestra network home; en uno de esos operadores confiamos y en otros no confiamos. Si la red de servicio no se autenticara dentro de los protocolos de comunicaciones es posible engañar al usuario con un nombre de red de servicio falso, de manera tal que el usuario estaría confiando en recibir servicio de la red que confía mientras que la red que le da servicio es la red en la que no confía. Esto es posible hasta 4G, pero en 5G, como la red da servicio es la que autentica el engaño es imposible [7].

El nombre de la red de servicio que recibe el usuario (UE) está autenticado por la network home, por lo tanto, las comunicaciones que está recibiendo son de la red de servicio (service network) que se ha autenticado.

Respecto de la protección de la información en las comunicaciones entre UE y la red que le da servicio, en la 5ª Generación se protege con las mismas claves que se han usado hasta 4G.

Los mensajes que no son de acceso son mensajes de control entre el UE y la función de gestión de movilidad, del tipo de actualización de registro, registro inicial, solicitud de servicio, etc. Estos mensajes se protegen en integridad y en confidencialidad con las dos claves, que son derivadas de la K_{AMF} que a su vez es derivada de la K_{SEAF}, como hemos visto antes [7].

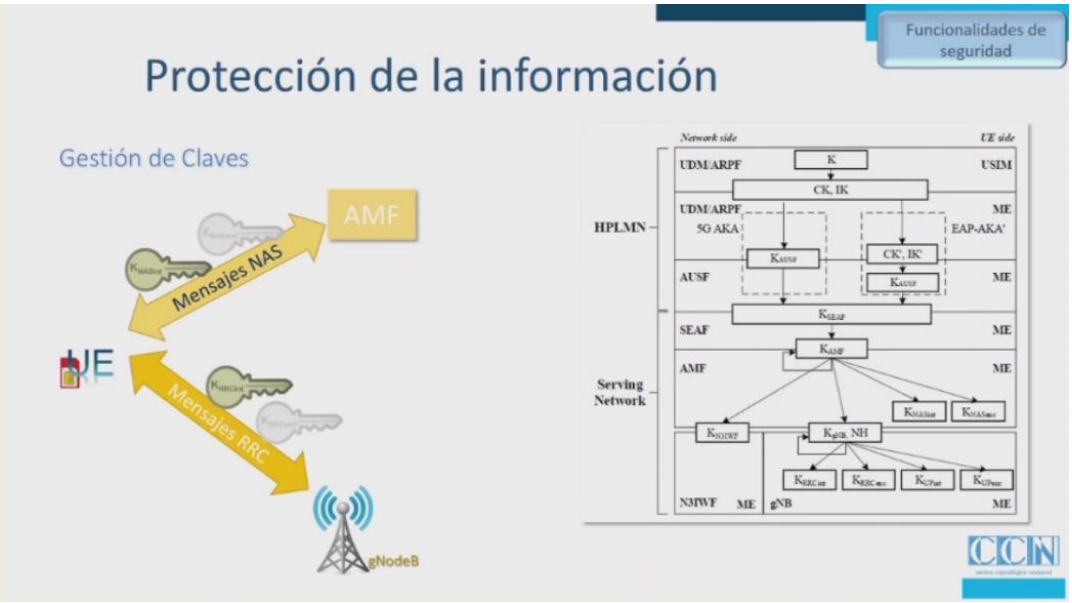

Ilustración 55. PROTECCION DE LA INFORMACIÓN
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Esto es igual en 4G y en 3G, y los mensajes en el nivel de radio, que es un nivel por debajo de los niveles de acceso, están protegidos también en confidencialidad e integridad mediante sendas claves después de un proceso de derivación de la K_{AMF}. Esas dos claves son las que protegen la comunicación en el plano de radio entre el UE y el nodo o estación base que está dando el servicio de radio en ese momento al acceso del UE.

Con respecto a las comunicaciones con el usuario, hasta 4G las mismas estaban protegidas en confidencialidad y a partir de 5G también se pueden proteger en integridad. Lo que pasa es que esta protección, según la norma, se deja a criterio del operador activarla o no. Por lo tanto, nuestros datos de usuarios van a estar protegidos en integridad, en el canal de radio, con nuestra red de servicio dependiendo del operador" [7].

Ilustración 56. GESTIÓN DE CLAVES
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

¿Cuáles son los algoritmos de cifrado que se soportan?

1- SNOW 3G de 128 bits
2- AES based algorithm de 128 bits
3- ZUC based algorithm de 128 bits

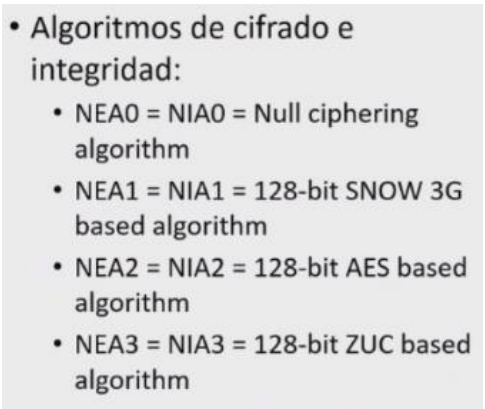

Ilustración 57. Algoritmos de Cifrado en 5G
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“Hemos dicho que la protección de las comunicaciones del usuario a nivel de radio, en integridad y confidencialidad se dejaba a elección del operador, pero… ¿De qué operador? ¿Sería la red de servicio o la red home?

Lo que dice la norma es que la red home puede definir una política para que cada PDU Session, es decir, cada sesión de datos entre el terminal y la red que da servicio sea protegida en integridad o en confidencialidad. La red home es la encargada de establecer estas políticas" [7].

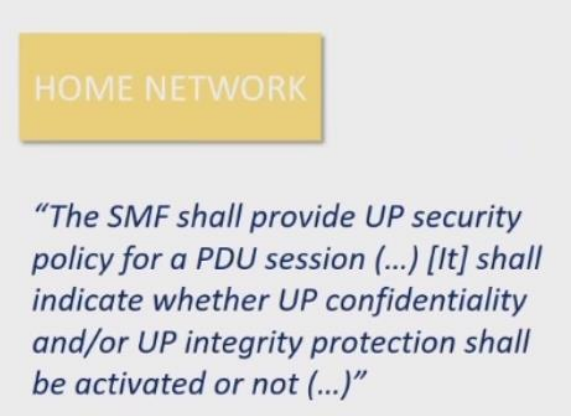

Ilustración 58. Políticas para cada PDU Session de la HN
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Sin embargo, la norma también dice que la función local de gestión de sesiones de la red que está dando servicio (service network) puede desentender o desactivar esa política según los siguientes criterios.

- Cuando hay un mandato obligatorio, es decir cuando el país de la red que está dando el servicio tiene un mandato legal que así lo exige y por lo tanto la red que está dando servicio puede, con ese mandato legal, desactivar esa protección que la red home ha activado con su terminal que está haciendo roaming.
- También es posible que existan acuerdos de roaming entre la service network y la home network que establecen que no se aplicará la política de seguridad.
- La norma permite que la service network a criterio propio puede decidir en base a políticas locales desactivar esta protección. Por lo tanto, quien va a decidir si estas comunicaciones están protegidas o no en la interfaz de radio va a ser la red que da servicio" [7].

Ilustración 59. Políticas para cada PDU Session de la SN
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"¿Cómo se protegen las comunicaciones cuando el acceso se produce a través de una red no confiable, a través de internet? Lo que ocurre es que se establece un túnel IPSec entre el UE y un elemento al que el UE pueda acceder porque lo tiene preconfigurado que es el N3IWF. Esta es una función de red de la red core que está expuesta en internet. El UE establece el túnel IPSec con este elemento, por dentro se establece un túnel EAP 5G para hacer el transporte del mensaje de autenticación, y también que este N3IWF pueda hacer de relay, haciendo a través de este túnel todo el mecanismo AKA explicado con anterioridad.

Aquí de nuevo hay que decir que la autenticación del N3IWF es opcional porque se deja a elección del del operador el proporcionar un certificado para poder atender a este N3IWF. Por lo tanto, es posible que estemos comunicando con un N3IWF que no sea del operador. En este supuesto la autenticación con la red core 5G no sería posible realizarla puesto que siempre va contra el AMF propia de la red core 5G y si no tenemos acceso a los vectores de autenticación a partir de la clave precompartida, no vamos a poder acceder [7].

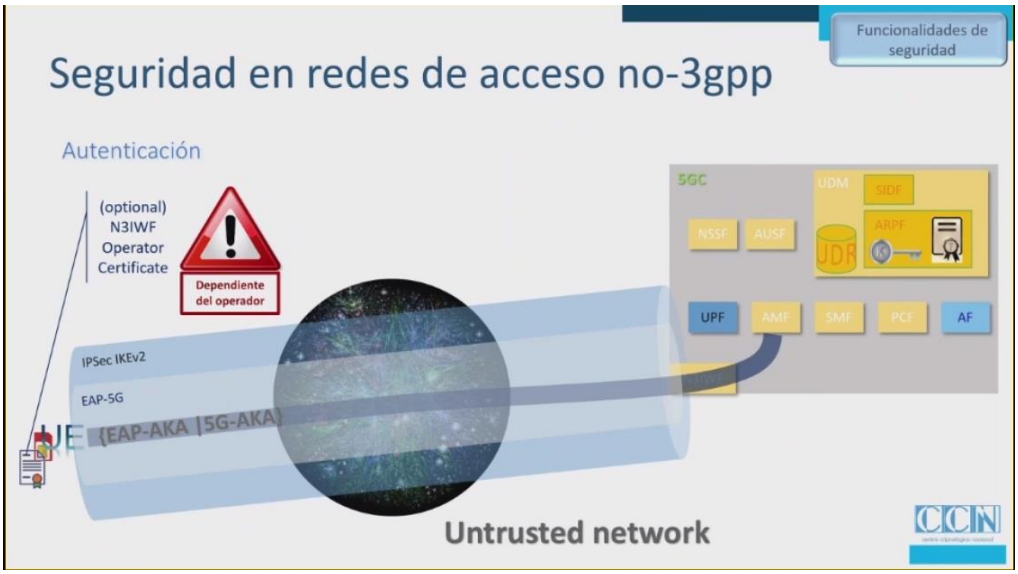

Ilustración 60. SEGURIDAD EN REDES NO CONFIABLES
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

CAPITULO 4: EL SISTEMA DE SEÑALIZACIÓN SS7

Después de la segunda guerra mundial, en 1956, el CCIF y la CCIT se unieron formando el CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía). A este grupo se le encargó la realización de las recomendaciones que serían conocidas posteriormente como Sistema de Señalización SS7. En los años siguientes los subcomités fueron reorganizados y la CCITT fue reemplazada por la actual ITU-TS.

Existieron 6 versiones anteriores, pero éstas nunca pasaron del papel a la práctica. El sistema anterior al SS7, por ejemplo, se denominaba CCIOS6 (*Common Chanel Interoffice Signalling System*) [5].

ARQUITECTURA DEL SISTEMA DE SEÑALIZACIÓN SS7.

Para realizar el proceso de enrutamiento de una llamada el sistema de señalización SS7 se vale de los siguientes elementos:

STP: En la red pública de telefonía conmutada (PSTN) el elemento que conecta todos los componentes de la red se denomina Centro de Conmutación. En el sistema de señalización SS7 dicho elemento tiene el nombre de STP (*SIGNAL TRANSFER POINT*). Este sistema requiere el uso de líneas de transmisión que estén siempre disponible. Estas conexiones permanentes reciben el nombre de links y pueden ser individuales o están agrupados (T1 o E1) [5].

El STP examina el mensaje recibido, verifica el destino, consulta una tabla una tabla de enrutamiento y envía los mensajes a través del link establecido en la tabla. Estos links pueden estar conectados a nodos finales o a otros STP, que completan el enrutamiento de las comunicaciones que no son directas. Para el correcto funcionamiento de la red se necesita redundancia, por dicha razón los STP se encuentran duplicados. Dichos links se denominan con letras, de la A a la F, y tiene relación con los dispositivos que conectan o con la función que desempeñan.

SEP: El SEP (*SIGNAL END POINT*) es un punto final dentro de la red SS7, al igual que el teléfono lo es en la red PSTN. Posee una dirección que se conoce como SPC (*SIGNAL POINT CODE*).

SPC: Es la dirección que identifica un SEP. Posee tres partes: Red, Clúster y Miembro, al igual que un número telefónico posee Código de país, Código de Área y número de línea, aunque en este caso el SPC no corresponde a una zona geográfica [5].

Los links que proporcionan acceso de un SEP a la red se denominan Access Link o A link.

Los STP se encuentran conectados a sus vecinos por medio de links denominados Bridge Links o B Link.

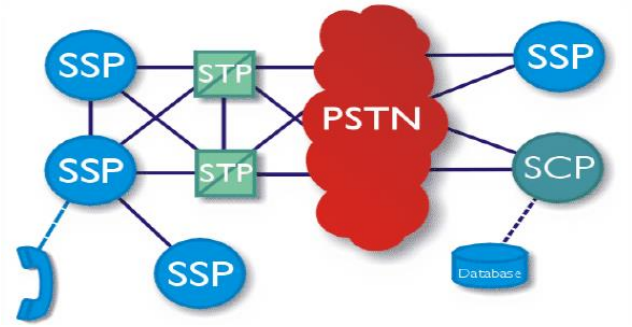

Ilustración 61 Arquitectura SS7
Fte: El Sistema GSM

Existen otros link codificados hasta la letra F que se encargan de interconectar otros componentes dentro de la arquitectura [5].

4.1 MODELO DE CAPAS SS7

El protocolo de señalización SS7 es un conjunto o pilas de protocolos ordenados por capas análogos al modelo OSI.

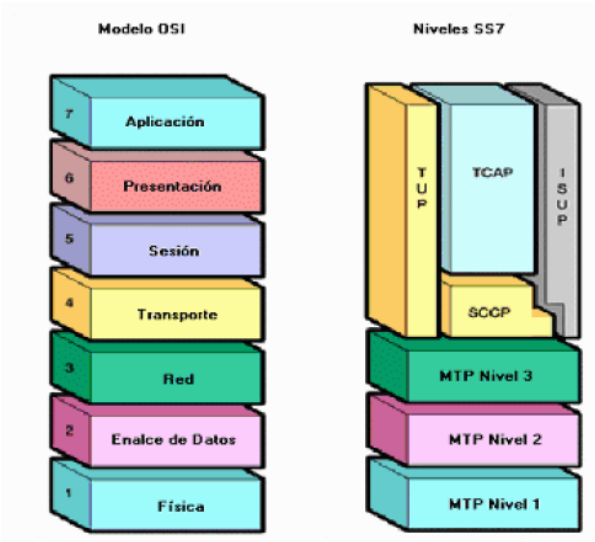

Ilustración 62. Modelo de Capas SS7
Fte: El Sistema GSM

Las tres primeras capas del protocolo SS7 se la denomina MTP (*Message Transfer Part*), encima de estas tres capas existen varios protocolos que realizan funciones de control de llamada, búsqueda de información de suscriptores entre otras.

MTP 1: Es la capa física como en el modelo OSI, su función es el mantenimiento del enlace físico, además establece la conexión de SP y convierte los mensajes en señales eléctricas.

MTP 2: Es la capa de enlace de datos, su función es proveer la transferencia de datos entre SP de una maneja segura, revisa cada dato en busca de errores y de ser posible los corrige, también se encarga del control de flujo de los mensajes.

También se encarga de empaquetar los mensajes salientes denominados MSU (*Message Signal Units*), estos paquetes son los que transportan los mensajes SS7 desde las capas superiores.

MTP 3: Haciendo comparación al modelo OSI es la capa de Red, esta se encarga del enrutamiento de los mensajes y de la gestión de red es decir control de errores, control de tráfico, etc.

Las capas superiores a MTP3 se las puede denominar usuarias, todas confían en este protocolo para que entregue de manera segura los mensajes enviados. Debido a que existen diferentes capas encima de este, se ha implementado una manera de para saber a qué capa debe ser entregada la información, cada MSU tiene en su empaquetado un código denominado SIO (*Service Information Octect*) que permite diferenciarlos, ósea que cada capa tiene un SIO diferente.

En las capas superiores encontramos protocolos encargados del control de llamadas de circuitos como ISUP, TUP y protocolos que brindan servicios no orientados a circuitos como lo es SCCP (*Signalling Connection Control Part*).

ISUP (*ISDN User Part*): Este protocolo es el encargado del establecimiento de las llamadas telefónicas y de su gestión, abarca las llamadas de voz y de transmisión de datos.

ISUP se deriva de TUP, tienes los principios básicos de este, además permite la integración con redes ISDN [5].

TUP (*Telephone User Part*): Fue diseñado para el control de establecimiento de llamadas, fue el primer usuario SS7 designado por la ITU-T. TUP no soporta la transmisión de servicios de datos ISDN por lo cual fue

reemplazado por ISUP, aunque en algunos países aún se sigue usando este protocolo.

SCCP: Este protocolo utiliza métodos de direccionamiento más avanzados para transmitir la información de señalización a su destino de una manera adecuada y segura. Es capaz de llegar a la base de datos correcta, mediante la combinación del SSN (*Subsystem Number*) y su PC (*Point Code*).

TCAP (*Transaction Capabilities Application Part*): Está diseñado para hacer consultas a bases de datos y obtener información de ellas, como logra esto, gracias al protocolo SCCP, cada vez que TCAP hace una consulta a una base de datos esta lleva consigo un número que la identifica. [10]

CAPITULO 5: ATAQUES CONOCIDOS

A pesar de que el 5G en las calles lo encontramos a nivel de prototipo ya hay ataques publicados. La mayoría son ataques que se han descripto sobre la norma, encontrando errores, y algunos otros que se han demostrado funcionales también en 5G. [7]

Los ataques conocidos se pueden resumir en los siguientes:

1. IMSI Catching Tradicional
2. aLTEr ATTACK
3. ToRPEDO
4. IMISI-Cracking
5. Ataques de Trazabilidad
6. Ataques de Condición de Carrera
7. Ataque de Señalización
8. Problemas pendientes respecto de Estaciones Bases Falsas

5.1 ATAQUE IMSI CATCHING TRADICIONAL

El funcionamiento del IMSI Catching en 4G era muy sencillo y estaba basado en el tipo de mensaje de identificación que define la norma y que se utiliza cuando un usuario pide su servicio a una estación base. La estación base en cualquier momento puede decidir solicitarle su IMSI, le envía un

mensaje de Identity Request y el móvil está obligado a enviarle el IMSI, en texto plano. [7]

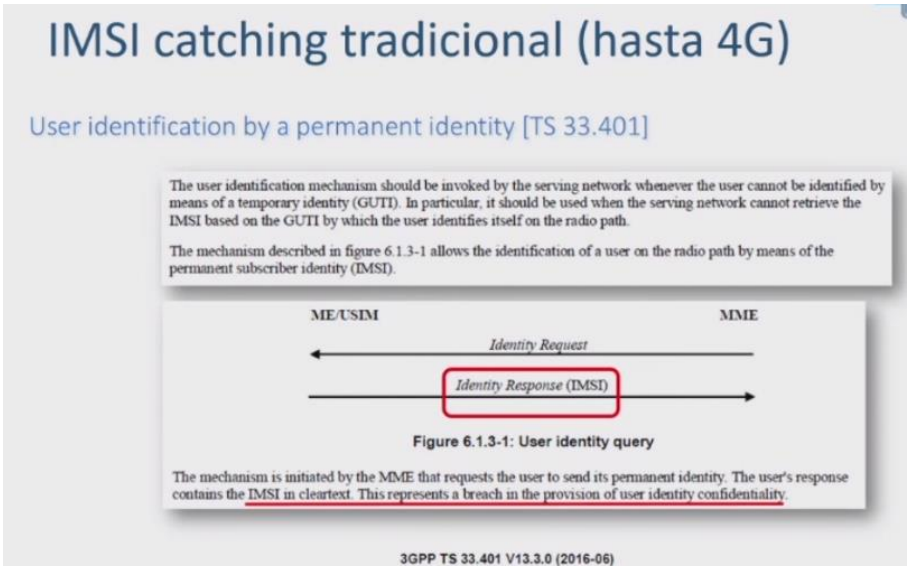

Ilustración 63. Ataque IMSI Catching. Identity Request
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Esto ya en la norma correspondiente se decía que era un problema de seguridad y como esto ocurría antes de que se produjera la autenticación y el establecimiento de clave AKA, el IMSI se enviaba en texto plano" [7].

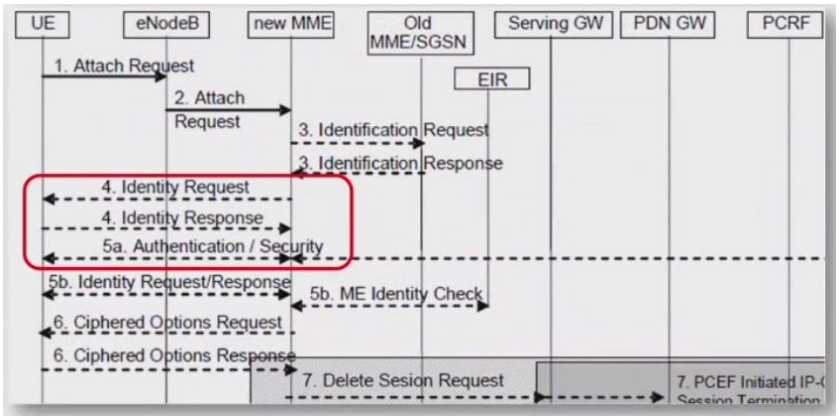

Ilustración 64. Ataque IMSI Catching. Authentication
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

La imagen siguiente muestra un ejemplo de este ataque en 4G mediante una estación base montada en el laboratorio, mediante un software libre disponible en internet. [7]

Utilizando un software de propósito general se puede hacer funcionar una estación base y configurarla para que cuando un terminal móvil se conectara le preguntara el IMSI [7].

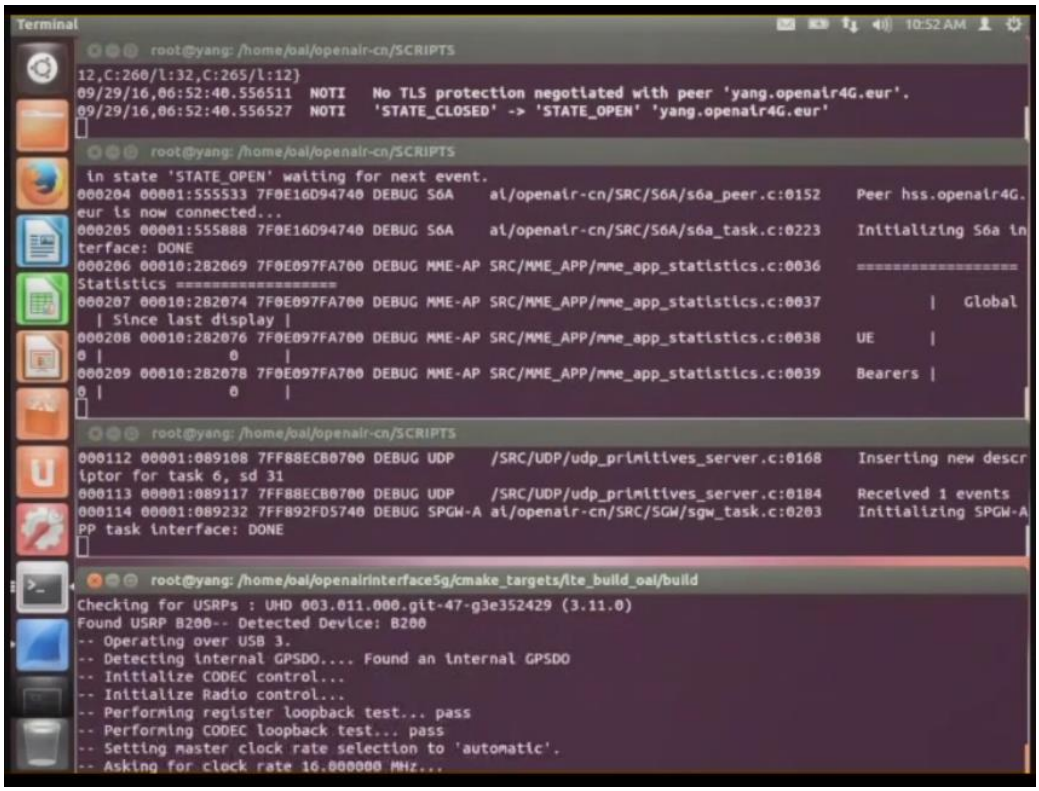

Ilustración 65. Ataque IMSI Catching. Software de propósito Gral.
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Se configuró el equipo para que todas las tramas que se enviaran o se recibieran por el aire se enviaran también se enviaran a un puerto concreto del local host donde se estaba ejecutando el software para poder verlo en la aplicación Wireshark.

En consecuencia, se pueden ver las trazas de red, que son paquetes encapsulados en UDP, por la interfaz de aire. Vemos un mensaje Identity Request y un mensaje Identity Response, en el que la red exige que le diga cuál es el IMSI al dispositivo móvil que es estaba conectando y este le responde. [7]

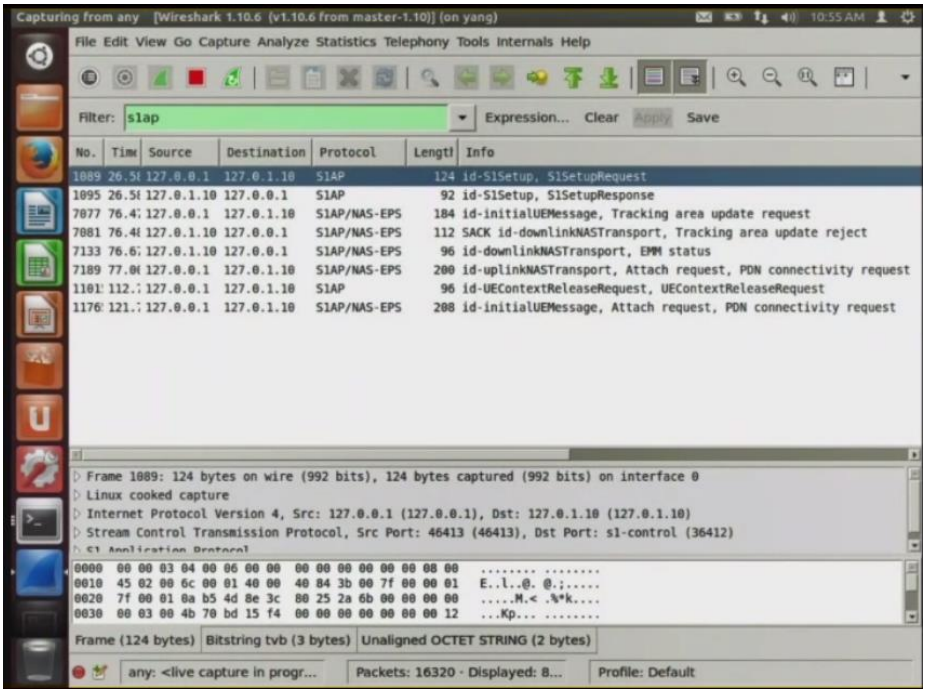

Ilustración 66. Ataque IMSI Catching. Trazas de Red_1
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

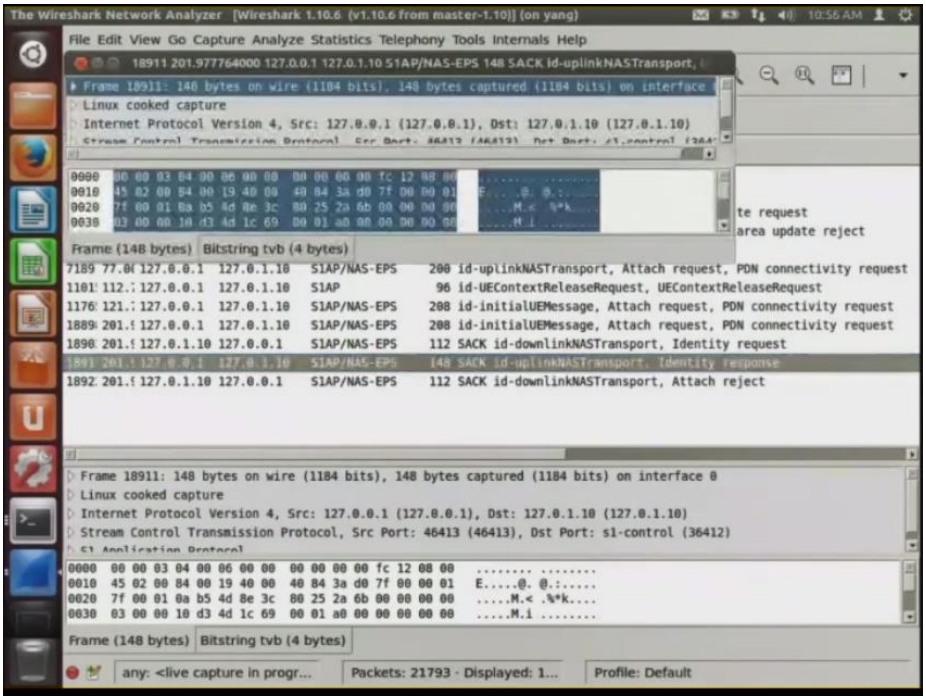

Ilustración 67. Ataque IMSI Catching. Trazas de Red_2
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

En uno de los campos podemos ver cuál es el IMSI en claro.

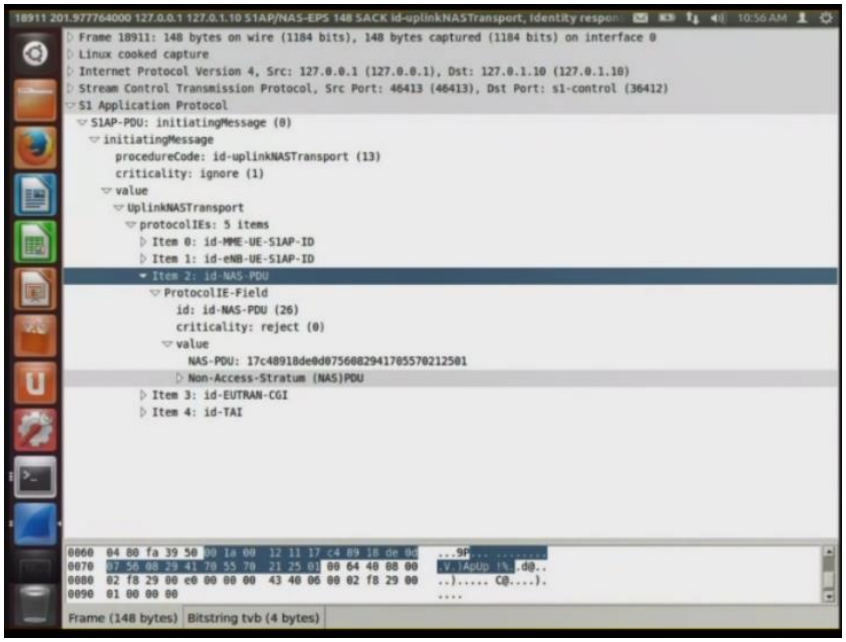

Ilustración 68. Ataque IMSI Catching. Trazas de Red_3
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

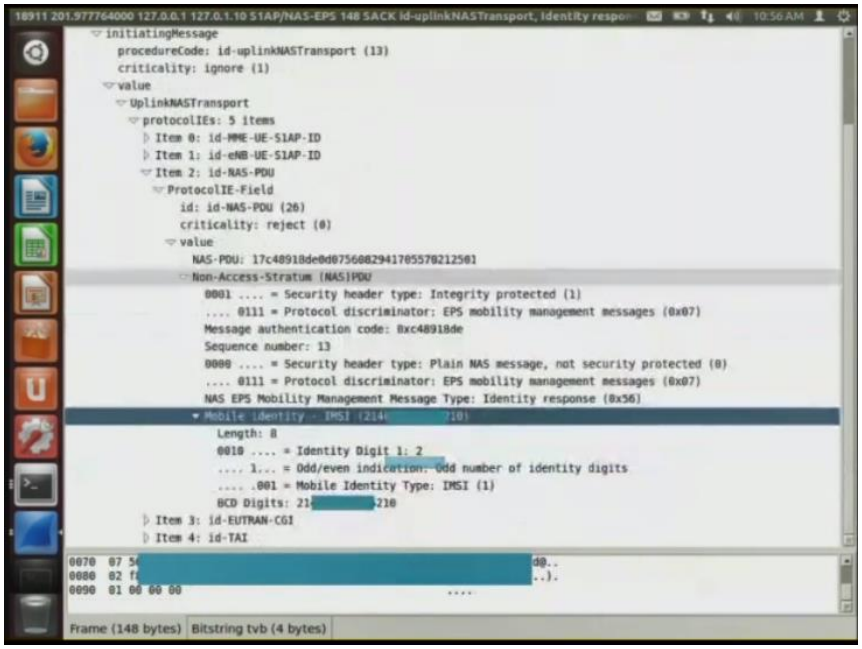

Ilustración 69. Ataque IMSI Catching. Respuesta del IMSI
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Tener un IMISI CATCHER era tan sencillo como poner una estación base falsa, esperar a que los móviles empiecen a contestar, y pedirles el IMSI, los cuales estaban obligados a suministrar en claro. Esta brecha de seguridad en 5G, en teoría, se habría resuelto.

En 5G lo que responde el móvil ya no es el IMSI sino el SUCI (*Subcription Concealed Identifier*)

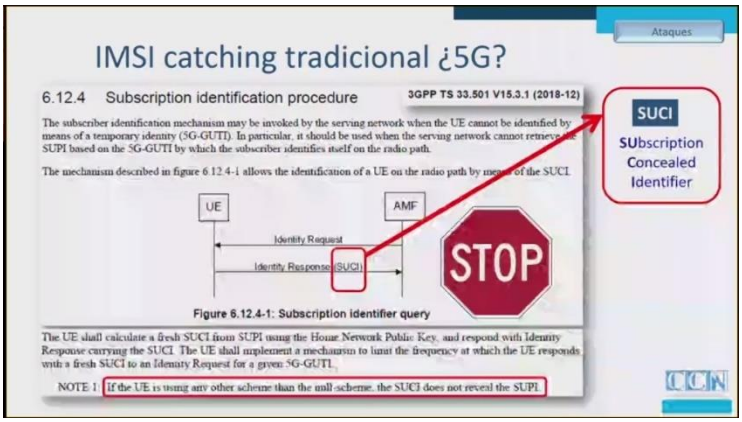

Ilustración 70. Ataque IMSI Catching. SUCI
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Este SUCI se encuentra cifrado con la clave pública del operador por lo tanto quien podrá descifrar el código será quien posea la clave privada que será el propio operador. Con este método se evita el ataque de IMSI Catching, salvo que alguien rompa este mecanismo de cifrado. Lo que se debe tener en cuenta en este punto, como se ha mencionado anteriormente es que depende del operador el uso de esta función de seguridad, es decir, de que el operador haya aprovisionado la clave privada e incorporado en las tarjetas SIM la clave pública de cifrado" [7].

5.2 ATAQUE aLTEr ATTACK

"Este mecanismo de ataque está orientado a la tecnología 4G. Hay un sitio web donde se pueden ver todos los detalles del método" [7].

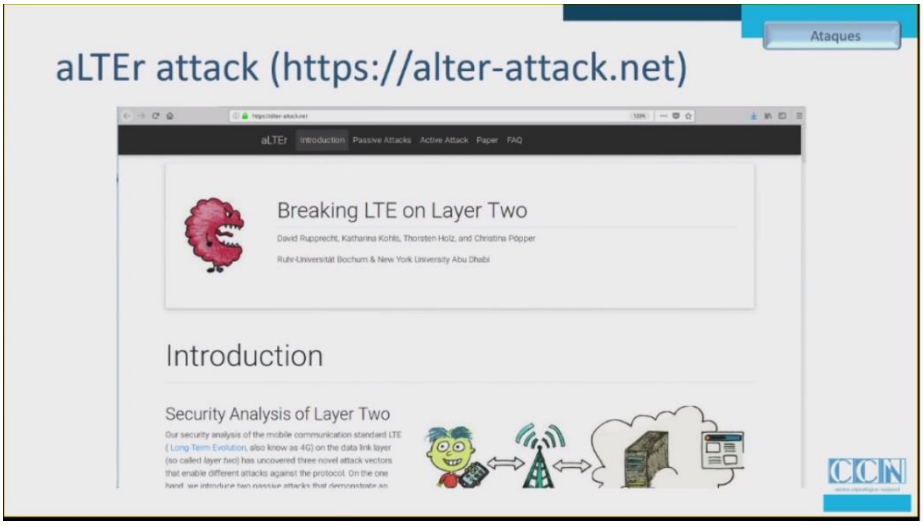

Ilustración 71. Ataque aLTEr
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

La base del problema hallado es que el cifrado en 4G se hace en AES en "*Counter Mode*" y funciona de la siguiente forma:

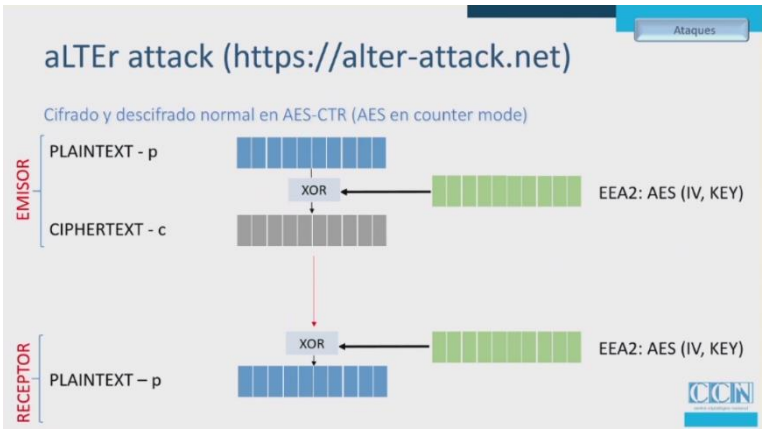

Ilustración 72. Ataque aLTEr. AES Counter Mode
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Por un lado, tenemos el emisor que quiere enviar un mensaje en texto plano y eso lo combina en XOR con una secuencia pseudoaleatoria generada a partir de un vector de inicialización y una clave que conoce. Se hace la operación y se obtiene como consecuencia el texto cifrado. Ese CIPHERTEXT viaja hacia el receptor y este lo único que tiene que hacer es combinarlo con la misma secuencia pseudoaleatoria que el receptor también puede generarla porque también posee la clave de sesión que se está usando (KEY). Entonces

el receptor haciendo XOR nuevamente vuelve a aparecer el texto plano. Así es como funciona el cifrado normal en 4G.

Lo que se pudo ver es que este mecanismo tiene protección de confidencialidad, pero no tiene protección de integridad de forma que el receptor no puede verificar de alguna manera si el texto cifrado que recibe es el que de verdad cifró el emisor o si ha sido manipulado por el camino.

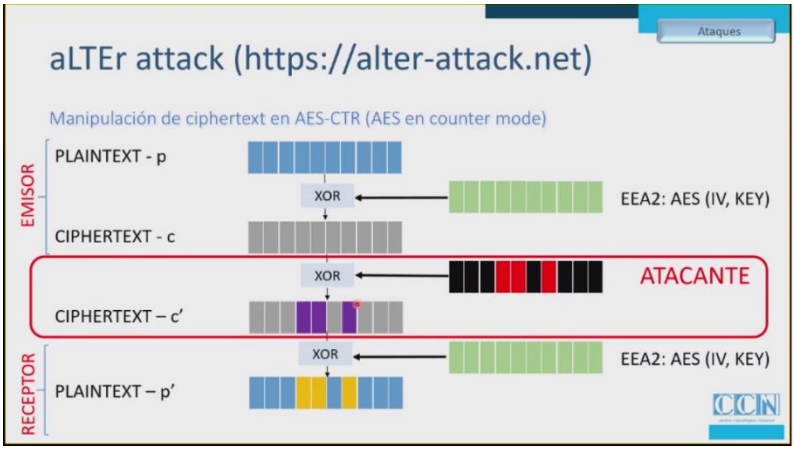

Ilustración 73. Ataque aLTEr. Falla a la Integridad
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Entonces, si un atacante se pone en medio, antes que el mensaje llegue al emisor, captura el mensaje y lo puede manipular, lo que se aprecia en la figura como los bloques de color negro y rojo con la leyenda ATACANTE. Lo que este ha generado es una secuencia de bits compuesto por todos bits ceros (0), los de color negro y lo que se ve en color rojo son los bits que se han puesto en uno (1). Si se hace lo anterior se tiene una máscara con todo ceros y uno pocos bits en uno. Luego si se hace XOR con lo que sea, lo que sucede es que los bits que están en esa posición (color rojo) se cambian (color amarillo). Es decir que solo esos bits son los que cambian, los que son cero pasan a ser unos y viceversa. Luego el texto cifrado C´ (CIPHERTEXT -C´) es parecido al anterior, pero hay unos cuantos bits que han cambiado, los que el atacante ha querido" [7].

"Ese texto cifrado C´ que ha recibido el receptor, luego si se lo combina con la secuencia pseudoaleatoria EEA2, que de hecho es la que usó el emisor en su momento. Lo que resulta es lo que él cree que se trata del texto plano del mensaje, pero como por el camino le han cambiado tres bits, luego del

XOR habrá unos bits modificados. El problema es que, como no hay protección de integridad el receptor no puede saber si esos bits son correctos o no, entonces no tiene manera de saber si el resultado del descifrado es exactamente lo que cifró el emisor.

El atacante puede realizar la maniobra exitosamente, pero si no sabe el contenido del mensaje no puede saber cuáles son los bits que debe modificar para que en verdad de un resultado que sea interesante.

Los que publicaron la falla realizaron una prueba de concepto y encontraron que de algunas tramas sí se sabe lo que hay dentro. Por ejemplo, en las peticiones DNS si sabes cuáles son los servidores DNS que ese operador le debe haber dado a ese cliente, se puede inferir que esos paquetes por las peticiones UDP del servidor DNS y entonces asumir ciertos valores" [7].

Ilustración 74. Peticiones DNS
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Entonces, cuando se encuentra un paquete que es una petición DNS a un servidor como el 8.8.8.8 del ejemplo, asumiendo que se trata realmente de un paquete con una petición a un servidor DNS, se puede modificar unos cuantos bits para que el lugar de la dirección mencionada figure por ejemplo 10.10.10.10 y algunos otros bits para que el checksum de la cabecera UDP encaje y entonces con ese paquete UDP modificado en la estación base falsa (RELAY) se ha logrado hacer un MITM (*Man in the Middle*) entre el UE que es la víctima y la Estación Base legítima. Si bien en la Estación Base falsa no se puede cifrar o descifrar, lo que sí se puede hacer es reenviar los paquetes modificados" [7].

Luego, la Estación Base legítima va a recibir la información y como no puede comprobar la integridad, cree que era verdad lo que decía el paquete y

luego lo envía a la IP destino, con ruta a internet, a un servidor DNS falso que ha sido creado exprofeso por el atacante para que responda. [7]

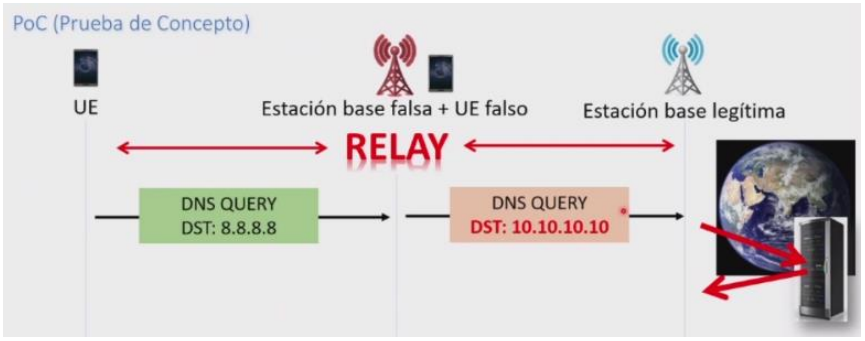

Ilustración 75. Reenvío de Paquetes
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Lo que se consigue con esto es redirigir los paquetes a un servidor que controla el atacante y la respuesta que se va a obtener es la que pretenda este, traduciendo el nombre a otra dirección IP, haciendo que la respuesta (1) que la Estación Base legítima le va a enviar al UE la va a recibir primero la Estación Base falsa, la cual va a tener que modificar la dirección nuevamente pare que el UE reciba la dirección correcta y la acepte. Entonces este traduce un nombre de dominio donde se ha tenido que conectar y ahora el navegador va a conectarse al servidor web que no es el rea" [7]l.

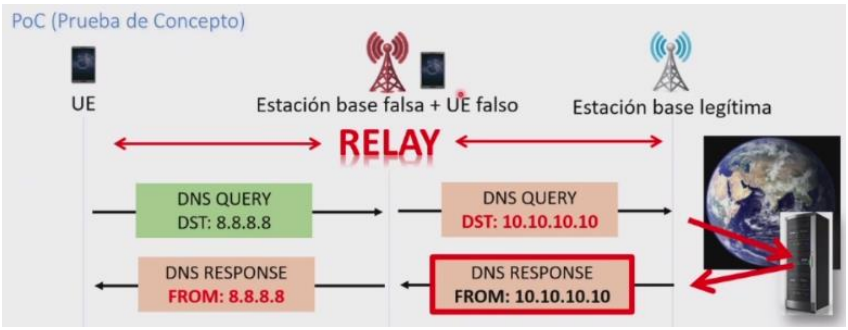

Ilustración 76. Respuesta del DNS falso
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5G dispone de protección de integridad, aunque nos encontramos en el miso caso del ataque de IMSI Catching, en el sentido de que su uso es optativo por parte del operador [7].

Ilustración 77. Ataque aLTEr en 5G
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.3 ATAQUES ToRPEDO, IMSI Cracking y PIERCER

Se trata de un conjunto de ataques que se han publicado en el mes de febrero del año 2019 aunque la investigación data del año 2018. Los dos primeros ataques mencionados servían tanto para 4G como para 5G y el último, en principio, solo para 4G. [7]

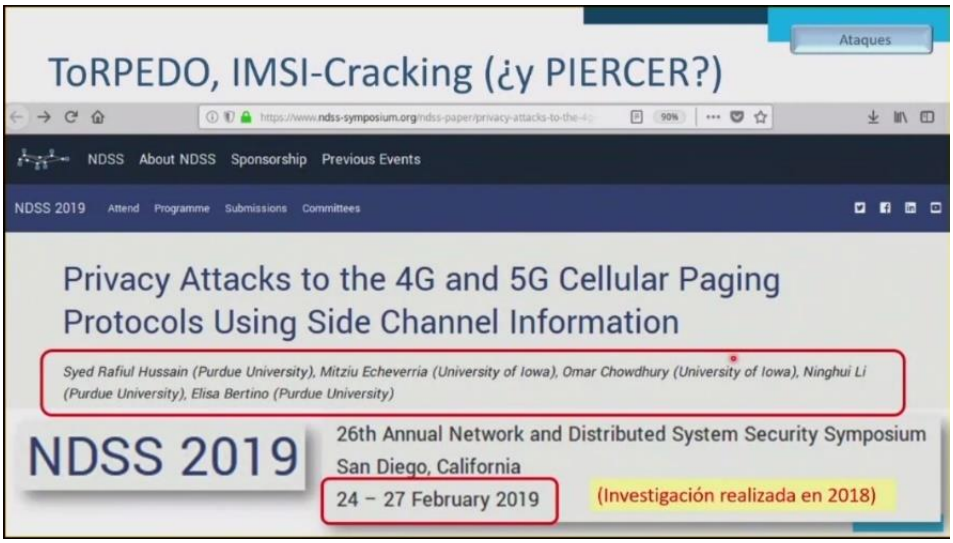

Ilustración 78. ToRPEDO
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“Lo que se debe tener en cuenta en principio en estos ataques es el concepto de PAGING OCCASION. El momento del PAGING es el momento del aviso de llamada. Para que los terminales no estén consumiendo batería en todo momento, escuchando todo el tiempo para saber si hay una llamada para ellos, lo que establece la norma es que a cada móvil se le asigna un momento del tiempo de la secuencia de tramas y subtramas dentro de las tramas que se van enviando y que se van repitiendo periódicamente, es decir que se les asigna un slot de tiempo.

Cuando el móvil está en estado IDLE (*Encendido*) o sea que no están haciendo nada, lo que debe hacer solamente es monitorear en esos momentos de tiempo. Es decir que el móvil permanece “dormido” y cada cierto tiempo se despierta para ver si hay alguna llamada para él, es decir, un mensaje de PAGING en el que el destinatario es él mismo. Es decir, se despierta y ve si tiene algún PAGING y si no lo tiene entonces se vuelve a dormir hasta el siguiente ciclo. A esto se le denomina PAGING OCCASION” [7].

No hay tantos PAGING OCCASION como terminales móviles entonces, para cada una de estas subtramas hay un conjunto de móviles asignados.

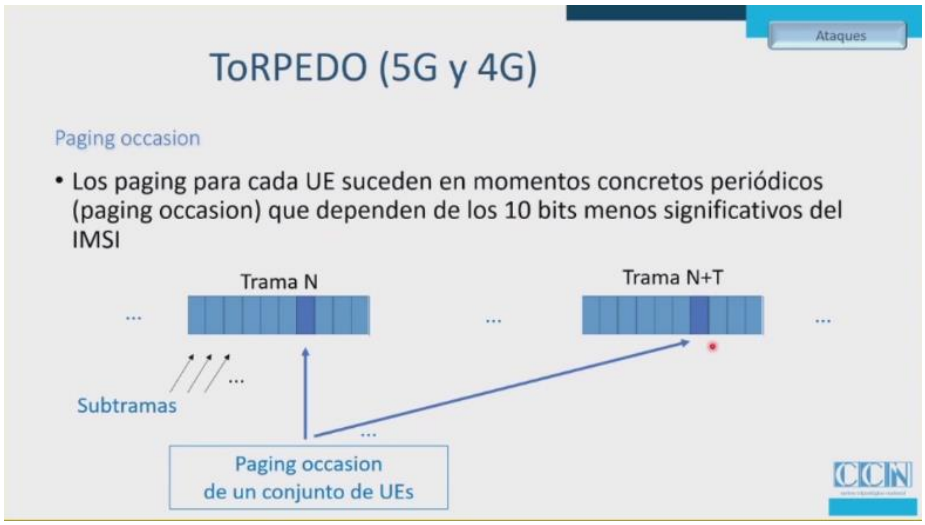

Ilustración 79 Fig. 70. ToRPEDO. Paging Ocassion
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“¿A qué terminal se le asigna cada subtrama? La norma define que calcula con los últimos diez bit de su IMSI. Luego, todos aquellos terminales cuyos últimos diez bit de su IMSI son coincidentes entonces se despertarán en la misma subtrama o sea en los mismos momentos” [7].

Para este ataque se observó que se puede enviar un mensaje o comunicación silenciosa contra el terminal móvil, un SMS silencioso en modo PDU, no en modo texto, de manera tal que la red intenta contactar con ese móvil, en este caso la víctima. En entonces lo que se está haciendo es escuchar todas las tramas y subtramas, observando cuántos mensajes de paging hay en las diferentes ocasiones, entonces se hace el envío silencioso y se mira si en algunos de esos momentos hay más paging y luego se detiene la maniobra. La idea luego es analizar la distribución y detectar la misma subtrama en la que se hace el intento de conexión con el móvil víctima, es decir, un mensaje de paging intentando despertar al móvil, avisándole que hay una llamada entrante o un mensaje entrante [7].

“Si se observa una distribución pareja pero cada vez que se hace un intento se produce un pico en la distribución en una de las subtramas, entonces sé que esa subtrama es el Paging Ocassion de la víctima y de otros cuantos también, pero el de la víctima que me interesa seguro que es. Sé que ese es el momento asignado para despertarlo así que los últimos diez bit de su IMSI ya los conozco y también sé que está en la zona, porque si no estuviera en la zona, cuando se hace el intento de llamada silenciosa, la red enviaría las tramas a otra zona y no se podrían ver los paging en esta. Con hacer este mecanismo de escucha y envío de comunicación silenciosa, determino esta tres cosas, si está en la zona, cuál es el momento en que se despierta o sea su paging ocassion y los últimos diez bit del IMSI. Lo importante es que funcionaría, aunque la red no esté utilizando el IMSI. Para hacer el aviso de llamada, podría estar utilizando el TMSI, el aviso temporal, es decir, aunque el TMSI estuviera cambiando en todo momento, simplemente lo que hacemos es ver si hay un pico en la distribución en el paging que hay en las subtramas” [7].

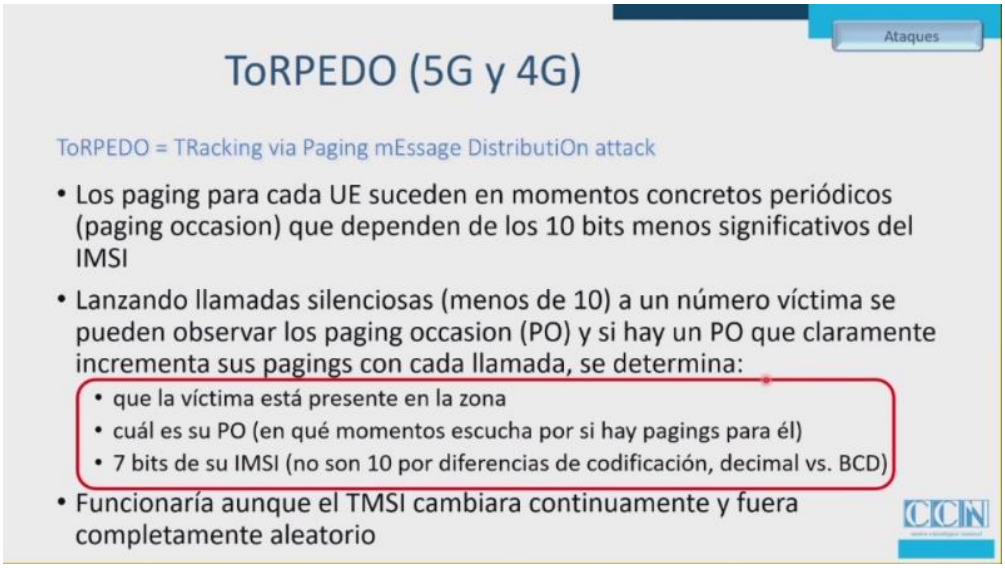

Ilustración 80. Análisis de PO
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Si sabemos los siete bits finales del IMSI (tiene 49 bits en USA y más o menos lo mismo en el resto de las países), y los primeros 18 bits representan al país del operador, entonces lo que queda al final son 24 bits desconocidos y esta cantidad sí que es manejable para hacer un ataque en fuerza bruta. En 13 horas se puede llegar a hacer un ataque de este tipo, de manera que se obtenga el IMSI concreto de la víctima" [7].

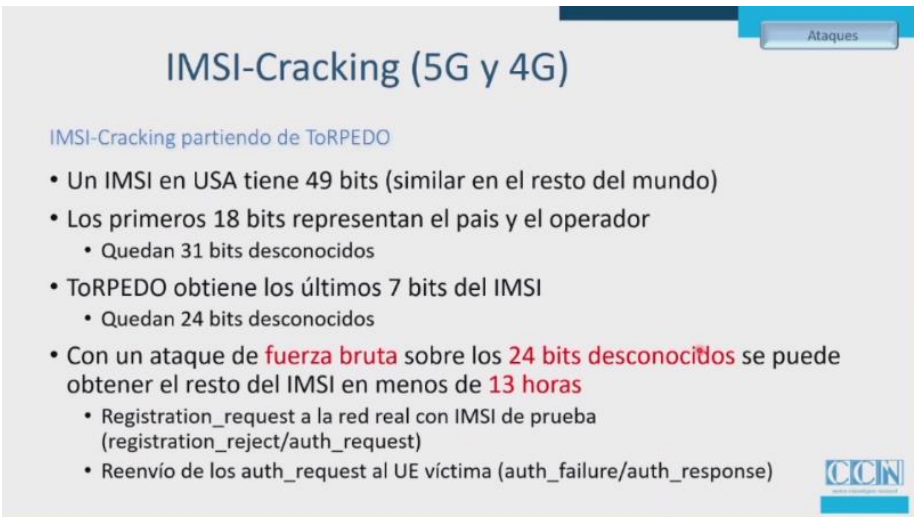

Ilustración 81 Fig. 72. IMSI Cracking partiendo de ToRPEDO
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“En el ejemplo, se ve al atacante en el medio del gráfico como la estación base y un terminal falsos. Con el terminal falso se envía un mensaje de REGISTRATION REQUEST a la red, con un IMSI que queremos probar. La red va a responder o bien con REGISTRATION REJECTED si el IMSI no existe o con un AUTH REQUEST si el IMSI existe, aunque todavía no sepamos si se trata de la víctima o no. El atacante, si ha recibido un AUTH REQUEST se lo reenvía al móvil víctima. Luego si el IMSI que se ha puesto en el AUTH REQUEST es el suyo entonces responderá con un AUTH RESPONSE, en caso contrario, si el IMSI no es el suyo, entonces responderá con un AUTH FAILURE. Repitiendo este proceso entonces se pueden ir probando los IMSI´s y en 13 horas aproximadamente, por medio del ataque de fuerza bruta, probando los 24 bits mencionados podemos hallar el IMSI correcto” [7].

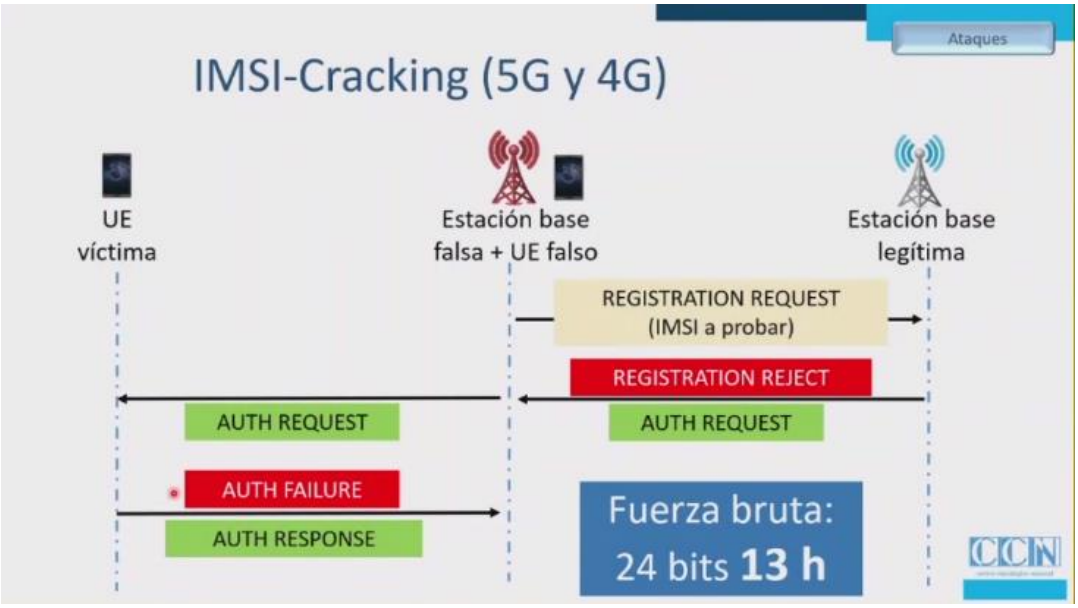

Ilustración 82 Fig. 72. IMSI Crackin
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.4 ATAQUE PIERCER (4G)

Este ataque lo que hace es obtener el IMSI sin el cracking, pero partiendo del ataque TORPEDO.

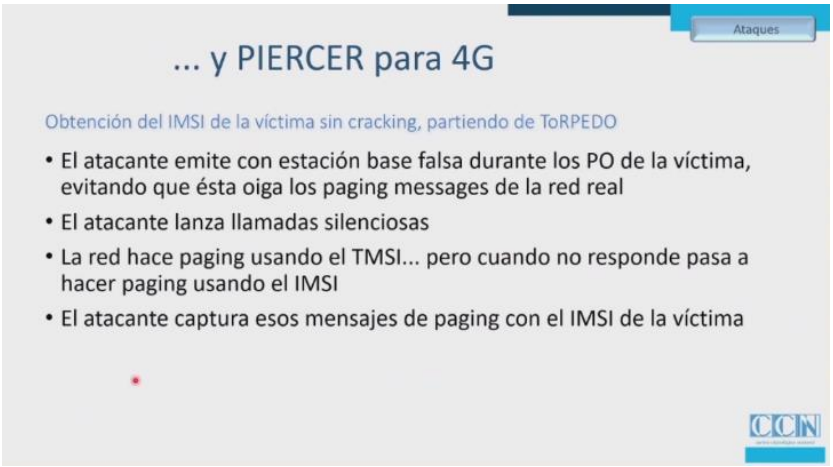

Ilustración 83 Fig. 73. Ataque PIERCER
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Lo que se hace es capturar los PAGGING OCASSION (PO) de la víctima. Sabemos cuándo se despierta entonces lo que se hace es emitir cosas en esos momentos para que el terminal víctima no escuche los reales. Luego se hace un intento de llamada a ese móvil. La red real va a hacer un PAGGING al terminal real, aunque originalmente usará el PAGGING-TMSI en lugar del IMSI. Esta situación se repetirá un par de veces y si no resulta, finalmente emitirá el PAGGING-IMSI para que no se pierda la llamada. Así es como se comporta en 4G ya que es como está definida la norma" [7].

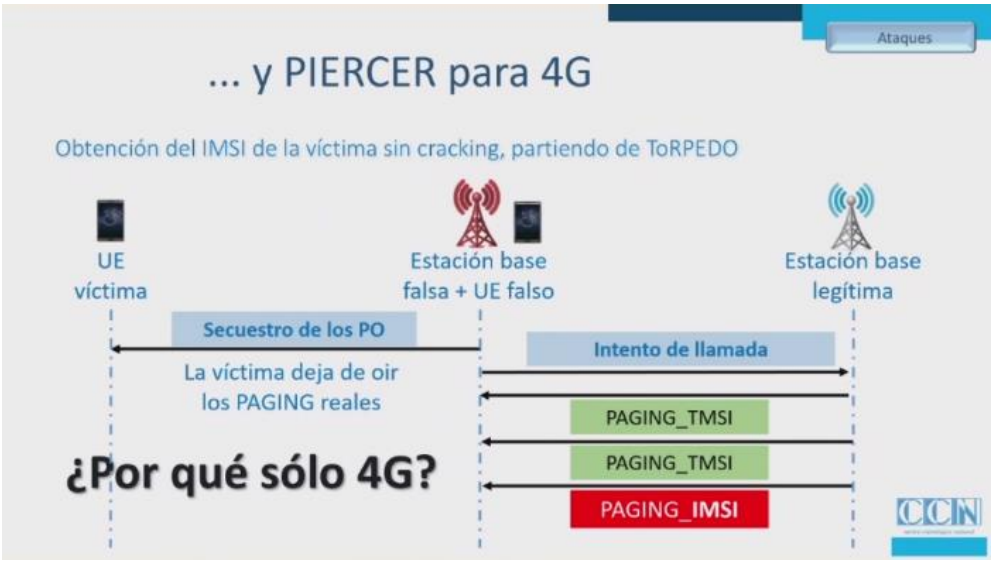

Ilustración 84 Fig. 74. Ataque PIERCER para 4G
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“En principio, como se mencionó, el ataque funciona para 4G. En el siguiente gráfico se muestra la diferencia del PAGING entre 4G y 5G. En 4G se puede hacer el PAGING o bien utilizando el TMSI o bien el IMSI. En cambio, en 5G se le ha agregado el identificador temporal NG-5G-S-TMSI y otros identificadores, pero no está el IMSI. En 5G está prohibido que el operador envíe un PAGING indicando el IMSI en claro del usuario. Ya no es decisión del operador, si da cumplimiento a la normal” [7].

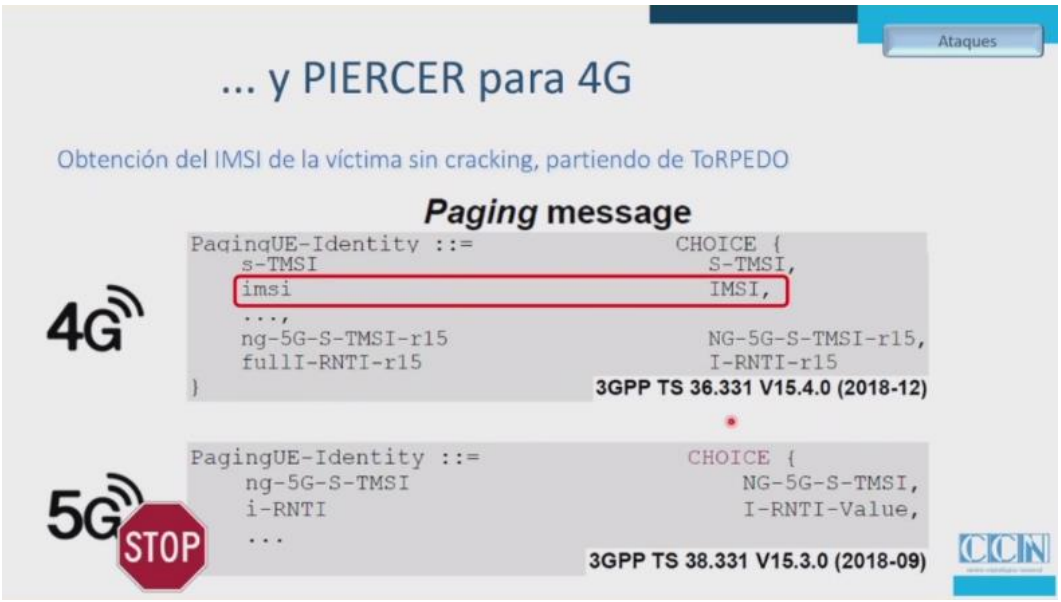

Ilustración 85. Obtención del IMSI partiendo de ToRPEDO
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.5 COORDINATE VULNERABILITY DISCLOSURE (GSMA CVD)

“GSMA es la asociación de la industria de GSM que, si bien no son quienes emiten la norma que en este caso es el organismo denominado 3GPP, tienen cierta influencia para solicitar modificaciones en los protocolos al 3GPP.

Los ataques TORPEDO, IMSI CRACKING Y PIERCER, si bien se hicieron público en febrero del año 2019, los investigadores se lo comunicaron antes de esta fecha a la GSMA quien estuvo trabajando en resolver estos

temas. Este organismo tiene una página donde reconocen el esfuerzo de los que hayan reportado vulnerabilidades. La figura siguiente muestra quienes reportaron los ataques” [7].

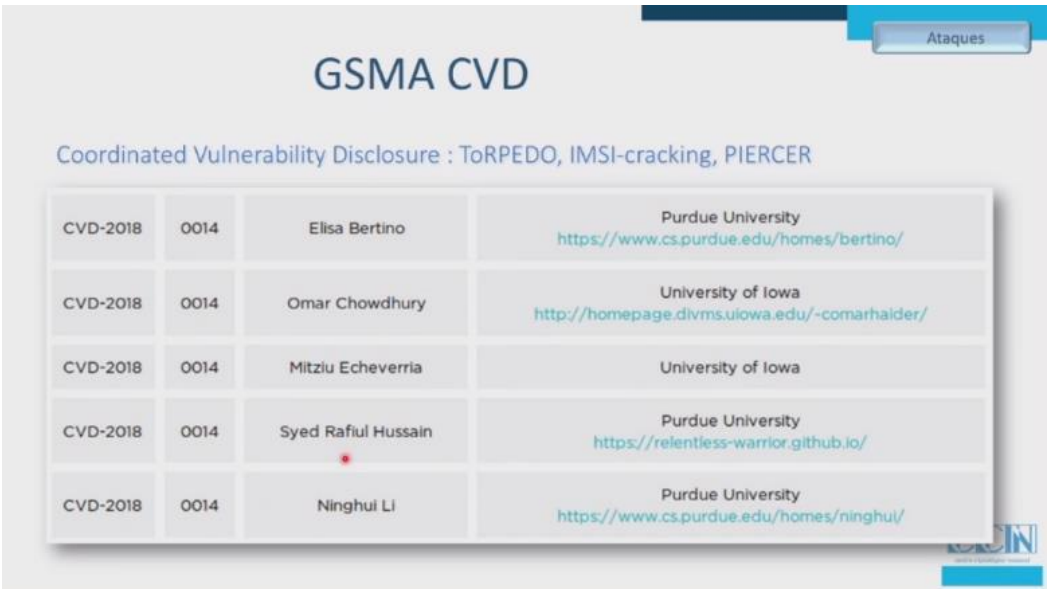

Ilustración 86. GSMA CVD

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“El resultado fue que desde el momento que ellos encontraron el problema y lo reportaron hasta que lo hicieron público en febrero, la organización 3GPP se ocupó del tema y generó las actualizaciones en su documentación.

En la siguiente figura se puede observar la versión de junio del 2018 y de septiembre del mismo año” [7].

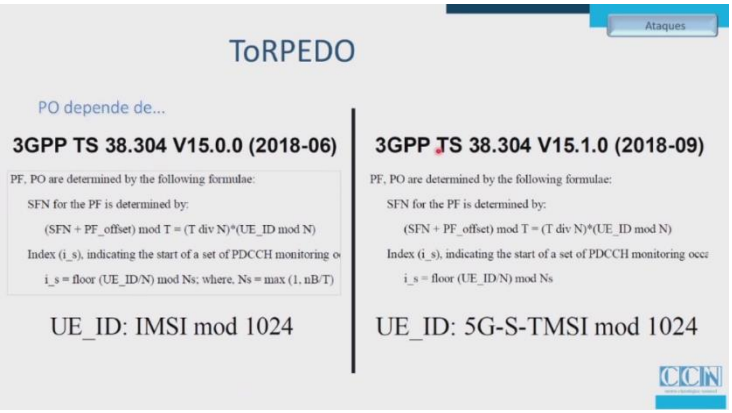

Ilustración 87. GSMA CVD Versión junio 2018

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Podemos ver en las versiones V15.0.0 y V15.1.0 de la sección del documento 38.304 donde se definen los PO (PAGING OCASSION), que en la versión de junio para el cálculo del UE_ID se utilizaba una función módulo 1024 con lo cual se podía hacer uso de los últimos 10 bits; sin embargo, eso cambia en la próxima versión y para el mismo cálculo ahora se cambia el IMSI por el TMSI. Con este cambio en la norma desaparece la posibilidad de hacer el ataque TORPEDO revelando el IMSI del usuario. Se sigue logrando encontrar cuando se produce el PO del terminal asociado a su TMSI y si este cambia varias veces ya no se puede concretar el ataque citado.

Desde luego, conseguir éxito con el IMSI CRACKING que se lograba porque quedaban solo 24 bits desconocidos, con este cambio también la posibilidad de hallar el IMSI desaparece, ya no se cuenta con el ataque torpedo y son 31 bits los que se tienen que encontrar y no 24, eso hace crecer exponencialmente el tiempo que se necesita para el ataque por fuerza bruta y entonces ese tipo de ataque ya no aplica" [7].

5.6 ATAQUES DE TRAZABILIDAD

"Aquí no vamos a encontrar el IMSI concreto del usuario, no vamos a poder descifrar sus comunicaciones, no vamos a tener control completo, pero se pueden conseguir ciertos datos que para algunos atacantes es útil. Consiste simplemente en poder determinar si un determinado terminal móvil

que estamos viendo en un determinado momento es el mismo que se vio en el pasado. Sirve por ejemplo si se está haciendo seguimiento de alguien, saber si esa persona vuelve a estar en la misma zona. Es decir, de los TMSI que estoy viendo en un momento determinado, alguno de ellos es el mismo visto en otra oportunidad y en la misma zona. Hay varios procedimientos publicados, aunque solo se citarán tres de ellos" [7].

MENSAJE DE FALLO MAC/SYNC FAILURE (Método 1): Se basa en que en 5G AKA, el procedimiento de autenticación y establecimiento de claves proporciona privacidad del SUPI, o sea que el identificador y el IMSI van cifrados si el operador lo configura correctamente pero no implementa protección contra reenvío de mensajes, entonces el atacante puede almacenar mensajes que se ven en el aire para luego reenviarlos en el momento que interesa y obtener conclusiones con esto. En concreto, hace replay de algunos de esos mensajes enviándoselos al UE, el terminal que queremos determinar si es el mismo que vimos antes

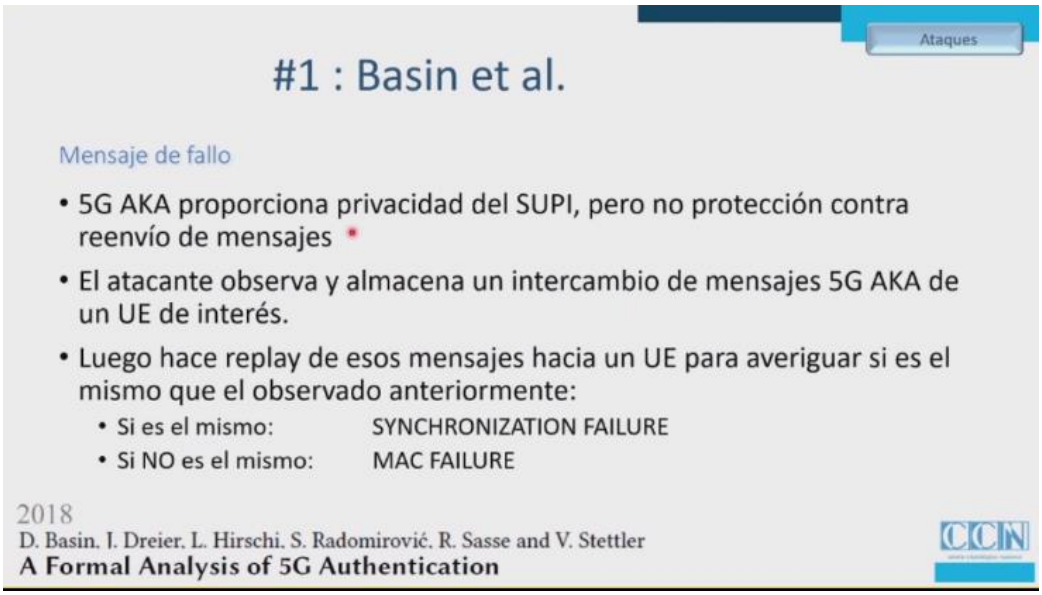

Ilustración 88. Ataques de Trazabilidad.
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“En la primera etapa, la víctima se comunica con la estación base legítima, envía el mensaje inicial, la red le envía una AUTH REQUEST y el terminal contesta con una AUTH RESPONSE y si todo va bien la red le dará servicio como corresponde. Hasta aquí el atacante lo único que hizo fue capturar tráfico y almacenarlo. Posteriormente, se verifica que en la zona hay un teléfono (UE incógnita) y tenemos el interés de determinar si es el mismo móvil del cual se capturó el tráfico. Para ello se debe contar con una estación base falsa para que el UE nos envíe el mensaje inicial para solicitar servicio y luego la base falsa el mensaje envía una respuesta con el AUTH REQUEST que oportunamente le envió la estación base legítima y cuyo mensaje teníamos almacenado. Luego pueden pasar dos cosas. El UE o bien responde con un MAC FAILURE (este mensaje no es para mí) que sería el caso en que la identidad IMSI del móvil al que se dirige el mensaje no es el mismo que generó el tráfico inicial o bien con un mensaje de error de sincronización (SINC FAILURE). Para el caso de que el mensaje es para él no va a enviar un mensaje AUTH RESPONSE como en el caso original porque los números de secuencia que se mantiene entre el móvil y la red ya fueron usados. En ese caso el UE enviará un mensaje de error de sincronización (SYNC FAILURE), diciendo que la red está utilizando un mensaje viejo. En ninguno de los casos se establece la comunicación, pero el atacante ya obtuvo lo que quería y es saber si ese móvil es el mismo que se había visto antes en la zona de cobertura de la antena; si responde MAC FAILURE no es el mismo visto anteriormente y si responde SYNC FAILURE, entonces sí que es el mismo [7].

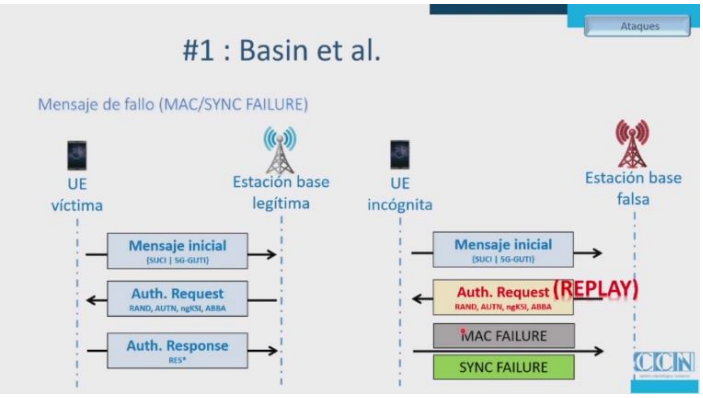

Ilustración 89. Ataques de Trazabilidad. Mensaje de Fallo
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

MENSAJE DE FALLO. REENVÍO DEL IMSI CIFRADO (Método 2):

Este método se basa en el mismo problema narrado en el método anterior, en el sentido de que se pueden reenviar mensajes y las entidades no van a progresar en el diálogo, pero van a reaccionar en forma diferente y esto nos permite determinar si el móvil es el mismo o no. En este caso el atacante (estación base falsa) se ubica en el medio, entre el terminal y la estación base legítima; el móvil envía un mensaje inicial solicitando servicio, el atacante, suponiendo que cuenta con la captura del tráfico de dicho terminal en una oportunidad anterior y quiere saber si éste es el mismo o no, envía a la estación base legítima el mensaje inicial del móvil capturado anteriormente. Seguidamente, la estación base legítima responde con un mensaje AUTH REQUEST que el atacante se lo reenvía al terminal móvil víctima; luego pueden pasar dos cosas: O bien esa respuesta sí que va destinada terminal objetivo, a la tarjeta SIM que tiene generando el mensaje AUTH RESPONSE ya que no se han producido errores de secuencia, o bien, si es destinatario no es el terminal, si el IMSI no es el suyo, entonces responderá con un mensaje MAC FAILURE, como en el caso anterior. En este punto ya se ha determinado si ese terminal es el mismo que vimos antes o no, que era el objetivo del ataque. [7]

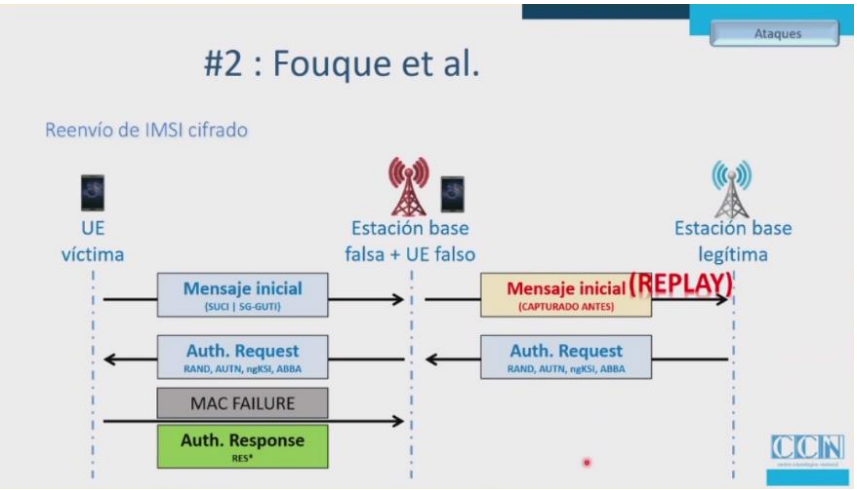

Ilustración 90. Ataques de Trazabilidad. Envío de IMSI cifrado
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

MENSAJE DE FALLO. OBTENCIÓN DEL NÚMERO DE SECUENCIA SQN (Método 3):

“Este ataque se basa en la obtención del número de secuencia que se genera en este protocolo de autenticación. En este caso el terminal móvil mantiene el número de secuencia de las autenticaciones que se han producido con éxito, la red mantiene también el número de vectores de autenticación que ha ido generando, de CHALLENGES es decir de retos o desafíos. Lo normal es que vayan avanzando a la vez, entonces cuando se produce el CHALLENGE, el número de secuencia coincide y luego este se acepta. ¿Pero qué ocurre cuando la red y el terminal se desincronizan? Ya sea porque la red haya generado varios vectores de autenticación que no han llegado con éxito al móvil y entonces, cuando el móvil pide servicio, la red le envía un vector de autenticación que no está en el rango que el móvil espera, entonces, lo que dice la norma es que hay que arreglar esta situación porque de esta manera no van a poder conectarse nunca. La forma en que se arregla es que el móvil envía un mensaje SYNCH FAILURE a la red informando que hay un error de sincronización e informando en ese mismo mensaje cuál es el número de secuencia correcto para el móvil. El número de secuencia no lo envía en claro y va anonimizado con una clave, la ANONYMIZATION KEY (AK). Lo que ocurre es que esa clave solo depende del CHALLENGE y de la clave precompartida del usuario y entonces, si para dos instantes de tiempo, el challenge que se ha intentado utilizar es el mismo, antes y después, entonces como la clave precompartida no va a cambiar porque es el de la tarjeta SIM y si el CHALLENGE que se ha utilizado es el mismo, entonces en esos dos instantes de tiempo la calve de anonimización sería la misma. El atacante no puede saber cuál es la AK que se ha utilizado, pero puede utilizar una propiedad o algoritmo (ver imagen), que es la propiedad de que, si se hace XOR con los mismos parámetros, es decir XOR de la misma cosa es como si no estuviera en la ecuación. Si se captura en un instante de tiempo un mensaje SQN_UE_t1 que contiene el número de secuencia del terminal en el instante uno, XOR la clave AK, y en un tiempo posterior hacemos lo mismo, obtenemos el número de secuencia del móvil en otro instante dos,

SQN_UE_t2 anonimizado con la misma clave AK, si el reto o challenge que se ha utilizado es el mismo (luego se verá cómo se utiliza el mismo challenge).

De esta forma se comprueba que la clave AK utilizada en t1 y t2 es la misma y ese parámetro de desprecia en el cálculo o ecuación mencionado y solo queda el XOR de los números de secuencia en los dos instantes. Haciendo XOR entre ellos lo que se verifica es cuáles son los bit que han cambiado. Si bien no se tiene el número de secuencia, sí se conoce cuáles son los bit que cambiaron. Haciendo este mecanismo repetidas veces se puede llegar a conocer al menos los bit menos significativos del número de secuencia que está usando el terminal. Si esto se consigue, analizando estos números se puede llegar a ciertas conclusiones. Por ejemplo, si el número de secuencia que se ha obtenido a la tarde o noche difiere en cinco del obtenido a la mañana puede significar que ha habido poca actividad del móvil, caso contrario si la diferencia es de doscientos, por ejemplo. De esta forma se puede establecer cuánta actividad ha tenido el terminal como así también si se trata del mismo móvil" [7].

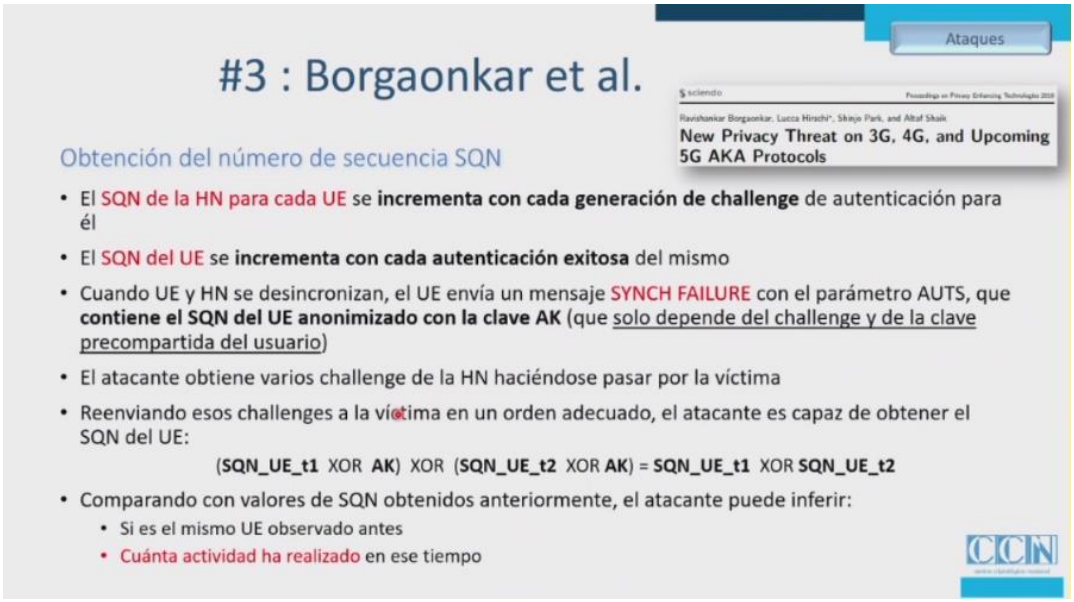

Ilustración 91. Ataques de Trazabilidad. Nro. SQN

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.7 ATAQUES DE SEÑALIZACIÓN

En señalización, como se ha comentado, 2G y 3G utilizaban el protocolo SS7, en 4G DIAMETER y en 5G se ha pasado a SBA (*Service Based Architecture*). Ahora el diálogo se va a mantener utilizando TLS en el medio con servicios HTTP, por encima, intercambiando JSON.

Tanto en SS7 como en DIAMETER se conocen ataques desde hace mucho tiempo debido a que, si un operador solicita información sobre un terminal móvil que le interesa, en este caso la víctima, depende cómo estén configurados, la home network se lo entrega. Le puede dar la clave de cifrado que esté usando ese móvil, la ubicación que tiene ese móvil, etc. Para mitigar este fallo los operadores han ido agregando firewalls a nivel de aplicación para distinguir entre “queries” que tienen sentido que se hagan de las que no lo tienen y que simplemente se rechazan [7].

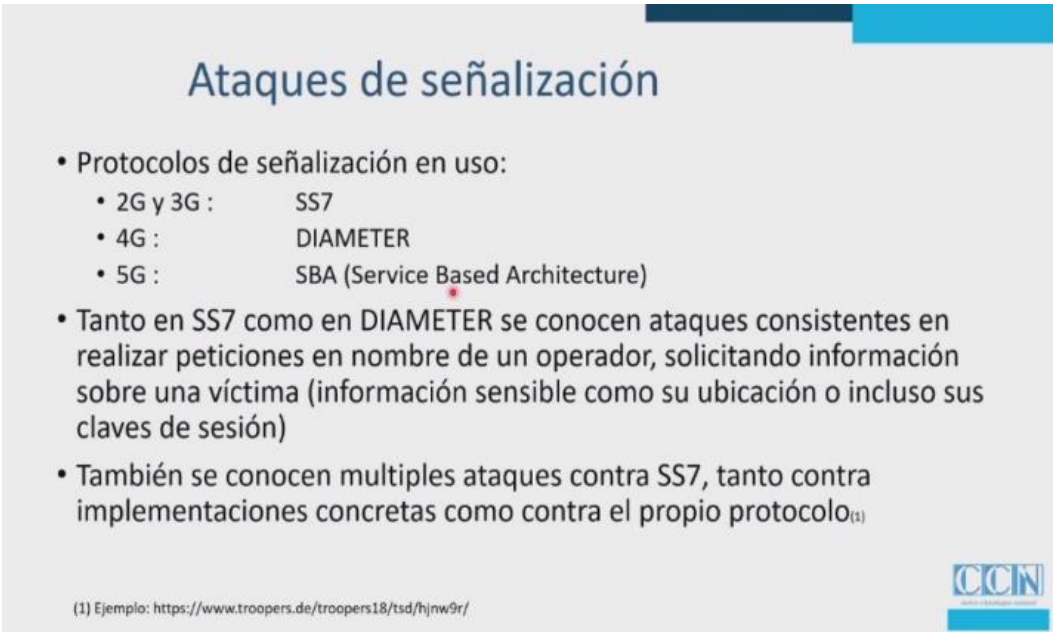

Ilustración 92. Ataques de Señalización

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

También se conocen ataques contra SS7, contra el propio protocolo y contra implementaciones. Se pueden llegar a explotar algunas vulnerabilidades en la codificación del ASN1, por ejemplo.

En 5G donde funciona la SBA, con la seguridad proporcionada por el protocolo TLS, al momento no se han publicado ataques a la vulnerabilidad del protocolo, lo que no significa que no existan [7].

5.8 ATAQUES DE SEÑALIZACIÓN VIA SBA

"En principio la seguridad en SBA está planteada para que el diálogo entre los operadores se lleve a cabo a través de los "próxies" (vSEPP y hSEPP) y que la información circule cifrada y autenticada.

Ilustración 93. Ataques de Señalización SBA

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

El problema de base sigue siendo el mismo y es que esa red por la que van a comunicarse multitud de operadores no pude garantizarse que todos ellos vayan a comportarse bien, entonces un operador o una entidad maliciosa que tenga acceso a estas interfaces tendrá que autenticarse y enviar la petición. En esa petición lo que se hace es requerir la clave de cifrado que está usando un determinado usuario y resulta que la red a la que se lo piden lo entrega. Se estaría en el mismo problema que cuando se tenía SS7" [7].

Ilustración 94. Ataques de Señalización SBA. Modelo de Confianza

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"La comunicación en principio va autenticada y protegida, pero distinguir entre peticiones, qué debo responder y qué no debo responder es un problemas de firewall a nivel de aplicación en los próxies. Distinguir entre peticiones legítimas y no legítimas al final no es tan fácil. Lo que sí sería viable, por ejemplo, es distinguir si un usuario estableció sesión en una red por ejemplo en china y una hora después lo hizo en argentina lo cual sería por el momento físicamente imposible de que ocurra" [7].

Ilustración 95: Ataques de Señalización SBA. Proxies

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.9 PROBLEMAS PENDIENTES

"Los ataques mencionados hasta aquí de alguna manera ya han sido resueltos y corregidos en la Release 15. Sin embargo, hay algunos ataques que por el momento no tienen solución. De hecho, existe el documento 33.809 para la Release 16 en la que se recopila el conjunto de problemas relacionado con ataques de estaciones bases falsas que todavía están por resolver y que se plantea solucionarlo a partir de esta última Release.

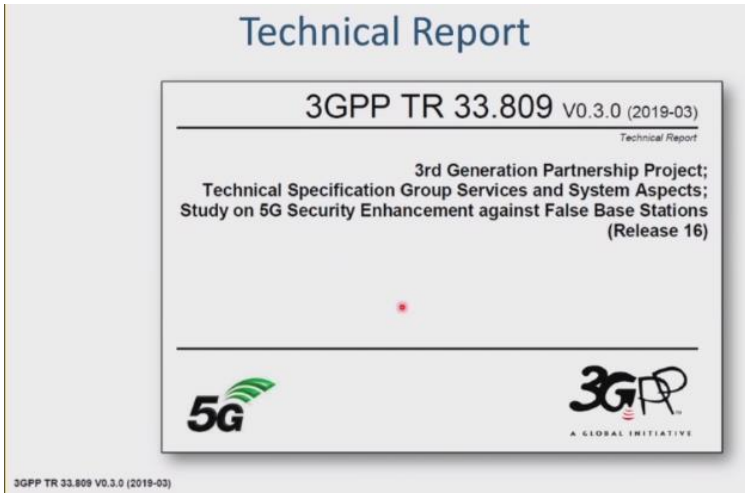

Ilustración 96. Reporte Técnico 3GPP sobre Seguridad Mejorada

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

Seguidamente se enumeran los problemas pendientes de resolución en relación con las estaciones bases falsas:

1. Seguridad de mensajes unicast sin protección (RRC y NAS)
2. Protección de información del Sistema (SI)
3. Detección de estaciones base falsa cercanas
4. Protección frente a envenenamiento de SON
5. Protección frente a Authentication Relay
6. Resistencia frente a inhibición de radiofrecuencia
7. Protection frente a ataques man in the middle" [7].

5.10 PROBLEMAS DE MENSAJES UNICAST SIN PROTECCIÓN

“Es un problema conocido en el pasado y es que tanto a nivel de radio, al solicitar un canal de radio y su asignación al nivel de red del NAS que es cuando hay asignación de canal de radio y ya se está dialogando a nivel de red core, donde se solicita y se entrega el servicio o se rechaza, en ambos niveles existen excepciones a mensajes que tienen que ir protegidos en integridad. En general toda la señalización va protegida en integridad de acuerdo con la norma, pero hay excepciones. Entre esas excepciones se encuentran los mensajes de rechazo tanto a nivel de radio como a nivel de red. A nivel de radio, cualquier estación base falsa sin necesidad de ninguna clave, ya que para enviar estos mensajes no lo necesita, se puede enviar un mensaje RRCREJECT a un móvil que solicita servicio. En generaciones anteriores se podía hacer un rechazo para no dar servicio, pero, por cierto, se podría indicar también que el móvil cuenta con una estación base 2G en la zona que sí podría dar servicio, entonces se conseguía hacer una redirección a la estación base falsa muy específica y con solo este mensaje REJECT. Esto en 5G ha mejorado mucho; en ese mensaje lo único que se puede hacer es indicar un TIMEOUT o seas indicar cuánto tiempo hay que esperar para volver a preguntar, con lo cual ya no se puede realizar la redirección directa, pero lo concreto es que el mensaje se sigue pudiendo enviar sin autenticación.

En el caso de nivel de red o nivel de NAS, cuando ya se tiene la conexión de radio y se está comunicando con la red central, la solicitud de servicio, el mensaje REGISTRATION REQUEST puede ser contestado con un AUTENTICATION REQUEST o con REGISTRATION REJECT y este mensaje de REGISTRATION REJECT puede llevar un código con el motivo del rechazo y entre los códigos indicados están el que indica que el terminal es ilegal (UE) o es una tarjeta SIM ilegal (ME). Lo que le sucede a un móvil que recibe este mensaje de rechazo es que se convence de que efectivamente es ilegal y entonces se queda sin servicio” [7].

Ilustración 97. Mensajes Unicast sin protección

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

"Hasta 4G esto suponía que el móvil se quedaba sin servicio en absoluto, con solo llamadas de emergencia, pero en 5G el terminal se queda sin ningún tipo de servicio, incluso sin llamada de emergencia. El suscriptor queda en este estado, sin servicio en forma persistente hasta que el equipo se reinicie. Este proceso constituye un típico ataque de denegación de servicio y puede pasar mucho tiempo hasta que la situación sea advertida por el usuario.

Si un atacante quisiera denegar servicio persistentemente en una zona, solo debería pasar por la zona generando rechazo a todos los móviles que pidan registrarse. Estos suscriptores quedarían en ese estado hasta que cada uno lo reinicie y para entonces, el atacante puede estar muy lejos de allí" [7].

Ilustración 98. Denegación de Servicio

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

“Esta vulnerabilidad de poder enviar mensajes de REJECT y dejar el terminal sin servicio hasta que se reinicie está presente desde 2G, y se encuentra publicada desde el año 2012. En el año 2016 se probó y demostró esa falla en 3G y en el año 2015 ocurrió lo mismo para 4G. En 5G sigue estando, aunque se ha limitado el impacto, ya que se queda sin ningún servicio, pero de 5G; esto si bien es una mejora, no resuelve el problema porque si el atacante tiene una estación base falsa 5G que recibe el rechazo y otra base falsa en 4G que también recibe el rechazo se asegura dejar sin servicio el móvil, excepto llamada de emergencia” [7].

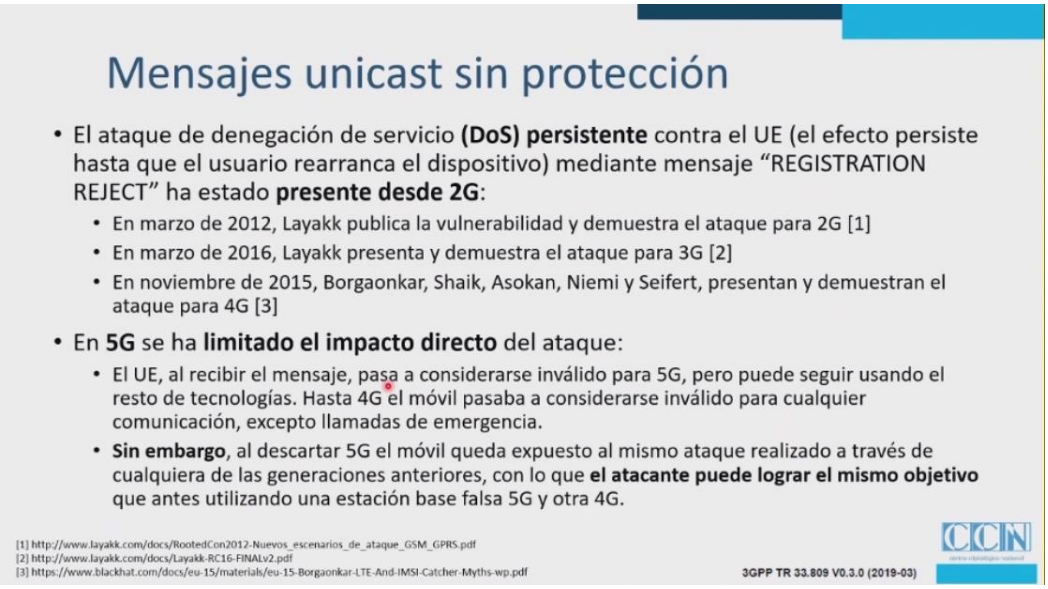

Ilustración 99. Mensaje Unicast sin protección. Situación en 5G

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.11 PROTECCIÓN DE INFORMACIÓN DEL SISTEMA

“En el mensaje broadcast que envían las estaciones bases, transmiten abundante información en forma periódica y en claro, para que todos los móviles que están en la zona puedan escuchar e interpretar el mensaje emitido, incluso entes de solicitar servicio y decidir a cuál de ellas le solicitan servicio. A esa información se le llama SI (*SYSTEM INFORMATION*) y, todavía en 5G, no va protegida de ninguna manera. El móvil no puede validar de ninguna manera que esa información sea fiable, es decir, si esa

información la ha enviado la red real o lo ha hecho una estación base falsa, o si la han modificado por el camino.

Entonces si un atacante envía información falsa, como por ejemplo de cuáles son las frecuencias que utiliza una estación base y cuáles son las frecuencias de las estaciones bases vecinas, que es información que forma parte del SI, transmitido por las estaciones bases en forma de broadcast, un atacante puede tener su propia celda emitiendo y diciendo que esa celda tiene tal identificador y que no hay celda vecina. Entonces si un móvil decide conectarse a esa estación falsa no va a estar escuchando al resto de las celdas que hay en la zona porque en la lista de celdas vecinas no figura ninguna. Esto es un problema que se conoce desde hace mucho tiempo y en el documento mencionado (Release 16) se intentan plantear soluciones. Lo que sucede es que solucionarlo no es fácil ya que, por ejemplo, si se decide utilizar criptografía para que se firmen todos los datos que envía la red real entonces todos los móviles tendrán que disponer de la clave pública que les permita eso que se está enviando, si ha sido firmado correctamente y eso los lleva al problema de distribución de claves o gestión de claves entre los distintos móviles y diferentes operadores, lo cual es un problema que hasta el momento no está claro cómo se va a solucionar" [7].

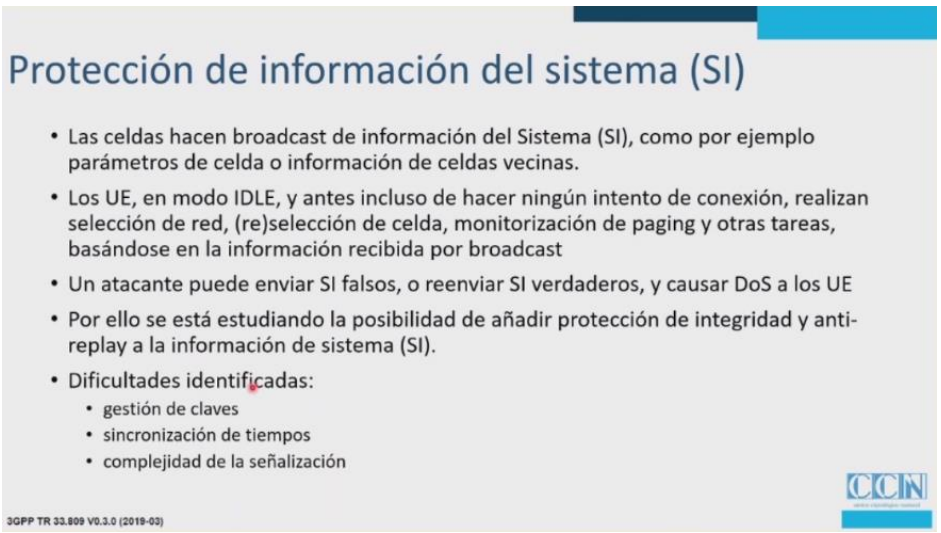

Ilustración 100. Protección de Información del Sistema (SI)

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.12 DETECCIÓN DE ESTACIONES BASES FALSAS

“Otro problema grave es el de no poder detectar es si hay estaciones bases falsas. Dicho de otra manera, sería útil para los operadores que pudieran advertir o detectar la presencia de estaciones bases falsas e informar a los usuarios correctos para que estos las ignoren.

Uno de los mecanismos que se plantea para esto es aprovechar los procedimientos de reportes que ya define la norma.

La norma ha definido procedimientos de reporte para que los móviles informen a la estación base de muchas de las circunstancias que están observando en el entorno radioeléctrico. La idea es que la red se pueda reconfigurar ante situaciones anómalas que se están produciendo. Ya que esa información puede ser reportada por los móviles lo que se plantean aquí es que la misma sea utilizada, con cierto análisis, como por ejemplo la frecuencia de uso en el entorno o los identificadores de celda registrados, para llegar a la conclusión de que hay una estación base falsa en la zona.

Los reportes están definidos con ciertos valores y lo que hace el documento es plantear el uso de estos proponiendo seguir investigando y proponiendo mejoras en la información que envíen los móviles y su análisis, como mecanismo de detección de estaciones bases falsas” [7].

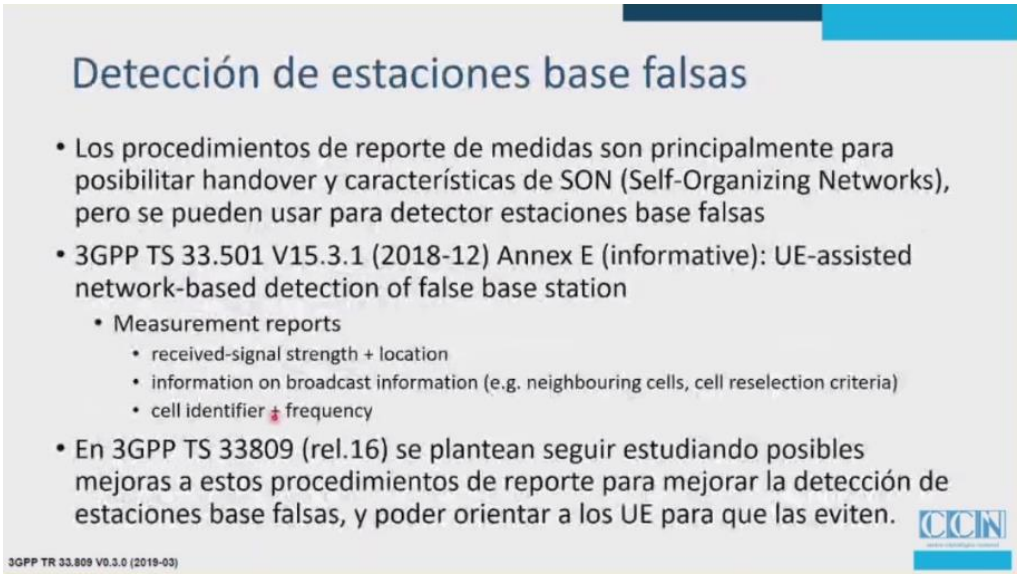

Ilustración 101. Detección de Estaciones Bases Falsas
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.13 ENVENANAMIENTO DE SON

“Otro tipo de ataque que también está pendiente de resolver es el ENVENENAMIENTO DE SON (*Self Organized Network*) que está relacionado con lo mencionado anteriormente de la reconfiguración de la red. En 4G se ha demostrado que un atacante puede querer denegar el servicio de una estación base real colocando una estación base falsa, configurándola para que se identifique con un número determinado (300 en el ejemplo). Un terminal móvil que se encuentre en la cona puede ver la estación base falsa y querer conectarse. La estación base lo que hace es producir algún tipo de error en la comunicación de manera que el móvil no puede conectarse. Lo próximo que hará el móvil, siguiendo la recomendación de la norma, es ignorar esta BTS y buscar otra en la zona para pedirle servicio y cuando consiga una de la red real lo que hará es enviar un reporte o informe de lo que ha pasado. Va a reportar que la estación base con el identificador 300 ha causado un problema. Entonces la red ante ese reporte puede por ejemplo ignorar el reporte o puede tomar decisiones y una de estas decisiones puede ser la de apagar la radiobase en virtud de que varios terminales móviles reportaron esa estación base como maliciosa. Entonces la propia red se autodeniega el servicio de la estación base legítima en base a información verdadera que le han enviado los móviles los cuales han sido inducidos a informar esa situación mediante la intervención de la estación base ilegal. Luego, usando un atacante una estación base falsa logró que la red saque de servicio a una estación base verdadera. La norma no establece exactamente cómo debe responder ante cierta información que le envían los móviles; lo que hace es dejar abierto el mecanismo para que ellos envíen la información y luego es responsabilidad de cada operador el implementar las reglas de qué hacer con tal o cual información, es decir que depende de la implementación que tenga cada

operador, de sus capacidades de SON, para evitar o no esta denegación de servicio” [7].

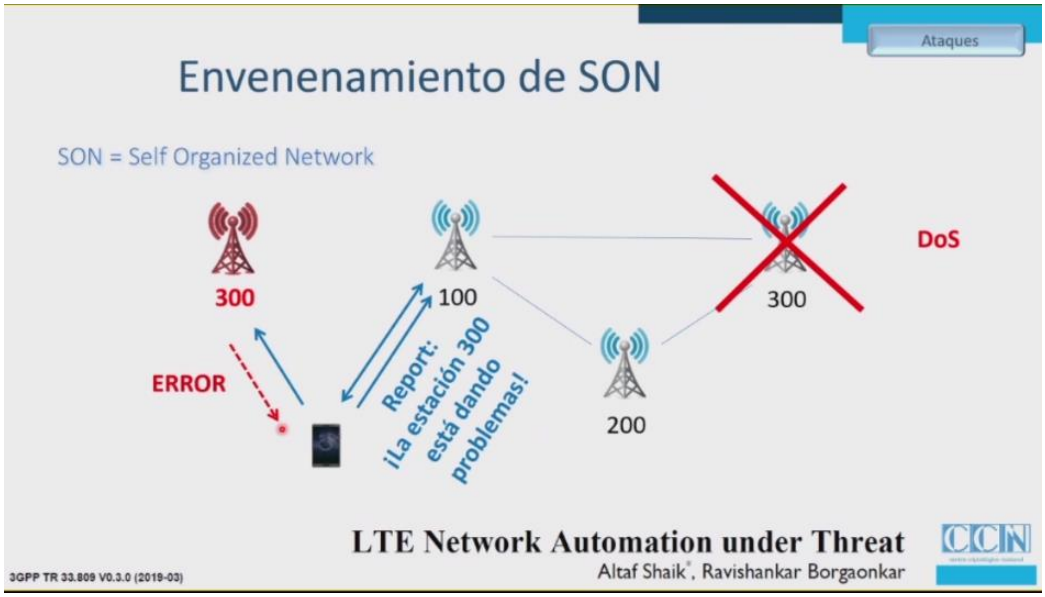

Ilustración 102. Envenenamiento de SON
Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.14 AUTHENTICATION RELAY

“Otro problema muy grave que ya se encuentra planteado en la Release 15 y que se está intentando resolver para la próxima versión del documento, es qué hacer ante un ataque de relay de la autenticación. Todo el mecanismo de autenticación explicado anteriormente es vulnerable a un ataque de este tipo.

Teniendo el atacante una estación base falsa y un terminal móvil falso en comunicación entre sí, sin estar necesariamente en el mismo entorno físico, pueden estar ubicados incluso en continentes distintos (en el ejemplo la estación base se encuentra en Valencia y el terminal móvil en Roma), un móvil real ubicado en la zona de cobertura de la antena falsa intentándose conectar a ella, en lugar de responder al pedido de conexión del terminal real envía la información del pedido de registración al móvil falso, quien envía a su vez esa información a la estación base legal en Italia, la estación real ante la petición real de un móvil responde, esa respuesta el móvil falso se la reenvía a la estación base falsa y luego ésta última le envía esa respuesta al terminal

móvil real en España, y así, enviando los paquetes de un lado para otro se termina estableciendo la comunicación. No se puede descifrar la comunicación que está por le medio, entre la estación base y el terminal falsos, pero se ha conseguido que el móvil real que se encuentra en Valencia, a la red que se encuentra en Roma le haga entender que el móvil se encuentra en su red. Eso tiene implicancias muy serias ya que permite que, por ejemplo, una persona se encuentre en España que parezca que se encuentra en Italia, lo cual sería una buena coartada para un delincuente y de esta manera podría aparecer en todos los registros que verdaderamente se encontraba en Italia.

También es un problema el cargo de roaming ya que el servicio que le van a facturar los operadores al celular real será con el Roaming activado con lo cual se le incrementará el monto a pagar de manera considerable, ya que para todos los efectos de la red ese terminal móvil se encuentra en Roaming.

Con este método se puede hacer también denegación de servicio completo o selectivo ya que el atacante se encuentra en el medio reenviando los mensajes de un lado para otro, pero cuando llega un aviso de llamada para el terminal móvil, a ese mensaje no se lo reenviamos, entonces el usuario está con su móvil y no le llega un aviso de llamada, entonces se le está denegando el servicio o cierta parte de este.

El ataque a SON es que el móvil real va a estar reportando lo que considera que debe reportar a la red real, pero es recibido por la estación base falsa, cuando en realidad esos reportes van a estar llegando a la estación base real en otra ubicación física, en el ejemplo Italia. Lo curioso es que el terminal móvil real va a estar informado lo que ve en las celdas o estaciones bases reales que detecta en la zona de su incumbencia (Valencia). Cuando la información llega a la estación base legal en Italia para esta el reporte no tiene sentido y esto puede llegar a provocar decisiones en la reconfiguración de la red que sean problemáticas” [7].

Ilustración 103. Ataque Authentication Relay

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.15 INHIBICIÓN DE RADIOFRECUENCIA

"En 5G hay algunas características que mejoran el rechazo a este ataque, para que sea más resistente a interferencias, pero al final un ataque de inhibición de frecuencia mediante el cual se genera ruido electromagnético siempre es posible.

En el documento lo único que se indica es que es necesario seguir trabajando en intentar mejorar la resistencia frente a este ataque ya que eliminarlo no sería posible. Lo que sugiere es que se haga hincapié en la detección y localización de cualquier fuente de inhibición, que al menos si se produce pueda detectarse y se identifique exactamente dónde se ubica la

fuente. El documento tampoco sigue más allá porque tampoco es responsabilidad de este grupo 3GPP" [7].

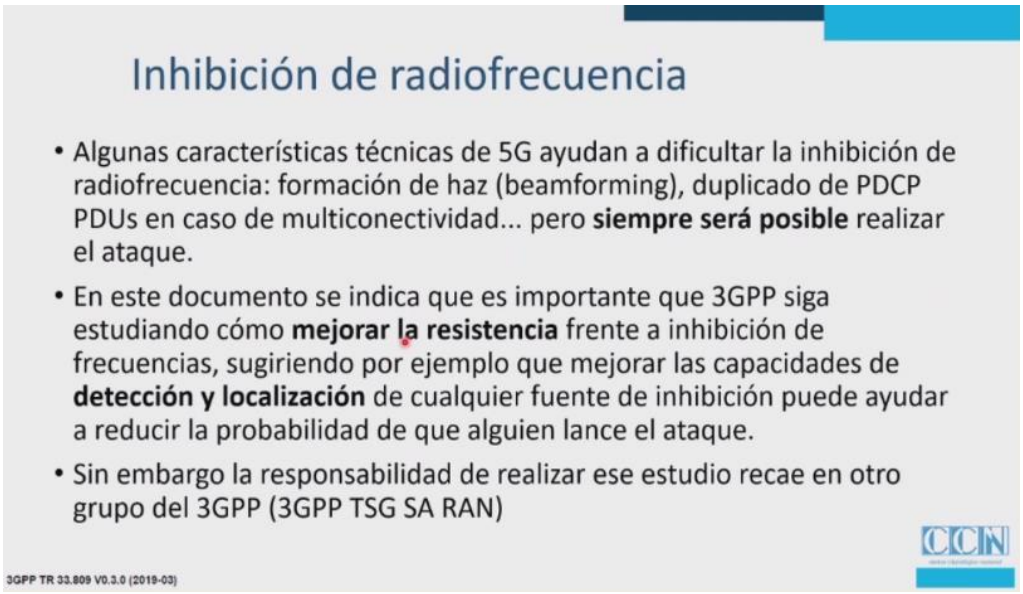

Ilustración 104. Ataque por Inhibición de Frecuencia

Fte: Visión General de la Seguridad en los Protocolos de Comunicaciones 5G

5.16 ATAQUES MAN IN THE MIDDLE

"Otro tema que queda pendiente es protegerse contra ataques de MITM (*MAN IN THE MIDDLE*). Ya hemos mencionado el ataque AUTHENTICATION RELAY que no es más que una forma de MITM. El hecho de que el atacante se interponga en la red y trafique datos entre las redes nos pone ante un ataque de estas características. De momento no se propone ninguna solución y simplemente se aclara que es un problema que se debería resolver" [7].

CAPITULO 6: GEOLOCALIZACIÓN MEDIANTE EL PROTOCOLO SS7

Mientras se desarrollaba este estándar, solo los operadores de línea fija tenían acceso a la red SS7, por lo que su seguridad no estaba primero en la lista de prioridades. En la actualidad la señalización la red no se encuentra aislada, y esto permite que un intruso explote sus defectos e intercepte

llamadas y SMS, omita la facturación, robe dinero de cuentas móviles o afecte la operabilidad de la red móvil.

Aunque las nuevas redes 4G, con tecnología LTE (*Long Term Evolution*) utilizan otro sistema de señalización, *Diameter*, SS7 no se ha dejado de utilizar porque los operadores móviles deben garantizar la interacción entre redes de diferentes generaciones, 2G y 3G. Además, las investigaciones muestran que Diameter, que parece ser una mejora sobre SS7 en términos de seguridad con el uso de IPsec / TLS, con autenticación basada en certificados, también es propenso a las mismas amenazas. [12]

Las vulnerabilidades en las redes móviles basadas en SS7 permiten a un intruso con habilidades básicas realizar ataques peligrosos que pueden conducir a la pérdida financiera directa, la fuga de datos confidenciales, la interrupción de los servicios de comunicación o descubrir la ubicación de un suscriptor. Para estos distintos tipos de ataques el intruso no necesita equipamiento sofisticado, en general se hace uso de una computadora basada en Linux y un SDK disponible públicamente para generar paquetes SS7. Por lo general los ataques se basan en mensajes o comandos SS7 legítimos los cuales no pueden ser filtrados simplemente por la red ya que pueden tener un impacto negativo en la calidad del servicio de comunicaciones.

Los principios a través de los cuales son factibles los ataques de este tipo son en primer lugar los datos de movilidad de los suscriptores deben estar almacenados en la red para poder comunicarlos entre sí y con terminales fijas, y en segundo lugar la itinerancia dentro de la red y entre distintas redes.

Un atacante puede ser una persona o un grupo de personas lo suficientemente calificado para construir un nodo para emular el de un operador de telefonía móvil. Para acceder a una red SS7, los atacantes pueden adquirir la conexión de un proveedor existente en el mercado negro y obtener autorización para operar como operador de telefonía móvil en países con leyes de comunicaciones laxas. Además, cualquier hacker que trabaje como especialista técnico en un operador de telecomunicaciones, podría conectar su equipo ilegal a la red SS7 de la compañía. También puede

penetrar en la red de un proveedor a través de un dispositivo de borde comprometido (GGSN o una femtocelda).

El ataque mediante el cual se puede determinar la ubicación de un suscriptor está basado en una vulnerabilidad en el protocolo. El ataque se basa en una solicitud no autorizada de la ubicación del suscriptor cuyos datos entregados por la red se usan comúnmente para la tarificación en tiempo real de las llamadas entrantes del suscriptor. Los datos iniciales son el IMSI y la dirección actual de MSC / VLR [20]

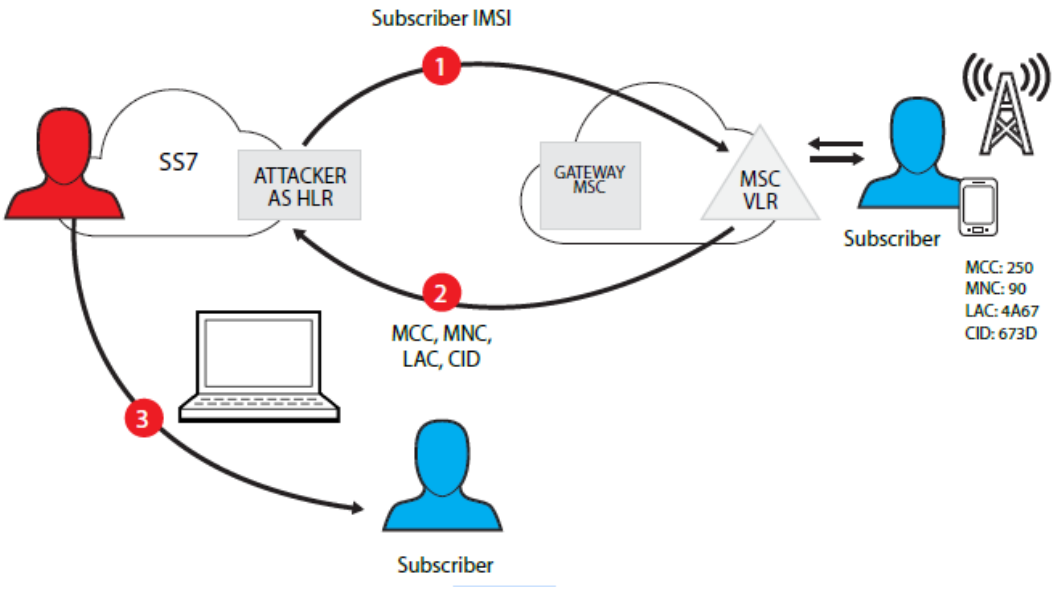

Ilustración 105. Ataque de localización de un suscriptor

Fte: SIGNALING SYSTEM 7 (SS7) SECURITY REPORT

Resultado: el intruso obtiene el CGI (Identidad Celular Global), que consiste en:

1. Código de país móvil (MCC)
2. Código de red móvil de MNC (MNC)
3. Código de área de ubicación (LAC)
4. Identidad celular (CID)

“Como se ha mencionado, el Sistema de Señalización No.7 (SS7) es un protocolo de *Backend* móvil utilizado para la interconectividad entre redes de operadores de telecomunicaciones, que permite servicios móviles y de roaming en todo el dominio del operador. El protocolo se utiliza principalmente para la comunicación entre los elementos de la red y las distintas redes. Ha cumplido su propósito con éxito durante cuatro décadas siendo una fuente sustancial de ingresos para los proveedores de servicios y MNOs (*MOBILE NETWORK OPERATORS*). A pesar de su antigüedad, SS7 y su versión IP llamada SIGTRAN continúa siendo los protocolos más utilizados para interconexiones de roaming hasta la fecha, a fin de proporcionar servicios de roaming que podrían tener interconexiones solo a través de SS7, independientemente de la generación de tecnología móvil (como GSM, UMTS y LTE)” [19].

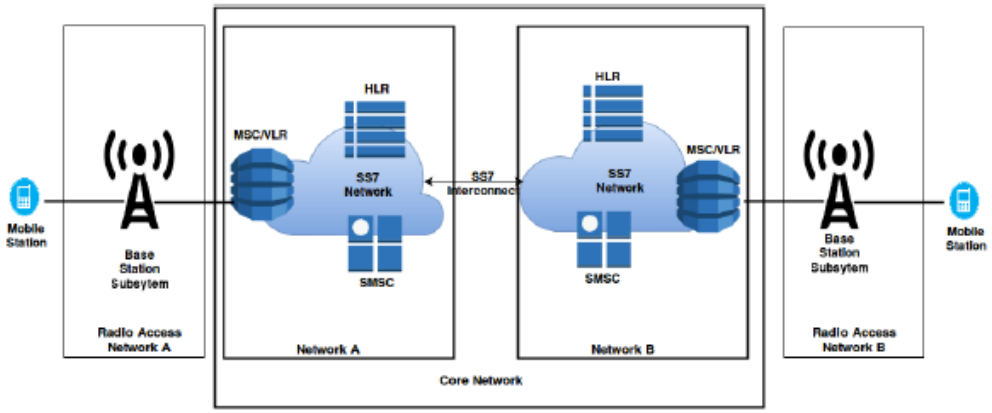

Ilustración 106. Dos redes conectadas vía SS7 pre-Release 8

Fte: User Location Tracking Attacks for LTE Networks Using the Interworking Functionality

El Protocolo de aplicación de mensajes (MAP) es una de las aplicaciones claves de la pila de protocolo SS7, que es el principal responsable para la comunicación entre los elementos del red core, la gestión de movilidad y los servicios complementarios. Los siguientes elementos o nodos de la red central interactúan entre sí utilizando el protocolo MAP, a saber:

(1) (HLR), que contiene las claves de suscriptor y el usuario información de perfil,

(2) (MSC), que gestiona la movilidad del usuario y

(3) (VLR), que se encarga de un usuario en roaming.

Debido a la evolución de las tecnologías de red y de los nuevos servicios, la especificación MAP ha crecido sustancialmente para soportar una amplia gama de servicios.

A diferencia de la generación anterior de redes de roaming en las que la HPMN (Red Móvil Pública del Hogar del Suscriptor) y la VPMN (Red Móvil Pública Visitante) están vinculadas con la interconexión SS7, las nuevas redes LTE reemplazan el SS7 con interconexión IP a través de la red de intercambio de Roaming IPX / GRX. Como se muestra en la figura, el tráfico proveniente de la interconexión IPX / GRX es enrutado a través del DEA (*Diameter Edge Agent*).

Como evolución de HLR, el HSS (*Home Subscriber Server*) contiene los perfiles del suscriptor y es uno de los nodos más importantes en una red LTE.

La MME (*Mobility Management Entity*) puede verse como la evolución del MSC, que se encarga de la gestión de la movilidad del usuario. [19]

La hPCRF (*Home Policy Charging and Rule Function*) es la entidad que habilita la facturación. Cuando el suscriptor está en una red visitante, la misma funcionalidad es manejada por la vPCRF (*Visited Policy Charged Rule Function*).

El SGSN (*Serving GPRS Support Node*) maneja datos de paquetes conmutados dentro de la red y habilita el roaming de datos.

Como se mencionó anteriormente, la actualización de la red de SS7 a DIAMETER fue un proceso gradual. La mayoría de los operadores actualizan su infraestructura de red gradualmente para evitar la interrupción del servicio y optimizar el retorno de la inversión de su infraestructura. Durante tales actualizaciones los equipos viejos a menudo se venden a los operadores en países en desarrollo, donde el gasto de capital es limitado y la rotación por usuario es baja. La figura muestra la simple conexión directa entre dos operadores, ambos funcionan con DIAMETER.

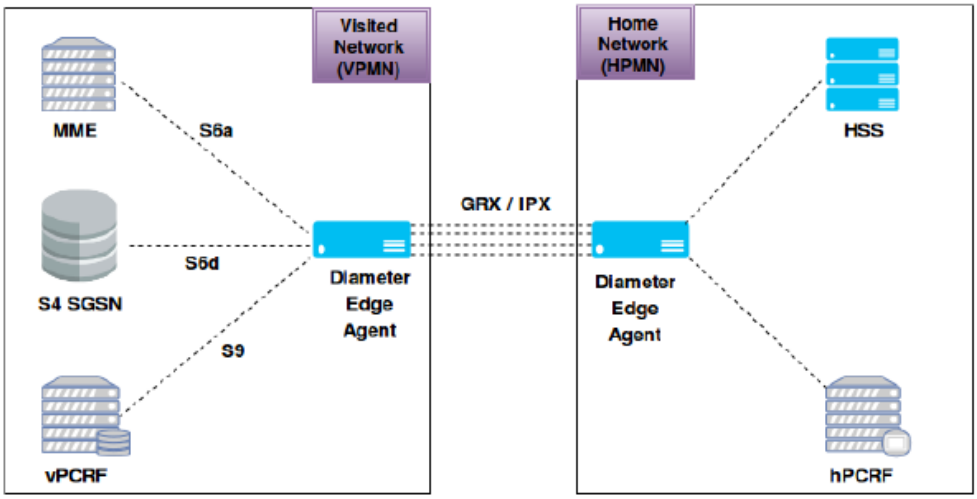

Ilustración 107. Roaming Diameter entre dos redes LTE

Fte: User Location Tracking Attacks for LTE Networks Using the Interworking Functionality

"La situación de la vida real es mucho más compleja. El número de competidores puede escalar a alrededor de miles, cuyos nodos son de diferentes versiones de software y hardware. La razón para una configuración tan heterogénea y compleja encontrada se debe a lo mencionado anteriormente en cuanto al proceso de actualización gradual de la infraestructura de red de soporte, o debido al limitado capital de los operadores" [19].

Esta falta de homogeneidad en las configuraciones de red proporciona algunos vectores de ataque interesantes desde la perspectiva de la seguridad.

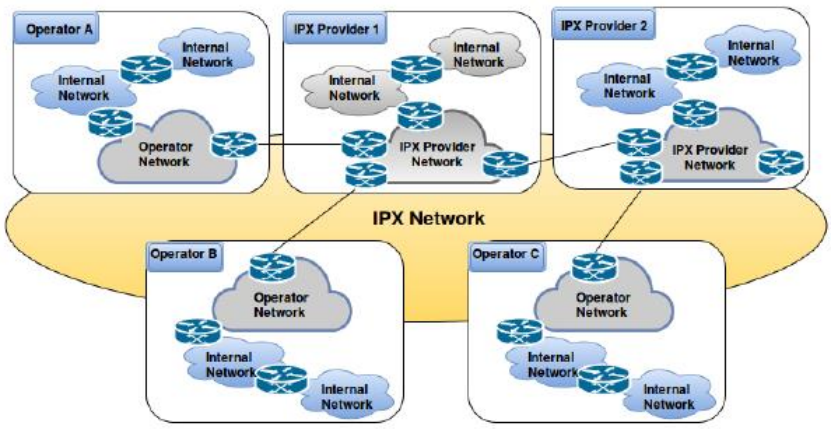

Ilustración 108. Rooming de Redes interconectadas

Fte: User Location Tracking Attacks for LTE Networks Using the Interworking Functionality

“La configuración no homogénea simplemente implica la posibilidad de existencia de nodos dentro de una red que son de diferentes versiones y, por lo tanto, admiten diferentes protocolos. También implica que las redes entre sí en la interfaz de roaming pueden usar SS7 o DIAMETER o la combinación de ambos, dependiendo del nodo y la red” [19].

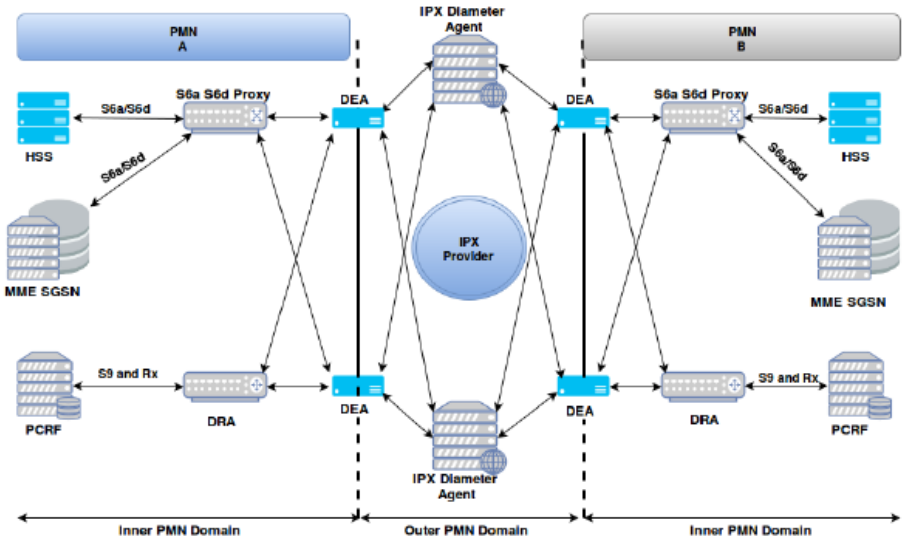

Ilustración 109. Roaming entre redes SS7-DIAMETER

Fte: User Location Tracking Attacks for LTE Networks Using the Interworking Functionality

“Por razones de interoperabilidad con sus competidores, los nodos mejorados y los nodos mismos a menudo tienen la capacidad de traducir entre los protocolos Diameter y MAP. Diameter es especificado para estar protegido con NDS / IP (*Network Domain Security*) e IPSec como protocolo de seguridad. Sin embargo, incluso los nodos DIAMETER tienen que soportar a los competidores que utilizan nodos SS7 heredados, donde la criptografía, la seguridad en términos de autenticación, así como la confidencialidad e integridad están ausentes” [19].

6.1 FUNCIÓN DE INTERCONEXIÓN (*IWF*)

“Por lo general, 3GPP estandariza las funcionalidades y especificaciones para la comunicación entre nodos que tienen la misma versión. Pero hay casos en los que funcionalidades específicas han sido estandarizadas para permitir la interoperabilidad entre diferentes versiones y

tecnologías. En este ámbito, la especificación técnica (TS) 29.305 y el Informe técnico no vinculante (TR) 29.805 describe cómo los AVP´s (*Atribute Value Pairs*) de DIAMETER y los mensajes SS7-MAP se pueden asignar a cada otro. Los AVP pueden considerarse como variables que a menudo cambian durante la comunicación móvil, como la identidad del usuario, fuente de mensajes, etc. Aunque esto se especifica como una característica de principalmente nodos de borde (por ejemplo, DEA) llamados IWF (*Interworking Function*), la función se implementa prácticamente en otros tipos de nodos, directamente, para permitir la interoperabilidad dentro de las redes de distintos operadores, donde encontramos nodos de diferentes versiones. En tal caso, donde la IWF se usa directamente en el nodo, a menudo se llama escenario de soporte de dominio múltiple. Debido a la actualización gradual dentro del dominio de un operador, esta es una configuración bastante común" [19].

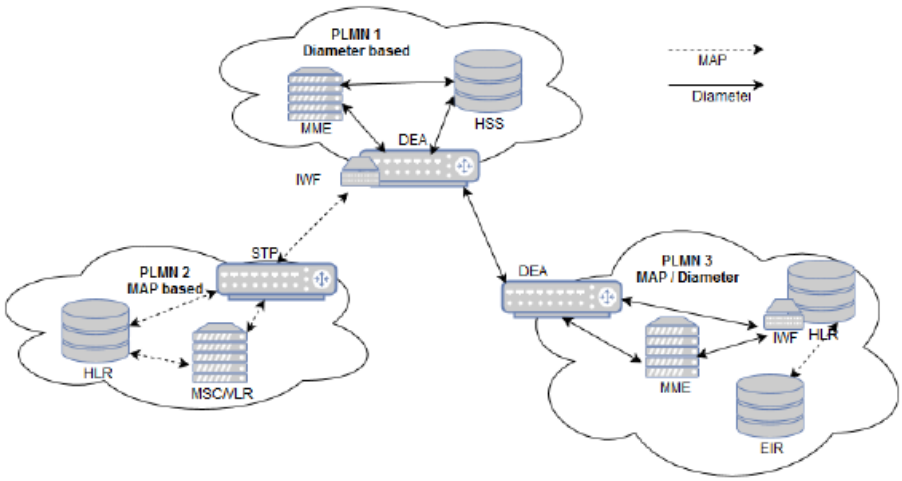

Ilustración 110. Tres redes con diferentes protocolos

Fte: User Location Tracking Attacks for LTE Networks Using the Interworking Functionality

"Ataques exitosos recientes en SS7 han demostrado que un atacante con acceso a la red de interconexión SS7 puede tomar el control de la información personal de los usuarios, ubicación de los suscriptores, datos de facturación y SMS, además de intervenciones telefónicas.

En el nivel conceptual, la idea es validar si las redes de DIAMETER son vulnerables a los ataques de localización SS7, utilizando la IWF para ataques de traducción. Para ello se asume que el atacante accedió a la red SS7" [19].

6.2 DIVULGACIÓN DE UBICACIÓN MEDIANTE MENSAJES DE CONFIGURACIÓN DE LLAMADAS:

"El atacante con acceso a la red SS7 pretende ser GMSC (Global MSC), competencia del operador de la víctima. El ataque también puede funcionar con un GT (*Global Title*) aleatorio. El GT identifica de forma exclusiva un nodo en la red SS7, similar a una dirección MAC en una red IP. El objetivo aquí es el HLR, el nodo que contiene datos cruciales del suscriptor.

1) El atacante se hace pasar por un GMSC y ejecuta la rutina de procedimiento de configuración de llamada desde el punto donde el GMSC se supone que recibe el IAM (*Initial Address Message*). Al principio, adjunta el MSISDN (número de teléfono) de la víctima en un mensaje MAP SRI (*Send Routing Information*) al HLR en la Home Network de la víctima, siempre que aprenda el GT del HLR (a menudo se encuentra usando la fuerza bruta al rango GT que tiene un operador).

2) El HLR compara el MSISDN con el IMSI, seguida de una consulta al VLR de la red visitante de la víctima, enviando un mensaje Request MAP PRN (Provide Roaming Number). El IMSI es sumamente importante ya que es la identidad interna del suscriptor en la red, requerida por la mayoría de los comandos MAP y DIAMETER.

3) Las respuestas legítimas de VLR a través del mensaje ACK MAP PRN contiene el IMSI de la víctima y el GT.

4) Esta información se devuelve a través del MAP *Routing Information* ACK del atacante, como un falso GMSC. El GT de VLR aprendido aquí se puede utilizar para detectar la ubicación aproximada de la víctima en contexto

Este ataque solo da una estimación aproximada de la ubicación de una víctima, pero sirve para identificar si está viajando. Dependiendo de la intención, podrían ser suficiente para el atacante" [19].

6.3 DIVULGACIÓN DE LOCALIZACIÓN MEDIANTE EL SERVICIO DE LOCALIZACIÓN DE EMERGENCIAS:

"Los operadores móviles están legalmente obligados a proporcionar una ubicación precisa de sus suscriptores durante situaciones de emergencia tales como accidentes (iniciado por los suscriptores, p.ej. número de emergencia 911) o seguimiento criminal (iniciado por los operadores en nombre de los funcionarios encargados de hacer cumplir la ley). En el caso de este último, el operador inicia un comando de red interno llamado MAP *Provide Subscriber Location* (PSL). Esta el comando también se puede explotar para el seguimiento de ubicación ilegítimo de un abonado.

El atacante necesita saber el IMSI de la víctima y el MSC/VLR GT. Puede obtener esos identificadores a través del Protocolo SMS o al ataque basado en mensaje de configuración de llamada, como el mencionado anteriormente.

1) Ahora el atacante consulta el MSC / VLR en la red visitante para conocer la información precisa de ubicación de la víctima enviando MAP *Provide Subscriber Location* (PSL). Para hacerlo, el atacante debería omitir la autenticación del cliente LCS (*Location Cliente Service*) - en circunstancias regulares, las autoridades policiales son la autenticación de clientes LCS legítimos- en el GMLC (Gateway Mobile Location Center), enviando directamente el mencionado mensaje PSL a MSC/VLR. En esta situación provoca que el MSC / VLR no pueda comprobar la autenticación real.

2) El MSC / VLR detecta la ubicación de la estación base móvil de la utilizando alguno de los métodos posibles (p. ej. Solicitud RRLP)

3) El MSC/VLR luego responde al atacante con el mensaje MAP Provide Subscriber Location Response, el cual contiene la ID de celda de la ubicación del abonado.

La ID de la estación base de radio se puede asignar a una ubicación real en términos de coordenadas geográficas de la víctima, utilizando servicios web como por ejemplo *Open Cellid*. En algunos casos, el mensaje LCS también podría revelar las coordenadas GPS de las radiobases más cercanas de la víctima junto con la identificación de la celda de servicio. Sin embargo,

no se garantiza que sea tan preciso como la información GPS proporcionada por las mismas móviles (por ejemplo, usando cualquier aplicación de GPS en el móvil).

Cabe señalar que el ataque antes mencionado solo funciona cuando un operador admite la función de localización de emergencia.

En los ataques señalados suponemos que un atacante tiene acceso a la red roaming de interconexión, pero ¿cómo se puede tener este acceso? Hay varias formas, a saber:

• La mayoría de los operadores tienen un departamento que alquila el acceso a terceros y varios servicios a proveedores externos.

• La red de roaming es global y cubre numerosos países o regiones donde tener acceso legal a los datos del suscriptor está permitido debido a una regulación menos estricta de la privacidad.

• Hay nodos comprometidos o mal configurados que son visibles en

Internet (por ejemplo, a través de una base de datos conectada a Internet como como Shodan.io). Estos nodos podrían actuar como los puntos potenciales de entrada de los atacantes.

• El ataque interno (por ejemplo, mediante ingeniería social o soborno) puede conducir a un acceso no autorizado por parte de delincuentes.

El primer paso para un atacante es obtener el IMSI de la víctima, ya que es uno de los principales identificadores de usuario, necesario para la mayoría de la comunicación dentro de la red de interconexión. Hay varias formas de obtener el IMSI. El ejemplo muestra un vector de ataque que usa la IWF y describe el procedimiento para obtener IMSI basado en el conocimiento de MSISDN en una red basada en el protocolo Diameter.

El atacante comienza su ataque consultando la red objetivo de la víctima, utilizando el comando MAP SRI SM. Sin embargo, el éxito de este ataque está garantizado solo en ausencia del *Home Routing* y si la interconexión Diameter del operador objetivo es establecida sobre la interface S6c con soporte adicional de IWF. El IWF de la red objetivo se traduce el MAP SRI SM al Diameter Send Routing Info For SM Request (SRR), como se muestra en la figura” [19].

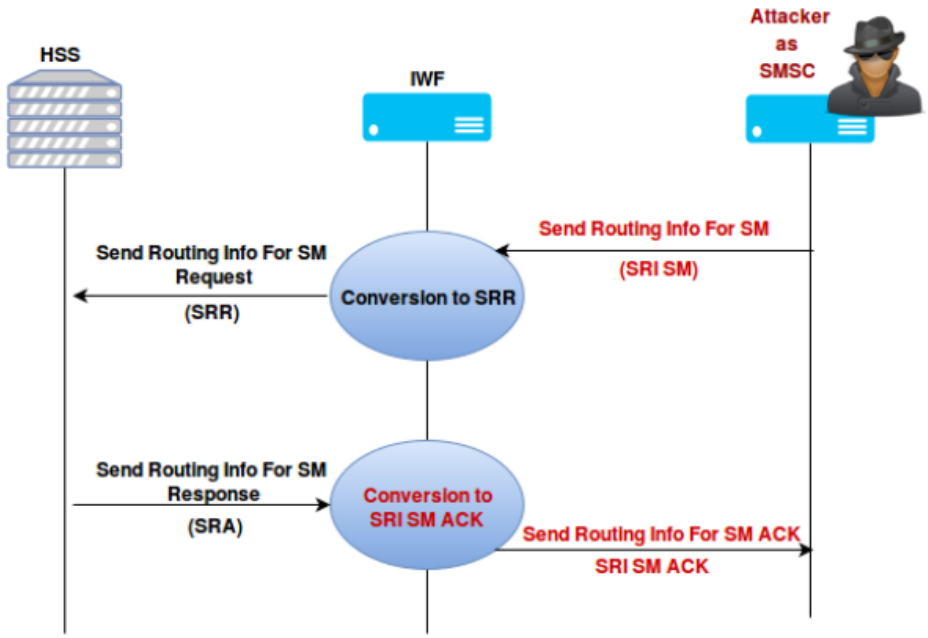

Ilustración 111. Ataque de divulgación de IMSI usando SRI SM

Fte: User Location Tracking Attacks for LTE Networks Using the Interworking Functionality

"El atacante se hace pasar por un SMSC de otro operador o un IWF (para los escenario IWF) en la red consultada y solicita solo el soporte *Legacy* SS7 MAP enviando el *Request* MAP SRI a través de la red de interconexión.

1) El atacante envía una solicitud MAP SRI SM que contiene el MSISDN a la red de la víctima objetivo. Sobre la capa de protocolo subyacente que facilita el enrutamiento (enrutamiento generalmente es facilitado la capa SCCP de la pila de protocolos SS7), el atacante puede usar su propio CgPA (Global Title Calling Party Address), ya que no se realiza ninguna comparación entre capas SCCP y el resto de las capas MAP. Además de los parámetros antes mencionados, como el MSISDN de la víctima y CgPA, el atacante requiere SCA (Service Centre Address) y configurar una bandera de prioridad SM-RP-PRI para crear el comando de solicitud MAP SRI SM. El atacante puede engañar al SCA para ocultar su identidad, mientras que la bandera SMR lo habilita para recibir información relevante desde el HSS de la red objetivo, incluso cuando la red no le está dando servicio al suscriptor.

2) El IWF de la red objetivo recibe la solicitud SRI de MAP SM solicita y lo convierte a Diameter SRR por mapeo de los parámetros MAP recibidos para el correspondiente Diameter AVP´s. Por ejemplo, los AVP´s Diameter, como los SC-Adress, MSISDN, y los SM-RP-PRI son ingresados basados en los correspondientes parámetros MAP. El *Origin Host/Realm* y el *Destination Host/Realm* AVP´s son mapeados desde el SCCP CgPA y el CdPA, respectivamente.

3) Una vez que el mapeo se descripto en el paso anterior está hecho, la IWF dirige el SRR hacia HSS de la red objetivo vía DEA/DRA. El HSS responde con el comendo Diameter SRA (*Send Routing Info For SM Answer*), el cual contiene el IMSI y el *User Name* AVP, y el nodo de servicio de la víctima. El comando SRA se enruta de nuevo a la IWF a través de DEA/DRA.

4) Las IWF de la red objetivo recibe el Diámetro SRA y lo convierte en respuesta MAP SRI SM mediante mapeo los AVP recibidos para los correspondientes parámetros MAP. La IWF dirige la respuesta MAP SRI SM hacia la interconexión roaming. Si el ataque es exitoso, el comando SRA contiene todos los AVP´s que espera un atacante. En tales casos, la IWF rellena la respuesta MAP SRI SM asignando el AVP recibidos a los parámetros MAP correspondientes como siga (solo se enumeran los parámetros más importantes):

- IMSI: Se rellena con el valor contenido en el SRA *User-Name* AVP.
- *Network -Node Number*: Se rellena con valor contenido en cualquiera de los SRA MME *Number* para MT SMS, MSC *Number*, SGSN *Number* o el IP-SM-GW-*Number* AVP´s. Este campo contiene el nodos que actualmente están sirviendo a la víctima y, por lo tanto, puede ser utilizado por el atacante para lanzar ataques adicionales o para estimar la ubicación aproximada ya sea basado en el número MSC o MME.
- Host/Realm origen y destino Los AVP son mapeados al SCCP CgPA de la dirección HSS de la red objetivo y a la dirección de la red SCCP DcPA del atacante, (es decir, el GT real permite el atacante para recibir la respuesta) respectivamente.

5) Además, el IWF de la red objetivo enviará el mensaje MAP *Inform Service Center* al atacante para confirmar la entrega completa de información solicitada. Sin embargo, desde el punto de vista del atacante, este mensaje es rudimentario, ya que él ya habría recibió la información deseada, como ser el MSI de la víctima, dirección de nodo de servicio y posiblemente la dirección del HSS

El ataque de recuperación IMSI mencionado anteriormente es crucial, ya que el IMSI se utiliza a priori para iniciar el ataque de localización. Esto se debe principalmente al uso extensivo de IMSI en las comunicaciones basadas en Diameter, en lugar de solo el MSISDN o el MSRN (*Mobile Station Roaming Number*) de redes basadas en SS7. Existen varias otras formas de obtener el IMSI, como el uso de una estación base falsa, un punto de acceso WLAN y protocolo EAP-AKA. Sin embargo, se omitirá una descripción más detallada sobre esos métodos, ya que están más allá del alcance de este trabajo" [19].

CAPITULO 7: HERRAMIENTAS DISPONIBLES

Las vulnerabilidades en el SS7 no son nuevas. Una de las primeras presentaciones públicas sobre las vulnerabilidades de SS7 se realizó en 2008 en la Conferencia *"Chaos Computer Club"*, en Alemania. El investigador alemán Tobías Engel mostró cómo podría determinarse la ubicación de un teléfono móvil [13]. Sin embargo, los riesgos asociados con las vulnerabilidades de SS7 se conocen desde hace mucho tiempo. Mucho antes de la demostración de Engel, los ingenieros de telecomunicaciones habían advertido que varios ataques con SS7 eran posibles [14, 15 y 16]. Algunos gobiernos también sabían de las posibles amenazas. Por ejemplo, el libro "Cómo hacer trampa en la seguridad de VoIP" de Thomas Porter y Michael Gough (2007) contiene el siguiente extracto de un informe oficial de los Estados Unidos sobre posibles amenazas GSM:

"El riesgo de ataque ha sido reconocido en los Estados Unidos al más alto nivel, y la oficina del presidente indica preocupación por SS7. Se entiende

que T1, un grupo estadounidense, está considerando seriamente el tema" [17].

Por razones obvias, los proveedores no querían que el público supiera sobre estos riesgos asociados. Sin embargo, el tema recibió publicidad en 2013 cuando el ex especialista de la CIA Edward Snowden reveló el hecho de que la Agencia de Seguridad Nacional (NSA) había estado explotando las vulnerabilidades de SS7 para espiar a las personas [18].

Poco después, una gran cantidad de empresas privadas comenzaron a ofrecer una gama de servicios disponibles comercialmente (como los descritos) al público en general. Por ejemplo, *Verint Systems*, con sede en EE.UU., Proporciona un servicio llamado *SkyLock* para determinar la ubicación de un suscriptor móvil en cualquier parte del mundo. [12]

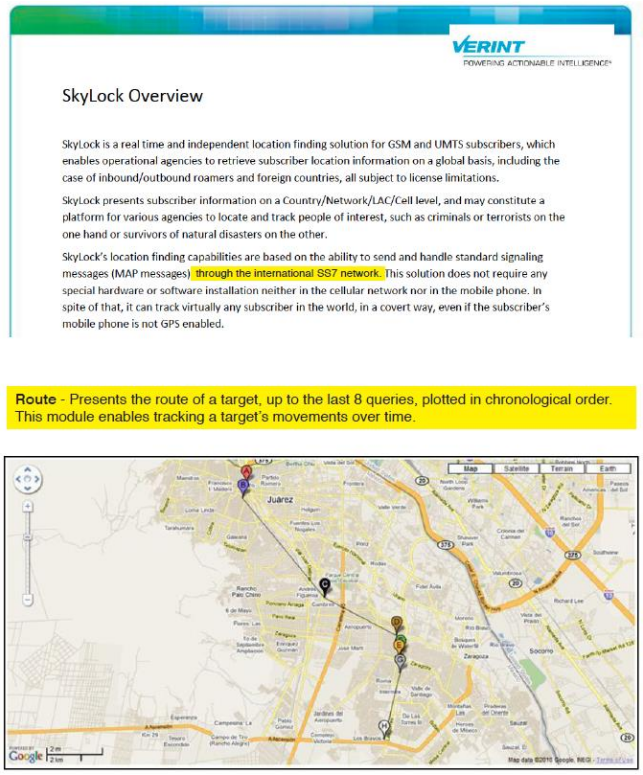

Ilustración 112. Plataforma SkyLock de la firma Verint Systems

Fte: SIGNALING SYSTEM 7 (SS7) SECURITY REPORT

Hay varios servicios disponibles en la Web que permiten determinar la ubicación de una radiobase mediante estos identificadores. En ciudades y

áreas urbanas, la precisión de la ubicación del suscriptor puede ser de unos pocos cientos de metros.

A nivel comercial, empresas israelíes ofrecen soluciones web, a decir por ellas, sólo a organismos oficiales, como por ejemplo GEO y GEOMATRIX, las cuales realizan geolocalizaciones de suscriptores en todo el mundo, excepto en USA e Israel. En ellas solo es requerido el número de abonado para devolver como parte de la consulta no solo la localización del suscriptor sino otros datos relacionados con el dispositivo móvil como ser el IMEI, incluso el modelo y marca del dispositivo que son datos que se podrían obtener por separado al disponer ya del IMEI. También entregan datos relacionados a la red que presta servicio, como ser el CEELID y el LAC. Otro dato importante entregado por estar soluciones es el IMSI que como ya hemos visto está relacionado con la tarjeta SIM.

Ilustración 113. Plataforma GEOMATRIX

Fte: Propia

CONCLUSIONES

El Sistema de Señalización No.7 (SS7) es un protocolo utilizado para la interconectividad entre redes de operadores de telecomunicaciones, que permite servicios móviles y de roaming a nivel local y global. A pesar de su antigüedad, SS7 y su versión IP llamada SIGTRAN continúan siendo los protocolos más utilizados, independientemente de la generación de tecnología móvil (como GSM, UMTS y LTE).

Las vulnerabilidades en las redes móviles basadas en SS7 permiten realizar ataques que pueden conducir a la ubicación de un suscriptor, entre otras cosas. Para estos distintos tipos de ataques el intruso no necesita equipamiento sofisticado. Por lo general los ataques se basan en mensajes o comandos SS7 legítimos los cuales no pueden ser filtrados simplemente por la red ya que pueden tener un impacto negativo en la calidad del servicio de comunicaciones. La facilidad de estos ataques se basa fundamentalmente en que los datos de movilidad de los suscriptores deben estar almacenados en la red para poder comunicarlos entre sí y con terminales fijas, y en segundo lugar la itinerancia dentro de la red y entre distintas redes.

Como hemos visto, los terminales móviles deben actualizar su posición ante la red para que pueda esta rutear la llamada hacia la radiobase que le da servicio. Este dato se actualiza permanentemente y se almacena para poder ser consultada en ocasión de rutear una comunicación o de llevar adelante la función de roaming cuando el suscriptor se encuentra en una red diferente a la red de la empresa prestataria del servicio de la cual fuera cliente, ya sea a nivel nacional o internacional.

El capítulo 6 desarrolla la mecánica pare explotar la vulnerabilidad (6.2 y 6.3). Como se expresa, el objetivo, en general, es comprometer los siguientes elementos o nodos de la red central que interactúan entre sí, utilizando el protocolo MAP, a saber: El HLR, que contiene las claves de suscriptor e información de perfil del usuario; el MSC, que gestiona la movilidad del usuario y el VLR, que se encarga de un usuario en roaming. El VLR contiene información de la última actualización de la posición del terminal móvil en base a la ubicación (coordenadas geográficas) de la antena que le

dio servicio. Pese a estar en una misma ubicación, los dispositivos móviles pueden registrarse en diferentes antenas en el transcurso del tiempo, dependiendo esto de cuál de las antenas de su entorno le brinda mejor calidad de servicio. Se puede entonces, por medio de triangulación, conocer con mayor o menor precisión, la ubicación física del terminal.

En señalización, como se ha comentado, 2G y 3G utilizaban el protocolo SS7, en 4G DIAMETER y en 5G se ha pasado a SBA, utilizando TLS en el medio con servicios HTTP, por encima, intercambiando JSON. Si bien la evolución de las redes de telefonía móvil hacia la tecnología 5G aporta incontables beneficios para la sociedad, todavía queda pendiente resolver cuestiones de seguridad del protocolo de señalización que las interconecte, como ser, la Seguridad de mensajes unicast sin protección (RRC y NAS), la Protección de información del Sistema (SI), la Detección de estaciones base falsa cercanas, la Protección frente a envenenamiento de SON, la Protección frente a Authentication Relay, la Resistencia frente a inhibición de radiofrecuencia y la Protection frente a ataques Man in the Middle.

Con respecto a las comunicaciones con el usuario, hasta 4G las mismas estaban protegidas en confidencialidad y a partir de 5G también se pueden proteger en integridad. Esta protección, según la norma, se deja a criterio del operador activarla o no. En este sentido, es la red home quien puede definir una política para que cada PDU Session, es decir, que cada sesión de datos entre el terminal y la red que da servicio sea protegida en integridad o en confidencialidad. La red home entonces, es la encargada de establecer estas políticas. Sin embargo, la norma también dice que la función local de gestión de sesiones de la red que está dando servicio (service network) puede desentender o desactivar esa política según los siguientes criterios: Cuando hay un mandato obligatorio, cuando existan acuerdos de roaming entre la service network y la home network que establecen que no se aplicará la política de seguridad y cuando la norma permita que la service network a criterio propio pueda decidir en base a políticas locales desactivar esta protección. Por lo tanto, quien va a decidir si estas comunicaciones están protegidas o no en la interfaz de radio va a ser la red que da servicio. Estos aspectos desalentadores, sumados a la convivencia con redes de

generaciones anteriores cuyas vulnerabilidades ya se han mencionado, seguirán dejando abierta la puerta que posibilita la geolocalización de dispositivos móviles.

Se puede vislumbrar a nivel mundial que aquellos países con menos recursos económicos tendrán más dificultades para desplegar redes de telecomunicaciones con las últimas tecnologías de telefonía móvil (5G) lo cual implica convivir durante muchos años con protocolos de señalización antiguos (SS7 y SIGTRAN), con todas sus debilidades en cuanto a seguridad.

Finalmente, en base al estudio de las diferentes generaciones de las redes de telefonía celular se puede concluir, como queda demostrado en el presente trabajo, que es posible localizar dispositivos móviles a través de diferentes vulnerabilidades en los protocolos de señalización, las cuales son transversales a todas las tecnologías y operadores.

BIBLIOGRAFÍA

1] M. F. d. l. Cruz., «Introducción a los Sistemas de Telefonía Celular.,» HASA, 2008.

2] J. M. H. Moya., «Comunicaciones Móviles. Sistemas GSM, UMTS y LTE.,» Alfaomega, 2012.

3] R. S. E. y. S. E. Antonio, «Primera Generación Móvil (1G),» Antonio Salazar, 4 Agosto 2015. [En línea]. Available: https://prezi.com/ppvcls817rt7/primera-generacion-movil-1g/. [Último acceso: 10 Noviembre 2019].

4] GitBook, «Sistemas de Telefonía y Comunicaciones Móviles. Noviembre 2019,» [En línea]. Available:

https://mastermoviles.gitbook.io/tecnologias2/sistemas-de-telefonia-y-comunicaciones-moviles. [Último acceso: 5 Noviembre 2019].

5] L. G. Roberto, «“El Sistema GSM”,» Proyecto Fin de Carrera. (riunet.upv.es), [En línea]. Available: https://riunet.upv.es/bitstream/handle/10251/19023/Memoria_Lizon_Gonzalez_Roberto.pdf. [Último acceso: 1 Noviembre 2019].

6] wikipedia.org, «IMEI,» 14 Abril 2012. [En línea]. Available: https://es.wikipedia.org/wiki/IMEI. [Último acceso: 25 Octubre 2019].

7] J. P. y. D. Pérez, «Visión General de la Seguridad en los Protocolos de Comunicaciones 5G.,» Centro Nacional Criptográico. España, 28 Mayo 2019. [En línea]. Available: https://vanesa.ccn-cert.cni.es/userportal/#/player/vod/Ua8def480a0804faeb9a95113bc553255. [Último acceso: 15 Octurbre 2019].

8] wikipedia.org, «DIAMETER,» 18 Enero 2015. [En línea]. Available: https://es.wikipedia.org/wiki/Diameter_(protocolo). [Último acceso: 20 Noviembre 2019].

9] l. S. Gonzalez, «Seguridad en Redes de Comunicaciones. Protocolo EAP,» Universidad de Cantabria, [En línea]. Available: https://ocw.unican.es/pluginfile.php/307/course/section/250/tema_03.pdf. [Último acceso: 20 Octubre 2019].

10] I. A. C. C. y. R. D. G. Rodríguez, «Análisis e implementación de un dispositivo virtual en PHP,» Escuela Superior Politécnica del Litoral. Guayaquil. Ecuador, 2015. [En línea]. Available: https://www.dspace.espol.edu.ec/retrieve/90375/D-84712.pdf. [Último acceso: 9 Octubre 2019].

11] B. E. G. R. L. M. W. M. M., «Simulación de la señalización de un usuario móvil y un usuario fijo usando SS7,» Escuela Superior Politécnica del Litoral. Guayaquil. Ecuador, 2014. [En línea]. Available: https://www.academia.edu/6323187/Simulación_de_la_señalización_

de_un_usuario_móvil_y_un_usuario_fijo_usando_SS7. [Último acceso: 18 Octubre 2019].

12] P. Technologies, «SS7 VULNERABILITIES AND ATTACK EXPOSURE REPORT 2018,» 2018. [En línea]. Available: https://www.gsma.com/membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf. [Último acceso: 23 Septiembre 2019].

13] T. Engel, «Locating Mobile Phones Using Sgnalling System #7,» 2008. [En línea]. Available: https://www.scribd.com/document/359370710/31c3-ss7-locate-track-manipulate-pdf. [Último acceso: 12 Septiembre 2019].

14] L. Ostman, «A Study of Location-Based Services,» 2001. [En línea]. Available: http://epubl.ltu.se/1402-1617/2001/254/LTU-EX-01254-SE.pdf. [Último acceso: 6 Septiembre 2019].

15] G. Association, «SMS SS7 Fraud 3.1,» 2003. [En línea]. Available: https://www.gsma.com/newsroom/wp-content/uploads/2012/12/IR7031.pdf. [Último acceso: 26 Agosto 2019].

16] J. D. M. F. I. G. J. K. Katerina Dufková, «Can Active Tracking of Inroamer Location Optimise a Live GSM Network?,» CTU-Ericsson-Vodafone R&D,, 2007. [En línea]. Available: http://www.rdc.cz/en/publications/publications/dufkova07ss7tracker.pdf. [Último acceso: 14 Agosto 2019].

17] M. G. Thomas Porter, «How to Cheat at VoIP Security,» 2007. [En línea]. Available: http://www.amazon.com/How-Cheat-at-VoIP-Security/dp/1597491691. [Último acceso: 12 Agosto 2019].

18] W. Post, «New documents show how the NSA infers relationships based on mobile location data.,» 2013. [En línea]. Available: http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-

relationships-based-on-mobile-location-data/. [Último acceso: 10 Agosto 2019].

19] S. P. R. I. O. Silke Holtmanns, «Networks, User Location Tracking Attacks for LTE,» ISBN 978-3-901882-84-5, IFIP Networking 2016 © 2016 IFIP 322, 2016. [En línea]. Available: http://dl.ifip.org/db/conf/networking/networking2016/1570236202.pdf. [Último acceso: 24 Agosto 2019].

20] P. Technology, «SS7-Security Report,» Positive Technology, 28 Diciembre 2014. [En línea]. Available: https://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf. [Último acceso: 10 Diciembre 2019].