MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

TRABAJO FIN DE MASTER

Estudio de seguridad del núcleo de una red 5G en herramientas *open source* e implementación de ataques basados en HTTP/2

Autor: Javier Valero Martí

Director: Pedro Cabrera Cámara

Co-Director: Miguel Gallego Vara

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

ESTUDIO DE SEGURIDAD DEL NÚCLEO DE UNA RED 5G EN HERRAMIENTAS *OPEN SOURCE* E IMPLEMENTACIÓN DE ATAQUES BASADOS EN HTTP/2

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2023/24 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

Fdo.: Javier Valero Martí Fecha: 12 / 07 / 2024

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Pedro Cabrera Cámara Fecha: 12 / 07 / 2024

Firmado por CABRERA CAMARA PEDRO - ***7854, el día 12/07/2024 con un certificado emitido por**

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. JAVIER VALERO MARTÍ

DECLARA ser el titular de los derechos de propiedad intelectual de la obra: ESTUDIO DE SEGURIDAD DEL NÚCLEO DE UNA RED 5G EN HERRAMIENTAS *OPEN SOURCE* E IMPLEMENTACIÓN DE ATAQUES BASADOS EN HTTP/2, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.

d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 12 de JULIO de 2024

ACEPTA 

Fdo: JAVIER VALERO MARTÍ

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

MASTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIONES

TRABAJO FIN DE MASTER

Estudio de seguridad del núcleo de una red 5G en herramientas *open source* e implementación de ataques basados en HTTP/2

Autor: Javier Valero Martí

Director: Pedro Cabrera Cámara

Co-Director: Miguel Gallego Vara

Madrid

Agradecimientos

Gracias a Pedro y Miguel, de Ethon Shield, por su paciencia, su mentoría y su cercanía. Sin ellos, este trabajo no habría sido posible.

ESTUDIO DE SEGURIDAD DEL NÚCLEO DE UNA RED 5G EN HERRAMIENTAS *OPEN SOURCE* E IMPLEMENTACIÓN DE ATAQUES BASADOS EN HTTP/2

Autor: Valero Martí, Javier
Director: Cabrera Cámara, Pedro
Co-Director: Gallego Vara, Miguel
Entidad Colaboradora: Ethon Shield SL.

RESUMEN DEL PROYECTO

El desarrollo del proyecto se ha centrado en el estudio de la seguridad en el núcleo de una red 5G, con especial atención a las complicaciones que puedan derivar del uso de HTTP/2 como protocolo de comunicación en este entorno. Para ello, se han utilizado distintas herramientas de código abierto para construir redes de laboratorio, en las cuales se ha probado que la carencia de los adecuados mecanismos de protección en el núcleo permite alcanzar severos compromisos de seguridad con un impacto crítico en la red.

Palabras clave: 5G, red móvil, núcleo de red, código abierto, HTTP/2, seguridad

1. Introducción

Una red móvil es una infraestructura cuyo principio funcional es simple: permitir la comunicación entre dos usuarios, de forma remota, a través de los medios dispuestos por un operador encargado de administrar el servicio. La principal diferencia que este modelo presenta con respecto a la telefonía tradicional es que, en una red móvil, la conexión entre los equipos de usuario y los equipos de red del operador se realiza de forma inalámbrica. La primera definición de red móvil, comúnmente referenciada como primera generación (1G), apareció en la década de los 80 y únicamente tenía capacidad para soportar la transmisión de voz. Sin embargo, a lo largo de los años, la sucesión de generaciones de redes móviles ha ido ligada a la adopción de nuevas tecnologías que han derivado en una serie de cambios de paradigma muy importantes en el sector de las comunicaciones. Estos cambios, además de los beneficios lógicos que implican en términos de prestaciones de la red y mejora de la experiencia de los usuarios, también deben ser considerados como potenciales vectores de riesgos de seguridad que deben ser analizados, especialmente en la tecnología 5G, por ser la más novedosa en ser incluida en los entornos comerciales de las operadoras.

2. Definición del proyecto

La quinta generación de redes móviles o 5G representa uno de los cambios más disruptivos en la historia de este sector, tanto por sus aplicaciones prácticas como por los principios tecnológicos que constituyen su base. En cuanto a sus aplicaciones prácticas, además de su comercialización para el gran público, también se plantea como mecanismo de comunicación entre máquinas autónomas, con miras a sectores como la logística o el desarrollo de ecosistemas *IoT.* Por otra parte, en lo relativo a la descripción técnica de esta infraestructura, cabe destacar la adopción de ciertos mecanismos y protocolos de comunicación tradicionalmente utilizados en comunicación web, con el propósito de hacer este sector más accesible a perfiles profesionales vinculados con el ámbito IT. Entre estas medidas, destacan:

- La elección de una arquitectura basada en servicios como el paradigma de comunicación en el núcleo de la red.

- La adopción de HTTP como protocolo de comunicación entre funciones en el núcleo de la red.

El desarrollo del proyecto se ha centrado, por tanto, en analizar las implicaciones que tiene para la seguridad de una infraestructura 5G el hecho de utilizar el protocolo HTTP, en su versión 2, para comunicar las diferentes funciones de red, o NFs, mediante interfaces SBI.

3. Metodología

La metodología seguida consta de una fase inicial de documentación, en la cual se ha investigado sobre el estado del arte de las implementaciones *open source* de redes móviles, con especial interés en las relacionadas con la quinta generación. Seguidamente, se ha realizado un análisis de seguridad general de una infraestructura 5G, identificando y categorizando posibles amenazas y vectores de ataque, para posteriormente plantear un modelo centrado en aquellas que afectan directamente al núcleo de la red. Tras esto, se han utilizado herramientas de código abierto para desplegar una red 5G de laboratorio y realizar sobre ella una serie de pruebas de seguridad, centradas en el uso del protocolo HTTP/2.

Para construir el entorno experimental, se han empleado una serie de herramientas y tecnologías gratuitas de código abierto. Por un lado, para la parte hardware, se ha utilizado un equipo modelo Slimbook ELEMENTAL como entorno de ejecución para las herramientas *open source* y un dispositivo USRP B200 mini para ejecutar el elemento transceptor. Por otro lado, la parte software del entorno está compuesta por el gNB desarrollado por srsRAN y las implementaciones del núcleo de red de OpenAirInterface y Open5gs, con objeto de establecer una comparación entre ambas.

A fin de automatizar la ejecución de las pruebas lo máximo posible, se ha optado por el desarrollo de una herramienta en lenguaje de programación *bash*. Esta herramienta ha sido configurada para hacer uso del protocolo HTTP/2 e interactuar con las funciones de red, partiendo de la base de que el equipo en el que se ejecuta la herramienta tiene un interfaz de comunicación en la misma red que el núcleo de la arquitectura 5G.

4. Resultados

Escenario	***Probabilidad de ocurrencia***
Insider	**Baja**
Compromiso de credenciales de usuario operador	**Baja**
Compromiso de credenciales de usuario administrador	**Baja**
Compromiso de capa de virtualización / orquestación	**Baja**
Interconexión insegura entre redes	**Media**

Tabla 1. Probabilidad de ocurrencia de los escenarios de ataque sobre el núcleo de una red 5G

El análisis de seguridad permite concluir que existen diversos escenarios a partir de los cuales un atacante podría ganar acceso al núcleo de una infraestructura 5G, reflejados en la Tabla 1. A partir de estos escenarios, se ha elaborado una taxonomía de potenciales amenazas sobre el núcleo de la red, algunas de ellas basadas en la utilización de mensajes HTTP/2 para interactuar directamente con las funciones de red.

Para comprobar la viabilidad de materializar estas amenazas, se ha elaborado una herramienta que permite automatizar una serie de ataques y se ha puesto a prueba sobre dos implementaciones de código abierto del núcleo de una red 5G.

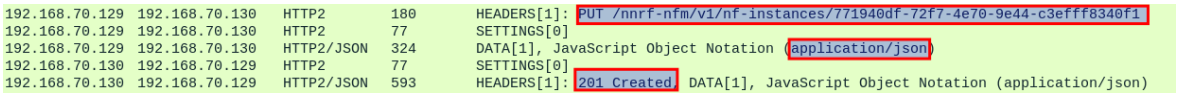


Ilustración 1. Petición realizada para el registro de una NF falsa en OAI

Ilustración 2. Resultado de registrar una NF falsa en OAI

Los resultados de las pruebas reflejan que, si no se implementan las adecuadas medidas de seguridad, un atacante con acceso al núcleo de la red podría llegar a comprometer la misma en términos de confidencialidad, integridad y disponibilidad. Las ilustraciones 1 y 2, muestran el resultado de ejecutar la herramienta para registrar una NF falsa en la red, ilustrando, en este caso, un ataque sobre la integridad de la misma.

5. Conclusiones

Los resultados obtenidos se pueden resumir en la siguientes conclusiones generales:

- El análisis de seguridad revela que hay escenarios donde un atacante podría acceder al núcleo de la red 5G de una operadora. Además, algunos estudios sugieren que las operadoras podrían no estar implementando rigurosamente los mecanismos de seguridad necesarios, permitiendo potenciales accesos no autorizados mediante HTTP/2.
- Utilizar HTTP/2 en la red 5G presenta riesgos, ya que es un protocolo comúnmente usado y comprendido en el ámbito IT, facilitando que un atacante pueda interpretar el tráfico y ejecutar ataques.
- Crear entornos de red 5G en laboratorios con herramientas de código abierto ofrece beneficios como reducción de costos, personalización, apoyo de comunidades activas y la capacidad de realizar pruebas de seguridad documentadas y reproducibles.

STUDY OF 5G NETWORK CORE SECURITY IN OPEN SOURCE TOOLS AND IMPLEMENTATION OF HTTP/2-BASED ATTACKS

Author: Valero Martí, Javier
Director: Cabrera Cámara, Pedro
Co-Director: Gallego Vara, Miguel
Collaborating Entity: Ethon Shield SL.

ABSTRACT

The development of the project has been focused on studying the security of the core of a 5G network, with special attention to the complications that may arise from using HTTP/2 as a communication protocol in this environment. To this end, various open-source tools have been used to build laboratory networks, in which it has been demonstrated that the lack of adequate protection mechanisms in the core can lead to severe security compromises with a critical impact on the network.

Keywords: 5G, mobile network, core, open source, HTTP/2, security

1. Introduction

Mobile networks are infrastructures whose functional principle is simple: to allow communication between two users remotely, through the means provided by an operator responsible for managing the service. The main difference between this model and traditional telephony is that, in a mobile network, the connection between user equipment and the operator's network equipment is wireless. The first definition of a mobile network, commonly referred to as the first generation (1G), appeared in the 1980s and could only support voice transmission. However, over the years, the succession of mobile network generations has been linked to the adoption of new technologies that have resulted in significant paradigm shifts in the communications sector. These changes, besides the logical benefits they entail in terms of network performance and improvement of the user experience, should also be considered as potential vectors of security risks that need to be analyzed, especially in 5G technology, as it is the newest technology to be included in the commercial environments of operators.

2. Project description

The fifth generation of mobile networks, or 5G, represents one of the most disruptive changes in the history of this sector, both due to its practical applications and the technological principles that constitute its foundation. Regarding its practical applications, besides its commercialization for the general public, it is also envisioned as a communication mechanism between autonomous machines, targeting sectors such as logistics or the development of *IoT* ecosystems. On the other hand, concerning the technical description of this infrastructure, it is worth mentioning the adoption of certain mechanisms and communication protocols traditionally used in web communication, with the aim of making this sector more accessible to professionals linked to the IT field. Among these measures, the following stand out:

- The choice of a service- based architecture paradigm in the core of the network.
- The adoption of HTTP as the communication protocol between functions in the network core.

The project's development has therefore focused on analyzing the security implications of using the HTTP protocol, in its second version, to communicate the different network functions, or NFs, through SBI interfaces.

3. Methodology

The methodology used consists of an initial documentation phase, in which the state of the art of open source mobile network implementations has been investigated, with special interest in those related to the fifth generation. Subsequently, a general security analysis of a 5G infrastructure has been carried out, identifying and categorizing possible threats and attack vectors, to then propose a model focused on those that directly affect the network core. Following this study, open-source tools have been used to deploy a laboratory 5G network and conduct a series of security tests on it, based on the use of the HTTP/2 protocol.

To build the experimental environment, a series of free, open-source tools and technologies have been used. On the hardware side, a Slimbook ELEMENTAL model was used as the execution environment for the open-source tools and a USRP B200 mini device to run the transceiver element. On the software side, the environment consists of the gNB developed by srsRAN and the network core implementations by OpenAirInterface and Open5gs, aiming to establish a comparison between the two.

To automate the execution of the tests as much as possible, a tool was developed using the bash programming language. This tool has been configured to use the HTTP/2 protocol and interact with the network functions, based on the assumption that the device on which the tool is executed has a communication interface on the same network as the core of the 5G architecture.

4. Results

Scenario	***Probability of occurrence***
Insider	**Low**
Obtained credentials for operations user	**Low**
Obtained credentials for administrator user	**Low**
Obtained access to virtualization / orchestration layer	**Low**
Insecure interconnection between networks	**Medium**

Table 1. Probability of occurrence for attack scenarios affecting the core of a 5G network

The security analysis concludes that there are various scenarios through which an attacker could gain access to the core of a 5G infrastructure, as reflected in Table 1. Based on these scenarios, a taxonomy of potential threats to the network core has been developed, some of which are based on the use of HTTP/2 messages to interact directly with the network functions.

To verify the feasibility of these threats having an impact on security, a tool has been developed to automate a series of attacks and has been tested on two open-source implementations of the core of a 5G network.

```
192.168.70.129  192.168.70.130   HTTP2        180       HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/771940df-72f7-4e70-9e44-c3efff8340f1
192.168.70.129  192.168.70.130   HTTP2        77        SETTINGS[0]
192.168.70.129  192.168.70.130   HTTP2/JSON   324       DATA[1], JavaScript Object Notation (application/json)
192.168.70.130  192.168.70.129   HTTP2        77        SETTINGS[0]
192.168.70.130  192.168.70.129   HTTP2/JSON   593       HEADERS[1]: 201 Created, DATA[1], JavaScript Object Notation (application/json)
```

Ilustration 1. Request used to register a fake NF in OAI core

```
Enter the requested paramenters to register a new NF

NF Type: UDM
NF IP Address: 192.168.70.155
NF ID: 771940df-72f7-4e70-9e44-c3efff8340f1
NF fqdn: oai-udm2
NF instance name: FAKE-UDM

NF has been registered with parameters:
{"capacity":100,"fqdn":"oai-udm2","heartBeatTimer":10,"ipv4Addresses":["192.168.70.155"],"json_data":null,"nfInstanceId":"771940df-72f7-4e70-9e44-c3efff8340f1","n
nfStatus":"REGISTERED","nfType":"UDM","priority":1,"udmInfo":{"externalGroupIdentifiersRanges":[],"gpsiRanges":[],"groupId":"","internalGroupIdentifiersRanges":[]

Keep alive started with PID: 208153
```

Ilustration 2. Result of registering a fake NF in OAI core

The test results indicate that, without proper security measures, an attacker with access to the network core could compromise it in terms of confidentiality, integrity, and availability. Illustrations 1 and 2 show the result of running the tool to register a fake NF in the network, illustrating, in this case, an attack on its integrity.

5. Conclusions

Obtained results can be summarized in the following general conclusions:

- The security analysis reveals that there are scenarios where an attacker could access the core of a 5G network operated by a telecom provider. Additionally, some studies suggest that operators may not be rigorously implementing the necessary security mechanisms, allowing potential unauthorized access via HTTP/2.
- Using HTTP/2 in the 5G network implies certain risks, as it is a commonly used and well-known protocol in the IT field, making it easier for an attacker to interpret the traffic and execute attacks.
- Creating 5G network environments in laboratories with open-source tools offers benefits such as cost reduction, customization, support from active communities, and the ability to conduct documented and reproducible security tests.

Índice de la memoria

Índice de figuras

Índice de tablas

Capítulo 1. INTRODUCCIÓN

1.1 COLABORACIÓN

Este proyecto se ha realizado en colaboración con *Ethon Shield,* empresa dedicada al ámbito de la ciberseguridad, con especial interés en el sector de las telecomunicaciones y redes móviles. *Ethon Shield* cuenta con una amplia experiencia en este sector, adquirida a raíz de la realización de auditorías de seguridad y la puesta en práctica de labores de investigación, divulgadas en documentos científicos y conferencias. En este sentido, la experiencia de *Ethon Shield* es clave para asegurar que el desarrollo del trabajo se realiza desde una perspectiva técnica adecuada y ajustada a la realidad del estado actual de las redes 5G.

1.2 METODOLOGÍA

La metodología seguida se ha basado en un plan de trabajo por fases, partiendo de un periodo de formación y familiarización con el ecosistema de redes móviles y las tecnologías de código abierto, y finalizando con un estudio de seguridad y ejecución de distintas pruebas basadas en el uso del protocolo HTTP/2 en el núcleo de la red. Las referidas fases son:

- Introducción y familiarización con el empleo de soluciones tecnológicas de código abierto para el despliegue de redes 2G, 3G y 4G.
- Introducción y familiarización con el empleo de soluciones tecnológicas de código abierto para el despliegue de redes 5G: *OpenAirInterface*, *srsRan* y *Open5gs.*
- Implementación de las soluciones tecnológicas anteriores en un orquestador para automatizar despliegues de la red 5G.
- Realización de un estudio de seguridad sobre la tecnología 5G, centrado en el núcleo y en la seguridad de las funciones de red.
- Estudio y aplicación de técnicas de ataque sobre las funciones de red basadas en el empleo del protocolo HTTP/2.

1.3 ESTRUCTURA DEL TRABAJO

El **Capítulo 2.** ofrece al lector una visión resumida del marco teórico sobre el que se apoya el proyecto. Comienza con un breve comentario a las generaciones de redes móviles precedentes a 5G, para continuar con una descripción de las características fundamentales de esta tecnología. Con este propósito, se tratan aspectos como la arquitectura de la red, los componentes del núcleo y consideraciones generales de seguridad.

En el **Capítulo 3.** se realiza un breve resumen del estado del arte de la cuestión, mencionando los documentos y publicaciones principales que se han utilizado como referencia para este proyecto y exponiendo los resultados de mayor relevancia.

El **Capítulo 4.** se utiliza para presentar las herramientas y soluciones tecnológicas empleadas durante el desarrollo de la parte práctica del trabajo, mencionando a sus fabricantes o creadores e indicando su utilidad concreta en el proyecto.

El **Capítulo 5.** se ha dedicado a la exposición de un análisis de seguridad de la tecnología 5G, en el que se hacen referencia a las principales amenazas y riesgos relacionados, haciendo hincapié en aquellos que afectan de alguna manera al núcleo de la red.

El **Capítulo 6.** expone el resultado de las pruebas de seguridad realizadas sobre el núcleo de una red 5G, utilizando para ello la versión del *core* desarrollada por dos proveedores distintos de herramientas *open source.* En este capítulo se detallan los resultados de las pruebas, explicando los compromisos logrados en términos de confidencialidad, integridad y disponibilidad de la información, y estableciendo una comparación cualitativa entre las tecnologías probadas.

Finalmente, el **Capítulo 7.** expone las conclusiones obtenidas tras la realización de las pruebas y presenta vías de trabajo futuras que podrían contribuir al desarrollo de la línea de investigación seguida durante este proyecto.

Capítulo 2. MARCO TEÓRICO

2.1 EVOLUCIÓN DE LAS REDES MÓVILES

Una red móvil es una infraestructura cuyo principio funcional es simple: permitir la comunicación entre dos usuarios, de forma remota, a través de los medios dispuestos por un operador encargado de administrar el servicio [1]. La principal diferencia que este paradigma presenta con respecto al modelo de red de telefonía tradicional es que, en una red móvil, la conexión entre los equipos de usuario y los equipos de red del operador se realiza de forma inalámbrica, haciendo uso de ondas electromagnéticas de baja potencia.

La primera definición de red móvil, comúnmente referenciada como *primera generación* (1G), apareció en la década de los 80. El diseño de esta red tenía la capacidad de permitir la transmisión de voz humana de forma analógica, aunque presentaba muchas limitaciones, principalmente en términos de calidad de servicio y cobertura , las cuales fueron subsanadas en generaciones posteriores. Además, al tratarse de la primera especificación de red móvil que se implementó en el mercado de las comunicaciones, todavía no consideraba la implantación de mecanismos de seguridad.

La s*egunda generación* (2G), también conocida como GSM, hizo su aparición a principios de la década de los 90. La principal diferencia que esta tecnología presenta con respecto a su predecesora es la sustitución del modelo de comunicación analógica por el digital, buscando mejorar la calidad de las llamadas y la capacidad de la red. Aunque inicialmente su propósito seguía siendo el de soportar el servicio de llamadas de voz entre usuarios, también se introduce la funcionalidad de enviar mensajes de texto cortos (SMS). Otra de las aportaciones más relevantes de la tecnología GSM al mundo de las telecomunicaciones fue el desarrollo e incorporación del servicio GPRS, diseñado para la transmisión de datos digitales. Este servicio supone un nuevo cambio de paradigma, pues conlleva la introducción del modelo de conmutación de paquetes, en contraposición con el modelo tradicional de circuitos. Este nuevo modelo, basado en la idea de fragmentar los datos a enviar y hacer uso

de la red únicamente cuando haya datos que transmitir en lugar de utilizar un canal dedicado para la comunicación, permite hacer un uso más eficaz del ancho de banda, lo cual derivó en una mejora de la calidad de los servicios prestados. Gracias a esto fue posible ofrecer, entre otros, los primeros servicios de comunicación por Internet en redes móviles, aunque estos presentaban unas prestaciones todavía muy limitadas en términos de velocidad de transmisión. De hecho, este nuevo cambio de paradigma resultó tan importante que parte de la literatura relacionada lo considera como una generación independiente, convenientemente bautizada como 2.5 G. Sin embargo, formalmente es más adecuado considerarlo como una especificación que extiende la funcionalidad original de GSM [2].

En lo relativo a las consideraciones de seguridad, GSM especifica mecanismos para autenticar la identidad de los usuarios y permitir el cifrado de las comunicaciones, buscando garantizar la confidencialidad de la información. No obstante, también presenta debilidades tales como:

- El usuario no es capaz de autenticar la identidad de la red, lo que hace posible ataques basados en una red falsa que suplante una legítima.
- La identidad del usuario (IMSI) puede ser conocida por un atacante, puesto que se envía sin cifrar en ciertas ocasiones.
- Ciertas debilidades criptológicas asociadas a los mecanismos de cifrado empleados.

La *tercera generación* de redes móviles (3G), también denominada UMTS, busca corregir estos potenciales vectores de ataque, al mismo tiempo que mantiene una arquitectura muy similar a la especificada para GSM. Aunque sigue manteniendo la segregación entre los dominios de circuitos y paquetes, el diseño de esta tecnología puso énfasis en la optimización de la transmisión de datos, con el objetivo de incluir las redes móviles como parte del ecosistema de comunicaciones que se estaba configurando alrededor de Internet.

En cuanto a la seguridad de UMTS, es cierto que se introducen mecanismos para permitir la autenticación mutua entre el usuario y la red, y se refuerzan los algoritmos que llevan a cabo las operaciones de cifrado de las comunicaciones. Sin embargo, a pesar de que también se toman medidas para la protección de la identidad del usuario (habilitando un identificador

de identidad temporal, T-IMSI), esto no mitiga por completo los ataques de captura de IMSI, que siguen siendo posibles mediante la escucha del interfaz radio [3].

La siguiente etapa en la evolución de las redes móviles es la protagonizada por la tecnología LTE, nombre formal que recibe la *cuarta generación* (4G). Durante el proceso de redacción de requisitos para esta tecnología, Internet acabó por consolidarse como pilar fundamental en el mundo de las telecomunicaciones. Este hecho derivó en que la gran mayoría de los sistemas de comunicaciones existentes optasen por adoptar un modelo de protocolos basado en IP, con la intención de favorecer la interoperabilidad con este ecosistema cuyo número de usuarios activos aumentaba a una velocidad vertiginosa. Consecuentemente, no es de extrañar que la especificación de esta tecnología acabase por descartar el dominio de circuitos y adoptar un modelo basado completamente en la transmisión de paquetes. La unificación de los dominios de voz y datos hizo necesario el desarrollo de capacidades como la transmisión de voz sobre IP, al tiempo que fue ligado a una mejora considerable de las velocidades de transmisión y la capacidad de la red.

Realmente, la primera especificación de LTE no cumplía con todos los requisitos que el cuerpo de estandarización ITU-R había definido para que un sistema pudiese considerarse como parte de 4G. Sin embargo, se trata de un precursor esencial de la tecnología que hoy día constituye las base de las redes 4G comerciales, denominada LTE-Advanced. Esta especificación consiguió las prestaciones de velocidad de transmisión, eficiencia espectral y capacidad de la red más elevadas de todas las redes móviles desplegadas hasta la fecha. Como consecuencia, esta arquitectura de red posibilitó el consumo por parte de los usuarios de servicios como los vídeos en *streaming* de alta definición, cuya demanda se encontraba en auge.

Desde el punto de vista de seguridad, la especificación de LTE plantea un marco robusto, asentado sobre las bases de autenticación mutua entre usuario y red, la protección de la confidencialidad de los usuarios y el uso de algoritmos criptográficos seguros y eficientes. Además, se hace hincapié sobre la protección de zonas que hasta entonces no se habían considerado críticas, como el *backhaul*. No obstante, diversos análisis han señalado que esta

tecnología no se encuentra exenta de amenazas, pues se recalcan posibilidades como: ataques de renegociación que puedan inducir a un usuario a establecer conexión con una red GSM o UMTS (*downgrade attacks)*, localización de usuarios por medio de su IMEI/IMSI o ataques tipo MiTM mediante interceptación del canal radio [4].

El último gran hito en la historia de las redes móviles fue el desarrollo e implantación de la tecnología 5G, cuyas características serán explicadas en profundidad en la **Sección 2.2.** La adopción de la *quinta generación* de redes móviles supone importantes retos para las operadoras, al tratarse de un cambio de paradigma de magnitud considerable teniendo en cuenta las importantes diferencias existentes entre esta arquitectura de red y sus predecesoras.

Finalmente, cabe destacar que la idea una *sexta generación* se encuentra actualmente en desarrollo, aunque su implantación todavía genere muchas incógnitas que deberán ser resueltas en el futuro. No obstante, eventos como la puesta en órbita por parte de China de un satélite de pruebas para 6G [5] llevan a pensar que dicho futuro podría no extenderse demasiado.

2.2 QUINTA GENERACIÓN DE REDES MÓVILES – 5G

2.2.1 INTRODUCCIÓN A LA TECNOLOGÍA 5G

La definición de la *quinta generación,* también denominada 5G, supone uno de los cambios más disruptivos en la historia de las comunicaciones móviles. La primera especificación de esta nueva tecnología fue publicada en 2017 por el cuerpo de estandarización 3GPP, en un documento bautizado como *Release-15,* el cual contiene el primer conjunto de estándares definidos para una red 5G.

En cuanto a objetivos de rendimiento, esta generación pretende alcanzar las prestaciones más elevadas ofrecidas hasta el momento, en términos de velocidad de transmisión de datos, baja latencia y disponibilidad de la red. Con estas capacidades, los operadores son capaces de ofrecer a los usuarios una experiencia de consumo más gratificante, pudiendo acceder a

todos los servicios de Internet con una calidad óptima. No obstante, el enfoque puramente comercial no es el único que se plantea en el horizonte de esta tecnología. La organización ITU-R resume en tres puntos los principales escenarios de uso donde se considera que la implementación de tecnología 5G podrá resultar determinante [6]:

- ***Enhanced Mobile Broadband (eMBB):*** Se trata del caso de uso más enfocado a la comercialización de servicios al gran público. Mediante la ampliación del ancho de banda puesto a disposición de los usuarios se pretende dar servicio a áreas urbanas densamente pobladas, alcanzando velocidades de 1 *Gbps* en interiores y 300 *Mbps* en exteriores. Estas velocidades de descarga de datos son base suficiente para que los usuarios puedan acceder a vídeos en *streaming* de altísima definición (UHD), hacer uso de servicios en línea sin interrupciones o acceder con máxima velocidad a datos y aplicaciones en la nube.

  Consecuentemente, este caso de uso se erige como respuesta a las demandas actuales de los usuarios de redes móviles, cuyo número crece de manera considerable y cuyas necesidades se encuentran cada vez más ligadas al hecho de disponer de un acceso rápido y de calidad a Internet.

- ***Massive Machine Type Communications (mMTC):*** La arquitectura 5G se plantea como posibilidad para dar soporte a casos de uso que implican comunicación entre máquinas. En este sentido, destacan dos escenarios principales:

  - *Machine-to-Machine (M2M):* La comunicación entre máquinas sin intervención humana es un escenario esencial para funcionalidades que requieren un alto nivel de eficiencia y automatización. Por ejemplo, en el sector de logística se plantea como solución para el seguimiento de objetos mediante etiquetas RFID [7]
  - *Internet of Things (IoT):* En este caso, se busca interconectar un elevado número de dispositivos inteligentes, de manera que puedan compartir

información y tomar decisiones de forma autónoma, aplicables a diferentes escenarios productivos.

En ambos casos, un elevado número de dispositivos conectados simultáneamente y baja latencia en las comunicaciones son requisitos indispensables para el correcto funcionamiento y, a los cuales, una adecuada implementación de una arquitectura 5G podría dar soporte.

- ***Ultra-Reliable and Low-Latency Communications (URLLC):*** Es el caso de uso con un enfoque más concreto, pues está pensado para escenarios donde la velocidad de transmisión no es tan crítica como la baja latencia (por debajo de $1ms$) . El escenario de mayor trascendencia para el cual se ha planteado esta funcionalidad serían las operaciones de cirugía asistidas a distancia. [8]

Los escenarios planteados suponen un enfoque tremendamente novedoso de las aplicaciones de las redes móviles. Es por ello que las especificaciones de la tecnología 5G deben seguir una línea innovadora para poder adaptarse a estas nuevas realidades. El diseño de esta generación de redes móviles incluye una serie de cambios disruptivos con respecto de las generaciones anteriores, basados en un nuevo diseño de la etapa radio y el núcleo de la red, así como la incorporación nuevas tendencias tecnológicas. Entre las características más representativas de esta nueva arquitectura se encontrarían:

En la etapa radio:

- **Uso de ondas milimétricas:** La posibilidad de hacer uso de frecuencias en la banda de $24GHz$ a $100GHz$ sería uno de los habilitadores esenciales para conseguir una elevada tasa de transmisión de datos. Sin embargo, la parte negativa se encuentra en el mayor grado de atenuación que sufrirían estas ondas, reduciendo el alcance de la comunicación.
- ***Beamforming*:** La aplicación de esta técnica permite crear haces de señales muy directivos enfocados hacia los dispositivos de usuario, lo cual hace posible que estos

reciban señales con un relación señal-ruido más elevada [9]. Idealmente, esto se traduciría en una conexión más rápida y estable para los usuarios.

- **MIMO:** Esta tecnología posibilita el uso de múltiples antenas en transmisión y recepción, lo cual se traduce en un incremento de la capacidad de la red y las velocidades de transmisión alcanzables.

En el núcleo de la red:

- **Virtualización de funciones de red (NFV):** La arquitectura NFV representa un modelo en el cual funcionalidades concretas de la red se abstraen de los elementos *hardware* sobre los que se ejecutan. Según esto, los nodos de red pasan a ser entidades *software* que se ejecutan sobre un entorno virtual, dotando al despliegue de mayor flexibilidad y posibilidad de escalado.
- **Redes definidas por *software* (SDN):** El paradigma SDN pretende establecer una separación entre el plano de control y los dispositivos destinados al enrutamiento de los datos. De esta manera, se consigue centralizar el control de la red en un elemento *software,* consiguiendo despliegues más flexibles, con mayor capacidad de adaptación a cambios y con una gestión más eficiente del tráfico en la red.
- ***Network Slicing*:** La idea principal detrás de este término es separar, de manera lógica, distintos flujos de tráfico que se establecen sobre la misma infraestructura física. Las aplicaciones de esta función son múltiples: desde diferenciar entre la calidad de servicio ofrecida para diferentes grupos de usuarios por parte de una operadora, hasta configurar una topología de red diferente para diferentes servicios, buscando optimizar el funcionamiento de los mismos.

2.2.2 VISIÓN GENERAL DE LA ARQUITECTURA

En el alto nivel, la arquitectura de una red 5G se puede dividir en 3 componentes principales [10] de manera análoga a sus predecesores, todos ellos representados en la Ilustración 1 :

- **UE:** Hace referencia a cualquier dispositivo terminal que establece conexión con la red móvil. Se trata del elemento de la arquitectura que menos cambios ha

experimentado con respecto a generaciones anteriores, aunque tradicionalmente hacía referencia a objetos como *smartphones* o tabletas, mientras que ahora puede referirse también a otro tipo de dispositivos (sensores IoT, maquinaria industrial, vehículos …)

- **NG-RAN:** Se trata de la etapa radio, responsable de establecer una comunicación entre los dispositivos de usuario y el núcleo de la red. Su diseño con respecto a generaciones anteriores sí ha experimentado importantes variaciones, algunas anteriormente mencionadas, con el objetivo de incrementar las prestaciones generales de la red. El elemento de red encargado de comunicarse con cada UE se denomina gNB y su funcionalidad es análoga a la del eNB en 4G-LTE.
- **NG-MC:** Este término comprende todas las funciones que constituyen el núcleo de una red 5G, las cuales posibilitan el desarrollo de múltiples servicios: gestión de la movilidad de usuarios, enrutamiento de datos de usuario hacia Internet, diferenciación de calidad de servicio, facturación, funciones de seguridad…

  El diseño del núcleo de la red supone un enfoque tremendamente innovador y disruptivo con respecto a todas las generaciones de redes móviles precedentes, por lo que merece ser analizado en profundidad en la Sección 2.2.3

Además de estos tres componentes, que la mayor parte de la literatura considera como los principales, la última descripción aportada por la legislación española hace referencia a dos componentes adicionales que es merecido comentar. El Real Decreto 443/2024 [11] diferencia también los siguientes elementos:

- **Transporte *backhaul*:** El término engloba la conexión entre la red *backhaul* y el núcleo de red. El nodo de red principal en esta parte de la arquitectura se denomina *SecGW* y sería el encargado de asegurar esta interconexión, ofreciendo funciones como cifrado de tráfico y ocultación de la topología de red.
- **Interconexión *roaming:*** El término engloba la conexión entre el núcleo de red 5G y otra red diferente. Se trata de una función esencial para los operadores de red, pues hace posible ofrecer a los usuarios un servicio con capacidad de movilidad internacional. El nodo de red principal en esta parte de la arquitectura se denomina

SEPP y sería el encargado de asegurar que la interconexión se realiza de forma segura.

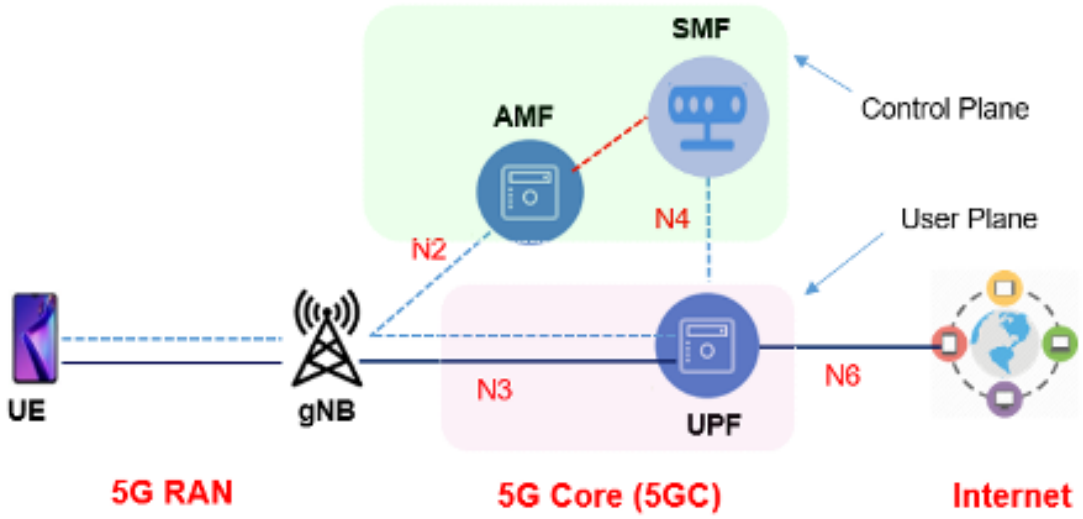


Ilustración 1. Componentes principales de la arquitectura 5G [12]

2.2.3 NÚCLEO DE UNA RED 5G

El núcleo de red es la parte central de una arquitectura 5G, pues es la que soporta todas las funciones que un operador de red tiene a su disposición para ofrecer servicios a sus usuarios. También es la parte que presenta diferencias más significativas con respecto a las arquitecturas que anteriormente constituían el mercado, pues incluye paradigmas de trabajo y tecnologías que nunca antes habían sido empleadas en el contexto de una red móvil, como podrían ser la virtualización, la contenerización de funciones o el despliegue de microservicios.

Una característica clave desde el punto de vista de diseño es que el núcleo de red 5G está pensado para ser independiente de la tecnología de acceso que se use para conectar con él. En este sentido, la estrategia se basa en establecer un interfaz de conexión capaz de comunicar con cualquier tecnología de acceso relevante, incluyendo incluso aquellas no definidas por la 3GPP. El criterio seguido para tomar esta decisión es que el núcleo de red

sea lo menos sensible posible a cambios que en el futuro se puedan producir en las tecnologías de acceso, ofreciendo un interfaz estándar para garantizar la conectividad.

Otra de las características clave, y una de las más disruptivas, es la sustitución del concepto de "nodo" por el concepto de "elemento o función de red" (denominado NF, por sus siglas en inglés). Tradicionalmente, un nodo de red era un elemento que combinaba *hardware* y *software*, el cual realizaba una serie de tareas en la red y se comunicaba para ello con el resto de nodos que la constituían. No obstante, la arquitectura 5G define lo que denomina como *funciones de red*, las cuales son elementos *software* que pueden abstraerse del *hardware* en el que se ejecutan y que ofrecen una serie de servicios muy concretos que pueden ser consumidos por otras funciones de red.

2.2.3.1 Funciones de red

Un despliegue del núcleo de una red 5G puede realizarse de diferentes formas o "sabores". Una característica que permite diferenciar estas posibilidades son las funciones de red que las constituyen. Aunque hay múltiples funciones definidas por la 3GPP, aquellas que forman parte de cualquier despliegue 5G [13] serían:

- **AMF –** Es la función donde se concentra la mayor parte de la "inteligencia" de la red, pues se encarga de gestionar la mayoría de los flujos de señalización entre la red y los usuarios. Es, por tanto, el punto principal de control para tareas como el registro de los usuarios, la gestión de su movilidad y el establecimiento de sesiones de comunicación. Generalmente, se compara su funcionalidad con la del nodo MME en una red de *cuarta generación*. Sin embargo, existen dos diferencias significativas que cade destacar: la AMF no se encarga de la gestión de sesiones activas ni de realizar la autenticación de usuarios, sino que delega estas funcionalidades en otros elementos.
- **SMF –** Gestiona todo lo relativo a las sesiones de comunicación de los usuarios. Esto es, la lógica detrás de su establecimiento, modificación y liberación, la cual requiere de funcionalidades tan críticas como la asignación de direcciones IP a los dispositivos de usuario para permitir la navegación por Internet. Como punto

adicional, este elemento también desempeña un papel importante en la función de tarificación de las operadoras.

- **UPF –** Su funcionalidad se encuentra íntimamente ligada al plano de datos de usuario, sirviendo como punto de enlace entre el núcleo de la red 5G y otras redes IP. Además del reenvío de paquetes de datos, puede desempeñar otras funciones adicionales, como la inspección de paquetes (a fin de aplicar sobre ellos ciertas políticas en función de su contenido) o el establecimiento de Calidad de Servicio (QoS) para priorizar unos flujos de tráfico sobre otros.
- **UDM –** Las funciones principales de este elemento comprenden las generación de datos de autenticación para los usuarios, control de accesos basados en autorizaciones y gestión de identidades de los usuarios. En cierto modo, actúa como intermediario en la comunicación entre el resto de funciones con el UDR.
- **UDR –** Es la base de datos en la que se almacenan datos clave relativos a las suscripciones de los usuarios y las políticas de tarificación que tienen asociadas.
- **AUSF –** Es la función de red que tiene como cometido central la autenticación de los usuarios que tratan de registrarse y hacer uso de la red 5G, procesando las credenciales generadas por el UDM.

Otras funciones de red muy comunes en los despliegues y cuya funcionalidad merece la pena comentar, serían:

- **NRF –** Es una función esencial dentro del nuevo paradigma de un núcleo basado en servicios, pues se encarga de descubrir los servicios disponibles en la red y comunicarlos a aquellas funciones de red que lo requieran. Permite, por tanto, la comunicación entre diferentes elementos de red.
- **PCF –** Gestiona las políticas que se deben aplicar a otras funciones de red. Esta funcionalidad se encuentra ligada a otras como las gestión de sesiones, implantación de QoS y tarificación.
- **SEPP –** Se trata de la función de red que sirve como punto de interconexión entre redes en escenarios de *roaming.* Su cometido principal es de seguridad, permitiendo el filtrado de tráfico y la ocultación de la topología de la red.

- **NEF –** Permite la exposición segura de las capacidades de la red a funciones de red internas y externas al operador.
- **NSSF –** Es la función encargada de posibilitar el *Network Slicing*, pues se encarga de seleccionar los fragmentos o *slices* de red y las instancias de AMF que deben servir a un determinado usuario, de acuerdo con las políticas establecidas.
- **UDSF –** Función de carácter opcional que ofrece a otras funciones de red la capacidad de almacenar datos de forma dinámica, actuando como un repositorio externo a la propia función.

2.2.3.2 Perspectiva dual del núcleo

Las funciones de red anteriormente explicadas representan los elementos cuya integración e interacción constituye el concepto denominado como núcleo de una red 5G. Sin embargo, no existe una única forma de representar cómo estos elementos se comunican entre ellos. La especificación técnica de la arquitectura de un sistema 5G, publicada por el organismo 3GPP, hace referencia a una perspectiva dual del núcleo, exponiendo dos formas diferentes de representar el mismo desde un punto de vista esquemático.

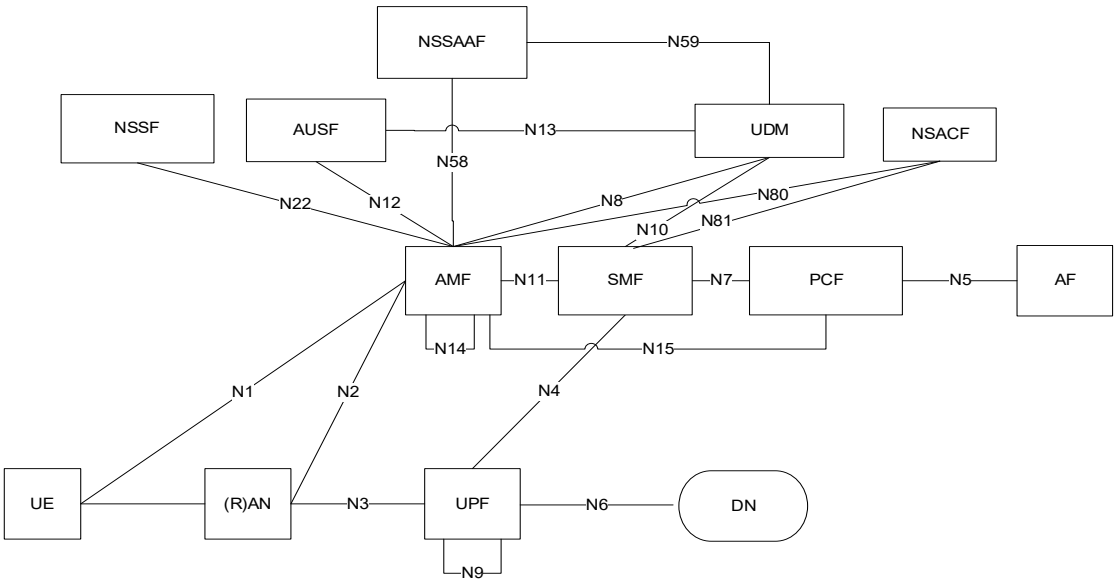


Ilustración 2. Representación de la arquitectura 5G mediante conexiones punto a punto [14]

Por un lado, se puede representar la comunicación entre NFs mediante el concepto de interfaces *punto-a-punto.* Esta representación sería más cercana al modelo tradicionalmente usado por otras arquitecturas, en el que todos los elementos que se comunican entre sí comparten un canal de comunicación definido por dos interfaces. A modo de esquema, es común emplear el representado en la Ilustración 2. En este caso, se puede ver qué NFs llegan a interactuar con otras en un escenario real de operación de la red, puesto que existe una línea que las une. Por tanto, se podría decir que el principal valor aportado por este tipo de representación es que facilita la identificación de interacciones entre las funciones de red [13], una tarea de base complicada, debido al número de las mismas y la gran cantidad de casos de uso en los que existe comunicación entre ellas.

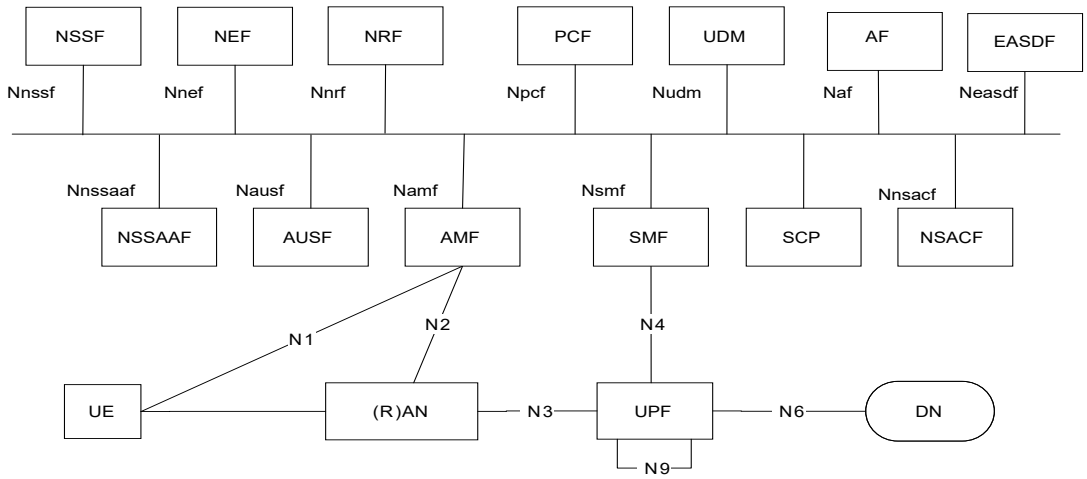


Ilustración 3. Representación de la arquitectura 5G como arquitectura basada en servicios [14]

Por otro lado, la definición de un sistema 5G ofrece la posibilidad de representar el funcionamiento del núcleo mediante el concepto de *arquitectura basada en servicios*. Se trata de un concepto novedoso en el contexto de las redes móviles y que contribuye al mencionado cambio de paradigma asociado a la *quinta generación.* Según este modelo, las

funciones de red no establecen comunicación con otras funciones punto-a-punto, sino que exponen *servicios* que pueden ser consumidos por aquellas funciones que lo requieran. El concepto tradicional de interfaz es sustituido por el de *interfaz basado en servicios,* usado para representar de forma lógica el punto en el que las NFs exponen sus servicios al resto. Se trata de una representación compleja, que no permite ver fácilmente los posibles flujos de comunicación que se pueden establecer pero, al mismo tiempo, es una representación más cercana al funcionamiento real del núcleo de la red. El esquema utilizado para modelo esta perspectiva del núcleo se encuentra en la Ilustración 3 y es explicado con mayor nivel de detalle en el apartado 2.2.3.3.

2.2.3.3 Arquitectura basada en Servicios (SBA)

Como se ha comentado anteriormente, el concepto de SBA hace referencia a un modelo lógico por el cual las funciones del núcleo de una red 5G se comunican entre sí exponiendo servicios y consumiendo los servicios expuestos por otras funciones. De forma práctica, cada NF es capaz de realizar una serie de operaciones o funcionalidades que pueden ser invocadas por otras funciones mediante una API. La configuración de las APIs utilizadas se ajusta al tradicional paradigma "HTTP REST", el cual es desarrollado en el apartado 2.2.3.4.

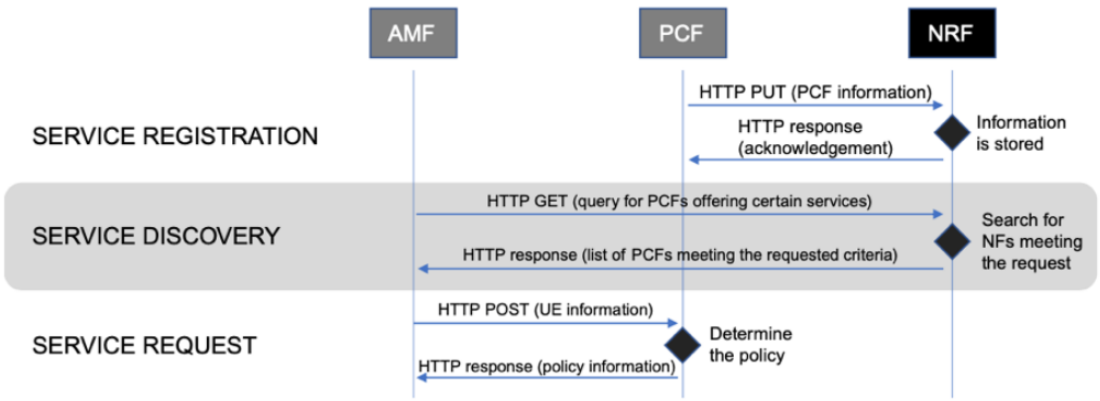


Ilustración 4. Operaciones en la arquitectura basada en servicios para 5G

Desde el punto de vista operativo, en un escenario normal de comunicación entre NFs, cada una adopta un rol diferente. La función que realiza el servicio o funcionalidad se denomina *Service Producer (SP)* y aquella que solicita hacer uso de dicha funcionalidad se denomina *Service Consumer (SC).* Dependiendo del caso de uso o escenario de comunicación una misma función puede adoptar un rol u otro indistintamente. A continuación, se procede a tomar un ejemplo práctico de interacción entre NFs para explicar las fases básicas de un escenario de comunicación según este modelo.

Durante la fase de registro de un abonado en la red, se realiza un procedimiento de autenticación que permite verificar la identidad del mismo. En dicho procedimiento, intervienen varias funciones y se ejecutan varias operativas, pero una de las más destacables es la solicitud, del AUSF al UDM, de generación de datos de autenticación. En este escenario, el UDM actuaría como productor del servicio (*SP)* y el AUSF, como consumidor (*SC)*. A partir de esta base, se pueden distinguir tres fases principales necesarias para que esta interacción se pueda desarrollar adecuadamente [13], representadas en la Ilustración 4:

- ***Service Registration:*** El primer paso para que una funcionalidad pueda ser invocada es que dicho servicio se encuentre registrado. Para ello, es indispensable la intervención de un NRF, actuando como *SP* en este contexto. Siguiendo el ejemplo propuesto, el UDM solicita al NRF registrarse como función de red indicando varios datos, entre ellos los servicios que expone a otras funciones.
  Se puede observar como el UDM, que en el contexto general del ejemplo actúa como *SP,* previamente debe interactuar con el NRF bajo el rol de *SC.*

- ***Service Discovery:*** La siguiente fase parte de la necesidad del AUSF de hacer uso de un servicio ofrecido por un UDM, en este caso la generación de información relevante para el procedimiento de autenticación. A fin de descubrir qué UDM en la red le puede dar el servicio requerido, debe producirse una interacción previa, de nuevo con un NRF.

El AUSF solicita al NRF información sobre un UDM que puede proporcionar el servicio deseado y esta petición es respondida con el identificador de una instancia de esta función que pueda satisfacer las necesidades requeridas.

- ***Service Request:*** El último paso es la interacción propiamente dicha entre las NFs protagonistas de este ejemplo. Como culminación del procedimiento, el AUSF solicita al UDM sobre el que ha recibido información la ejecución de un determinado servicio. Tras la realización de la tarea asociada, el UDM responderá a la petición del AUSF con el resultado de la funcionalidad solicitada, quedando así concluida la interacción entre ambas funciones de red.

De esta manera, queda plasmado el funcionamiento básico del modelo de *arquitectura basada en servicios* y cómo esta representación ayuda a entender el funcionamiento normal del núcleo de un red 5G durante el tiempo en que se encuentre operativo. Por último, cabe señalar que este modelo aplica a escenarios de comunicación en los que se intercambia información enmarcada dentro del plano de señalización o control. El intercambio de mensajes correspondiente al plano de datos de usuario seguirá otro paradigma diferente.

2.2.3.4 Protocolos de comunicación

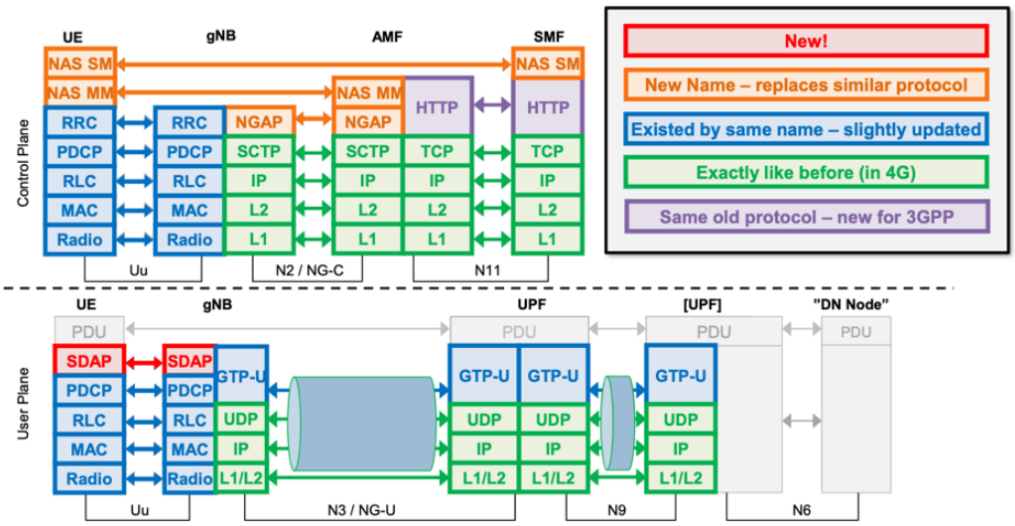


Ilustración 5. Pila de protocolos de los plano de control y datos para la tecnología 5G [15]

La Ilustración 5 expuesta muestra la pila de protocolos que intervienen en los diferentes planos de comunicación de una arquitectura 5G. Una pila de protocolos básicamente es una representación por capas de las reglas de comunicación que aplican y regulan el intercambio de información entre dos entidades funcionales. Como se puede observar, la principal diferencia existente entre la *quinta generación* y sus predecesoras, en el contexto del plano de control, es el uso del protocolo HTTP como protocolo de mayor nivel en la pila.

El uso del protocolo HTTP supone una novedad en el contexto de las redes móviles, aunque se encuentra muy extendido en entornos tradicionales de comunicación IT. Aunque no existe ninguna obligación relativa al uso del mismo, su adopción generalizada por parte de la comunidad ha convertido el uso de HTTP en un estándar de facto para comunicación a través de Internet, especialmente dedicado a escenarios de comunicación que necesitan de un intercambio de recursos entre clientes y servidores web.

En arquitecturas anteriores, toda la pila de protocolos empleados, tanto en la etapa radio como en las comunicaciones del núcleo, eran protocolos específicos de este ámbito de la tecnología. Por lo tanto, poder trabajar con ellos o, simplemente, comprender su funcionamiento, requería de un cierto grado de especialización y experiencia trabajando con arquitecturas de una red móvil.

La adopción de un protocolo como HTTP, ampliamente estudiado y utilizado, pretende democratizar la operación del plano de control del núcleo de una red 5G. Sin embargo, aunque esto puede ser visto como un beneficio, pues elimina barreras de entrada para que diferentes perfiles técnicos puedan operar y contribuir al desarrollo de las redes de *quinta generación,* también puede tener repercusiones negativas desde el punto de vista de la seguridad de la red, tal y como se expondrá en apartados posteriores.

2.2.4 CONSIDERACIONES DE SEGURIDAD

Si bien la seguridad es área crítica a tener en cuenta en el desarrollo de cualquier sistema, en una arquitectura de red móvil cobra una importancia añadida debido a las particularidades que esta presenta y que le diferencian de otros ecosistemas de comunicación. Una de la más

obvias es el uso del aire como canal de comunicación inalámbrico. Debido a esto, hay que considerar con especial criticidad riesgos de seguridad relativos a la intercepción de las comunicaciones en este interfaz, pues se trata de un medio expuesto públicamente y accesible por cualquier usuario de equipos de comunicación radio. Además, también hay que tener en cuenta a los diferentes actores que intervienen en la operación de una red móvil. Esto incluye, no solo a los abonados que hacen uso del servicio, sino también a la operadora que provee dicho servicio y a otros operadores que puedan verse obligados a interactuar entre sí para facilitar escenarios de comunicación en *roaming.*

Como se puede comprobar, se trata de un ecosistema complejo, con muchas particularidades y matices de funcionamiento, que hacen aún más difícil la tarea de diseñar los aspectos de seguridad. A lo largo de las diferentes generaciones de redes móviles, la seguridad ha ido adoptando un papel cada vez más relevante en la fase de diseño, hasta el punto de que el planteamiento de base de cada nueva generación trata de mejorar o subsanar las debilidades presentadas por generaciones anteriores, tal y como se ha tratado de reflejar en el apartado 2.1

A fin de comentar los aspectos más relevantes de seguridad de la arquitectura 5G, se ha optado por comenzar exponiendo los aspectos principales de seguridad en una implementación de red móvil, para terminar haciendo hincapié en aquellas particularidades o retos que acompañan a la implantación de la *quinta generación.*

2.2.4.1 Aspectos generales de seguridad

Los pilares básicos de seguridad inherentes al funcionamiento de cualquier red móvil pueden ser resumidos en tres aspectos principales [13] cuyas implicaciones se procede a exponer a continuación:

- **Autenticación de los usuarios**

Cuando un usuario desea hacer uso de los servicios de una red, generalmente se somete a un procedimiento de autenticación, mediante el cual se verifica que su identidad se encuentra registrada y que puede hacer uso de los servicios de la red. El mecanismo de autenticación

adoptado en las arquitecturas de redes móviles se basa en una serie de procesos, en los que participan dos entidades (usuario y red), y que les permiten probar que ambos tienen acceso a un secreto compartido (una clave).

Este mecanismo sigue un patrón común a la mayoría de las tecnologías, denominado *challenge*, consistente en:

- La red envía al UE una secuencia aleatoria para aplicar sobre ella ciertos algoritmos.
- A partir de esta secuencia, tanto la red como el UE generan unos vectores de autenticación, para cuyo cómputo se utiliza también la clave secreta que, en teoría, ambos comparten
- La comparación de estos vectores es la que permite confirmar el procedimiento de autenticación como exitoso o, de lo contrario, privar al usuario de acceso a los servicios de la red.

A partir de la *tercera generación* se estableció el concepto de autenticación mutua, lo que implica que no solo la red se encarga de verificar la identidad del usuario, sino que el usuario también es capaz de comprobar la legitimidad de la red. Esta política previene de ataques de suplantación de la red.

- **Privacidad de los usuarios**

Previo a la autenticación, se debe realizar un procedimiento de identificación, por el cual el usuario comunica su identidad a la red. La identidad de un usuario en el contexto de redes móviles suele estar asociada a un identificador llamado IMSI, consistente en una secuencia numérica de 15 dígitos. Este identificador vincula unívocamente un usuario con una identidad, por lo que su conocimiento podría comprometer aspectos críticos de la privacidad del usuario como su ubicación geográfica en un determinado momento.

A fin de prevenir ataques contra la privacidad de los usuarios, una de las medidas adoptadas a partir de la *segunda generación* fue la posibilidad de emplear identidades temporales. Se trata de una práctica que contribuye a que el IMSI se transmita un menor número de veces por el interfaz aire, que como se ha comentado, es sensible a sufrir ataques de interceptación.

Sin embargo, también conlleva un incremento de la complejidad lógica de la red, que necesitará mantener una base de datos con información actualizada sobre la vinculación entre los IMSIs de los usuarios registrados y sus identidades temporales.

Además, existen escenarios en los que la transmisión del IMSI sigue siendo necesaria, como por ejemplo la conexión de un usuario por primera vez a una determinada red, ya que en este punto no ha sido posible generar un identificador temporal.

- **Protección de las comunicaciones**

La protección de las comunicaciones es otro aspecto crítico de la seguridad en redes móviles y se puede condensar en los términos de confidencialidad e integridad:

  - El mantenimiento de la confidencialidad es responsabilidad de los mecanismos de cifrado adoptados en la tecnología. Una vez completado el procedimiento de autenticación, tanto usuario como red pueden acordar una clave de cifrado común, evitando tener que enviarla en texto claro por un canal inseguro. También es importante que ambos nodos acuerden un algoritmo de cifrado común, idealmente evitando algoritmos antiguos cuya seguridad se puede encontrar comprometida.
  - Los mecanismo de integridad permiten, por su parte, asegurar que la comunicación no ha sido alterada durante su transmisión a través del canal.

2.2.4.2 Aspectos específicos de la tecnología 5G

La definición de la arquitectura y los requerimientos de seguridad para la tecnología 5G se encuentra plasmada en el documento TS 33.501, elaborado por el organismo 3GPP [16]. Se trata de una descripción técnica centrada en los aspectos de seguridad para el sistema 5G. Específicamente, define los requisitos y arquitecturas de seguridad necesarios para proteger las comunicaciones y datos en la red 5G, abarcando desde la autenticación y la protección de la integridad y confidencialidad de los datos, hasta la gestión de claves y la seguridad de la señalización.

Dentro de las múltiples particularidades que presenta esta nueva generación con respecto a las anteriores, cabe destacar los siguientes aspectos relativos a los pilares de la seguridad en redes móviles anteriormente comentados:

- **Mecanismo de autenticación**

El mecanismo primario de autenticación definido para la arquitectura 5G se denomina 5G AKA. Aunque comparte muchas similitudes con su predecesor de *cuarta generación*, EPS AKA, presenta algunas diferencias importantes [17]:

  - 5G AKA confiere un mayor control sobre la autenticación a la red doméstica en caso de *roaming*, al permitir que elementos como el AUSF puedan verificar la autenticación de un determinado usuario. Con EPS AKA esta tarea solo era realizada por el nodo MME en la red visitada y el HSS de la red doméstica recibía una confirmación de autenticación, pero con 5G AKA se involucra directamente a elementos de la red doméstica en el proceso. De esta manera se trata de reforzar la seguridad en escenarios de *roaming*
  - 5G AKA puede ser utilizado sobre tecnologías de acceso *no-3GPP*. Este hecho tiene varias implicaciones positivas, pues favorece la interoperabilidad con otras soluciones tecnológicas de acceso a la red, permite a los operadores mejorar su eficiencia operativa centralizando la gestión de la autenticación y facilita el desarrollo de nuevas aplicaciones asociadas a un acceso *no-3GPP*, como podrían ser las redes de dispositivos IoT.

Estas mejoras hacen que 5G AKA no solo sea una evolución de EPS AKA, sino una herramienta fundamental para la seguridad y la flexibilidad de las redes 5G.

- **Protección añadida sobre la privacidad de los usuarios**

La definición de requisitos de seguridad en la tecnología 5G aborda directamente el riesgo de privacidad de los usuarios asociado a la transmisión, en texto claro, del IMSI a través del interfaz aire en determinadas ocasiones.

La especificación TS 33.501 denomina SUPI al identificador único de usuario para la tecnología 5G e indica expresamente que no debe ser enviado en texto claro, salvo en algunas excepciones como el procedimiento de llamadas de emergencia. Para permitir esto, se define otro identificador, denominado SUCI, el cual se transmite cifrado y permite la posterior autenticación del usuario.

La adopción de esta medida trata de mitigar ataques de "captura de IMSI" o "*IMSI Catchers*", los cuales ponían en serio riesgo de vulneración la privacidad de los usuarios en generaciones anteriores.

- **Mecanismos de protección sobre HTTP**

La adopción del protocolo HTTP como protocolo de comunicación entre funciones de red en el núcleo de la arquitectura tiene su justificación en las implicaciones positivas comentadas en el apartado 2.2.3.4. Sin embargo, también supone una serie de retos de seguridad que deben ser abordados mediante una adecuada implementación del mismo. Principalmente, nos referimos a la implantación de medidas de protección de los mensajes enviados con este protocolo, tales como la incorporación de una capa TLS/SSL para protección de la confidencialidad de la información y utilización de flujos OAuth2.0 para asegurar que se cumplen las políticas de autorización.

2.3 PROTOCOLO HTTP/2

El protocolo HTTP/2 es la última versión revisada de HTTP, siglas de *Protocolo de Transferencia de Hipertexto.* Se trata del mecanismo para intercambio de recursos entre clientes y servidores web, cuyo uso generalizado lo ha convertido en el estándar de comunicación más utilizado entre servicios a través de Internet.

La descripción del protocolo HTTP fue el resultado de un proyecto de colaboración entre el Consorcio WWW y el cuerpo de estandarización IETF, el cual culminó en 1999 con la publicación de una serie de documentos de definición, RFCs, siendo el más importante el número 2616 por ser aquel que especifica la versión 1.1, la más utilizada hasta la fecha. En

el año 2015 y debido al exponencial aumento del tráfico en Internet, se hizo necesario implementar una serie de mejoras funcionales que optimizasen el funcionamiento de este protocolo, lo cual se acabó traduciendo en una revisión del mismo y en la definición de una nueva versión en la RFC 7540 publicada en el año 2015.

2.3.1 FUNDAMENTOS DEL PROTOCOLO HTTP 1.1

Aunque no se trata de la última versión definida de HTTP, la versión 1.1 sigue siendo, en la actualidad, la más empleada por la mayoría de sitios web. Además, a nivel de funcionamiento general y semántica, mantiene amplias similitudes con su versión posterior, por lo que entender las bases de HTTP 1.1 permite comprender fácilmente las bases de la versión 2 y el impacto que tienen las mejoras implementadas sobre el rendimiento del protocolo.

2.3.1.1 Mecanismo de comunicación petición - respuesta

El fundamento principal del funcionamiento de este protocolo es que la comunicación se produce a partir de transacciones denominadas *petición-respuesta.* Esto implica que los mensajes siempre serán entendidos como parejas, pues toda petición debe tener asociada su respuesta y viceversa. Ambos tipos de mensajes presentan una estructura similar, compuesta por los siguientes elementos:

- Una línea inicial, donde se describe la instrucción a realizar o el resultado de ejecución de la misma.
- Una serie de cabeceras donde se definen diferentes características asociadas a la comunicación.
- El cuerpo de la petición, en el que viajan datos relevantes asociados a la misma, como podría ser la descripción, en formato HTML, de una página web.

No obstante, dependiendo del tiempo de mensaje, el contenido de estos elementos será diferente.

Peticiones

Las peticiones HTTP son aquellos mensajes enviados desde el cliente al servidor, que sirven para solicitar el envío de un determinado recurso o la ejecución de una determinada acción. El elemento principal de una petición es la línea inicial, pues en ella se indica qué tipo de solicitud se está realizando y el destinatario de la misma. Esta información es detallada mediante:

- El método de la petición, que es una palabra que simboliza la acción solicitada. Los principales métodos empleados son:
    - GET – solicita información del servidor sin realizar ninguna modificación.
    - POST – sirve para enviar información al servidor.
    - PUT – modifica información existente en el servidor.
    - DELETE – ordena la eliminación de información en el servidor.

  Otros métodos menos empleados pero de funcionalidad también importante serían:

    - HEAD – sirve para conocer las cabeceras que contendría la respuesta a una petición GET.
    - TRACE – se utiliza para probar el correcto funcionamiento de una comunicación.
    - OPTIONS – permite conocer las opciones de comunicación disponibles para un destinatario determinado.
- El destinatario o *target* de la petición, el cual hace referencia a la entidad que deberá dar respuesta a la misma. El formato en el que se expresará esta información varía según el tipo de petición, pero lo más habitual es que se trate de una URL, un localizador que sirve para identificar unívocamente a un recurso concreto de un servidor conectado a Internet.

Respuestas

Las respuestas HTTP son aquellos mensajes que se envían por parte de los servidores como contestación a una petición de un determinado cliente. La primera diferencia que presentan

con respecto a las peticiones es que en su línea inicial no se indica el método solicitado, sino que se incluye un *código de estado,* el cual se trata de una secuencia numérica de tres dígitos que sirve para representar el resultado de ejecutar la petición solicitada. Dependiendo del dígito inicial del código, se pueden distinguir los siguientes significados:

- 1XX – Respuestas informativas
- 2XX – Resultado exitoso
- 3XX – Redirección
- 4XX – Error del lado de cliente
- 5XX – Error del lado del servidor

No obstante, la parte más importante de una respuesta suele encontrarse en el cuerpo de la petición. Aunque no todas las respuestas poseen información en el cuerpo, es habitual que la solicitud de recursos web sea respondida mediante un mensaje en el que viaje el código HTML de una página web, embebido en el cuerpo del mensaje.

En cuanto al tipo de cuerpo que pueden presentar los mensajes HTPP, se suelen clasificar en tres categorías:

- Único recurso de longitud conocida – Se define mediante dos cabeceras:
  - *Content-Type*: Define el tipo de recurso enviado.
  - *Content-Length*: Define la longitud del recurso enviado, en bytes.
- Único recurso de longitud desconocida – En este caso, el recurso se codifica en segmentos o *chunks* de longitud variable.
- Múltiples recursos – El cuerpo se divide en diferentes secciones que contienen diferentes tipos de información.

El mecanismo de comunicación *petición-respuesta* es ampliamente utilizado en el ecosistema de los sistemas de información, principalmente debido a su facilidad de implementación y uso, así como su fiabilidad en la entrega de información. No obstante, este procedimiento tiene asociadas algunas características que van en contra de su idoneidad para algunos tipos de aplicaciones, especialmente aquellas que requieren baja latencia o soporte

para comunicación asíncrona. Además, el hecho de que todo envío de información deba ir precedido por una petición del cliente, sumado a los datos que inevitablemente son enviados con cada mensaje, como la información de cabeceras, puede derivar en el envío de comunicación redundante y/o un exceso de tráfico intercambiado. El objetivo de definir la nueva versión de HTTP fue, por tanto, mejorar estas capacidades para permitir que el uso de este protocolo fuese viable en un mayor de escenarios de comunicación.

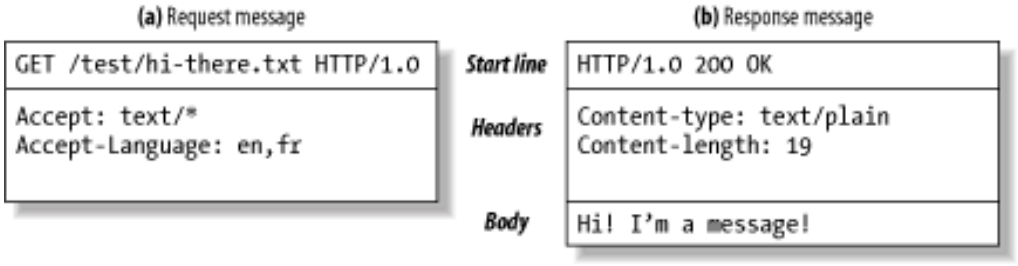


Ilustración 6. Estructura básica de petición y respuesta en HTTP [18]

2.3.2 MEJORAS INTRODUCIDAS EN HTTP/2

El crecimiento del número de usuarios activos en Internet tuvo como consecuencia natural un aumento del tráfico y fue ligado a un incremento de los requisitos de calidad de servicio. Es por ello que el principal objetivo del IETF con la definición de HTTP/2 fue mejorar la latencia percibida por el usuario y, en consecuencia, su experiencia en el uso de servicios en Internet.

Para ello, la primera novedad destacable incluida en esta nueva versión supone un cambio de paradigma en cuanto al formato de organización de los mensajes. HTTP/2 divide los mensajes en *marcos* o *frames,* que a su vez son empaquetados dentro de *flujos* o *streams*. Los *frames* pasan a ser la unidad mínima de información en el contexto de HTTP, lo que permite que los datos sean gestionados de manera más ordenada y eficiente. Además, las cabeceras de información y los datos o contenido del mensaje pertenecen ahora a distintos *frames*, lo cual facilita aplicar diferentes criterios a su tratamiento.

Ilustración 7. Organización de mensajes en frames en HTTP/2 [19]

El concepto de *frame* es fundamental para poder aplicar algunos de los cambios que contribuyen a una mejora considerable en el rendimiento de HTTP en su versión 2. A continuación, se procede a comentar las principales novedades que presenta este protocolo y que tienen un impacto directo sobre su eficiencia.

2.3.2.1 Multiplexación

La multiplexación es un concepto que, tradicionalmente, hace referencia al procedimiento que permite combinar dos o más señales en un único canal de información. En lo relativo al funcionamiento de HTTP/2, se utiliza este término para describir la posibilidad de intercalar el envío de *frames* de diferentes *streams* utilizando una misma conexión de red.

La inclusión de esta capacidad aborda directamente el problema denominado *head-of-line blocking,* el cual supone uno de los principales inconvenientes para el rendimiento de HTTP 1.1. Este protocolo se basa en el envío de peticiones y respuestas dentro de una misma conexión y una de las máximas de funcionamiento es que cada petición debe esperar su correspondiente respuesta. Esto ocasiona que peticiones lentas de procesar puedan retrasar

el envío de peticiones posteriores y, a consecuencia, afectar negativamente a la latencia de la comunicación.

Para solventar este obstáculo, HTTP/2 permite dividir mensajes en *frames* y agruparlos en flujos de envío de mensajes relacionados, de manera que si un flujo tiene un tiempo de procesamiento alto, se puede aprovechar dicho tiempo para enviar *frames* de otros flujos, utilizando de forma más eficiente el canal de comunicación.

2.3.2.2 Priorización de contenido

La priorización, en el contexto de intercambio de recursos web, se refiere al orden o secuencia en la que se cargan las piezas de contenido que el servidor transmite al cliente. Distintos tipos de contenido tendrán asociadas diferentes latencias de carga (por ejemplo, un texto plano requerirá de menos tiempo que una imagen) por lo que, el orden de carga de los elementos en un sitio web tendrá un impacto directo sobre la latencia general percibida por el usuario.

El protocolo HTTP/2 ofrece a los desarrolladores de contenido web la posibilidad de controlar este flujo de carga, mediante el empleo de una multiplexación selectiva. Esta función, en algunas fuentes denominada *priorización ponderada* [20] , permite a los desarrolladores asignar a cada flujo de datos un determinado valor de prioridad, que sirve como indicación al cliente de qué fragmento de contenido debe cargar primero. Con ello, se produce una mejora considerable en la calidad de servicio percibida por los usuarios una vez que estos solicitan la carga de recursos web a un servidor.

2.3.2.3 Server Push

Según la definición de HTTP/2, un servidor puede responder a la petición de un cliente con un mayor número de datos que los que fueron solicitados inicialmente, lo cual supone otro cambio importante con respecto a los fundamentos originales de HTTP.

Esto permite a los servidores enviar información que anticipa futuras peticiones del cliente, lo que reduce el tráfico en la conexión y los tiempos de carga asociados. Un ejemplo fácil de aplicación de este término se da cuando un cliente solicita el código HTML de una página

web y el servidor, además de dicho código, también entrega los recursos CSS y JS asociados sin necesidad de esperar a una solicitud posterior del mismo cliente. Esta práctica contribuye positivamente a la experiencia de usuario, quien experimenta una mayor agilidad en la visualización de recursos web.

2.3.2.4 Compresión de encabezados

El último gran rasgo característico de HTTP/2 al que se hará referencia en este apartado es la capacidad para aplicar métodos de compresión sobre las cabeceras de los mensajes. En la versión 1.1 del protocolo tanto las cabeceras como el cuerpo del mensaje se enviaban sin comprimir, lo cual requería de la utilización de un mayo ancho de banda para la comunicación. Sin embargo, el empleo de *frames* independientes para agrupar cabeceras y datos hace posible la aplicación de métodos de compresión que reduzcan el tamaño de los datos enviados.

El procedimiento se basa en que, en lugar de enviar los encabezados completos cada vez, se utiliza un algoritmo, denominado HPACK, para comprimirlos y enviar solo las diferencias entre los encabezados nuevos y los previamente enviados. Esto reduce significativamente la cantidad de datos transmitidos, agilizando el proceso de carga de páginas web y mejorando el rendimiento general de la red.

2.3.3 SEGURIDAD DEL PROTOCOLO

Como ya se ha mencionado, los requerimientos tenidos en cuenta a la hora de diseñar e implementar la versión 2 de HTTP son fundamentalmente funcionales, y se pueden resumir en reducir la latencia, aprovechar de forma más eficiente el ancho de banda y ofrecer una experiencia más fluida y de mejor calidad a los usuarios. No obstante, los requerimientos de seguridad son inherentes a cualquier tecnología y, con el aumento del número de usuarios, la seguridad adquiere inevitablemente un papel más relevante.

2.3.3.1 Beneficio del formato binario

Alguna de las modificaciones funcionales de HTTP/2 sí tienen un impacto directo y positivo sobre la seguridad del protocolo. Este es el caso del cambio de formato de los mensajes,

tradicionalmente en texto plano, por un formato binario. Además del impacto positivo que la adopción de este formato tiene sobre la eficiencia de la transmisión de datos, debido a que los mensajes son más compactos y rápidos de procesar, también supone una mejora en la seguridad del protocolo con respecto a la versión anterior.

El uso de un formato textual permitía ciertos ataques conocidos como *response splitting* o división de respuestas. En estos ataques, un adversario es capaz de inyectar espacios en blanco u otros caracteres especiales en los encabezados de respuesta para manipular cómo los navegadores y los *proxies* interpretan las mismas. Esta práctica pueden resultar en comportamientos inesperados o, incluso, en la ejecución de código malicioso.

El cambio a un formato binario en HTTP/2 evita esta vulnerabilidad debido a la diferente forma en la que se estructuran los datos. En lugar de depender de delimitadores de texto que pueden ser alterados, el formato binario utiliza una estructura más rígida y definida que no permite manipulaciones de esta naturaleza.

2.3.3.2 Ausencia de cifrado y aplicación de SSL/TLS

La característica de HTTP/2 con un mayor impacto sobre la seguridad del protocolo y que, además, es heredada de la definición de HTTP 1.1, es la determinación de que el uso de cifrado sea opcional al desarrollador. Al definir como opcional el uso de mecanismos de cifrado de la información, se expone el uso de este protocolo a serios compromisos de seguridad, en términos de confidencialidad de los datos transmitidos y la autenticación de las partes implicadas.

La solución adoptada, también heredada de la versión anterior del protocolo, es el uso de una capa adicional que aporta estos mecanismos de seguridad, denominada capa SSL/TLS. Estas siglas hacen referencia a un procedimiento por el cual se puede crear un canal de comunicación seguro entre un servidor y un cliente web, verificando la identidad de cada uno de ellos y previniendo que un tercer actor no autorizado pueda interceptar la comunicación y visualizar en claro los datos enviados.

Este procedimiento se puede resumir en cuatro tareas principales [21]:

- **Elegir una versión del protocolo:** Existen diferentes versiones de TLS y no todos los servidores y los clientes tendrán soporte para las mismas, por lo que es necesario que, en primer lugar, acuerden qué versión del protocolo se va a utilizar. Se trata de un punto crítico del procedimiento, pues versiones antiguas de TLS ya han sido descontinuadas por presentar fallos de seguridad. Por tanto, conviene que tanto servidores como clientes únicamente soporten las versiones más recientes, generalmente desde la 1.2 en adelante, a fin de minimizar los riesgos.
- **Elegir una *suite* de cifrado:** Se trata de seleccionar un conjunto de algoritmos criptográficos para realizar el cifrado de la información en tránsito, creando el canal de comunicación seguro. De nuevo, debe existir un acuerdo para la selección de algoritmos cuyo soporte sea común a ambas partes.
- **Verificar la identidad de las partes mediante certificados:** La autenticación de las partes se consigue mediante el intercambio de sus correspondientes certificados digitales y la utilización de fundamentos de criptografía asimétrica. Mediante la confianza en la entidad de certificación que emitió cada certificado, cada una de las partes es capaz de verificar la identidad de la otra.
- **Crear claves de sesión:** La última tarea consistirá en la creación de claves para que ambas partes puedan aplicar un procedimiento de cifrado simétrico sobre los datos a transmitir. Mediante este proceso, ambos actores comparten un clave de cifrado que aporta confidencialidad a la comunicación, realizando un proceso simétrico con las ventajas de velocidad y eficiencia que tiene respecto a uno asimétrico.

De forma general, estas tareas se pueden resumir en una serie de pasos en los que cliente y servidor se intercambian información, en un procedimiento que recibe el nombre de “saludo” o *handshake*:

- El cliente envía un mensaje *Client Hello* con la siguiente información: la versión de TLS y los algoritmos de cifrado soportados, una cadena de caracteres aleatoria que recibe el nombre de *client random* y la técnica de compresión de datos empleada.
- El servidor responde con un mensaje *Server Hello* conteniendo los siguientes datos: el algoritmo de cifrado acordado, una cadena de caracteres aleatoria que recibe el

nombre de *server random,* un identificador de sesión y el certificado digital del servidor junto con su clave pública.

- El cliente verifica la identidad del servidor contactado a la autoridad de certificación responsable de la emisión del certificado.
- Comienza el procedimiento de intercambio de claves, con el cliente extrayendo la clave pública del certificado que acaba de ser verificado. Esta clave se utiliza para cifrar otra secuencia aleatoria, *premaster secret,* que envía al servidor.
- El servidor descifra esta cadena utilizando su clave privada, compartiendo desde este momento un secreto con el cliente.
- El cliente envía un mensaje cifrado con la clave secreta compartida indicando que ya forma parte del canal seguro establecido.
- El servidor responde con un mensaje indicando que también comparte dicho canal seguro.
- En este punto, cliente y servidor pueden empezar a comunicarse aplicando cifrado simétrico de lo datos enviados utilizando la clave que comparten.

En el caso de que alguno de lo pasos de este procedimiento no pueda realizarse, se finalizará la conexión establecida con el servidor notificando al cliente un código de estado de error 503, *Service Unavailable*.

La aplicación de SSL/TLS permite dotar a la comunicación vía HTTP de una capa adicional de seguridad que garantiza la confidencialidad, integridad y autenticación en la comunicación. Su uso es tan significativo que recibe una denominación especial, HTTPS, para indicar que la comunicación hace uso de un protocolo seguro. En la aplicación de HTTP/2, los desarrolladores suelen distinguir entre dos implementaciones, *h2c* y *h2*, para distinguir si se aplica cifrado o no, y se le otorga tanta importancia a la seguridad que, en muchos casos, se programa el empleo de HTTP/2 en un servicio web únicamente si se pueden aplicar estos mecanismos de seguridad.

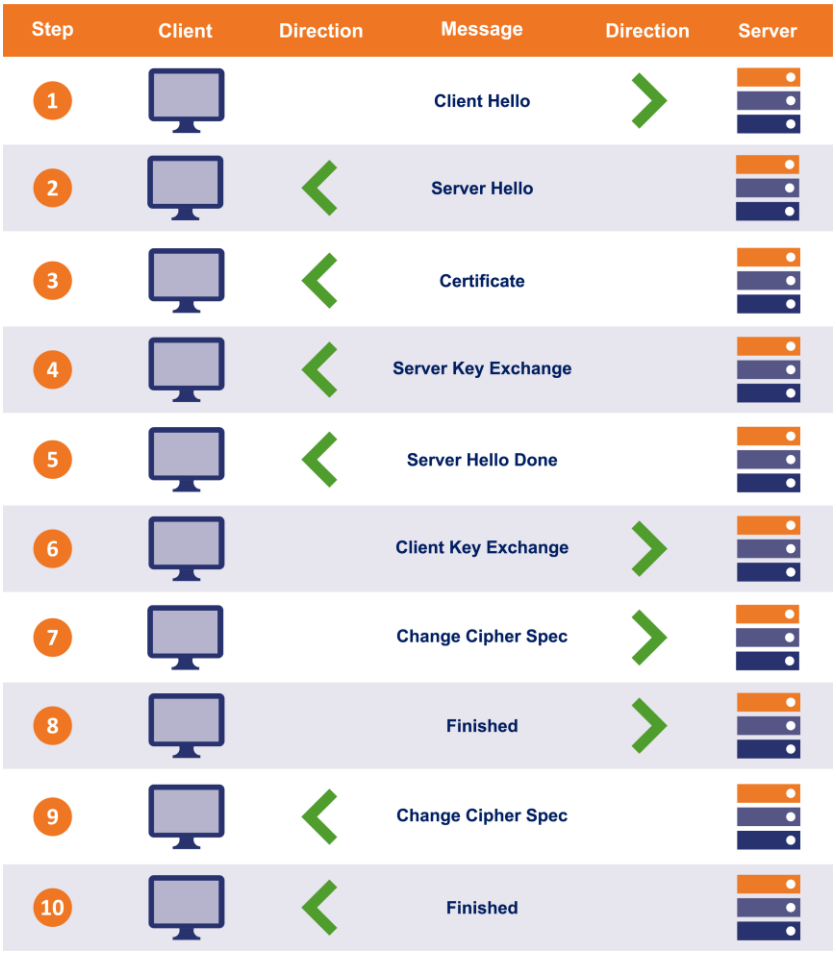


Ilustración 8. Mecanismo de handshake para SSL/TLS [22]

Capítulo 3. ESTADO DE LA CUESTIÓN

La realización de este trabajo tiene como referencia una serie de documentos de carácter científico que representan diferentes estudios sobre la materia, los cuales exponen resultados relacionados con el tema principal de la investigación, la seguridad en el núcleo de las redes 5G.

Køien [22], en un artículo publicado en el año 2021, analiza posibles amenazas sobre la seguridad de las redes 5G derivadas del uso de una arquitectura basada en servicios. Este paradigma es una de las novedades que presenta esta tecnología con respecto a sus predecesoras, y se basa en un modelo lógico por el cual las funciones del núcleo de una red 5G se comunican entre sí exponiendo servicios y consumiendo los servicios expuestos por otras funciones. La elección de esta arquitectura forma parte de un conjunto de novedades estructurales introducidas en la definición de las redes 5G las cuales tienen el propósito de aproximar una infraestructura de comunicaciones al enfoque y bases de la tecnología de comunicación web.

La adopción de procedimientos usados en el ecosistema de las comunicaciones web pretende simplificar y hacer más accesible la arquitectura 5G, principalmente a perfiles técnicos formados en un entorno IT, con el objetivo de fomentar el desarrollo de esta tecnología y facilitar su implementación en diferentes industrias. No obstante, estas prácticas no están exentas de riesgos, tal y como remarca el autor. Dentro de los riesgos señalados en el documento, cabe destacar:

- El hecho de que el paradigma SBA implique novedades de diseño entraña los riesgos inherentes a cualquier nueva implementación, como fallos o vulnerabilidades no detectadas durante su especificación.
- El uso del formato JSON en los mensajes entre NFs puede conllevar riesgos de seguridad, debido a la existencia de diferentes especificaciones para este formato que

pueden entrañar problemas de interoperabilidad entre implementaciones de distintos fabricantes.

- Las conexiones inseguras entre NFs y el uso de un protocolo conocido como HTTP amenaza la confidencialidad e integridad de la información transmitida. Aunque se trata de un riesgo que se puede mitigar mediante la implementación de mecanismos como TLS, la responsabilidad última de su implementación recae sobre las operadoras y fabricantes, por lo que algunos de ellos podrían optar por desplegar una solución insegura a cambio de ahorrar costes operacionales.
- En relación con el punto anterior, la adopción de un esquema de autorización basado en OAuth2.0 también es algo novedoso en la industria de las comunicaciones y que, por tanto, podría implementarse erróneamente o no implementarse debido al sobrecoste que ello podría suponer para la operadora, con los consecuentes riesgos de seguridad asociados.

Junto con estos riesgos, el autor elabora una taxonomía de amenazas, la cual será utilizada como referencia en el análisis de seguridad realizado en el Capítulo 5. Cabe destacar que es el primer autor que considera la mala praxis por parte de las operadoras en la implementación de esta tecnología como un riesgo real a tener en cuenta, sobre todo en la parte del núcleo de la red, por el impacto potencial que una posible intrusión en este entorno podría tener, debido al uso de protocolos de comunicación ampliamente conocidos en el ecosistema IT.

Como conclusión, se expone la criticidad de tener conocimiento de los riesgos de seguridad asociados a la arquitectura SBA y se hace especial hincapié en la necesidad de utilizar herramientas adicionales para garantizar la autenticación y autorización en las comunicaciones entre funciones de red, mencionando protocolos conocidos como SSL/TLS y OAuth2.0.

Por su parte, *Wehbe y otros* [23] y *Hu y otros* [24], en sus respectivos trabajos, ahondan en la seguridad de la arquitectura basada en servicios, centrando su estudio en la selección de HTTP/2 como protocolo de comunicación a utilizar en el núcleo de la red 5G para comunicar las diferentes funciones virtualizadas que realizan el papel tradicionalmente asignado a

elementos denominados "nodos". Ambos estudios ponen de manifiesto la posibilidad de utilizar este protocolo como vector de ataque, aprovechando vulnerabilidades conocidas y asociadas a las nuevas capacidades de HTTP/2, como la multiplexación de *streams* o el control de flujo de carga de recursos. Dentro de los hipotéticos ataques descritos en sendos trabajos, conviene destacar:

- **Denegación de servicio por multiplexación de *streams***: Consiste en aprovechar la posibilidad de transmitir múltiples *streams* del protocolo HTTP/2 utilizando una única conexión TCP para enviar gran número de peticiones computacionalmente complejas a una determinada función de red con el objetivo de provocar una denegación de servicio sobre la misma.
- **Ataque por control de flujo**: El control de flujo es una capacidad introducida en HTTP/2 para asegurar que los diferentes *streams* que se intercambien en una misma conexión no interfieran entre sí. Para ello, existe la posibilidad de que los elementos que se están comunicando fijen un tamaño máximo para la información que se puede enviar en un determinado *stream.* En este caso se teoriza con la posibilidad de que una NF maliciosa establezca una conexión con un NF legítima y requiera un determinado recurso, fijando el tamaño máximo de transmisión a un valor muy pequeño. De esta forma, conseguiría monopolizar los recursos de la NF legítima durante un largo período de tiempo, dando como resultado una posible denegación de servicio.
- **Ataque a la dependencia y priorización de *streams***: El protocolo HTTP/2 incluye mecanismos para establecer prioridad entre *streams* (cuáles deben procesarse antes) y dependencia entre los mismos (qué proporción de recursos deben ser dedicados a cada uno). De manera análoga al caso anterior, una NF maliciosa podría forzar a una legítima a construir un árbol de dependencia (modelo lógico a consultar para determinar de qué manera procesar cada tipo de *stream)* demasiado complejo, ocasionando un ataque de denegación de servicio, en este caso, por consumo exhaustivo de memoria y CPU en la NF afectada.

- **Ataques a la compresión de cabeceras**: Se teoriza sobre la posibilidad de aprovechar el mecanismo de compresión de cabeceras de HTTP/2, HPACK, para amenazar la confidencialidad y disponibilidad de una función de red. En primer lugar, existe el riesgo de fuga de información si la operación de compresión precede a una de cifrado y las cabeceras se comprimen en el mismo contexto que datos bajo el control del atacante. En segundo lugar, un atacante podría enviar un *stream* con un gran volumen de información en forma de cabeceras y, a continuación, una ráfaga de *streams* que requiriesen ejecutar la descompresión de dichas cabeceras. De esta manera, se estaría obligando a una NF a consumir un gran porcentaje de recursos, pudiendo ocasionar que no pueda dar servicio a otras peticiones de NFs legítimas.
- **Denegación de servicio por *server push***: El mecanismo de *server push* es otra de las características más destacables de HTTP/2, la cual permite mejorar la experiencia de los usuarios otorgando la capacidad a un entidad de enviar recursos a otra sin necesidad de una petición específica, anticipando posibles peticiones futuras. No obstante, esta capacidad arbitraria de envío de recursos se podría utilizar de forma maliciosa para saturar el ancho de banda que una NF tiene disponible para la transmisión de información.

Las amenazas expuestas hacen todas referencia al uso malintencionado de rasgos característicos y novedades asociadas a HTTP/2, por lo que forman parte del riesgo intrínseco asociado al uso de este protocolo para comunicación entre funciones de red. Este riesgo debe ser evaluado y tratado con especial consideración, pues el impacto potencial de las amenazas descritas, principalmente en forma de denegación de servicio, repercutiría directamente sobre el núcleo de la red, lo que ocasionaría una disrupción de servicio sobre la totalidad de la red 5G.

Giambartolomei y otros [25], en un documento publicado en 2024, agregan un grado más de especialización a los trabajos anteriores, estudiando la robustez de la redes 5G frente a ataques realizados con técnicas tradicionales de *penetración web*. El uso de HTTP/2 como protocolo de comunicación y la exposición de algunas funciones de red a Internet es lo que

hace posible que técnicas que tradicionalmente aplicaban al *hacking* de servidores y servicios web puedan llegar a resultar una amenaza real para las redes 5G.

En este contexto, se propone un modelo de amenazas sobre el núcleo de las redes 5G basado en un enfoque web y utilizando como referencia el marco de trabajo STRIDE, el cual describe seis tipos de vulnerabilidades (*Spoofing, Tampering, Repudiation, Information disclosure, Denial of service & Elevation of priviledge*) que pueden afectar a cualquier sistema. Como entorno de pruebas para verificar la existencia de estas vulnerabilidades, se hace uso de herramientas de diferentes herramientas de código abierto (*OAI, Free5gc & Open5GS)* , con el objetivo también de realizar un análisis de seguridad comparativo entre las mismas.

Los resultados exponen la existencia de vulnerabilidades en todas las tecnologías probadas, algunas tan críticas como la ausencia del principio de mínimo privilegio, lo que permite a usuarios normales realizar acciones que deberían estar reservadas para administradores del sistema o la ausencia de verificación sobre los datos introducidos por el usuario, lo cual puede derivar en la ejecución de ataques por inyección SQL y NoSQL.

En relación a la evaluación de seguridad en implementaciones *open source* de la arquitectura 5G, otro trabajo que sirve como referencia de gran valor es el publicado por *Alex Bui* en 2023 [26], en el que se evalúa la implementación de mecanismos de seguridad en las tres soluciones de código abierto previamente mencionadas, centrando el análisis en la existencia y correcta implementación del protocolo TLS en el núcleo de la red.

Es de especial interés para este trabajo los resultado obtenidos sobre las tecnologías *OpenAirInterface* y *Open5GS*, debido a que serán utilizadas durante las pruebas prácticas asociadas al proyecto. En este sentido, se destaca el hecho de que *OAI* no soporta el uso de mecanismo de cifrado para las comunicaciones entre funciones de red, mientras que *Open5GS* sí tiene una opción habilitada para ello. No obstante, la ejecución de varias herramientas de análisis estático y dinámico sobre esta solución permiten concluir que la implementación de *Open5GS,* a fecha de realización de este estudio, no cumplía con todos los requisitos expuestos por la 3GPP en términos de seguridad en el núcleo de la red 5G.

Por último, cabe mencionar el artículo publicado por *Dolente y otros* [27] en el año 2024, en el que se realiza un estudio de seguridad de la implementación de las funciones de red 5G en diferentes soluciones tecnológicas de código abierto. Mediante este trabajo, se realiza una interesante clasificación de las vulnerabilidades que afectan al núcleo de una red 5G y se demuestra la viabilidad de ataques, como la denegación de servicio o los conocidos *replay attacks,* sobre implementaciones de código abierto de funciones de red tan críticas como el AMF o el NRF.

De este artículo, cabe destacar que el objeto de estudio se centra en aspectos de seguridad relacionados con aquellas funciones de red que se encuentran, de alguna manera, expuestas al exterior del núcleo de la red. Este podría ser el caso del AMF, accesible mediante los interfaces N1 y N2, o del NRF/NEF, que puede actuar como intermediario entre el núcleo de una red 5G y aplicaciones de terceros, exponiendo servicios en forma de API. Consecuentemente, se elabora una metodología de ataque basada en probar ataques de denegación de servicio sobre el AMF y NRF, *replay attacks* sobre el AMF y ataques por inyección sobre la API del NRF.

Los resultados reflejados para estos últimos son de especial interés para la realización de este proyecto, pues se trata de evaluar la seguridad del núcleo de la red haciendo uso de peticiones HTTP/2 y aprovechando el enfoque de comunicación por interfaces API entre funciones de red. Las pruebas realizadas sobre las tecnologías *open source* utilizadas ponen de manifiesto una serie de vulnerabilidades a tener en cuenta para estudios posteriores:

- **Inconsistencia en las respuestas:** Se ha detectado que algunas respuestas no se ajustan al estándar JSON y exponen demasiada información sobre la implementación, lo cual podría ser considerado como una vulnerabilidad de fuga de información susceptible de ser explotada por un atacante.
- **Falta de verificación y tratamiento de los *input*:** Se ha detectado la falta de tratamiento sobre ciertos parámetros controlados por el usuario, lo cual podría derivar en ataques de inyección SQL o procedimientos similares.

- **Manejo incorrecto de métodos y parámetros:** En el caso de *OAI,* se ha observado que la solución no implementa un manejo adecuado de ciertos métodos alternativos a los definidos por el estándar, los cuales pueden llegar a ocasionar una disrupción en el funcionamiento del NRF y derivar en una potencial denegación de servicio. Por otro lado, en el caso de *Open5GS,* se detecta la posibilidad de registrar NFs indicando parámetros "vacíos", lo que refleja un incorrecto tratamiento de ciertos datos de entrada.
- **Implementación incompleta del estándar de API:** En las pruebas con *OAI*, se ha comprobado la inexistencia de implementación de ciertos servicios definidos en el estándar oficial de la 3GPP.

Estas vulnerabilidades específicas de las soluciones *open source* analizadas han podido ser detectadas debido a ciertas malas prácticas en la implementación de la arquitectura 5G, las cuales no solo son propias de una implementación de código abierto, sino que podrían manifestarse en entornos comerciales en los que se estuviese aplicando esta tecnología. Las más críticas a tener en cuenta serían:

- Ausencia de mecanismos de encriptación de tráfico entre interfaces SBI
- Ausencia de mecanismos de autorización para establecer un sistema de roles y permisos
- Ausencia de limitación en el envío de peticiones entre NFs
- Debilidad en los mecanismos de tratamiento y verificación de datos introducidos por el usuario en el contexto de la red

El análisis de seguridad realizado en este documento es el punto de partida más completo y reciente para la evaluación teórica y las pruebas prácticas llevadas a cabo durante la realización de este proyecto, expuestas en el Capítulo 5. y 6 de este documento.

Capítulo 4. DESCRIPCIÓN DE LAS TECNOLOGÍAS

La realización de este proyecto ha requerido del uso de diferentes herramientas y soluciones tecnológicas, cuyas características y utilización se procede a describir en este capítulo.

4.1 OPEN AIR INTERFACE

El nombre *OpenAirInterface* hace referencia a un proyecto [28] situado dentro del marco de trabajo de la OSA (*OpenAirInterface Software Alliance)*, un organismo sin ánimo de lucro que reúne a una comunidad grande de desarrolladores con objetivo de trabajar en la descripción e implementación de soluciones gratuitas y de código abierto de redes móviles, tanto de la parte radio (RAN) como del núcleo de la red (CN).

A fecha de realización del trabajo, el proyecto de red de acceso radio cuenta con la implementación de una instancia de gNB, tanto para los casos de red NSA como SA, así como también un modelo software emulador de un UE. Por su parte, el proyecto de desarrollo del núcleo de la red permite el despliegue de un núcleo funcional para una arquitectura 5G mediante la implementación de las siguientes funciones de red: AMF, SMF, NRF, UPF, UDM, AUSF, UDR, y NSSF. Por ello, este proyecto ofrece un ecosistema completo en el que poder desplegar y utilizar una red 5G de extremo a extremo, actualmente conforme con la descripción del 3GPP de la arquitectura 5G en su *Release 16*.

Para la realización de este proyecto, se ha hecho uso de las implementaciones del núcleo de la red y del gNB para el escenario SA, ambas en su versión v2.0.1.

4.2 OPEN5GS

Se trata de un proyecto de código abierto [29] centrado en la descripción e implementación del núcleo de una red móvil, el cual permite ejecutar entornos de una arquitectura 5G en sus variantes NSA y SA. Para poder dar soporte a sendos escenarios, el grupo de trabajo de

Open5GS trabaja en el desarrollo y soporte, en paralelo, de los elementos constituyentes de un núcleo tipo EPC (para el caso 4G/5G NSA) y de la funciones de red que componen el núcleo de una red 5GCN (para el caso 5G SA). Un aspecto positivo a destacar sobre esta tecnología sería su facilidad para interoperar con otras aplicaciones, lo cual ofrece un amplio abanico de posibilidades a la hora de construir entornos de laboratorio, pudiendo combinar diferentes implementaciones de gNB y UE.

Para el desarrollo del trabajo, se ha utilizado el código que implementa el núcleo 5GCN para una red 5G SA, en su última versión disponible, la cual manifiesta estar ajustada a la descripción del 3GPP de la arquitectura 5G en su *Release 17*. Esta versión del núcleo incluye soporte para las siguientes funciones de red: NRF, SCP, AMF, SMF, UPF, AUSF, UDM, UDR, PCF, NSSF, BSF y SEPP.

4.3 SRSRAN

El proyecto *srsRAN* es una plataforma de software de código abierto para redes de radio definidas por software (SDR) [30], desarrollada por la compañía *Software Radio Systems*, la cual implementa un sistema completo de comunicaciones móviles. Actualmente, el desarrollo del proyecto cuenta con dos líneas diferenciadas de trabajo, centradas en las tecnologías 4G y 5G respectivamente. La primera da soporte a las implementaciones de eNB, UE y núcleo EPC de la red, lo que permite el despliegue de una red 4G completa extremo a extremo utilizando elementos desarrollados por este grupo de trabajo. La segunda, por su parte, ofrece una implementación funcional de un gNB y un UE, mientras la parte del núcleo de la red 5G se encuentra todavía en desarrollo.

Para la parte práctica de este trabajo, se ha empleado la implementación del gNB puesta a disposición en este proyecto, catalogada como la versión 23.10 y declarando conformidad con el estándar de 3GPP en su *Release 17.*

4.4 USRP B200 MINI

La emulación de los equipos físicos que constituirían la parte radio de la red en un despliegue comercial tradicional se ha llevado a cabo mediante el empleo de equipos SDR o *Software Defined-Radio.* Este término hace referencia a un sistema de radiocomunicaciones el cual implementa en *software* elementos que tradicionalmente se encuentran en *hardware*. Este hecho hace que sea un componente realmente útil para la ejecución de redes móviles en entornos de laboratorio, fundamentalmente por su flexibilidad, ya que las características de la comunicación radio pueden ser modificados simplemente actualizando líneas de código, en lugar de cambiar componentes físicos.

Entre las diferentes opciones disponibles, se ha optado por hacer uso del producto USRP B200 en su versión *mini* [31], un sistema SDR desarrollado por Ettus Research.

4.5 ENTORNO LINUX Y HERRAMIENTAS ASOCIADAS

Las tecnologías anteriormente mencionadas y las herramientas que se han desarrollado durante la realización del proyecto han utilizado como base un sistema operativo de código libre de tipo Linux. Concretamente, se ha hecho uso de Ubuntu, una distribución de Linux basada en Debian, en su versión 20.04 [32]. La elección de esta versión de Ubuntu en lugar de otra más reciente tiene por objetivo asegurar la compatibilidad con todas las herramientas de código abierto mencionadas anteriormente.

Sobre la plataforma de Ubuntu Linux se han desarrollado diferentes funciones de código o *scripts* haciendo uso del lenguaje de programación *bash.* Este lenguaje de programación es capaz de interpretar comandos propios de la *shell* de Linux e interactuar con el sistema operativo para ejecutarlos, funcionalidad que es de gran utilidad para trabajar con las implementaciones de código abierto de elementos de una red 5G, pues muchas de ellas requieren de la ejecución de elementos que se interpretan como binarios del sistema operativo.

Como herramienta adicional de gran utilidad para el desarrollo del proyecto se ha empleado Wireshark. Esta herramienta permite la interceptación de tráfico de red en tiempo real, lo que posibilita el análisis de todos aquellos paquetes que sean transmitidos a través de los interfaces de comunicación disponibles en el equipo. El análisis de tráfico es una tarea de vital importancia para la parte práctica del trabajo y se ha realizado, fundamentalmente, con dos propósitos concretos:

- Interceptar el tráfico en el interfaz N1, para analizar los mensaje intercambiados entre el gNB y el AMF. Estos mensajes se enmarcan sobre el protocolo SCTP y permiten, en primera instancia, verificar que el gNB se ha conectado adecuadamente al núcleo de la red y, posteriormente, supervisar todas las interacciones del equipo de usuario con el núcleo de la red, monitorizando actividades como la autenticación del usuario o la asignación de una sesión de comunicación en el plano de datos.
- Interceptar el tráfico HTTP/2 entre NFs, con el objetivo de entender el formato de los mensajes y poder utilizar esta información para probar la seguridad del núcleo de la red haciendo uso de este mismo protocolo.

4.6 ORQUESTADOR DE REDES 5G

La integración de todas las tecnologías mencionadas ha requerido del desarrollo de una herramienta capaz de asegurar el despliegue y correcto funcionamiento de cada una de ellas. Con este propósito, se ha tomado como base el prototipo de orquestador de redes 5G desarrollado por EthonShield y se ha ampliado su funcionalidad para dar soporte a los requerimientos de este proyecto.

El prototipo inicial de orquestador, denominado *sharp-orchestrator*, tenía la funcionalidad de desplegar componentes de gNB y Core de la tecnología *OpenAirInterface*, deplegando una red 5G funcional en cuestión de segundos. Además, esta herramienta se encargaba de monitorizar la salud de todos sus elementos y de efectuar acciones para tratar de mantener la red en un estado funcional en caso de fallo en alguno de ellos.

A partir de este prototipo, la parte inicial del proyecto ha consistido en ampliar su funcionalidad, integrando el resto de tecnologías mencionadas. Se ha capacitado el orquestador para desplegar la parte *core* desarrollada por *Open5gs* y el gNB desarrollado por *srsRAN*.

La ejecución de la herramienta parte de un fichero de configuración en el que es posible seleccionar diferentes parámetros de la red como el MCC, MNC o TAC, así como las tecnologías deseadas para el núcleo y la parte radio de la red. Posteriormente, se ejecutan las fases de despliegue y verificación del correcto funcionamiento de los componente, de manera completamente automática. De esta manera, el resultado final es una herramienta que permite un despliegue rápido y controlado de una red 5G en un entorno de laboratorio, con el objetivo de realizar sobre ella cualquier tipo de prueba un labor de investigación.

Capítulo 5. ANÁLISIS DE SEGURIDAD

5.1 METODOLOGÍA Y REFERENCIAS

El propósito de este capítulo es realizar un análisis de seguridad del núcleo de una infraestructura de una red 5G genérica, el cual tenga por objeto el planteamiento y descripción de un modelo de amenazas y riesgos específico para esta tecnología. Dicho modelo debería considerar bajo qué condiciones puede materializarse una amenaza, qué activos se verían afectados si esto ocurriese y cuál sería el potencial impacto asociado sobre la seguridad.

Para la realización de este estudio, se tomará como referencia el análisis de riesgos expuesto en el Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G [33]. El referenciado análisis utiliza una metodología estructurada en fases basada en MAGERIT, un marco de gestión de riesgos de seguridad de la información desarrollado por el Centro Criptológico Nacional de España. De acuerdo con lo expuesto en el documento, la metodología empleada se compone de las siguientes fases:

a) Descripción y análisis de la arquitectura 5G así como de los entornos de red asociados y los activos que los componen.

b) Evaluación de la criticidad de los activos en cada parte o componente de la red 5G, teniendo en cuenta su relación con cada una de las cinco dimensiones de seguridad: Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad.

c) Identificación de las posibles amenazas presentes en este entorno específico, clasificación de las mismas por activos afectados e identificación del nivel de riesgo asociado.

d) Desarrollo de medidas de seguridad técnicas, organizativas y estratégicas para mitigar o reducir el nivel de riesgo de las amenazas identificadas en cada entorno de red.

e) Manejo de los riesgos y riesgos residuales, especialmente en aquellas amenazas cuyo nivel sea significativo y no pueda ser mitigado mediante ninguna medida adicional desde la fase de diseño.

Para el contenido de este capítulo, resulta de especial interés la clasificación de activos por nivel de criticidad y los tipos generales de amenazas identificados sobre la infraestructura 5G.

5.2 CRITICIDAD DE LOS ACTIVOS

En cuanto a la ponderación del nivel de criticidad de los activos, el Real Decreto 443/2024 utiliza una clasificación cualitativa en tres niveles (alto, medio, bajo). De acuerdo con esta clasificación, se identifica cómo de crítica es la seguridad del activo en relación con las cinco dimensiones de seguridad y se asigna al activo en cuestión la mayor criticidad de todas sus dimensiones.

En lo relativo a las dimensiones de la seguridad y su relación con los activos de la infraestructura, conviene hacer las siguientes aclaraciones:

- **Confidencialidad**: Se valora la capacidad de un activo para asegurar que la información contenida en él solo es expuesta a aquellos usuarios que están autorizados para ello.
- **Integridad**: Hace referencia a la aptitud de un activo para garantizar que los datos que maneja (almacenados o en tránsito) únicamente son modificados por fuentes autorizadas.
- **Trazabilidad**: Implica la capacidad de un activo para vincular inequívocamente las acciones realizadas sobre él a una determinada identidad (usuario, persona o proceso)
- **Autenticidad**: Se valora la capacidad de un activo para verificar que toda entidad que interactúa con él es quien dice ser.
- **Disponibilidad**: Se refiere a la capacidad de un activo para ofrecer su servicio sin interrupciones a aquellos usuarios que estén autorizados a hacer uso de él.

A continuación, se expone el resultado de este análisis para los elementos de red que componen el núcleo de la infraestructura 5G, puesto que es el área de mayor interés para el objetivo del capítulo:

Activo	*Criticidad*	*Dimensiones más críticas*
AMF	Alta	Confidencialidad
NRF	Alta	Confidencialidad, Integridad, Autenticidad y Trazabilidad
UDM	Alta	Todas
UDR	Alta	Todas
AUSF	Alta	Todas
NEF	Media	Confidencialidad, Integridad, Autenticidad y Trazabilidad
UPF	Baja	Todas
PCF	Baja	Todas
SEPP	Alta	Confidencialidad

Tabla 1. Criticidad de las funciones de red en la arquitectura 5G

El resultado del análisis refleja un grupo mayoritario de elementos del núcleo de red con criticidad alta. Esto implica la consideración de que el compromiso de al menos una de sus dimensiones de seguridad, puede resultar en un impacto crítico para la seguridad global de la infraestructura de red 5G.

5.3 IDENTIFICACIÓN DE LAS AMENAZAS

Una vez se ha realizado la clasificación de los activos en función de su criticidad, es conveniente proceder con la identificación de las amenazas asociadas. De acuerdo con la definición formal proporcionada por INCIBE [34], una amenaza es aquella acción que, aprovechando una vulnerabilidad conocida o desconocida en un sistema, puede suponer un impacto negativo sobre la seguridad del mismo.

En el Real Decreto 443/2024 se presenta una clasificación general de las amenazas a las que se expone una infraestructura de red 5G, cuyas categorías se procede a comentar a continuación:

- **Realización de acciones maliciosas como consecuencia de accesos indebidos a la infraestructura**:

Se trata de la categoría de amenazas más amplia, pues engloba todos los potenciales compromisos de seguridad que puedan derivar de un acceso malicioso o no autorizado a la infraestructura. La clasificación considera aquellas acciones realizadas por un atacante, interno o externo, el cual obtiene acceso a la infraestructura de red y lo utiliza para realizar algún tipo de ataque.

En este grupo se encuentran amenazas como: Exfiltración de información sensible de la red (topología de la red datos de usuarios, ficheros de configuración …), modificación de parámetros de configuración de los activos o ejecución remota de código para explotación de otras vulnerabilidades.

- **Acciones con impacto negativo sobre la seguridad de las comunicaciones y/o datos de usuario:**

Se consideran aquellas acciones destinadas a comprometer la confidencialidad, integridad o disponibilidad de las comunicaciones en la red a través de la interceptación, alteración o interrupción de las mismas, respectivamente.

- **Denegación de Servicio (DoS):**

Engloba amenazas sobre la disponibilidad de los activos, que puedan tener como impacto la interrupción, total o parcial, de los servicios que dichos activos están prestando. Se tienen en consideración tanto ataques volumétricos cuyo objetivo es conseguir una disrupción general en el servicio de la red, como ataques dirigidos a un determinado usuario o activo.

- **Amenazas físicas sobre los activos:**

Esta categoría recoge aquellas amenazas que afectan directamente a la integridad física de los activos, tanto acciones intencionadas como los efectos vinculados a fenómenos o catástrofes naturales.

- **Falta de concienciación de los empleados en materia de ciberseguridad:**

La falta de formación y concienciación de los empleados que interactúan con la infraestructura de red supone una categoría de amenazas en sí misma, al mismo tiempo que facilita la materialización de amenazas clasificadas en el resto de categorías.

La clasificación expuesta conforma una taxonomía en la que se ubican todas las posibles amenazas que pueden comprometer la seguridad de una red estándar de quinta generación. Sin embargo, no hace referencia a los posibles vectores de ataque que pueden llevar a la materialización de las amenazas en cada una de las categorías, así como también se obvia la probabilidad de ocurrencia de las mismas.

5.3.1 AMENAZAS SOBRE EL NÚCLEO DE LA RED

Para el objetivo de este capítulo, es de especial interés la identificación de aquellas amenazas que afecten directamente al núcleo de la arquitectura. Entre todas las posibles amenazas, habrá que considerar aquellas cuyo vector de ataque requiera que el atacante tenga acceso a alguno de los elementos del núcleo o la propia red que los interconecta, pudiendo interactuar con las funciones de red.

A fin de estructurar el análisis, se han considerado cuatro posibles escenarios mediante los que un atacante podría obtener acceso al núcleo de red. Cabe destacar que la selección de

estos escenarios se ha realizado sobre el contexto de una infraestructura de red 5G operada por un proveedor de servicios de comunicaciones:

- ***Insider* con acceso al núcleo de red -** Un empleado con intenciones maliciosas y poseedor de una identidad autorizada para operar el núcleo de la red tendría la capacidad para ejecutar ataques afectando directamente a este entorno.
- **Compromiso de una identidad con acceso al núcleo de red -** Se considera la posibilidad de que un empleado con acceso al núcleo de la red sufra un compromiso de sus credenciales de acceso, lo cual posibilite a un atacante suplantar su identidad y ejecutar acciones maliciosas haciendo uso de los permisos asociados a su rol. En este punto cabe distinguir dos posibles casos:
    - **Empleado con permisos de operación:** Si el empleado cuya identidad se hubiese visto suplantada tuviese capacidad para operar el núcleo de red, el atacante podría realizar acciones con un impacto similar al del punto anterior.
    - **Empleado con permisos de administración:** En este caso, si la víctima del compromiso de credenciales fuese un empleado con permisos de administración del núcleo de red, el potencial impacto asociado sobre la seguridad sería distinto. No obstante, también se considera la probabilidad de que el atacante consiguiese efectuar un movimiento lateral y obtener permisos de operación, explotando alguna vulnerabilidad existente en la configuración de la segregación funcional.
- **Compromiso de la capa de virtualización / orquestación:** Las funciones de red propias de una arquitectura 5G operan dentro de un entorno virtualizado y orquestado por una capa superior. El compromiso de la seguridad de esta capa podría derivar en un acceso malicioso al núcleo de red en caso de que un atacante lograse efectuar acciones de movimiento vertical (esto es, conseguir acceso a las funciones virtualizadas a partir de un acceso fraudulento a la capa de orquestación que opera en un nivel de abstracción más elevado)
- **Interconexión insegura entre redes:** El punto de interconexión *roaming* forma parte de la superficie de ataque del núcleo de la red 5G, pues representa un canal de

comunicación entre las funciones de red de una operadora y un agente externo. La seguridad de la interconexión queda delegada sobre la función de red SEPP, responsable de garantizar la confidencialidad e integridad de la comunicación extremo a extremo entre la red origen y destino. Por tanto, una configuración inadecuada de esta función posibilitaría la ejecución de ataques con un impacto negativo directo sobre la seguridad del núcleo de la red.

Los escenarios anteriormente planteados contemplan las posibilidades más plausibles a partir de las cuales una amenaza puede llegar a suponer un impacto sobre el núcleo de la red 5G de una operadora. En cuanto a las probabilidades de ocurrencia de los mismos, se han considerado las siguientes:

Escenario	***Probabilidad de ocurrencia***
Insider	Baja
Compromiso de credenciales de usuario operador	Baja
Compromiso de credenciales de usuario administrador	Baja
Compromiso de capa de virtualización / orquestación	Baja
Interconexión insegura entre redes	Media

Tabla 2. Probabilidad de ocurrencia de los escenarios de ataque sobre el núcleo de una infraestructura 5G

Teniendo como punto de partida estos escenarios, se han planteado las siguientes categorías de amenazas que podrían afectar al núcleo de la red:

- **Interceptación de tráfico:** La interceptación de tráfico en el núcleo de una red 5G se relaciona con amenazas sobre la confidencialidad de la información, tales como la exfiltración de información sensible o la exposición de la topología de la red. Si la

comunicación no se encuentra adecuadamente cifrada, un atacante podría capturar e interpretar el tráfico HTTP/2 intercambiado entre las funciones de red, obteniendo información valiosa como la topología de la red, los servicios habilitados en cada una de las NFs o información sensible sobre las identidades de los usuarios.

- **Obtención de información por interacción directa con una NF:** Existe la amenaza de que un atacante, una vez conocida la estructura de los mensajes intercambiados entre funciones de red, ejecute un escaneo activo, enviando peticiones directamente a las NFs y obteniendo información sensible en las respuestas. Se trata, por tanto, de una amenaza a la confidencialidad.
- **Modificación de parámetros de una NF:** En relación con los puntos anteriores, la interacción con una NF puede derivar, no solo a la obtención de información, sino también a la modificación de parámetros de la propia NF, amenazando la integridad de la red. Este tipo de ataques cobrarán especial relevancia en funciones de red encargadas de almacenar y gestionar datos de identidad de los abonados, como serían el UDR y UDM en la infraestructura 5G.
- **Registro de una NF maliciosa:** Se valora como amenaza la posibilidad de que un atacante ejecute una operación de registro de una función de red falsa o maliciosa, alterando la topología de la red y atacando de forma directa la integridad y la disponibilidad de la misma.
- **Disrupción de servicio de una NF:** Esta amenaza hace referencia a la posibilidad de que un atacante consiga interrumpir el servicio de una función de red, ocasionando de esta manera un impacto sobre el funcionamiento de la arquitectura. Existen diversas vías teóricas por las que podría efectuarse dicho ataque, desde la aplicación de la API de HTTP/2 para eliminar el registro de una NF hasta la modificación o *tampering* de peticiones legítimas buscando fallos de seguridad que puedan derivar en un mal funcionamiento de la NF consultada.

Estas amenazas han sido consideradas como las más críticas dentro de la taxonomía global que recoge todas aquellas amenazas a la arquitectura 5G, previamente referida.

En el Capítulo 6. se utilizarán diferentes herramientas *open source* para simular el despliegue de una red 5G y poner a prueba el potencial impacto que la materialización de estas amenazas podría tener sobre la seguridad de una red comercial.

Capítulo 6. PRUEBAS DE SEGURIDAD EN EL NÚCLEO DE UNA RED 5G

El objetivo de este capítulo es mostrar las pruebas de seguridad realizadas sobre una arquitectura 5G funcional, desplegada en un entorno de laboratorio creado utilizando herramientas de código abierto. Estas pruebas tienen por propósito evaluar el impacto que podría tener la materialización de las amenazas sobre el núcleo de una red 5G expuestas en el capítulo anterior, utilizando técnicas basadas en el conocimiento del protocolo HTTP/2.

Para construir el entorno experimental, se han empleado las herramientas y tecnologías a las que hace referencia el Capítulo 4. Por un lado, para la parte *hardware,* se ha utilizado un equipo modelo *Slimbook ELEMENTAL* como entorno de ejecución para las herramientas *open source* y un dispositivo USRP B200 *mini* para implementar el elemento transceptor. Por otro lado, la parte *software* del entorno está compuesta por el gNB desarrollado por *srsRAN* y las implementaciones del núcleo de red de *OpenAirInterface* y *Open5gs,* con objeto de establecer una comparación entre ambas. Cabe señalar que, debido a que se trata de proyectos actualmente en desarrollo y expuestos a modificaciones frecuentes, los resultados alcanzados deben ir ligados a la fecha de realización del proyecto.

A fin de automatizar la ejecución de las pruebas lo máximo posible, se ha optado por el desarrollo de una herramienta en lenguaje de programación *bash*. Esta herramienta ha sido configurada para hacer uso del protocolo HTTP/2 e interactuar con las funciones de red, partiendo de la base de que el equipo en el que se ejecuta la herramienta tiene un interfaz de comunicación en la misma red que el núcleo de la arquitectura 5G. La Ilustración 9 muestra el resultado de ejecutar dicha herramienta, que ofrece al usuario un menú en línea de comandos con ciertas funcionalidades que serán empleadas durante el desarrollo de las pruebas.

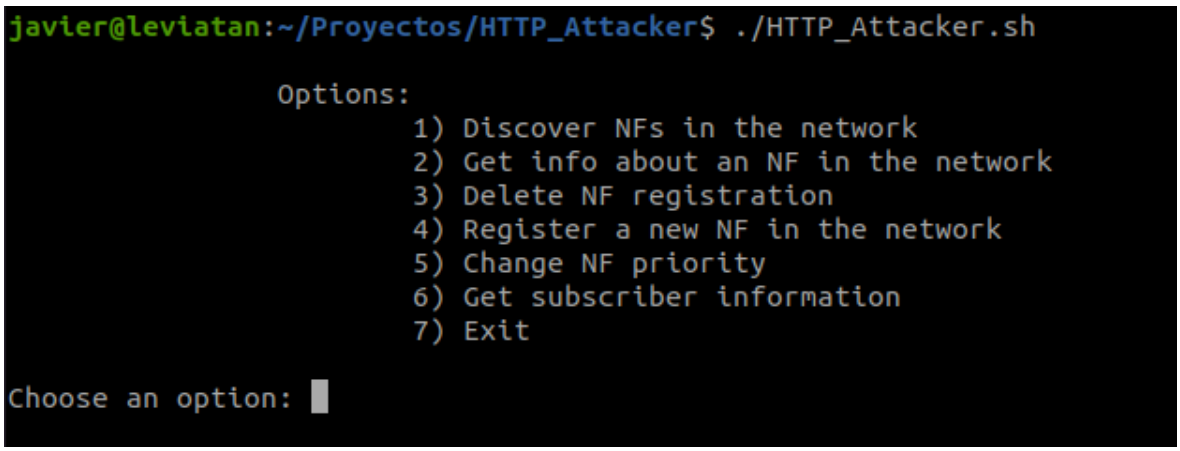


Ilustración 9. Herramienta para interacción con NFs en el núcleo de una red 5G

A continuación, se detallan la pruebas realizadas y los resultados obtenidos para las dos tecnologías probadas, incluyendo para ello imágenes que muestran capturas de tráfico realizadas con *Wireshark* y capturas del interfaz de línea de comandos que reflejan el resultado de operaciones realizadas por la herramienta desarrollada.

6.1 COMPROMISO DE CONFIDENCIALIDAD

En primer lugar, se han realizado pruebas para evaluar la confidencialidad de la red, es decir, la capacidad de asegurar que el acceso a la información solo es posible para aquellas identidades autorizadas para ello. Con este propósito, se han realizado técnicas de escaneo pasivo y activo, cuyas diferencias y resultados se procede a explicar en los subsiguientes apartados.

6.1.1 ESCANEO PASIVO

Las técnicas de escaneo pasivo son aquellas que se basan en la observación del tráfico de red y recopilación de datos sin que exista interacción directa con los sistemas objetivo, lo cual hace que sean más difíciles de detectar. Uno de los ataques más frecuentes asociados a la interceptación de tráfico es el ataque de “Man in the Middle” o MitM, consistente en que un atacante se sitúe en medio del flujo de comunicación entre dos partes que creen estar

comunicándose directamente, pudiendo interceptar e incluso alterar el tráfico que se envían entre ellas. Este escenario de ataque se puede alcanzar por diversos procedimientos siendo uno de los más comunes el envenenamiento de tablas ARP. En este caso, al estar ejecutando el núcleo de la red en un equipo bajo nuestro control, no es necesario aplicar este tipo de técnicas, pues se puede utilizar una herramienta como *Wireshark* para interceptar todo el tráfico enviado entre las NFs.

La interceptación del tráfico de red arroja una primera conclusión sobre la seguridad de las tecnologías utilizadas**: ninguna de ellas emplea, por defecto, un mecanismo de cifrado de tráfico para los mensajes intercambiados** entre funciones de red. Este hecho hace posible que el procedimiento de escaneo pasivo permita a un atacante estudiar la estructura y contenido de los mensajes HTTP/2 intercambiados entre NFs, un ejemplo de lo cual se muestra en la Ilustración 10.

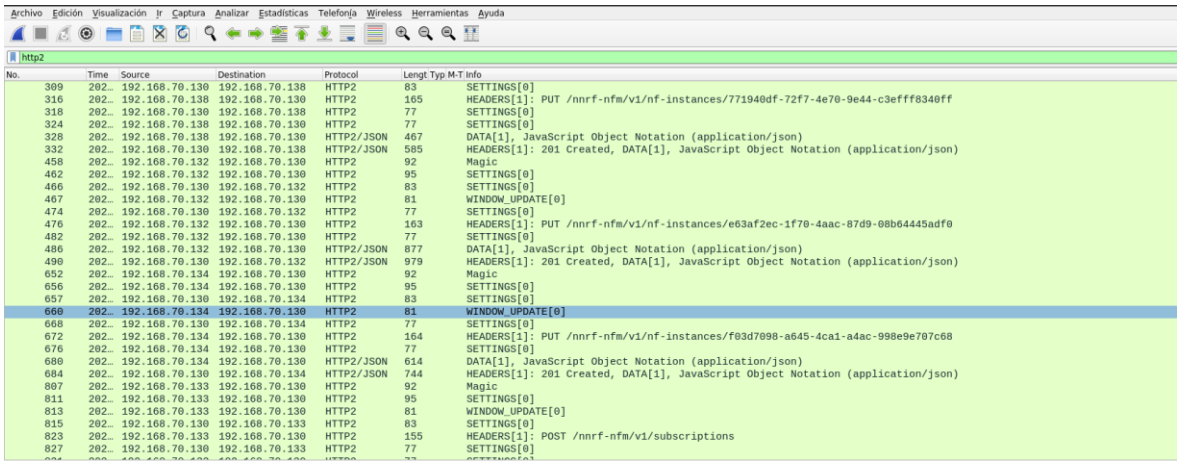


Ilustración 10. Ejemplo de tráfico HTTP/2 interceptado para OAI

El proceso de revisión de documentación y archivos de configuración de ambas tecnologías permite concluir, para las versiones de las herramientas utilizadas en este proyecto, lo siguiente: *OpenAirInterface* no implementa ningún mecanismo de cifrado de tráfico HTTP/2, mientras que *Open5gs* sí que ofrece la posibilidad de usar el protocolo TLS para asegurar la confidencialidad de estos mensajes, aunque dicha funcionalidad se encuentra

desactivada por defecto. Para que el desarrollo de las siguientes pruebas permita establecer una comparación adecuada entre ambas tecnologías, se procederá a no configurar la opción de cifrado con TLS en *Open5gs.*

El siguiente paso del proceso de escaneo pasivo consiste en tratar de identificar la topología de la red, esto es, qué NFs existen en la misma y cómo se comunican entre sí. Esta labor se puede llevar a cabo de manera sencilla con *Wireshark*, pues la herramienta posee una funcionalidad que nos permite ver de manera ordenada las conversaciones entre nodos que están teniendo lugar en un determinado segmento de red.

IPv4 · 7

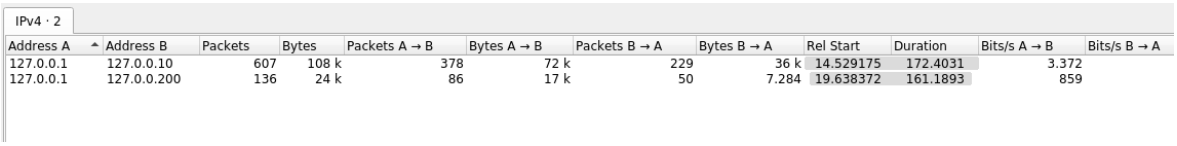
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.70.129	192.168.70.130	42	4.747	30	2.911	12	1.836	44.764679	0.0400	582 k	
192.168.70.132	192.168.70.130	182	21 k	124	14 k	58	7.460	13.032175	200.1096	565	
192.168.70.133	192.168.70.130	80	13 k	50	7.434	30	5.985	14.334298	202.0061	294	
192.168.70.134	192.168.70.130	189	21 k	126	14 k	63	7.565	13.739967	200.0067	561	
192.168.70.136	192.168.70.130	175	20 k	118	13 k	57	6.984	22.149370	190.2654	556	
192.168.70.137	192.168.70.130	181	21 k	124	13 k	57	7.216	12.396598	200.2210	557	
192.168.70.138	192.168.70.130	184	20 k	126	13 k	58	7.065	12.709369	200.2923	555	

Ilustración 11. Conversaciones HTTP/2 en el core de OAI

La Ilustración 11 muestra las conversaciones entre las NFs desplegadas en el núcleo de *OpenAirInterface*. Se puede observar que existen múltiples direcciones IP asignadas, todas dentro de un mismo rango de red típicamente utilizado para configurar una red privada. Este resultado es coherente, ya que el paradigma de despliegue de OAI se basa en que cada función de red se despliega dentro de un contenedor *Docker,* y estos contenedores deben estar en la misma red para poder comunicarse entre sí.

Además, atendiendo al flujo de las conversaciones, se puede observar que todas ellas comparten la misma dirección IP destino, lo que indica que una NF está siendo receptora de peticiones de todas las demás. Este resultado invitar a pensar que dicha función de red se corresponde con el NRF y que el resto de instancias de funciones envían mensajes para

registrar sus servicios y poder anunciarse a otras NFs, en caso de requieran de dichos servicios.



IPv4 · 2

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
127.0.0.1	127.0.0.10	607	108 k	378	72 k	229	36 k	14.529175	172.4031	3.372	
127.0.0.1	127.0.0.200	136	24 k	86	17 k	50	7.284	19.638372	161.1893	859	

Ilustración 12. Conversaciones HTTP/2 en el core de Open5gs

Por otra parte, la Ilustración 12 muestra las conversaciones HTTP/2 en el núcleo implementado con *Open5gs*. A simple vista, se observa que el paradigma de implementación debe ser diferente, pues únicamente se detectan 3 direcciones IP distintas involucradas en el procedimiento de comunicación HTTP/2. De nuevo, se trata de un resultado coherente, pues *Open5gs* ha optado por el empleo de un nodo tipo SCP para actuar de intermediario entre la NRF y el resto de funciones de red, enmascarando de esta manera la dirección IP vinculada al interfaz SBI del resto de NFs.

Esto permite concluir que **las dos tecnologías estudiadas utilizan dos aproximaciones diferentes, ambas utilizadas en las redes comerciales, para establecer comunicación entre las diferentes funciones del núcleo**. La ilustraciones Ilustración 13 y Ilustración 14 representan un esquema de las topologías identificadas para ambas soluciones.

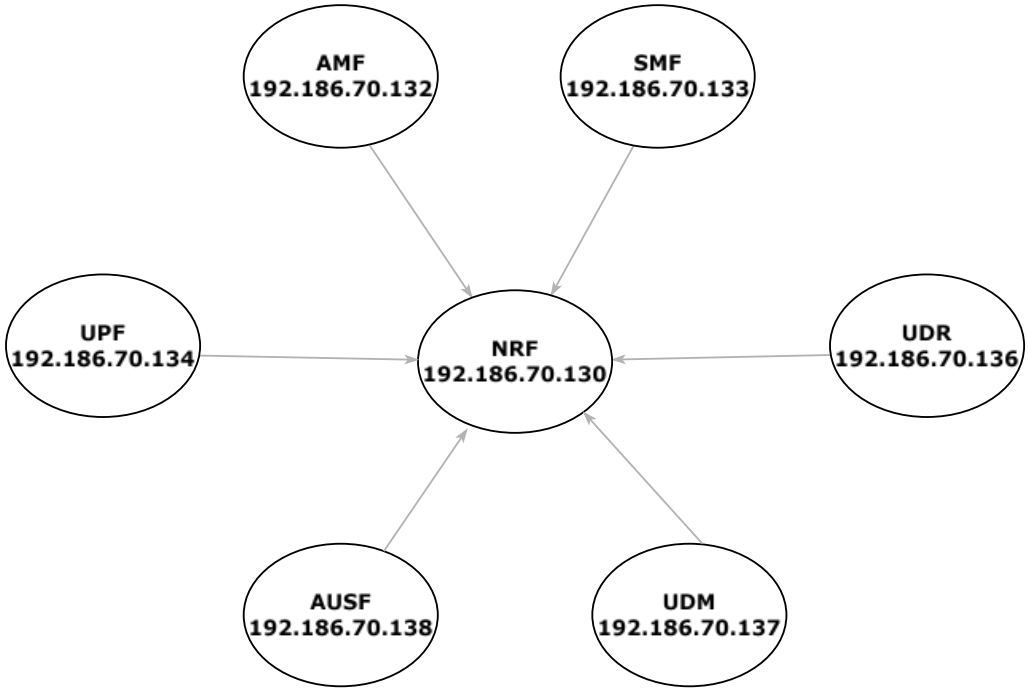


Ilustración 13. Topología identificada para el core de OAI

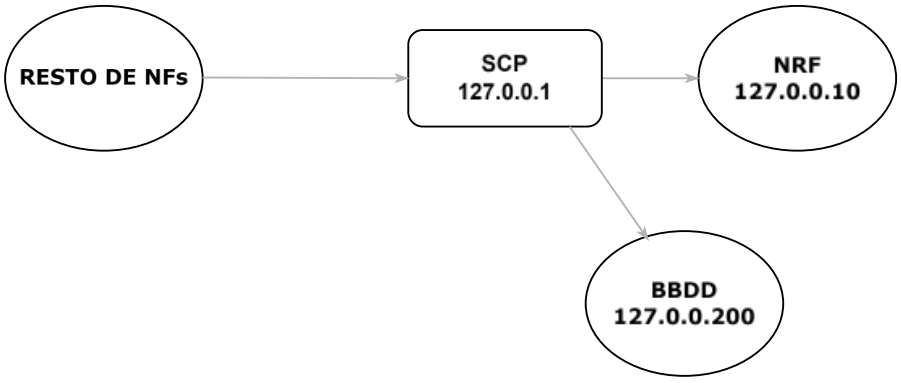


Ilustración 14. Topología identificada para el core de Open5gs

Como última actividad dentro de la fase de escaneo pasivo, se ha analizado el tipo de mensajes HTTP/2 intercambiados para tratar de identificar el comportamiento de las funciones de red. La conclusión más importante obtenida en esta fase, compartida para ambas soluciones, es que **el primer mensaje que todas las NFs envían una vez se han desplegado es un mensaje de registro al NRF utilizando el método PUT**.

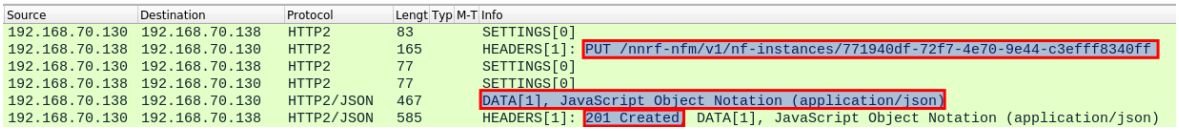


Ilustración 15. Ejemplo de registro de NF en core de OAI

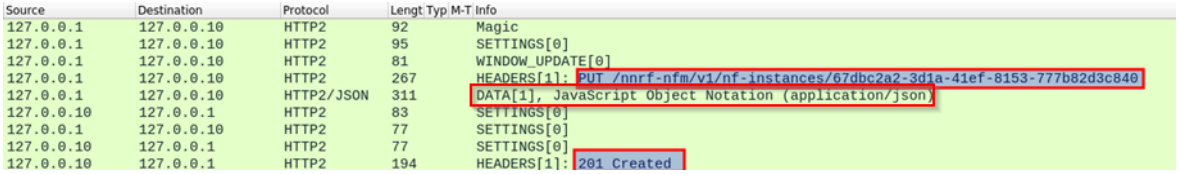


Ilustración 16. Ejemplo de registro de NF en core de Open5gs

Como se puede observar en la Ilustración 15, tomada como ejemplo en el *core* de *OAI*, este método se utiliza para indicar el registro de una función de red, comunicando al NRF una serie de parámetros en formato JSON. Este mensaje es respondido por la NRF con un código *201*, indicando que el resultado de la petición ha sido satisfactorio y que la NF solicitante ha quedado registrada dentro de la base de datos del NRF, de manera que su identidad podrá ser anunciada si se solicita algunos de los servicios que ofrece. La Ilustración 16 muestra que para *Open5gs* ocurre de forma análoga.

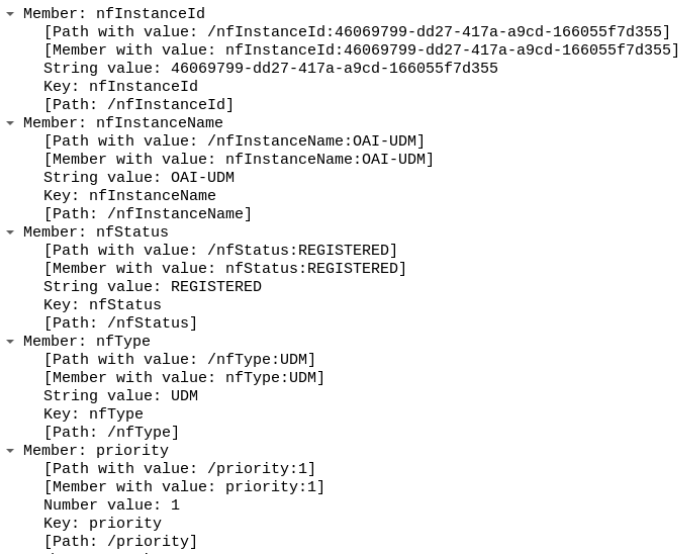


Ilustración 17. Parámetros de registro de NF en core de OAI

Por su parte, la Ilustración 17 muestra algunos de los parámetros que son intercambiados durante esta interacción. Destacan parámetros como *nfIntanceId,* una cadena de caracteres alfanuméricos que será empleada para identificar a la NF en el contexto de la red, o *priority*, un valor probablemente asociado a la prioridad que se debe tener en cuenta a la hora de anunciar una determinada instancia de una NF en lugar de otra al resto de funciones de la red. El hecho de que el tráfico no se encuentre cifrado y el contenido de los mensajes intercambiados entre funciones sea comprensible es especialmente crítico pues, como se verá en pruebas posteriores, **puede ser utilizado para configurar peticiones ilegítimas e interactuar con las NFs con propósitos maliciosos**.

6.1.2 ESCANEO ACTIVO

Los procedimientos de escaneo activo implican interactuar directamente con los sistemas objetivo enviando solicitudes y analizando las respuestas, lo cual puede ser más fácil de detectar por parte de los sistemas de seguridad, pero proporciona información más detallada y útil para la fase de reconocimiento de un ataque. En cuanto a las técnicas más comunes de escaneo activo, cabe destacar el empleo de *nmap*, una herramienta de código abierto

habitualmente utilizada en auditorías de seguridad para el escaneo y descubrimiento de redes e identificación de puertos abiertos y servicios. En este caso, en lugar de las peticiones a nivel TCP/IP realizadas por *nmap*, se utilizarán peticiones HTTP/2 creadas a mano para interactuar directamente con las funciones de red en esta fase de escaneo.

En primer lugar, se tratará de interactuar con la NRF, puesto que es la función de red que posee conocimiento sobre la existencia de todas las demás. Como ya se ha visto, la dirección IP de la NRF se puede conocer mediante técnicas de escaneo pasivo en ambas tecnologías: en *OAI*, se trata de la dirección que recibe peticiones de todas las demás, es decir, *192.168.70.130;* en *Open5gs*, se trata de la dirección que recibe los mensajes del interfaz de comunicación utilizado por el nodo SCP, en este caso, *127.0.0.10.*

Una vez se tiene conocimiento de estas direcciones, las pruebas a realizar consisten en enviar peticiones a determinadas rutas esperando obtener información sobre las NFs registradas en la red, tal como se muestra en la Ilustración 18 . Como referencia para confeccionar las rutas, se ha utilizado el estándar OpenAPI para el interfaz SBI en una arquitectura 5G [35].

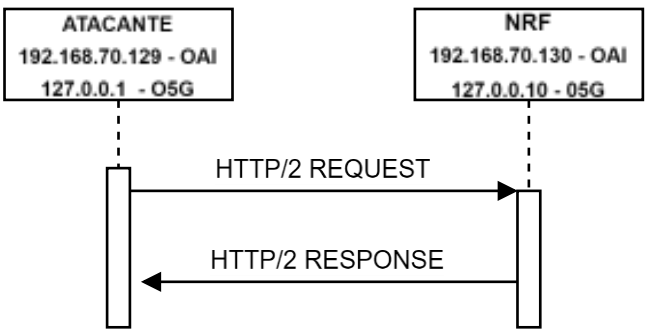


Ilustración 18. Esquema de procedimiento de escaneo activo para OAI y Open5Gs

En este caso, para ambas tecnologías ha sido posible encontrar una ruta la cual, tras aplicar una petición con método GET, es respondida con información acerca de un determinado tipo de NF en la red. Esta funcionalidad se ha implementado en la herramienta desarrollada a fin de automatizar un procedimiento de escaneo que devuelva como resultado todas las funciones de red registradas en el NRF, junto con su identificador alfanumérico y la dirección IP asociada al interfaz SBI.

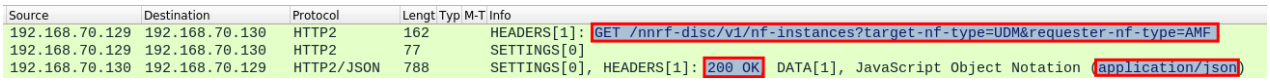


Ilustración 19. Petición a NRF para descubrimiento de NFs en OAI

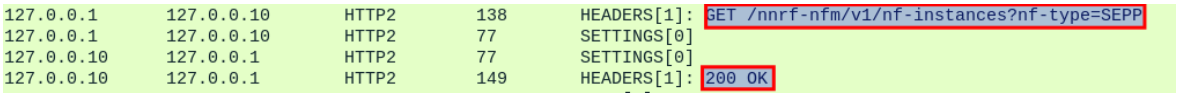


Ilustración 20. Petición a NRF para descubrimiento de NFs en Open5gs

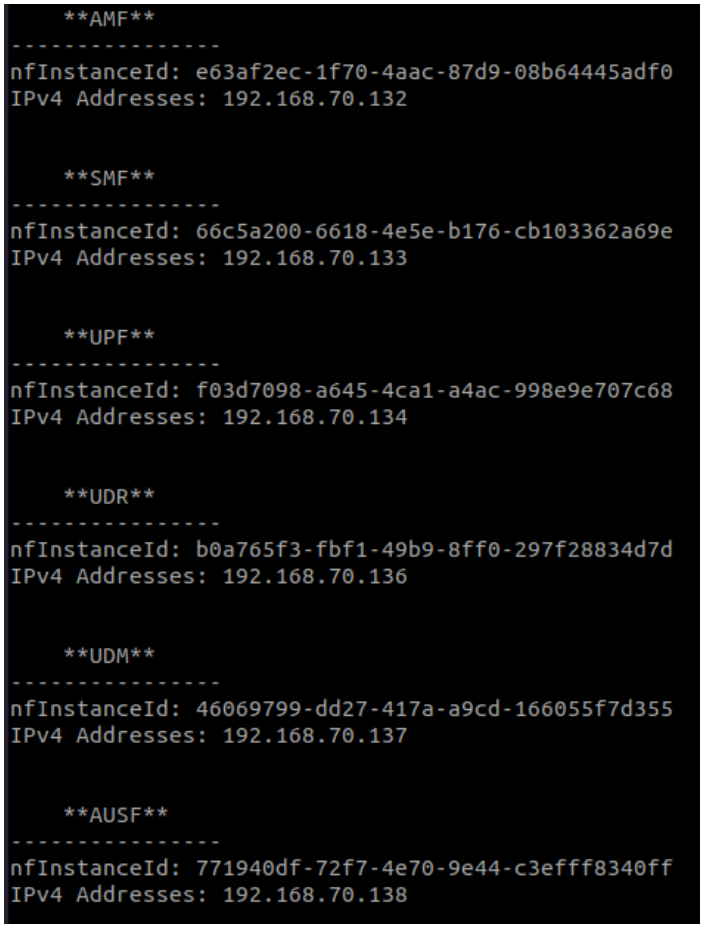


Ilustración 21. Resultado de escaneo de NFs en OAI

La Ilustración 19 muestra el aspecto de la petición enviada para la tecnología *OAI*, la cual es respondida con un mensaje portador de un JSON, en el que se indica información sobre la NF solicitada. Por su parte, la Ilustración 20 muestra a funcionalidad ejecutada para la implementación de *Open5gs,* donde se puede observar que la ruta utilizada para la petición es algo diferente.

La Ilustración 21 y la Ilustración 22 sirven para mostrar el resultado de ejecutar el escaneo de la topología en la herramienta desarrollada para ambas soluciones. Cabe destacar que la solución propuesta por *Open5gs* cuenta con un número mayor de NFs implementadas, tal y como se puede observar.

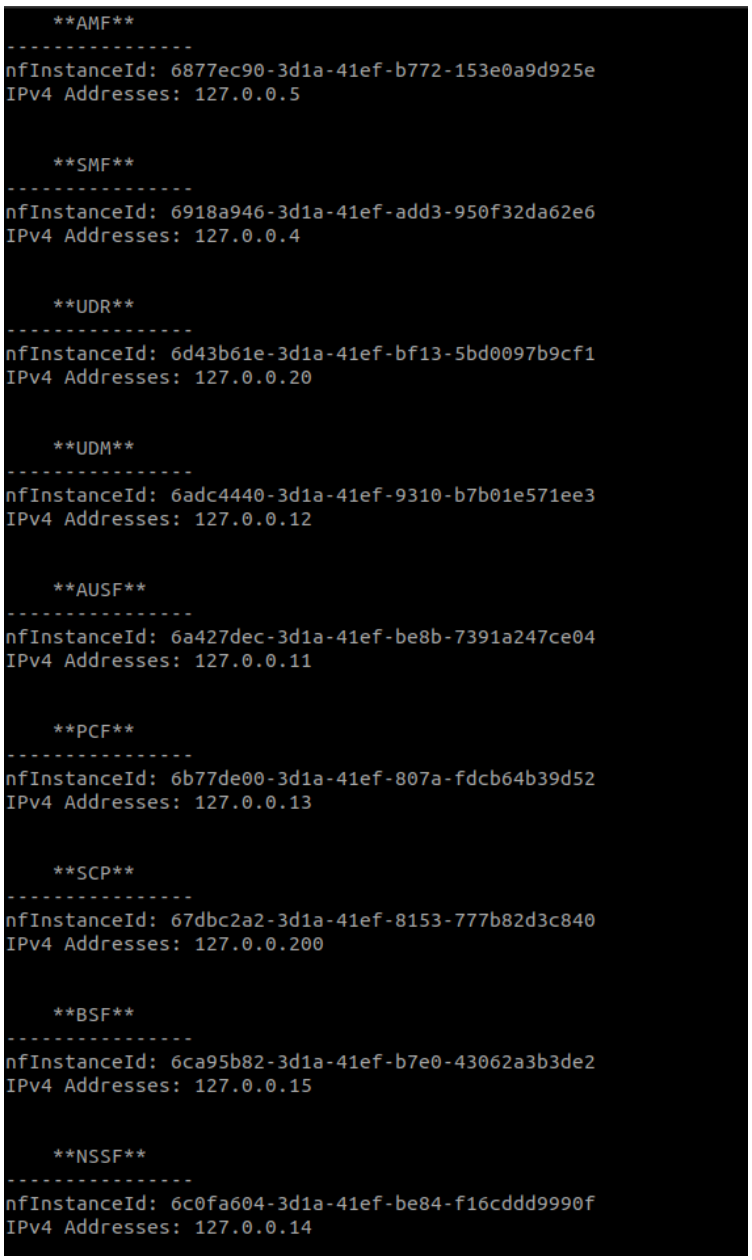


Ilustración 22. Resultado de escaneo de NFs en Open5gs

Una vez conocido el identificador asociado a cada NF, se ha empleado en la elaboración de peticiones destinadas a obtener más información sobre la implementación de una función de red concreta. La Ilustración 23 e Ilustración 24 muestran el resultado de esta prueba para la tecnología *OAI*, representando la petición enviada capturada con *Wireshark* y el resultado

de su ejecución automatizada en la herramienta para la función UPF. Este resultado se reproduce de forma análoga para *Open5gs,* sin necesidad de modificar la ruta utilizada ni ningún otro parámetro de la petición.

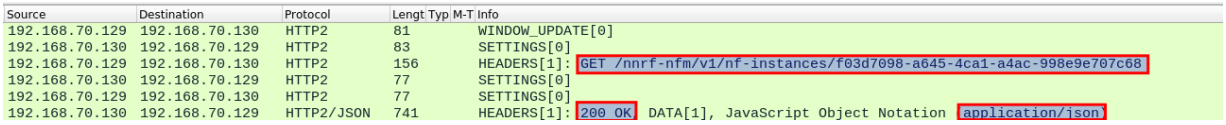


Ilustración 23. Petición a NRF para obtención de información sobre NF concreta en OAI según su UUID

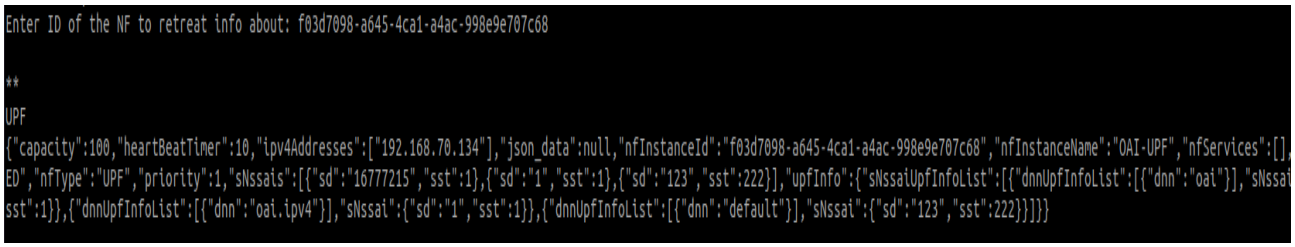


Ilustración 24. Resultado de obtención de información sobre NF concreta en OAI según su UUID

Como última prueba, se ha tratado de lograr un compromiso de confidencialidad crítico, obteniendo información sobre un usuario abonado a la red. Para ello, se ha provisionado información sobre un usuario ficticio de forma previa al despliegue de la red. Dicha información será almacenada en el UDR y debería ser accesible por el UDM mediante una consulta, pues se trata de una operación necesaria durante la fase de autenticación de un usuario.

Es este caso, la prueba ha consistido en utilizar la dirección IP vinculada al interfaz SBI del UDR para interactuar directamente con esta NF y solicitar información sobre un abonado concreto. El resultado obtenido es que, para ambas tecnologías, existe una ruta que proporciona información confidencial sobre un abonado y que es accesible sin ningún tipo de *token* ni parámetro de autorización.

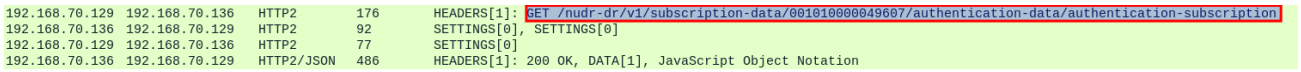


Ilustración 25. Petición al UDR para obtención de información sobre un abonado en OAI

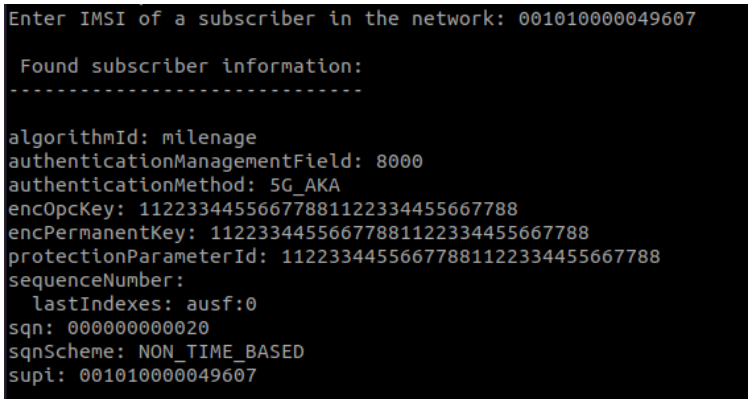


Ilustración 26. Resultado de obtención de información sobre un abonado en OAI

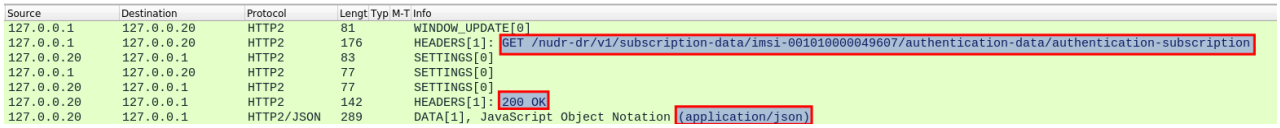


Ilustración 27. Petición al UDR para obtención de información sobre un abonado en Open5gs

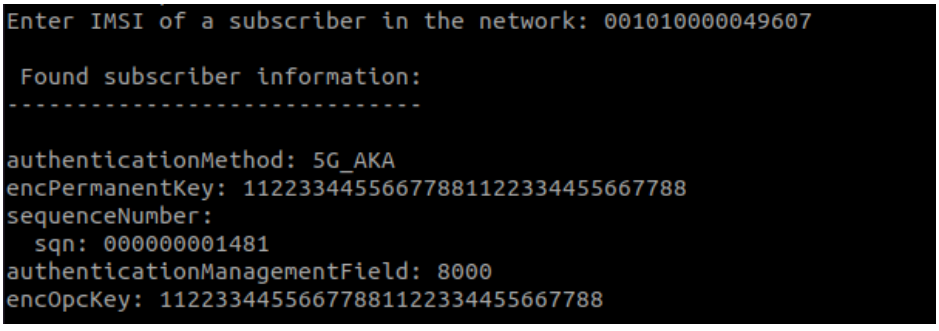


Ilustración 28. Resultado de obtención de información sobre un abonado en Open5gs

Las ilustraciones anteriores muestran la captura de la petición utilizada y el resultado de ejecutar una consulta directa al UDR, solicitando información de registro de un determinado abonado, para ambas soluciones. En ningún caso se ha requerido del uso de parámetros de autenticación y/o autorización para tener acceso a esta información, lo cual supone una vulnerabilidad con un impacto crítico para la confidencialidad de la información

Los resultados de esta primera fase de pruebas permiten concluir que **sería potencialmente posible lograr un compromiso de confidencialidad de la información en diferentes niveles**: ha sido posible descubrir la topología de la red, conocer información concreta sobre una determinada NF y tener acceso a información de un usuario almacenada en una NF.

6.2 COMPROMISO DE INTEGRIDAD

La siguiente fase de las pruebas se ha enfocado en tratar de comprometer la integridad de la red. Para ello, se ha bsucado realizar operaciones cuyo propósito sea modificar información o parámetros de las funciones de red.

En primer lugar, se ha tratado de interactuar con una NF legítima para modificar alguno de los parámetros con los que se registra por defecto en el NRF. Se ha seleccionado el parámetro *priority* para la prueba, puesto que se considera especialmente crítico, ya que modificar la prioridad de una NF a un valor de menor peso ocasionaría que dicha función se notificara a las demás con menos probabilidad.

Ilustración 29. Prioridad de AMF antes de la prueba de integridad en OAI

La Ilustración 29 muestra la información de registro del AMF en el núcleo de OAI antes de intentar comprometer su integridad, siendo posible ver que el campo *priority* posee un valor inicial de '1'.

```
192.168.70.129  192.168.70.130   HTTP2        180       HEADERS[1]: PATCH /nnrf-nfm/v1/nf-instances/e63af2ec-1f70-4aac-87d9-08b64445adf0
192.168.70.130  192.168.70.129   HTTP2        92        SETTINGS[0], SETTINGS[0]
192.168.70.129  192.168.70.130   HTTP2/JSON   130       DATA[1], JavaScript Object Notation (application/json)
192.168.70.129  192.168.70.130   HTTP2        77        SETTINGS[0]
192.168.70.130  192.168.70.129   HTTP2/JSON   977       HEADERS[1]: 200 OK, DATA[1], JavaScript Object Notation (application/json)
```

Ilustración 30. Petición para cambio de parámetro en NF para el núcleo de OAI

La Ilustración 30 muestra la petición realizada a la NRF para modificar un parámetro de una función de red registrada. En este caso, ha sido necesario emplear un método de tipo PATCH, acompañado de un archivo en formato *json* en el que se debe indicar el parámetro a modificar y el nuevo valor que se le quiere dar.

```
**
AMF
Priority of the AMF will be changed. Is that correct?
[y/n]y

NF parameters have been updated:
{"amfInfo":{"amfRegionId":"01","amfSetId":"001","guamiList":[{"amfId":"10041","plmnId":{"mcc":"901","mnc":"70"}},{"amfId":"10041","plmnId
mnc":"01"}}]},"capacity":100,"heartBeatTimer":10,"ipv4Addresses":["192.168.70.132"],"json_data":null,"nfInstanceId":"e63af2ec-1f70-4aac-8
ints":[{"ipv4Address":"192.168.70.132","port":8080,"transport":""}],"nfServiceStatus":"REGISTERED","scheme":"http","serviceInstanceId":"n
apiFullVersion":"1.0.0","apiVersionInUri":"v1"}]}],"nfStatus":"REGISTERED","nfType":"AMF","priority":10,"sNssais":[{"sd":"ffffff","sst":1
```

Ilustración 31. Prioridad de la AMF después de la prueba de integridad en OAI

El resultado de la prueba muestra que es posible realizar la modificación de un parámetro en una NF registrada en la red interactuando directamente con el NRF, sin necesidad de proporcionar información de autenticación ni autorización en la petición. En la Ilustración 31 se puede comprobar que el valor del campo *priority* ha sido modificado con éxito para la función de red AMF en OAI. Sin embargo, no ha sido posible reproducir esta misma prueba para el núcleo de *Open5gs,* pues en este caso la petición es rechazada.

El siguiente paso en la fase de pruebas de integridad ha consistido en intentar registrar una función de red falsa en el NRF, de manera que sea notificada al resto de funciones como una función legítima cuando sea solicitada.

Con este fin, se ha utilizado la información obtenida en la fase de escaneo pasivo mediante la captura de las peticiones de registro de las diferentes NFs. El análisis del contenido de estas peticiones ha permitido concluir que el registro se realiza a partir de un método PUT, acompañado de un archivo en formato *json* con información sobre los diferentes parámetros de la NF a registrar, junto con sus correspondientes valores. Esta labor se ha automatizado en la herramienta desarrollada, permitiendo a un usuario elegir el tipo de NF que desea registrar en la red y el valor que deben tomar ciertos parámetros en la misma.

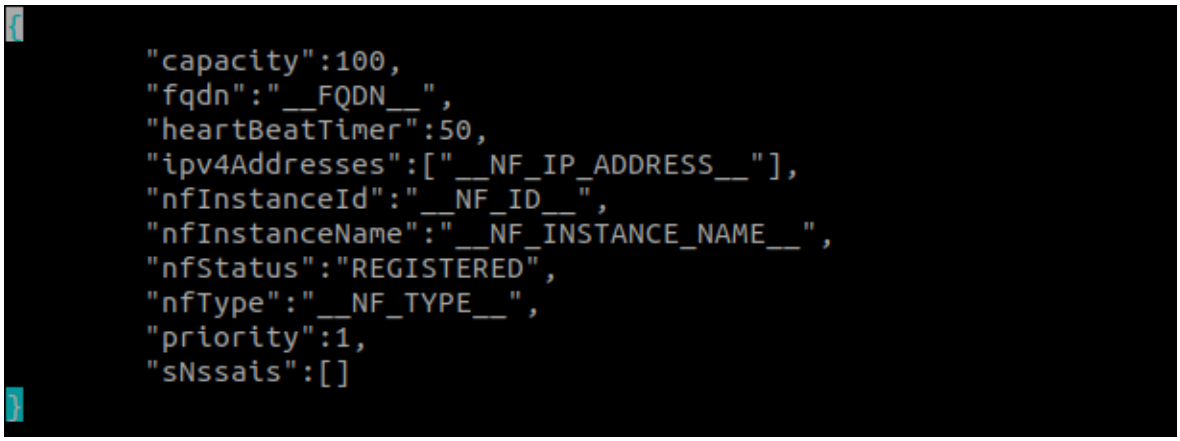


Ilustración 32. Modelo de json para registro de NF en OAI

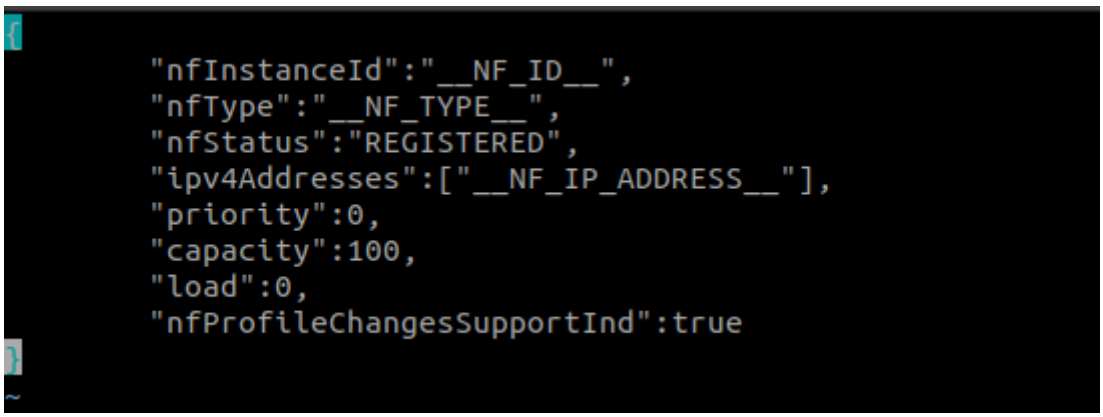


Ilustración 33. Modelo de json para registro de NF en Open5gs

Las ilustraciones Ilustración 32 y Ilustración 33 muestran el aspecto del archivo *json* utilizado para el registro de una NF falsa en ambas tecnologías, donde se puede observar que ciertos parámetros tienen un valor predefinido el cual es aceptado por la red como válido, mientras que otros son modificados con el valor indicado por el usuario en la herramienta. Se ha optado por esté método para tratar de dotar de la mayor flexibilidad posible al proceso de registro, sin dejar de asegurar que la función registrada es aceptada como legítima por parte del NRF.

```
192.168.70.129  192.168.70.130   HTTP2        180       HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/771940df-72f7-4e70-9e44-c3efff8340f1
192.168.70.129  192.168.70.130   HTTP2        77        SETTINGS[0]
192.168.70.129  192.168.70.130   HTTP2/JSON   324       DATA[1], JavaScript Object Notation (application/json)
192.168.70.130  192.168.70.129   HTTP2        77        SETTINGS[0]
192.168.70.130  192.168.70.129   HTTP2/JSON   593       HEADERS[1]: 201 Created, DATA[1], JavaScript Object Notation (application/json)
```

Ilustración 34. Petición realizada para registro de una NF falsa en OAI

```
Enter the requested paramenters to register a new NF

NF Type: UDM
NF IP Address: 192.168.70.155
NF ID: 771940df-72f7-4e70-9e44-c3efff8340f1
NF fqdn: oai-udm2
NF instance name: FAKE-UDM

NF has been registered with parameters:
{"capacity":100,"fqdn":"oai-udm2","heartBeatTimer":10,"ipv4Addresses":["192.168.70.155"],"json_data":null,"nfInstanceId":"771940df-72f7-4e70-9e44-c3efff8340f1","n
nfStatus":"REGISTERED","nfType":"UDM","priority":1,"udmInfo":{"externalGroupIdentifiersRanges":[],"gpsiRanges":[],"groupId":"","internalGroupIdentifiersRanges":[]

Keep alive started with PID: 208153
```

Ilustración 35. Resultado de registro de una NF falsa en OAI

```
Enter the requested paramenters to register a new NF

NF Type: UDM
NF IP Address: 10.0.0.10
NF ID: 6c0fa604-3d1a-41ef-be84-f16cddd99901

NF has been registered with parameters:
{"nfInstanceId":"6c0fa604-3d1a-41ef-be84-f16cddd99901","nfType":"UDM","nfStatus":"REGISTERED","heartBeatTimer":10,"plmnList":[{"mcc":"001","n

Keep alive started with PID: 7234
```

Ilustración 36. Resultado de registro de una NF falsa en Open5gs

La Ilustración 34 muestra la captura de la petición realizada en OAI, en la que es posible observar que la respuesta del NRF se caracteriza por utilizar un código *201 Created.* Esto indica que la petición ha sido realizada de manera exitosa, por lo que **se ha conseguido registrar una NF falsa en la red con ciertos parámetros cuyo valor ha sido elegido de forma arbitraria**. El formato de la petición a utilizar es el mismo para *Open5gs*

El aspecto de ejecutar esta funcionalidad en la herramienta queda plasmado en las ilustraciones Ilustración 35 y Ilustración 36, donde también es posible observar la indicación que informa sobre el inicio de un proceso paralelo de tipo *keep alive.*

Este proceso es necesario para asegurar que la nueva función creada permanece registrada por tiempo indefinido, ya que la información obtenida en la fase de escaneo pasivo también permite concluir que todas las funciones de red registradas envían al NRF, de forma periódica, un mensaje con el método PATCH mediante el que actualizan su estado. Este proceso se encuentra definido en los estándares publicados por el 3GPP, concretamente en la especificación TS 29.510 [36], donde se indica que las NFs deben enviar mensajes con el método PATCH para actualizar su estado y asegurarse de que sus servicios sigan registrados y disponibles en el NRF.

Es por ello que, para realizar el registro de una función de red falsa, es necesario implementar de alguna forma este procedimiento de actualización de estado, pues de lo contrario el NRF consideraría que dicha NF ha dejado de estar disponible y, consecuentemente, la eliminaría de su base de datos.

Como confirmación de éxito de esta prueba, en las ilustraciones Ilustración 37 y Ilustración 38 se puede observar cómo, ante un nuevo procedimiento de escaneo en el que se consulta a la NRF con información sobre las diferentes funciones de red registradas, la respuesta contiene los datos de la NF falsa que se ha registrado previamente, en este caso como una nueva instancia de UDM.

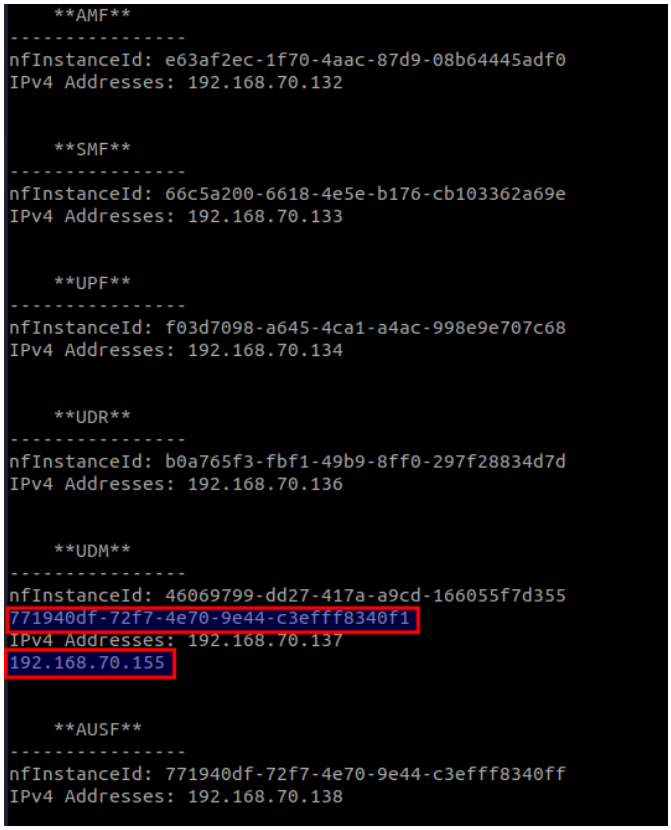


Ilustración 37. Escaneo de funciones de red tras registro de NF falsa en OAI

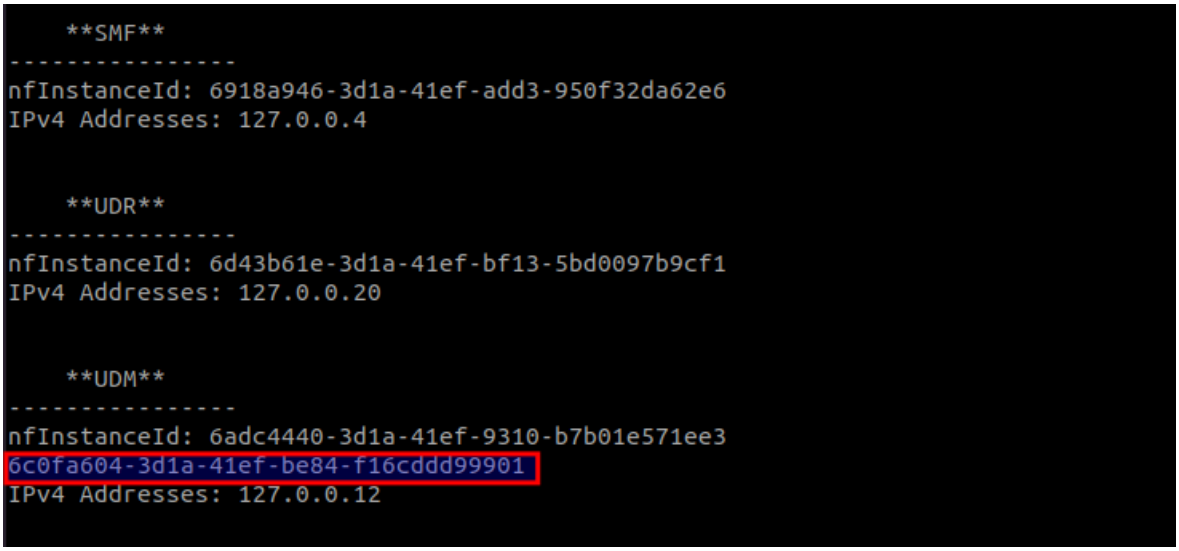
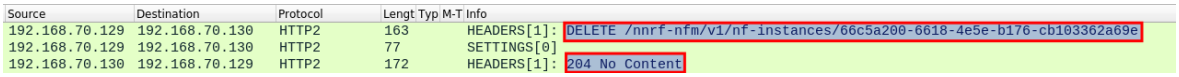


Ilustración 38. Escaneo de funciones de red tras registro de NF falsa en Open5gs

6.3 COMPROMISO DE DISPONIBILIDAD

Como última fase de las pruebas de seguridad, se ha tratado de comprometer la disponibilidad de la red. Para ello, se ha estudiado la forma de causar una disrupción en el servicio proporcionado por la arquitectura 5G, a través del empleo de peticiones sobre el protocolo HTTP/2.

La conclusión alcanzada es que la forma más sencilla de ocasionar un compromiso de disponibilidad minimizando el tráfico inyectado a la red es interactuar directamente con el NRF y notificar que una de las funciones registradas deja de estar disponible. Se ha encontrado una ruta en la cual es posible indicar un identificador de NF y utilizar un método de tipo DELETE para conseguir **que una función de red previamente registrada sea eliminada de la base de datos del NRF.** Esta ruta es compartida para ambas soluciones, por lo que únicamente se adjuntan evidencias para una de ellas.



Source	Destination	Protocol	Lengt	Typ	M-T	Info
192.168.70.129	192.168.70.130	HTTP2	163			HEADERS[1]: DELETE /nnrf-nfm/v1/nf-instances/66c5a200-6618-4e5e-b176-cb103362a69e
192.168.70.129	192.168.70.130	HTTP2	77			SETTINGS[0]
192.168.70.130	192.168.70.129	HTTP2	172			HEADERS[1]: 204 No Content

Ilustración 39. Petición para eliminar el registro de una NF en el core de OAI

La Ilustración 39 muestra el resultado de enviar dicha petición, mediante una captura del tráfico con *Wireshark.* Se puede observar que la respuesta de la NRF emplea un código de tipo *204 No Content* para informar de que la función indicada ha dejado de estar registrada en la red.

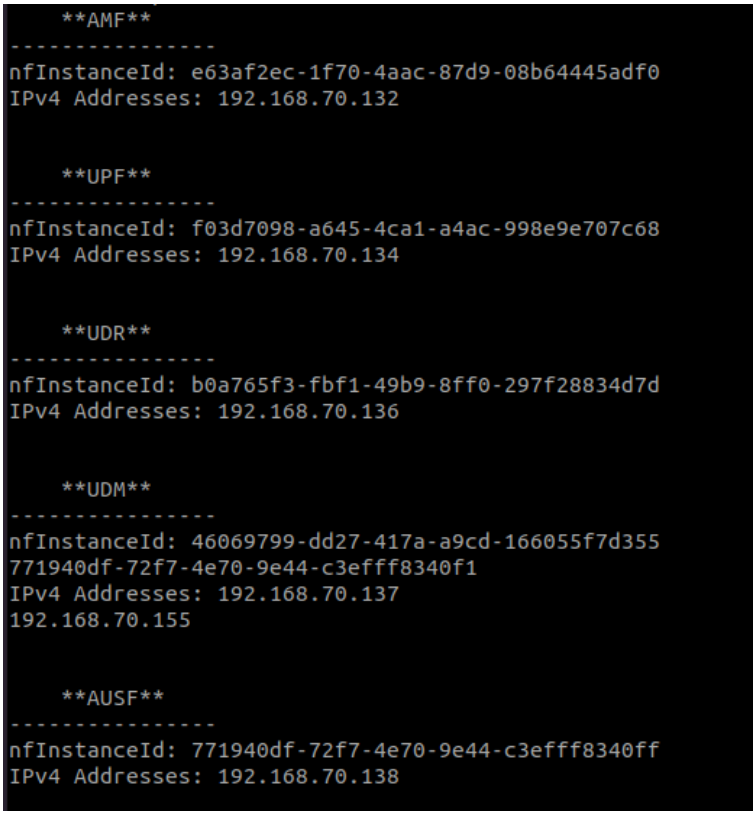


Ilustración 40. Resultado de escaneo tras eliminar registro de una NF en el core de OAI

Por otro lado, la Ilustración 40 nos ofrece el resultado de realizar un escaneo sobre las funciones de red disponibles tras haber ejecutado la petición anterior. Es este caso, se puede comprobar que la SMF, la función de red utilizada para ilustrar esta prueba, ha dejado de ser anunciada como una función de red válida.

El impacto potencial que tendría este suceso en términos de disponibilidad es muy alto, pues cualquier usuario que deseara hacer uso de los servicios de comunicación de la red necesitaría que se le asignase una sesión, para lo cual la función AMF debe de hacer una serie de consultas previas al SMF. Sin embargo, si esta función de red no pudiera ser anunciada por el NRF, el AMF no sería conocedor de ninguna instancia de SMF y no podría seguir con la operativa de gestionar una sesión de comunicación para un usuario, lo que derivaría en una denegación de servicio en la red.

Capítulo 7. CONCLUSIONES Y TRABAJOS FUTUROS

7.1 CONCLUSIONES

El primer objetivo de este último capítulo del documento es poner en relieve las conclusiones obtenidas a partir de la realización del mismo. Se ha considerado importante remarcar tanto aprendizajes obtenidos a partir del estudio del marco teórico y el análisis de seguridad de una arquitectura 5G, como las conclusiones aportadas por las pruebas de seguridad realizadas sobre un entorno de laboratorio sustentado en el uso de herramientas *open source.*

En cuanto a los puntos a destacar sobre el estudio teórico de la cuestión:

- El análisis de seguridad ha permitido concluir que existen ciertos escenarios mediante los que un adversario podría ganar acceso al núcleo de red dentro de la infraestructura 5G de una operadora. Además, el estado del arte presenta algunos autores que teorizan sobre la posibilidad de que las operadoras no hayan realizado una implementación rigurosa de los mecanismos de seguridad especificados para el núcleo de red. Por ello, se considera realista el escenario en el que un atacante pueda ganar acceso al núcleo e interactuar directamente con las funciones de red, utilizando el protocolo HTTP/2
- El empleo de HTTP/2 como protocolo de comunicación en la red 5G supone un riesgo de seguridad a tener en cuenta, pues se trata de un protocolo cuyo uso se encuentra muy extendido en el ecosistema IT, por lo que es más probable que un atacante que lograse ganar acceso al núcleo de red tuviera los conocimientos prácticos para interpretar el tráfico y utilizar la información obtenida para elaborar ataques. El objetivo de las pruebas de seguridad ha ido encaminado a poner de manifiesto la criticidad del impacto que esta situación podría ocasionar sobre la seguridad de la red.
- El uso de herramientas de código abierto para crear entornos de red 5G de laboratorio ofrece múltiples ventajas: reduce costes asociados, permite alta personalización del

entorno, cuenta con el respaldo de comunidades activas y facilita la realización de pruebas de seguridad documentables y reproducibles.

En cuanto a los puntos más destacables sobre la parte práctica del trabajo, basada en el estudio de seguridad de las implementaciones del núcleo de red asociadas a los proyectos de código abierto de *OpenAirInteface* y *Open5gs*:

- Ninguna de las soluciones emplea, por defecto, un mecanismo de cifrado para el tráfico intercambiado entre las funciones de red, aunque *Open5gs* sí permite modificar ciertas opciones de configuración para hacer uso de TLS. El hecho de que no se utilice un mecanismo de cifrado ha permitido, mediante técnicas de reconocimiento pasivo, la interceptación del tráfico y la interpretación de su contenido, la cual permite obtener información valiosa para interactuar con las funciones de red.
- Ninguna de las soluciones implementa mecanismos de autenticación y/o autorización sobre las peticiones realizadas con HTTP/2 al interfaz SBI de las funciones de red. Este hecho supone un riesgo crítico de la seguridad, pues permite que peticiones HTTP/2 enviadas desde cualquier origen sean capaces de iniciar la ejecución de procedimientos que pueden afectar a diferentes dimensiones de seguridad de la arquitectura.
- Partiendo de un entorno en el que se tiene acceso al núcleo de la red 5G y se descubre que no hay mecanismos de cifrado ni autorización asociados a la comunicación entre las funciones de red, es posible lograr compromisos en términos de confidencialidad, integridad y disponibilidad con un impacto potencial crítico para la seguridad de la red.

7.2 FUTURAS LÍNEAS DE TRABAJO

Como último propósito de este capítulo, se procede a plantear dos líneas de investigación que podrían servir para continuar o ampliar el alcance de este proyecto:

- La primera línea de investigación se centraría en el uso de técnicas de *fuzzing* para alterar el contenido de las peticiones HTTP/2. Este procedimiento de ataque consiste en enviar una serie de datos aleatorios, malformados o inesperados como entradas en las peticiones HTTP/2 para observar cómo responde el sistema. Se trata de un proceso fácilmente automatizable y que podría servir para encontrar vulnerabilidades que permitiesen a un atacante, no solo interactuar con la API del interfaz SBI implementada en las distintas funciones de red, sino afectar al propio *software* en ejecución de la función.
- La segunda línea de investigación se enfocaría en probar ataques conocidos al protocolo TLS, asumiendo que este se utiliza para proteger el tráfico en el núcleo de la red 5G. Esta investigación examinaría la resistencia de la implementación de TLS en el núcleo de una red 5G a varios tipos de ataques, como ataques de intermediario (MITM), renegociación insegura y otros vectores de explotación conocidos. Al probar la robustez del protocolo TLS en este contexto, se podrían identificar debilidades específicas y proponer medidas de mitigación para fortalecer la seguridad del tráfico en la red 5G, asegurando una protección adecuada contra intentos de interceptación y manipulación de tráfico.

Ambas líneas de trabajo están íntimamente relacionadas con el objeto de estudio de este proyecto y podría contribuir a ampliar la cantidad y calidad de los resultados obtenidos, con el fin último de contribuir de forma activa a mejorar la seguridad de las implementaciones de arquitecturas 5G.

Capítulo 8. BIBLIOGRAFÍA

[1] «¿cómo funciona una red móvil? - Las ondas», https://radio-waves.orange.com/. Accedido: 27 de mayo de 2024. [En línea]. Disponible en: https://radio-waves.orange.com/es/como-funciona-una-red-movil/

[2] «What is GSM (Global System for Mobile communication)?», Mobile Computing. Accedido: 27 de mayo de 2024. [En línea]. Disponible en: https://www.techtarget.com/searchmobilecomputing/definition/GSM

[3] J. P. García y D. P. Conde, *Hacking y seguridad en comunicaciones móviles GSM-GPRS-UMTS-LTE*. ZeroxWord Computing, 2014. [En línea]. Disponible en: https://books.google.es/books?id=rmAfrgEACAAJ

[4] M. Bartock, «LTE Security - How Good is it?».

[5] «China sends "world's first 6G" test satellite into orbit». Accedido: 28 de mayo de 2024. [En línea]. Disponible en: https://www.bbc.com/news/av/world-asia-china-54852131

[6] «Concepción de las IMT – Marco y objetivos generales del futuro desarrollo de las IMT para 2020 y en adelante».

[7] «5 Examples of M2M in Use», Top Connect. Accedido: 29 de mayo de 2024. [En línea]. Disponible en: https://topconnect.com/m2m-iot-connectivity/5-examples-of-m2m-in-use/

[8] «Practicada la primera operación teleasistida con 5G», www.nationalgeographic.com.es. Accedido: 29 de mayo de 2024. [En línea]. Disponible en: https://www.nationalgeographic.com.es/ciencia/actualidad/practicada-primera-operacion-teleasistida-5g_13948

[9] «Beamforming». Accedido: 29 de mayo de 2024. [En línea]. Disponible en: https://es.mathworks.com/discovery/beamforming.html

[10] «5G System Overview». Accedido: 30 de mayo de 2024. [En línea]. Disponible en: https://www.3gpp.org/technologies/5g-system-overview

[11] Ministerio para la Transformación Digital y de la Función Pública, *Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G*, vol. BOE-A-2024-8715. 2024, pp. 49754-49801. Accedido: 30 de mayo de 2024. [En línea]. Disponible en: https://www.boe.es/eli/es/rd/2024/04/30/443

[12] M. van der Kleij, «Blog - What is Service Based Architecture for 5G System», TUCANA. Accedido: 9 de julio de 2024. [En línea]. Disponible en: https://www.tucana.com/news/blog-what-is-service-based-architecture-for-5g-system/

[13] *5G core networks: powering digitalization*. London (GB) San Diego (Calif.): Elsevier AP, Academic press, an imprint of Elsevier, 2020.

[14] 3GPP, «System architecture for the 5G System (5GS); TS 23.501 ; V17.7.0». 2022.

[15] «5G Training Catalogue - Apis Training». Accedido: 9 de julio de 2024. [En línea]. Disponible en: https://apistraining.com/training-catalogue/5g-training/

[16] 3GPP, «Security architecture and procedures for 5G system; TS 33.501 ; V17.8.0». 2022.

[17] «A Comparative Introduction to 4G and 5G Authentication», CableLabs. Accedido: 6 de junio de 2024. [En línea]. Disponible en: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication

[18] «1.5. Messages - HTTP: The Definitive Guide [Book]». Accedido: 9 de julio de 2024. [En línea]. Disponible en: https://www.oreilly.com/library/view/http-the-definitive/1565925092/ch01s05.html

[19] «HTTP Messages - HTTP | MDN». Accedido: 10 de junio de 2024. [En línea]. Disponible en: https://developer.mozilla.org/en-US/docs/Web/HTTP/Messages

[20] «HTTP/2 vs. HTTP/1.1». Accedido: 11 de junio de 2024. [En línea]. Disponible en: https://www.cloudflare.com/es-es/learning/performance/http2-vs-http1.1/

[21] «What Is a TLS/SSL Handshake and How It Works», Sematext. Accedido: 12 de junio de 2024. [En línea]. Disponible en: https://sematext.com/glossary/ssl-tls-handshake/

[22] G. M. Køien, «On Threats to the 5G Service Based Architecture», *Wirel. Pers. Commun.*, vol. 119, n.º 1, pp. 97-116, jul. 2021, doi: 10.1007/s11277-021-08200-0.

[23] N. Wehbe, H. A. Alameddine, M. Pourzandi, E. Bou-Harb, y C. Assi, «A Security Assessment of HTTP/2 Usage in 5G Service-Based Architecture», *IEEE Commun. Mag.*, vol. 61, n.º 1, pp. 48-54, ene. 2023, doi: 10.1109/MCOM.001.2200183.

[24] X. Hu, C. Liu, S. Liu, W. You, y Y. Zhao, «Signalling Security Analysis: Is HTTP/2 Secure in 5G Core Network?», en *2018 10th International Conference on Wireless Communications and Signal Processing (WCSP)*, Hangzhou: IEEE, oct. 2018, pp. 1-6. doi: 10.1109/WCSP.2018.8555612.

[25] F. Giambartolomei, M. Barceló, A. Brighente, A. Urbieta, y M. Conti, «Penetration Testing of 5G Core Network Web Technologies». arXiv, 4 de marzo de 2024. Accedido: 7 de mayo de 2024. [En línea]. Disponible en: http://arxiv.org/abs/2403.01871

[26] A. Bui, «Analysing open-source 5G core networks for TLS vulnerabilities and 3GPP compliance», RADBOUD UNIVERSITY, 2023.

[27] F. Dolente, R. G. Garroppo, y M. Pagano, «A Vulnerability Assessment of Open-Source Implementations of Fifth-Generation Core Network Functions», *Future Internet*, vol. 16, n.º 1, p. 1, dic. 2023, doi: 10.3390/fi16010001.

[28] «OpenAirInterface – 5G software alliance for democratising wireless innovation». Accedido: 18 de junio de 2024. [En línea]. Disponible en: https://openairinterface.org/

[29] «https://open5gs.org/». Accedido: 18 de junio de 2024. [En línea]. Disponible en: https://open5gs.org/

[30] «srsRAN Project - Open Source RAN». Accedido: 18 de junio de 2024. [En línea]. Disponible en: https://www.srslte.com/

[31] E. R. Brand a National Instruments, «USRP B200MINI-I (1X1, 70 MHZ - 6 GHZ)», Ettus Research. Accedido: 2 de julio de 2024. [En línea]. Disponible en: https://www.ettus.com/all-products/usrp-b200mini-i-2/

[32] «Ubuntu 20.04.6 LTS (Focal Fossa)». Accedido: 2 de julio de 2024. [En línea]. Disponible en: https://releases.ubuntu.com/focal/

[33] «BOE-A-2024-8715 Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G.» Accedido: 3 de julio de 2024. [En línea]. Disponible en: https://www.boe.es/eli/es/rd/2024/04/30/443

[34] «Amenaza vs vulnerabilidad: cómo diferenciarlos | Empresas | INCIBE». Accedido: 3 de julio de 2024. [En línea]. Disponible en: https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-diferenciarlos

[35] J. de Gregorio, «jdegre/5GC_APIs». 2 de julio de 2024. Accedido: 5 de julio de 2024. [En línea]. Disponible en: https://github.com/jdegre/5GC_APIs

[36] 3GPP, «5G System; Network function repository services; TS 29.510 ; V17.7.0». 2022.

ANEXO A. ALINEACIÓN CON LOS ODS

Los Objetivos de Desarrollo Sostenible (ODS) son un conjunto de 17 metas globales adoptadas por todos los Estados Miembros de las Naciones Unidas en 2015 como parte de la Agenda 2030 para el Desarrollo Sostenible. Estos objetivos buscan abordar los principales desafíos globales, marcando diferentes metas a alcanzar en los próximos años con el propósito de avanzar en esta labor de desarrollo y cooperación entre Estados.

El contenido de este proyecto se puede considerar alineado con los siguientes objetivos:

Educación de calidad: Este proyecto se puede considerar alineado con el ODS 4, pues se fomenta el estudio de la tecnología 5G y de diferentes herramientas de código abierto. Estas soluciones *open source* pueden tener una gran utilidad en el aspecto formativo de profesionales que trabajen en la mejora de la seguridad en infraestructuras 5G.

Industria, Innovación e Infraestructura: Este trabajo se alinea con el ODS 9, ya que promueve la innovación tecnológica y el desarrollo de infraestructuras más seguras. La mejora de la seguridad de las redes 5G es esencial para asegurar que aquellas tecnologías que se apoyen en estas redes para labores de comunicación sean menos susceptibles de poseer vulnerabilidades que permitan la materialización de amenazas. Esto es crucial para el desarrollo de infraestructuras que soporten la industria 4.0, paradigmas como *IoT* y otras aplicaciones avanzadas, garantizando que estas sean resistentes a ciberataques y funcionen de manera eficiente y segura.

Paz, Justicia e Instituciones sólidas: El proyecto se alinea con el ODS 16, que promueve sociedades pacíficas e inclusivas, acceso a la justicia para todos y la construcción de instituciones eficaces, responsables e inclusivas. Mejorar la seguridad de las redes 5G es esencial para proteger la integridad y confidencialidad de los datos, garantizando así la privacidad de los usuarios y fortaleciendo la confianza en las instituciones digitales.

ANEXO B. DESCARGA E INSTALACIÓN DE HERRAMIENTAS *OPEN SOURCE*

-OPEN AIR INTERFACE-

Para trabajar con el núcleo de red de *OpenAirInterface* es recomendable seguir la guía disponible en el repositorio oficial del proyecto, accesible desde el siguiente enlace:

```
https://gitlab.eurecom.fr/oai/cn5g/oai-cn5g-fed/-
/blob/master/docs/DEPLOY_HOME.md
```

A continuación, se resumen los pasos necesarios para efectuar su instalación en una plataforma Ubuntu 20.04:

1. Descarga de las imágenes de Docker

De forma previa a la instalación del núcleo de red, se necesita contar con la instalación de las herramientas *Docker (mínimo versión 19.03), Docker-compose (mínimo versión 1.27)* y *python3* en el equipo. Seguidamente, se procede a descargar las imágenes de los nodos de red, disponibles en el repositorio oficial de OAI:

```
docker pull oaisoftwarealliance/oai-amf:v2.0.1
docker pull oaisoftwarealliance/oai-nrf:v2.0.1
docker pull oaisoftwarealliance/oai-upf:v2.0.1
docker pull oaisoftwarealliance/oai-smf:v2.0.1
docker pull oaisoftwarealliance/oai-udr:v2.0.1
docker pull oaisoftwarealliance/oai-udm:v2.0.1
docker pull oaisoftwarealliance/oai-ausf:v2.0.1
docker pull oaisoftwarealliance/oai-upf-vpp:v2.0.1
docker pull oaisoftwarealliance/oai-nssf:v2.0.1
docker pull oaisoftwarealliance/oai-pcf:v2.0.1
docker pull oaisoftwarealliance/oai-nef:v2.0.1
docker pull oaisoftwarealliance/trf-gen-cn5g:latest
```

2. Clonación del repositorio oficial

El siguiente paso consiste en clonar el repositorio oficial del proyecto, asegurando estar en la rama adecuada:

```
git clone --branch v2.0.1 https://gitlab.eurecom.fr/oai/cn5g/oai-cn5g-fed.git
cd oai-cn5g-fed
git checkout -f v2.0.1

# Synchronize all git submodules
./scripts/syncComponents.sh
```

3. Ejecución de los contenedores

Una vez clonado el repositorio del proyecto, simplemente se debe ejecutar un *script* que automatiza el despliegue de los contenedores en *Docker:*

```
cd docker-compose
python3 core-network.py
```

-OPEN5GS-

Para trabajar con la implementación del núcleo de red de *Open5gs,* es recomendable seguir la documentación oficial del proyecto, disponible en el siguiente enlace:

```
https://open5gs.org/open5gs/docs/guide/02-building-open5gs-from-sources/
```

A continuación, se resumen los pasos necesarios para efectuar su instalación en una plataforma Ubuntu 20.04:

1. Instalar MongoDB

En primer lugar es necesario instalar el servicio MongoDB, el cual será usado como gestor de base de datos por el núcleo de la red.

Para ello, se debe instalar la herramienta GNU Privacy Guard:

```
sudo apt update
sudo apt install gnupg
```

Posteriormente, se debe importar la clave pública utilizada por el gestor de paquetes e importar el repositorio de MongoDB como una fuente válida para el propio gestor.

```
curl -fsSL https://pgp.mongodb.com/server-6.0.asc | sudo gpg -o
/usr/share/keyrings/mongodb-server-6.0.gpg –dearmor

echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-
6.0.gpg] https://repo.mongodb.org/apt/ubuntu $(UBUNTU_CODENAME)/mongodb-
org/6.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list
```

Una vez hecho esto, ya es posible instalar los paquetes de MongoDB utilizando el gestor *apt*:

```
sudo apt update
```

```
sudo apt install -y mongodb-org
```

2. Configuración de interfaz TUN

La ejecución del *core* de *Open5gs* requiere crear previamente un interfaz TUN, que servirá para dar salida del tráfico hacia internet. Esto se puede realizar mediante los siguientes comandos:

```
sudo ip tuntap add name ogstun mode tun
sudo ip addr add 10.45.0.1/16 dev ogstun
sudo ip addr add 2001:db8:cafe::1/48 dev ogstun
sudo ip link set ogstun up
```

3. Clonar el repositorio e instalar los archivos

El siguiente paso consiste en clonar el repositorio del proyecto:

```
git clone https://github.com/open5gs/open5gs
```

Posteriormente, es posible compilar el código con *meson* y construir la herramienta con *ninja:*

```
meson build --prefix=`pwd`/install
ninja -C build
```

Es recomendable comprobar si ha habido algún error durante la compilación ejecutando el siguiente *script*:

```
./build/tests/registration/registration
```

También existen una serie de programas de *test* a ejecutar para verificar que la instalación se ha preparado adecuadamente:

```
cd build
sudo pkill -9 open5gs
sudo meson test -v
```

El último paso consiste en ejecutar la instalación de los binarios que constituyen el *core* de *Open5gs* en el equipo:

```
Perform the installation process:
```
cd build
ninja install
cd ../
```
```

-SRSRAN-

Para trabajar con la implementación del gNB de *srsRan* es recomendable seguir la documentación oficial disponible en la página web del proyecto:

```
https://docs.srsran.com/projects/project/en/latest/user_manuals/source/installation.html
```

A continuación, se resumen los pasos necesarios para efectuar su instalación en una plataforma Ubuntu 20.04:

4. Instalación de dependencias

Las dependencias necesarias para este proyecto se puede instalar automáticamente en Ubuntu utilizando el gestor de paquetes *apt*, mediante el siguiente comando:

```
sudo apt-get install cmake make gcc g++ pkg-config libfftw3-dev libmbedtls-dev libsctp-dev libyaml-cpp-dev libgtest-devg
```

5. Instalación de *drivers* de RF

Actualmente, este proyecto únicamente soporta el uso de los *drivers* de RF de los dispositivos UHD. Por ello, se recomienda descargar los mismo desde el repositorio oficial:

```
https://github.com/EttusResearch/uhd
```

**Nota: se recomienda utilizar la versión más reciente de UHD, p.e, 3.15 o 4.0*

6. Clonar el repositorio e instalar los archivos

El primer paso consiste en clonar el repositorio del proyecto:

```
git clone https://github.com/srsRAN/srsRAN_Project.git
```

Seguidamente, se deben ejecutar los siguientes comandos para compilar el código y construir la herramienta:

```
cd srsRAN_Project
mkdir build
cd build
cmake ../
make -j $(nproc)
make test -j $(nproc)
```

Si el resultado de la compilación es positivo, se puede proceder a ejecutar el nodo gNB desde la ruta:

```
srsRAN_Project/build/apps/gnb/
```