Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1814

(09/2022)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de las IMT-2020

Directrices de seguridad de los sistemas de comunicaciones IMT-2020

Recomendación UIT-T X.1814

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad de las aplicaciones	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Correo certificado	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1400–X.1429
Seguridad de las aplicaciones (2)	X.1450–X.1459
Seguridad de la web (2)	X.1470–X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590–X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de los datos	X.1770–X.1789
SEGURIDAD DE IMT-2020	**X.1800–X.1819**

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1814

Directrices de seguridad de los sistemas de comunicaciones IMT-2020

Resumen

Los dispositivos de la Internet de las cosas (IoT) conectados y las aplicaciones móviles necesitan un acceso a redes inalámbricas que sea resiliente, seguro y capaz de proteger la privacidad de las personas. Los sistemas de comunicaciones IMT-2020 deberían diseñarse conforme a estos requisitos de alto nivel. Es preciso definir un marco de seguridad para los sistemas de comunicaciones IMT-2020 que pueda servir de base para preparar una Recomendación técnica detallada sobre asuntos relacionados con la seguridad de IMT-2020.

En la Recomendación UIT-T X.1814 se identifican todos los componentes relacionados con la seguridad de los sistemas de comunicaciones IMT-2020 y se definen directrices de seguridad para dichos sistemas. Describe una arquitectura genérica de las IMT-2020 y sus dominios. También se definen las amenazas existentes y se especifican los requisitos aplicables a las capacidades de seguridad de cada componente, teniendo en cuenta las características únicas de la red. Esta Recomendación se basa en la arquitectura de seguridad 5G 3GPP.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1814	02-09-2022	17	11.1002/1000/14992

Palabras clave

Amenazas, capacidad, computación periférica multiacceso, directrices de seguridad, segmentación de la red, sistema de comunicación IMT-2020, virtualización de la red.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente o derecho de autor, que pueda ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Recomendación UIT-T X.1814

Directrices de seguridad de los sistemas de comunicaciones IMT-2020

1 Alcance

En la presente Recomendación se facilitan directrices de seguridad para el desarrollo de sistemas de comunicaciones IMT-2020. A tal efecto, se analizan todos los componentes relacionados con la seguridad de estos sistemas, es decir, los equipos de usuario, las redes de acceso y las redes troncales. Describe una arquitectura genérica de las IMT-2020 y sus dominios. Además se definen las amenazas existentes y se especifican los requisitos aplicables a las capacidades de seguridad de cada componente, teniendo en cuenta las características únicas de la red, incluidas la computación periférica de acceso múltiple, la interconexión de redes definidas por software, la virtualización dinámica de las funciones de red y la segmentación de la red. Esta Recomendación se basa en la arquitectura de seguridad 5G 3GPP.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación

[UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[UIT-T X.1038] Recomendación UIT-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.

3 Definiciones

3.1 Términos definidos en otros documentos

3.1.1 En la presente Recomendación se utilizan los siguientes términos de [UIT-T X.800]:

– control de acceso;
– autenticación;
– disponibilidad;
– confidencialidad;
– integridad de los datos;
– privacidad;
– repudio;
– servicio de seguridad.

Además, se utilizan los siguientes términos adicionales, definidos en otros documentos:

3.1.2 control [b-UIT-T X.1408]: Medida que modifica el riesgo.

NOTA 1 – Los controles incluyen todo proceso, política, dispositivo, práctica o medida capaz de modificar el riesgo.

NOTA 2 – Cabe la posibilidad de que los controles no siempre produzcan el efecto de modificación previsto o supuesto.

3.1.3 ataque de denegación de servicio distribuida (DDoS) [b-UIT-T Y.4807]: Acceso no autorizado a un recurso del sistema o retraso de las operaciones y funciones del sistema nocivo para múltiples sistemas, cuyo objetivo es saturar el ancho de banda o los recursos del sistema objetivo, con la consiguiente pérdida de disponibilidad para los usuarios autorizados.

3.1.4 directriz [b-UIT-T X.1401]: Descripción que aclara lo que debe hacerse y cómo, para lograr los objetivos establecidos en las políticas aplicables.

3.1.5 función de red [b-UIT-T Y.3100]: En el contexto de las IMT-2020, una función de procesamiento en una red.

NOTA 1 – Las funciones de red pueden incluir, entre otras, las funcionalidades de nodo de red, por ejemplo, gestión de sesión, gestión de movilidad y funciones de transporte, cuyo comportamiento funcional e interfaces están definidos.

NOTA 2 – Las funciones de red pueden implementarse en un hardware dedicado o como funciones de software virtualizadas.

NOTA 3 – Las funciones de red no se consideran recursos, sino que cualquier función de red puede instanciarse utilizando los recursos.

3.1.6 virtualización de las funciones de red [b-UIT-T X.1811]: Tecnología que permite crear segmentos de red lógicamente aislados en redes físicas compartidas de manera que en las redes compartidas pueden coexistir simultáneamente conjuntos heterogéneos de múltiples redes virtuales.

3.1.7 segmento de red [b-UIT-T Y.3100]: Red lógica que proporciona capacidades y características de red específicas.

NOTA 1 – Los segmentos de red permiten la creación de redes personalizadas, capaces de ofrecer soluciones flexibles para diferentes casos de mercado, con diversos requisitos, en lo que atañe a las funcionalidades, la calidad de funcionamiento y la atribución de recursos.

NOTA 2 – Un segmento de red puede ser capaz de exponer sus propias capacidades.

NOTA 3 – El comportamiento de un segmento de red se materializa a través de la instancia o instancias del segmento en cuestión.

3.1.8 orquestación [b-UIT-T Y.3100]: En el contexto de las IMT-2020, procesos destinados a la disposición, coordinación, instanciación y utilización automatizadas de las funciones y los recursos de red para las infraestructuras tanto físicas como virtuales mediante criterios de optimización.

3.1.9 capacidad de seguridad [b-ISO 81001-1]: Categoría amplia de controles técnicos, administrativos u orgánicos, destinados a la gestión de los riesgos en materia de confidencialidad, integridad, disponibilidad y rendición de cuentas de los datos y sistemas.

3.1.10 proveedor [b-ISO 10393]: Organización o persona que ofrece un producto o servicio.

3.1.11 sistema [b-ISO/CEI 27000]: Aplicaciones, servicios, bienes de tecnologías de la información o demás componentes de tratamiento de la información.

3.1.12 amenaza [b-X.1406]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.1.13 función de red virtualizada [b-UIT-T Y.3150]: Función de red cuyo software funcional está desvinculado del hardware y se ejecuta en una o varias máquinas virtuales.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 dominio: Agrupación de entidades de red en función de una serie de aspectos físicos o lógicos relevantes para una red IMT-2020.

3.2.2 sistema de comunicación IMT-2020: Sistema de gestión de procesos de comunicación IMT-2020 para servicios IMT-2020.

NOTA 1 – En el contexto del UIT-T, 5G equivale a IMT-2020.

NOTA 2 – En la presente Recomendación, los sistemas de comunicaciones IMT-2020 son idénticos a los sistemas IMT-2020.

3.2.3 ecosistema IMT-2020: Conjunto de partes interesadas que interactúan para conformar un sistema IMT-2020 operativo estable.

NOTA – Se refiere principalmente a la tecnología de comunicación IMT-2020, en cuyo marco una comunidad de organismos vivos, incluidos productores, consumidores y proveedores, contribuye con grandes cantidades de productos, tecnologías y conocimientos técnicos, a fin de que el sistema IMT-2020 funcione en diferentes niveles, véanse en especial los servicios, las infraestructuras, las redes, las plataformas y las aplicaciones.

3.2.4 servicio IMT-2020: Prestación proporcionada por un ecosistema IMT-2020.

3.2.5 ataque por desbordamiento de tabla de flujo: Ataque que consume las tablas de flujo que reenvían y procesan los paquetes de flujos, agotando así el espacio disponible para que otros flujos instalen nuevas reglas de flujo, lo que provoca una denegación de servicio (DoS) en la red.

4 Abreviaturas y acrónimos

En la presente Recomendación, se utilizan los siguientes acrónimos y abreviaturas:

4G	Cuarta generación de tecnologías de comunicaciones móviles (*fourth generation of mobile communication technology*)
AMF	Función de gestión del acceso y la movilidad (*access and mobility management function*)
API	Interfaz de programación de aplicaciones (*application programming interface*)
AUSF	Función de servidor de autenticación (*authentication server function*)
C-PDU	Unidad de datos de protocolo de control (*control protocol data unit*)
CU/DU	Unidad central/unidad distribuida (*central unit/distributed unit*)
DCI	Interconexión de centros de datos (*data centres interconnect*)
DDoS	Denegación de servicio distribuida (*distributed denial of service*)
DoS	Denegación de servicio (*denial of service*)
eMBB	Banda ancha móvil mejorada (*enhanced mobile broadband*)
FAT	Cuadro de atribución de archivos (*file allocation table*)
IMSI	Identidad internacional de abonado móvil (*international mobile subscriber identity*)
IMT-2020	Telecomunicaciones móviles internacionales-2020 (*international mobile telecommunications-2020*)
IoT	Internet de las cosas (*Internet of things*)
LTE	Evolución a largo plazo (*long-term evolution*)
MAC	Código de autenticación de mensajes (*message authentication code*)
MEC	Computación periférica de acceso múltiple (*multiaccess edge computing*)
MEHW	Equipo móvil físico (*mobile equipment hardware*)
mIoT	Internet de las cosas masiva (*massive Internet of things*)
mMTC	Comunicaciones masivas tipo máquina (*massive machine-type communications*)

MNO	Operador de red móvil (*mobile network operator*)
NAS	Estrato de no acceso (*non-access stratum*)
NF	Función de red (*network function*)
NFV	Virtualización de las funciones de red (*network function virtualization*)
NFVI	Infraestructura de la virtualización de las funciones de red (*network functions virtualization infrastructure*)
NRF	Función de almacenamiento de las funciones de red (*network function repository function*)
OAM	Operación, administración y gestión (*operation, administration and management*)
O&M	Operaciones y gestión (*operations and management*)
PII	Información de identificación personal (*personally identifiable information*)
PSK	Clave compartida previamente (*pre-shared key*)
RA/CA	Autoridad de registro y autoridad de certificación (*registration authority and certification authority*)
RRC	Control de recursos radioeléctricos (*radio resource control*)
SBA	Arquitectura basada en los servicios (*service-based architecture*)
SBI	Interfaz basada en el servicio (*service-based interface*)
SDN	Red definida por software (*software-defined networking*)
SMF	Función de gestión de sesión (*session management function*)
SQL	Lenguaje de consulta estructurado (*structured query language*)
SSL	Capa de zócalo segura (*secure sockets layer*)
TA	Ancla de confianza (*trust anchor*)
TLS	Seguridad de la capa de transporte (*transport layer security*)
TMSI	Identidad temporal de suscripción al servicio móvil (*temporary mobile subscriber identity*)
TPM	Módulo de plataforma de confianza (*trusted platform module*)
UDM	Gestión de datos unificados (*unified data management*)
UE	Equipo de usuario (*user equipment*)
UICC	Tarjeta con circuito integrado universal (*universal integrated circuit card*)
URLLC	Comunicaciones ultrafiables y de baja latencia (*ultra-reliable and low-latency communications*)
USIM	Módulo de identidad de abonado universal (*universal subscriber identity module*)
VM	Máquina virtual (*virtual machine*)
VNF	Función de red virtual (*virtual network function*)
VoIP	Protocolo de transmisión de voz por Internet (*voice over Internet protocol*)

5 Convenios

En la presente Recomendación, la expresión "debería" indica que se trata de una especificación recomendada y que, por ende, no es absolutamente obligatoria. El cumplimiento de esa especificación no es necesario para acreditar la conformidad.

6 Visión general de la seguridad de los sistemas de comunicaciones IMT-2020

6.1 Arquitectura IMT-2020 simplificada

En este apartado se aborda la seguridad de los sistemas de comunicaciones IMT-2020 en términos generales. Los dispositivos móviles conectados y las aplicaciones móviles requieren un acceso a redes inalámbricas que sea resiliente, seguro y fidedigno. Los sistemas de comunicaciones IMT-2020 deberían diseñarse conforme a esos requisitos de alto nivel.

Un sistema de comunicación IMT-2020 consta de una serie de dispositivos conectados a una red de acceso IMT-2020, que, a su vez, está conectada al resto del sistema, denominado red troncal IMT-2020.

La Figura 1 ilustra una versión simplificada de la arquitectura de sistema 5G 3GPP. La red de acceso IMT-2020 comprende diversas estaciones base radioeléctricas 3GPP y/o una red de acceso no 3GPP. La arquitectura de la red troncal IMT-2020 es muy superior a la 4G en lo que respecta a la capacidad del sistema para implementar la computación en nube y la Internet de las cosas (IoT), e incluye importantes mejoras en cuanto a la segmentación de la red y la arquitectura basada en el servicio (SBA).

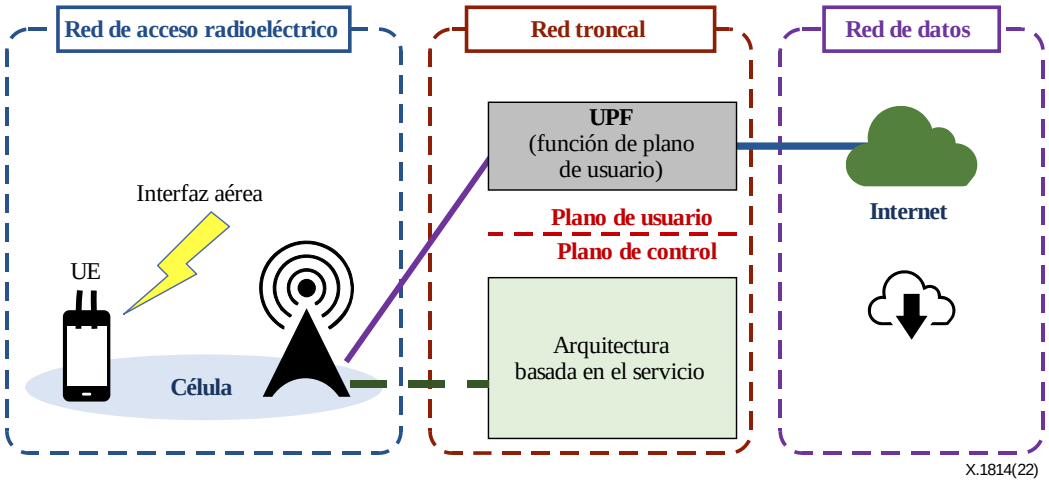

Figura 1 – Arquitectura IMT-2020 simplificada

6.2 Arquitectura general del sistema IMT-2020

El objetivo de un sistema IMT-2020 es ofrecer una amplia gama de servicios con distintos requisitos de calidad de funcionamiento. Los servicios ofrecidos a través de redes IMT-2020 pueden dividirse en tres categorías, de acuerdo con las especificaciones del 3GPP: 1) la banda ancha móvil mejorada (eMBB) soporta grandes velocidades de datos y una mayor movilidad del usuario que la cuarta generación de tecnologías de comunicaciones móviles/red de evolución a largo plazo (4G/LTE); 2) la Internet de las cosas masiva (mIoT) ofrece comunicaciones masivas tipo máquina; 3) las comunicaciones ultrafiables y de baja latencia (URLLC) soportan servicios esenciales de misión que exigen una mayor fiabilidad y una menor latencia. Un sistema IMT-2020 debe ser una plataforma flexible que permita novedades comerciales e integre sectores verticales, como la automoción, la manufactura, la energía, la cibersalud y el entretenimiento. Además, el despliegue y el mantenimiento de los sistemas IMT-2020 serán más fáciles que los de generaciones anteriores de redes móviles. Para

afrontar estos exigentes requisitos, los sistemas IMT-2020 introducen una serie de tecnologías innovadoras, como la segmentación de red, la virtualización de las funciones de red (NFV), la interconexión de redes definidas por software (SDN), la SBA y la separación unidad central/unidad distribuida (CU/DU).

La Figura 2 ilustra la arquitectura general de un sistema IMT-2020 [b-UIT-T X.1811], que incluye una capa de transporte, una capa de red, una capa de servicio y un plano de gestión, en función de las funcionalidades requeridas.

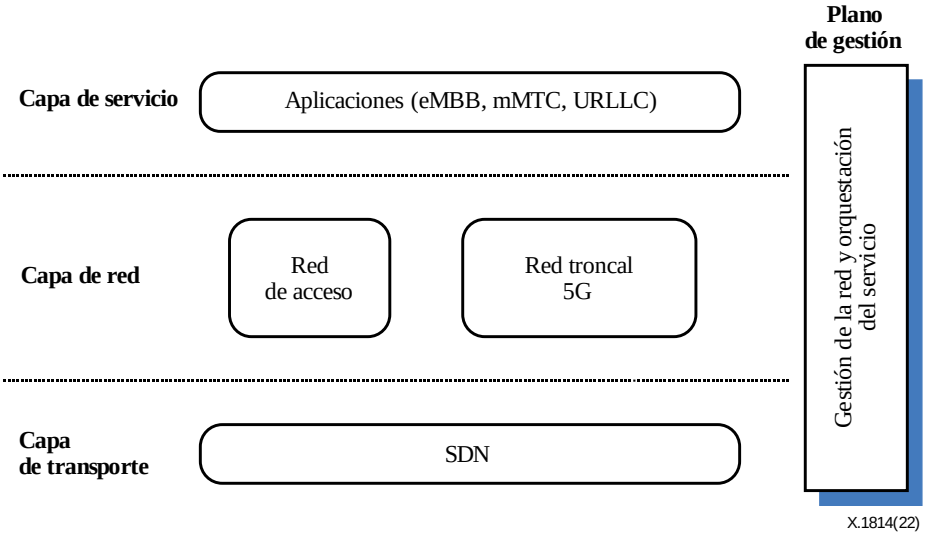

Figura 2 – Arquitectura general de un sistema IMT-2020 [b-UIT-T X.1811] [b-TS 33.501]

- Capa de transporte: esta capa se utiliza para transportar paquetes entre el origen y el destino. Además de las tecnologías de transporte heredadas (por ejemplo, MPLS), los sistemas IMT-2020 han introducido la tecnología SDN para lograr una mayor velocidad de transporte y simplificar la adaptación a los requisitos del servicio.
- Capa de red: esta capa se compone de la red de acceso y la red troncal. La primera permite al UE acceder a la red IMT-2020. La segunda se diseña teniendo en mente una SBA con fines de ampliabilidad y sencillez. Está formada por varias funciones de red que soportan la conectividad de datos y el despliegue del servicio. Ejemplos de funciones de red son la función de servidor de autenticación (AUSF), la función de gestión del acceso y la movilidad (AMF) y la función de gestión de sesión (SMF).
- Capa de servicio: esta capa está formada por las aplicaciones que se ejecutan en la parte superior del sistema IMT-2020 y que pueden ser aplicaciones eMBB, mMTC o URLLC.
- Plano de gestión: este plano es responsable de la gestión de la red y la orquestación del servicio.

6.3 Dominios del sistema IMT-2020

La seguridad de las IMT-2020 debería definirse en función de los dominios, las capas, los requisitos de seguridad y las capacidades de seguridad.

Un dominio se compone de diversas entidades de red, agrupadas en función de una serie de aspectos físicos o lógicos, que revisten interés para la red IMT-2020. El concepto de dominio segmentado se utiliza para integrar distintos aspectos relacionados con la segmentación de la red. En el contexto de las redes IMT-2020, puede representar diferentes funcionalidades, servicios y actores. La Figura 3 ilustra varios dominios característicos de las IMT-2020.

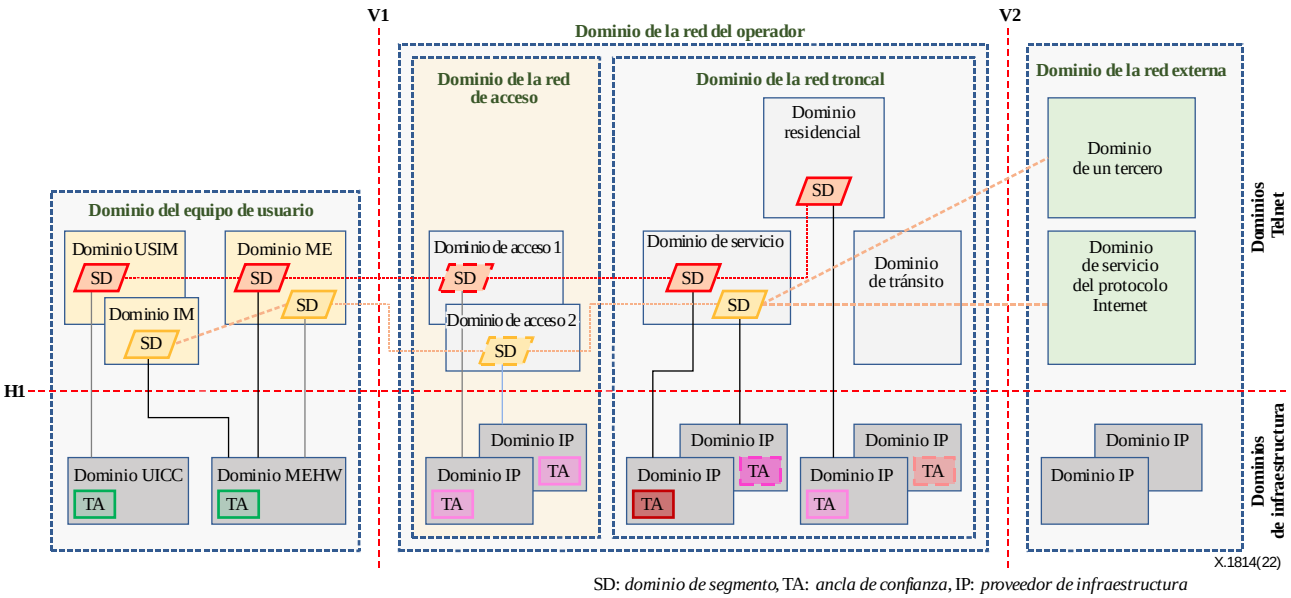

Figura 3 – Dominios característicos de las IMT-2020

En la Figura 3, los elementos de red situados por encima de la línea H1 representan partes de la red lógica, denominadas "dominios de arrendatario", y los situados por debajo de la línea H1 representan partes de la red física, denominadas "dominios de infraestructura". La línea V1 separa el dominio del equipo de usuario del dominio de la red de acceso, y la línea V2 separa el dominio de la red troncal del dominio de la red externa, véanse, por ejemplo, los servicios del protocolo Internet utilizados por la red del operador.

Los dominios de infraestructura contienen elementos de red implementados mediante soporte físico y soporte lógico y actúan como proveedor de infraestructura. Esto incluye hipervisores (soporte lógico que crea y ejecuta máquinas virtuales) así como anclas de confianza (entidad de autoridad para los que se asume la confianza y no se deriva) [b-UIT-T X.509].

En el lado del UE, por debajo de la línea H1, los dominios de UE consisten en la tarjeta con circuito integrado universal (UICC), que ofrece un módulo resistente a la manipulación, y el dominio de hardware del equipo móvil (MEHW), que ofrece soporte de hardware, incluido un entorno de ejecución de confianza.

En el lado red por debajo de la línea H1, hay un dominio de proveedor de infraestructura (IP) que consiste en un soporte físico específico de acceso (radioeléctrico), así como un soporte físico para el cálculo, almacenamiento e interfuncionamiento necesarios para la funcionalidad núcleo.

Las anclas de confianza (TA) se utilizan para ofrecer confianza a los sistemas virtualizados. Esto incluye garantizar la integridad del dominio de arrendatario y que este se ejecuta en una infraestructura designada y de confianza. Las TA también pueden utilizarse para verificar la integridad de un dominio de infraestructura y para vincular los dominios del arrendatario con los dominios de infraestructura.

Los dominios del arrendatario comprenden varios dominios lógicos que utilizan dominios de infraestructura con fines tales como ejecutar sus funciones. En el lado del UE, están formados por varios equipos móviles, el módulo de identidad de abonado universal (USIM), una de las diversas aplicaciones de software que reside en la parte del hardware, denominada UICC, que almacena la información relacionada con el abonado y ejecuta las funciones de seguridad relativas a la autenticación y el cifrado en el lado del usuario, y el dominio de gestión de la identidad. Los dominios del arrendatario en el lado de la red son los dominios de acceso (A), de servicio (S), residencial (H), de tránsito (T), de un tercero (3P), de servicio del protocolo Internet y de gestión (M).

6.4 Requisitos y capacidades generales de seguridad

En esta cláusula se resumen las dimensiones generales de seguridad (requisitos) descritas en [b-UIT-T X.805]. El objetivo de esta cláusula es sentar las bases de la capacidad de seguridad del sistema IMT-2020. En el Apéndice I se ofrece la arquitectura de seguridad de red genérica para la provisión de capacidades de seguridad de red de extremo a extremo.

Por capa de seguridad se entiende una jerarquía de agrupaciones de equipos de red y dispositivos [b-UIT-T X.805]. Por capa de seguridad se entiende una jerarquía de agrupaciones de equipos de red y dispositivos [b-UIT-T X.805]. La capa de seguridad comprende un conjunto de protocolos, datos y funciones relacionados con un aspecto de los servicios prestados por uno o varios dominios. La capa de la arquitectura de seguridad IMT-2020 proporciona un panorama detallado de protocolos, datos y funciones que están relacionados por cuanto están expuestos a un entorno común de amenazas y conllevan requisitos de seguridad similares. Algunas amenazas frecuentes a la comunicación entre el UE y la red de acceso radioeléctrico son las interferencias radioeléctricas, los ataques de estaciones base falsas, la introducción aérea de datos en el plano del usuario y los mensajes suplantados de control de recursos radioeléctricos. Por otra parte, el seguimiento de los identificadores de suscripción, la falsificación de mensajes del plano de control y la manipulación de capacidades de seguridad, entre otras, son amenazas comunes a las comunicaciones entre el UE y la red troncal. Algunos ejemplos de amenazas habituales contra los servicios de gestión en las redes IMT-2020 son los cambios de configuración no autorizados, la exposición de los certificados y las claves de red y la adición inmediata de una función de red maliciosa. La capa de gestión incluye aspectos relacionados con la gestión convencional de las redes (configuración, actualizaciones de software, gestión de cuentas de usuario del sistema, recopilación y análisis de registros, etc.) y, en particular, con la gestión de la seguridad (auditoría de control de seguridad, gestión de claves y certificados, etc.). También se engloban en este estrato los aspectos relacionados con la gestión de la virtualización y la creación/composición de servicios (orquestación, gestión de segmentos de red, aislamiento y gestión de máquinas virtuales (VM), etc.).

El área de seguridad aumenta los dominios de seguridad y está sujeta a los requisitos de seguridad de una o varias capas o dominios.

En general, una capacidad de seguridad se define como una categoría amplia de controles técnicos, administrativos u organizativos que permiten gestionar los riesgos en materia de confidencialidad, integridad, disponibilidad y rendición de cuentas de los datos y sistemas [b-ISO 81001-1]. En ese sentido, hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) de un aspecto de la seguridad, como la integridad. Además, contiene funciones y mecanismos de seguridad para evitar, detectar, frenar, contrarrestar o minimizar los riesgos inherentes a la seguridad de las redes IMT-2020, especialmente los riesgos relacionados con la infraestructura física y lógica de una red, sus servicios, los UE, los sistemas de señalización y los datos. En el Cuadro 1 se especifican los requisitos de seguridad de los dominios de seguridad.

Cuadro 1 – Requisitos de seguridad por ámbito de seguridad

Ámbito de seguridad	Requisitos de seguridad
Red de acceso	La determinación de los requisitos de seguridad relacionados con la capa y el dominio de acceso permite gestionar las amenazas asociadas a este dominio. La protección de la confidencialidad e integridad de los datos de usuario y de control y la movilidad segura son ejemplos de este tipo de requisitos.
Aplicación o servicio	La determinación de los requisitos de seguridad de la capa de aplicación que proporciona aplicaciones y servicios de usuario final (por ejemplo, VoIP, VoLTE) permite gestionar las amenazas asociadas a este dominio. La autenticación del usuario y la autorización para utilizar la detección de aplicaciones y servicios seguros son ejemplos de este tipo de requisitos.
Gestión	La determinación de los requisitos de seguridad de la capa y el dominio de gestión permite gestionar las amenazas asociadas a este dominio, véanse en especial la gestión de la seguridad (por ejemplo, actualizaciones seguras, orquestación segura) y el control de seguridad (esto es, seguimiento y gestión de claves y accesos).
UE	La determinación de los requisitos de seguridad relacionados con el dominio del UE, incluido el control de acceso al dispositivo, permite gestionar las amenazas asociadas a este dominio. La autenticación mutua con la red y el almacenamiento seguro del contexto de seguridad son ejemplos de este tipo de requisitos.
Red	Se determinan los requisitos de seguridad relacionados con la red troncal y las comunicaciones entre la red del operador y redes externas, incluidos los aspectos relacionados con el intercambio seguro de datos de señalización y de usuario final entre los nodos del operador y los dominios de red externa. La seguridad de las redes y la privacidad y la autenticación de los abonados son ejemplos de este tipo de requisitos.
Infraestructura y virtualización	Los requisitos de seguridad del dominio del IP se determinan, por ejemplo, con fines de certificación, segmentación/aislamiento seguro y confianza entre los dominios de arrendatario y entre los dominios de arrendatario y los dominios de infraestructura.

En el Cuadro 2 se describe la capacidad de seguridad de cada dimensión de seguridad [b-UIT-T X.805]. Se han adoptado de [b-UIT-T X.805] siete de ellas, a saber, gestión de identidad y acceso, autentificación, no repudio, confidencialidad, integridad, disponibilidad y privacidad Las otras tres, a saber, auditoría [b-ITU-T X.800], confianza y garantía y cumplimiento, son dimensiones de seguridad en la arquitectura de seguridad de las IMT-2020.

Cuadro 2 – Capacidades de seguridad

Dimensiones de seguridad	Capacidad de seguridad
Gestión de identidad y acceso	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) para el control de acceso y la gestión de credenciales y funciones.
Autenticación	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) para la autenticación, que permite verificar la validez de los atributos de autenticación de un usuario, como la identidad declarada.
No repudio	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y las contramedidas) de un servicio de no repudio, que protege frente a la falsa negación de participación en una acción concreta.
Confidencialidad	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) de un servicio de confidencialidad, que protege los datos frente a divulgaciones no autorizadas.
Integridad	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) de un servicio de integridad, que protege los datos en términos de creación o modificación.
Disponibilidad	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) relacionados con la disponibilidad de los recursos, incluso en caso de ataque. En esta clasificación se incluyen los mecanismos de recuperación en caso de catástrofe.
Privacidad	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) de un servicio de privacidad, que permite a las entidades garantizar su derecho a determinar el nivel de interacción y de divulgación de información de identificación personal.
Auditoría	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) de un servicio de auditoría, que se ocupa de revisar y examinar los registros y las actividades de un sistema a fin de determinar si la capacidad del sistema es adecuada y detectar brechas en su seguridad y capacidad. También se incluye una auditoría de recopilación de datos.
Confianza y garantía	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) de un servicio de confianza y seguridad, que permite transmitir información sobre la fiabilidad de un sistema.
Conformidad	Esta capacidad de seguridad hace referencia a un conjunto de funciones y mecanismos de seguridad (incluidas salvaguardias y contramedidas) de un servicio de conformidad, que permite que una entidad o sistema satisfaga sus obligaciones contractuales o legales.

7 Componentes y fiabilidad de los sistemas de comunicaciones IMT-2020

7.1 Componentes de las IMT-2020

Las aplicaciones móviles y los dispositivos de IoT conectados necesitan un acceso a redes inalámbricas que sea resiliente, seguro y capaz de proteger la privacidad de las personas. El diseño de los sistemas de comunicaciones IMT-2020 debería cumplir los requisitos especificados en las cláusulas 7.8 y 7.9 de [b-UIT-T Y.3101]. Una red IMT-2020 consta de cuatro componentes: UE, red de acceso radioeléctrico, red de transporte y red troncal (véase la Figura 4).

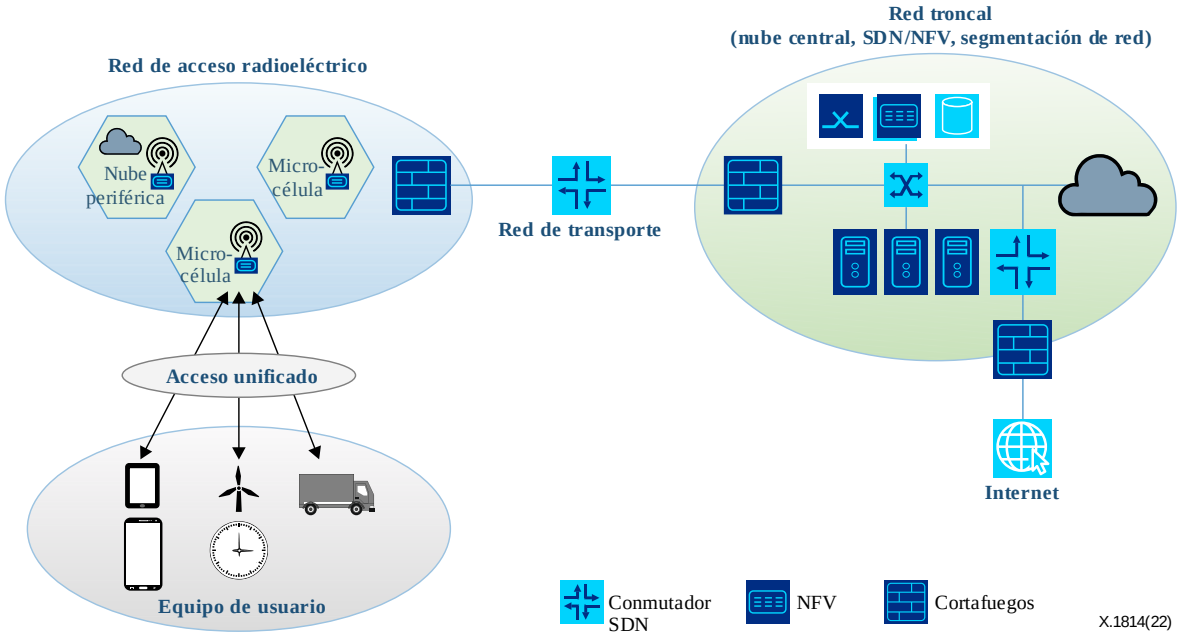

Figura 4 – Red de comunicaciones IMT-2020 (adaptación de [b-ITU workshop])

Los sistemas IMT-2020 se basarán en nubes móviles, SDN, NFV y segmentos de red para responder a los desafíos en materia de conectividad masiva, flexibilidad y minimización de costes. Por tanto, es preciso definir garantías de NFV, segmentación de redes y computación periférica en la nube.

La NFV aísla las funciones de red de los dispositivos de hardware patentados y los gestiona como software en las VM.

Una función de red virtual (VNF) es un resultado lógico de la NFV, que es una función de red cuyo software funcional está desvinculado del hardware y se ejecuta en una o varias VM [b-UIT-T Y.3100]. Las VNF se ejecutan en funciones de red específicas, como cortafuegos, conmutadores, sistemas de detección de intrusiones y sistemas de protección frente a intrusiones.

La segmentación de redes es un tipo de arquitectura de red virtual que utiliza los principios subyacentes de la SDN y la NFV en las redes fijas. Las redes IMT-2020 se subdividen en múltiples redes virtuales, cada una de las cuales está optimizada para una situación concreta, denominada segmento de red. Pueden abarcar varios dominios de red, como el acceso, la red troncal y el transporte, y desplegarse en múltiples operadores, tal y como se muestra en la Figura 5.

La arquitectura SDN pretende aumentar la agilidad y flexibilidad de las redes. Su objetivo es mejorar el control de las redes posibilitando la respuesta rápida de las empresas y los proveedores de redes a la evolución de los requisitos empresariales.

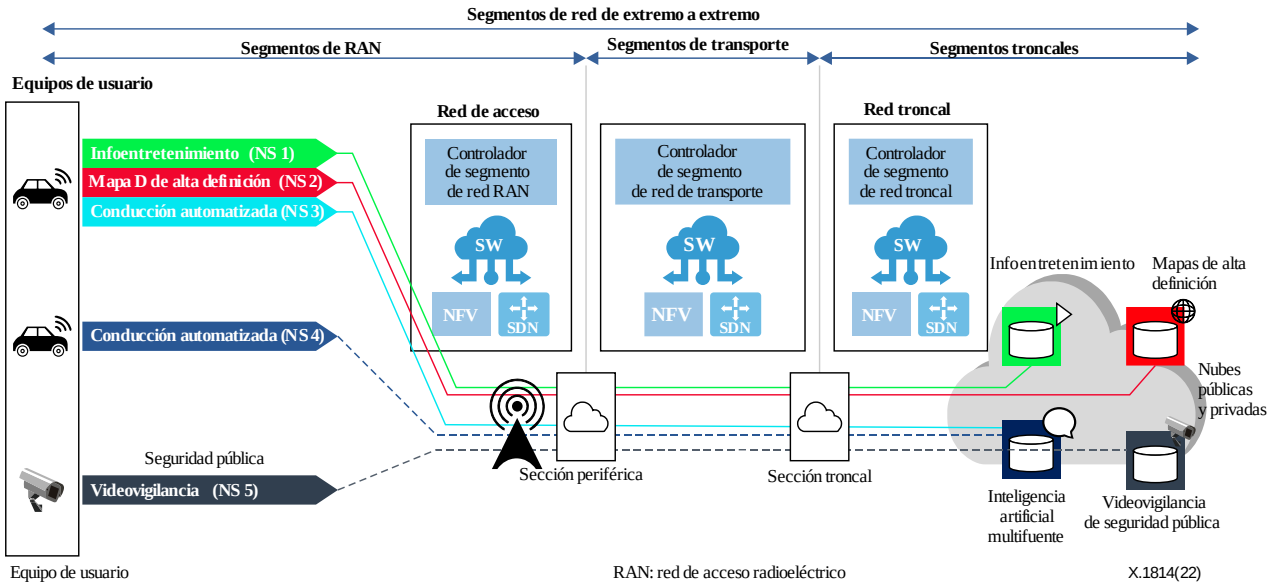

Figura 5 – Segmentos de red IMT-2020

Una red de transporte IMT-2020 es una infraestructura de transporte IP que proporciona telecomunicaciones IMT-2020 móviles.

La computación periférica acerca las capacidades de la computación en la nube al extremo de la red IMT-2020. Se trata de un paradigma de computación distribuida en el que la computación se ejecuta en su totalidad o en su mayor parte en nodos de dispositivos distribuidos denominados dispositivos inteligentes o dispositivos periféricos, en contraposición con la computación que se ejecuta principalmente en un entorno de nube descentralizada. La computación periférica acerca el procesamiento y almacenamiento de los datos al equipo. Esto permite a los dispositivos IoT prestar sus servicios con baja latencia.

7.2 Fiabilidad de los sistemas de comunicaciones IMT-2020

La fiabilidad de los sistema de comunicaciones IMT-2020 depende de cinco propiedades, a saber, la resiliencia, la seguridad de la comunicación, la gestión de identidades, la privacidad y la garantía de seguridad:

- La resiliencia es la capacidad de resistencia de una organización a verse afectada por perturbaciones. Las múltiples y muy diversas características complementarias y parcialmente duplicadas de las IMT-2020 pueden contribuir a la resiliencia de los sistemas de comunicaciones IMT-2020 frente a ciberataques y otros incidentes no malintencionados.
- La seguridad de la comunicación se aplica a la comunicación de datos en las IMT-2020. En un sistema de comunicaciones IMT-2020 es fundamental para los dispositivos y para la propia infraestructura que las comunicaciones sean seguras.
- La gestión de identidades comprende el proceso y las políticas necesarios para gestionar la vida útil y el valor, tipo y metadatos optativos de los atributos de las identidades conocidas de un dominio IMT-2020. Se debería facilitar la gestión segura de las identidades para identificar y autenticar a los abonados, se esté o no en itinerancia, garantizando que sólo los abonados genuinos pueden acceder a los servicios de la red. Debería basarse en primitivas criptográficas y características de seguridad sólidas.
- La privacidad de los datos se define como los derechos y obligaciones de los particulares y organizaciones con respecto a la obtención, utilización, conservación, divulgación y eliminación de información personal en [b-ISO/TS 21719-2]. La privacidad consiste en proteger la información de identificación personal (PII) que permite a las partes no autorizadas identificar a los abonados.

- La garantía de seguridad sirve de base para justificar la confianza en la afirmación de que se cumplen o van a cumplir los objetivos de seguridad. La garantía de seguridad es un medio de asegurar que un equipo de red cumple los requisitos de seguridad y se consigue adoptando procesos de desarrollo y de vida útil del producto seguros.

8 Amenazas a componentes y funciones

En la Figura 6 se muestran ejemplos de amenazas a los sistemas IMT-2020. Estas se clasifican en tres categorías: amenazas conocidas derivadas de vulnerabilidades de software, errores de configuración y ataques por inundación; amenazas derivadas del uso compartido de las infraestructuras, y amenazas asociadas al nivel de red, como las amenazas relacionadas con la SDN, la NFV, la segmentación de redes y la computación en la nube.

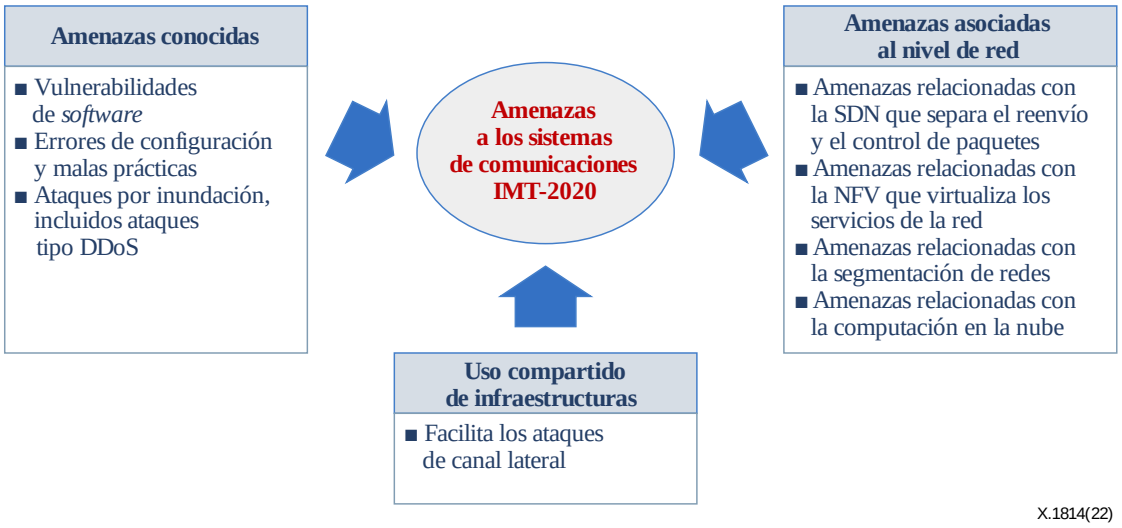

Figura 6 – Ejemplos de amenazas en las IMT-2020 [b-ITU workshop]

8.1 Amenazas genéricas

En [b-ENISA] se describen las amenazas siguientes:

- **Denegación de servicio (DoS)** [b-ENISA]: el objetivo de este ataque es inutilizar un recurso de red para los usuarios previstos, mediante la creación de interferencias temporales o indefinidas, o la interrupción del servicio de red a partir del envío de un número masivo de peticiones. Entre las amenazas que pueden dar lugar una DoS figuran los ataques por inundación, amplificación, errores de señalización generalizados y saturación. Los ataques DoS populares incluyen: 1) ataques de desbordamiento de memoria intermedia, es decir, el ataque DoS más común. El concepto consiste en enviar a una dirección de red más tráfico del que los programadores habían tenido en cuenta para construir el sistema. Estos incluyen los ataques que se enumeran más abajo, además de otros ataques diseñados para explotar errores específicos de ciertas aplicaciones o redes. 2) Los ataques por inundación ICMP se aprovechan de los dispositivos de red mal configurados enviando paquetes falsos que hacen ping en todos los ordenadores de la red objetivo, en lugar de centrarse en una máquina específica únicamente. A continuación, se activa la red para amplificar el tráfico. Este ataque también se denomina ataque "smurf" o "ping of death". 3) Los ataques por inundación SYN consisten en enviar una solicitud para conectar con un servidor, sin completar la toma de contacto. Dichos envíos prosiguen hasta lograr que todos los puertos abiertos se saturen de solicitudes y no quede ninguno disponible para la conexión de los usuarios legítimos.

- **Denegación de servicio distribuida (DDoS)** [b-ENISA]: en un ataque DDoS, múltiples sistemas lanzan un ataque DoS contra un único sistema, orquestando un ataque DoS sincronizado contra un único objetivo. La diferencia principal es que el ataque contra el objetivo no procede de una ubicación, sino de muchas ubicaciones a la vez.
- **Vulneración, fuga, robo, destrucción y manipulación de información** [b-ENISA]: incluye el robo y la posible publicación de PII mediante el acceso no autorizado a sistemas o redes o el acceso no autorizado a datos personales/biométricos/médicos, a información corporativa confidencial o a información gubernamental/estatal y su posible publicación. Los atacantes también pueden recurrir al robo, la vulneración o la fuga de otros tipos de datos, como credenciales de usuario, claves de cifrado, registros de seguridad de redes, configuración de software, etc., para llevar a cabo diferentes tipos de ataques.
- **Interceptación** [b-ENISA]: el término "interceptación" se utiliza para describir la interceptación no autorizada de información. Se trata de una amenaza en la que el intruso quiere modificar las capas de aplicación y comunicación de los diferentes elementos de red IMT-2020 (controlador de SDN, función de red, nodo periférico, orquestador de virtualización). Incluye el espionaje de datos de abonados, información confidencial, horarios del sistema, ubicaciones de abonados, mensajes electrónicos y señales de datos transmitidas por la red. El autor de la amenaza monitorea, espía o intercepta las comunicaciones de una organización para establecer las ubicaciones o acceder a información sensible.
- **Explotación de las vulnerabilidades de software y hardware** [b-ENISA]: en el marco de este tipo de amenazas, un atacante malicioso hace uso de fallos de software o hardware desconocidos (para el proveedor y el usuario) o de fallos conocidos, pero no corregidos, para ejecutar su ataque, por ejemplo, un colapso o desbordamiento de la memoria. También incluye la explotación de otras vulnerabilidades conocidas relacionadas con generaciones anteriores de telecomunicaciones móviles.
- **Código o software malicioso** [b-ENISA]: un código malicioso es cualquier código de cualquier guion o parte de un sistema de software destinado a causar efectos no deseados, violaciones de seguridad o daños en el sistema. La amenaza incluye la instalación y distribución de software malicioso o la implantación de un código o software específico en un producto o sus actualizaciones. Algunos ejemplos de software malicioso son el software maligno (malware), el software de secuestro (ransomware), los virus, los gusanos, los troyanos, la infiltración de lenguaje de interrelación de bases de datos (SQL) [b-SQL], el software de seguridad maligno, el software de fraude (rogueware) y el software con fines benéficos (careware). Un ejemplo de utilización de software malicioso en el contexto de las IMT-2020 es el uso de una VNF no autorizada que podría instalarse y registrarse de manera abusiva en la red troncal para exponer API maliciosas.
- **Cadena de suministro, vendedores y proveedores de servicios comprometidos** [b-ENISA]: si la cadena de suministro, el vendedor o el proveedor de servicios quedan comprometidos, los atacantes pueden introducir en el producto hardware o software malicioso oculto, así como fallos de software, y ejecutar actualizaciones de software no controladas, manipular las funcionalidades, añadir funciones para eludir los mecanismos de auditoría y crear puertas traseras.

  En ocasiones, se precisa la colaboración de personal externo que no es de confianza durante las pruebas, el mantenimiento y la configuración y utilización de los productos. Estos trabajadores tendrán que acceder a las instalaciones de gestión de red (tanto de forma local como a través de una interfaz remota) para ejecutar tareas de mantenimiento y prestar apoyo técnico. A raíz de este acceso privilegiado a la operación, administración y gestión (OAM) de la red, el personal puede acceder a diferentes tipos de datos, por ejemplo, los datos de configuración del abonado, el sistema y la red y la información telemétrica.

- **Amenazas dirigidas** [b-ENISA]: las amenazas dirigidas proceden de un malware destinado a una organización o industria concreta. Se trata de un tipo de software delictivo (crimeware) preocupante, ya que estas amenazas se han diseñado para captar información sensible. Los ataques muy sofisticados o las amenazas persistentes avanzadas pueden focalizarse en información sensible o en la disponibilidad de servicios críticos y sensibles.
- **Explotación de fallos en los procedimientos de seguridad, gestión y funcionamiento** [b-ENISA]: aunque no está relacionada directamente con las IMT-2020, será preciso tener en cuenta esta amenaza para abordar la complejidad de la tecnología y la necesidad de introducir procedimientos operativos en las labores de gestión de la red. Algunos ejemplos son la explotación de los fallos en la gestión del funcionamiento y la seguridad de las redes y en la configuración, actualización y gestión de los parches de software. Los errores derivados de la inexistencia o el diseño incorrecto de los procedimientos operativos y de seguridad pueden repercutir en la integridad y disponibilidad de la red.
- **Abuso de autenticación** [b-ENISA]: esta amenaza puede afectar a múltiples puntos de entrada de red, como el UE (dispositivos móviles e IoT), las interfaces de funcionamiento y gestión, la itinerancia y los servicios verticales. Además, está vinculada al robo de credenciales de usuario, los ataques con fuerza bruta contra cuentas de usuario, la obtención ilícita de contraseñas, el enmascaramiento de identidades de usuario y la alteración de las técnicas de autenticación de grupos de la IoT en tanto que técnicas utilizadas por los atacantes para hacer un uso incorrecto de los sistemas de autenticación IMT-2020.
- **Robo o suplantación de identidad** [b-ENISA]: el robo de identidad consiste en utilizar la identidad de otra entidad de forma deliberada. Puede constituir una amenaza si un atacante malicioso consigue determinar la identidad de una entidad legítima y se enmascara como esa entidad para lanzar más ataques. La suplantación de identidad es la acción de adoptar la identidad de otra entidad y utilizarla para alcanzar un objetivo. La suplantación de identidad constituye una amenaza contra cualquier componente de software o agente humano. En el marco de estos ataques, el atacante suplanta la identidad de un controlador legítimo e interactúa con las funciones de red controladas por dicho controlador (esto es, elementos del plano de datos) para activar otros tipos de ataques (provocar flujos de red, desviar el tráfico, etc.). Otras dos técnicas posibles para suplantar o robar credenciales de usuario son la ingeniería social y la obtención ilícita de cuentas de usuario/contraseñas por fuerza bruta. Por ejemplo, los ataques de captación de identidades internacionales de abonados del servicio móvil (IMSI) pueden mostrar la identidad de los abonados al captar las IMSI de los UE de los abonados en cuestión, o pueden establecer una estación base falsa que sea considerada como la estación base favorita de los UE que han perdido el acceso a una identidad temporal de abonado móvil temporal (TMSI). En estos casos, los abonados responden con su IMSI. Además, los agentes que participan en las redes IMT-2020 son distintos, por ejemplo, operadores de redes móviles virtuales (VMNO), proveedores de servicios de comunicaciones (CSP) y proveedores de infraestructura de red.

8.2 Amenazas al equipo de usuario

Se han identificado las amenazas de seguridad a UE siguientes:

- **Infección por software malicioso** [b-ENISA]: si se instala un software malicioso en un UE, el atacante puede utilizar el UE infectado para lanzar algunos tipos de ataques, por ejemplo, para robar datos personales contenidos en el UE, lanzar un ataque DDoS o intentar infectar otro UE. Algunos ejemplos de software malicioso son el malware, el ransomware, los virus, los gusanos, los troyanos y el rogueware. Cuando el software malicioso infecta el UE, el punto extremo móvil actúa como red robot.
- **Amenaza de redes robot** [b-Kahn]: las redes robot son un tipo de malware capaz de controlar un conjunto de dispositivos conectados a Internet. Las redes robot móviles pueden apuntar a muchos puntos extremos móviles para lanzar diferentes tipos de ataques (por

ejemplo, DoS) de manera automática contra sistemas IMT-2020. Dado que las IMT-2020 proporcionan conexión entre teléfonos móviles con mucha potencia informática, estas amenazas están aumentando. Además, la conexión de dispositivos IoT da pie a nuevos tipos de amenazas. Por tanto, los dispositivos IoT son vulnerables a los ataques de redes robot IoT. Un ejemplo es la red robot Mirai, que atacó a millones de cámaras IP en 2016.

- **Amenazas de malware móvil** [b-Kahn]: el malware móvil permite que los atacantes roben datos PII almacenados en dispositivos móviles e incluso inicien ataques (por ejemplo, de DoS) contra otras entidades, como otros UE, redes de acceso móvil y redes troncales de operadores móviles.
- **Acceso no autorizado a datos de usuario y señalización y destrucción, divulgación o modificación de esa información**: un atacante puede obtener acceso no autorizado a los datos de usuario y señalización transmitidos entre un UE y un nodo B de próxima generación o proceder a su destrucción, divulgación o modificación.
- **Manipulación con credenciales de abonado**: un atacante puede manipular una credencial de abonado que se utiliza con fines de autenticación y confidencialidad.

8.3 Amenazas a redes de acceso

Se han identificado las amenazas de seguridad a redes de acceso siguientes:

- **Tráfico elevado malicioso o accidental** [b-NGMN]: a medida que aumentan la capacidad de red y el número de elementos de UE, existe un riesgo elevado de que se produzcan cambios importantes en los patrones de tráfico de red malicioso o accidental a raíz de eventos grandes. A esta escala, no es posible establecer la intención de los incrementos de red, por lo que el objetivo principal consiste en prevenir los eventos maliciosos, teniendo en cuenta ambos escenarios.
- **Filtración de claves entre enlaces de operador** [b-NGMN]: la clave de cifrado (y, en ocasiones, de integridad) de la interfaz inalámbrica se calcula a partir de la red troncal residencial y se envía a la red inalámbrica visitada a través de un enlace de señal como SS7 (sistema de señalización N.° 7) [b-UIT-T Q700] o Diameter [b-RFC 3588]. Se trata de un punto de exposición evidente y muestra cómo se produce la filtración de la clave.
- **Puesta en peligro de la integridad del plano de usuario** [b-NGMN]: existe el peligro de que una sesión completa sea interceptada y utilizada para insertar datos erróneos en la conexión móvil (o de que se desperdicien los datos al transferirlos al punto extremo de servicio, ya desperdiciado).
- **Despliegue de seguridad opcional** [b-Kahn], [b-NGMN]: esta amenaza procede del despliegue de seguridad opcional. Existen muchas configuraciones de seguridad que no influyen en la interoperabilidad (principalmente con los UE) y que se han considerado históricamente como opciones de despliegue. Esta opción puede conllevar el riesgo de que el operador resulte inevitablemente afectado por las acciones de otros operadores, pese a no ser responsable de ellas. También pone en peligro las hipótesis de seguridad del nivel del sistema. Si no se realiza este paso de autenticación, el nivel principal no puede lograr uno de los objetivos previstos en su diseño, a saber, proteger a los clientes de las estaciones base defectuosas.
- **Amenaza basada en informes falsos sobre el estado de la memoria intermedia** [b-Kahn]: los atacantes pueden utilizar los informes sobre el estado de la memoria intermedia de los componentes de la red de acceso, incluidas las estaciones base, para obtener información variada (por ejemplo, sobre la planificación de paquetes, el equilibrio de carga y los algoritmos de control de admisión) a fin de ejecutar sus propósitos maliciosos. A continuación, el atacante podrá hacerse pasar por el UE legítimo para enviar informes falsos sobre el estado de la memoria intermedia y poner en peligro las operaciones.

- **Amenazas de inserción de mensajes** [b-Kahn]: la inyección de mensajes permite lanzar ataques DoS contra redes IMT-2020. Por ejemplo, permite sobrecargar un dispositivo SDN cuya tabla de flujos se haya actualizado de manera incorrecta. El atacante también puede inyectar unidades de datos de protocolo de control (C-PDU) en el sistema durante su activación para ejecutar ataques DoS contra UE recién llegados.
- **Amenazas asociadas a microcélulas** [b-Kahn]: se ha reducido drásticamente el tamaño físico de las estaciones base, que se han trasladado a instalaciones interiores, como centros comerciales, lugares públicos, estadios y hospitales. Además, la adopción de frecuencias nuevas, como la frecuencia mmWave, facilitará el uso de microestaciones base. Sin embargo, estas no son tan seguras desde el punto de vista físico como las macroestaciones base utilizadas en las redes previas a las IMT-2020. Asimismo, el mayor número de estaciones base incrementará las vulnerabilidades potenciales de las redes IMT-2020.
- **Pirateo de sesión** [b-ENISA]: en un ataque por pirateo de sesión, que está relacionado con la interfaz inalámbrica, el atacante toma el control de una sesión de usuario. Si se trata de una sesión autenticada legítima, el atacante controla toda la sesión de tráfico específico con el objetivo de lanzar otro tipo de ataque.
- **Amenazas procedentes de redes de acceso falsas** [b-ENISA]: si la seguridad de una estación base está comprometida, el atacante puede hacerse pasar por una estación base legítima y lanzar un ataque de intermediario o modificar el tráfico de red. Esta amenaza implica manipular la comunicación entre el UE móvil y la red para iniciar la otra acción.
- **Manipulación de los datos de configuración de la red de acceso** [b-ENISA]: cuando un elemento de la red de acceso, por ejemplo, una estación base, se ve comprometido, el atacante puede falsificar los datos de configuración y lanzar otros ataques (por ejemplo, DoS).
- **Amenazas asociadas a la captación de identidades (IMSI)** [b-ENISA]: cuando se utilizan protocolos de radiobúsqueda celular, el atacante puede asociar la identidad virtual de la víctima con la instancia de radiobúsqueda. Un atacante malicioso podrá verificar la información sobre la ubicación de la víctima, introducir mensajes de radiobúsqueda fabricados y lanzar ataques DoS.
- **Interrupción del servicio en respuesta a una solicitud de conexión RRC manipulada**: cuando un atacante manipula el mensaje de solicitud de conexión RRC transmitido como texto sin formato, puede utilizar la información de identificación temporal de la víctima para bloquear la posterior conexión de red de la víctima. El escenario de ataque detallado se describe en el Apéndice II.

8.4 Amenazas a redes definidas por software

Las amenazas a las SDN se describen en [UIT-T X.1038].

8.5 Amenazas a la red troncal

A continuación, se describen las amenazas a la seguridad de la red troncal:

- **DDoS** [b-Kahn]: los ataques DDoS se pueden iniciar como amplificación de señalización y saturación de AUSF y UDM utilizando redes robot que controlan múltiples UE infectados.
- **Amenazas relacionadas con la seguridad de la capa de transporte (TLS)/capa de conexiones seguras (SSL)** [b-Kahn]: las comunicaciones basadas en TLS/SSL que se utilizan en las redes troncales basadas en SDN son vulnerables a los ataques DDoS TCP/SYN (sincronizados), a los sesgos RC4 en TLS, a los ataques por explotación maliciosa de navegadores contra SSL/TLS (BEAST), a los ataques por filtración de información de ratio de compresión (CRIME), el ataque LUCKY 13 [b-LUCKY] y a los ataques por oráculos de relleno en cifrados antiguos degradados (POODLE) [b- POODLE], entre otros.

- **Barrido de SDN** [b-Kahn]: un atacante puede analizar el tráfico de SDN y recabar manualmente la información de la red, incluidos el protocolo de infraestructura y los elementos de red principales del controlador SDN. Esta información puede utilizarse para ejecutar varios tipos de ataques, por ejemplo, DoS, reinicio del TCP, repetición y suplantación.
- **Desviación maliciosa del tráfico** [b-ENISA]: cuando un elemento de red está expuesto, los atacantes pueden desviar los flujos de tráfico e interceptar el tráfico de red. La desviación del tráfico es una amenaza que afecta a los elementos de red del plano de datos. Un ejemplo típico en las redes virtualizadas consiste en invadir el segmento de red. Esta amenaza puede producirse cuando el aislamiento entre los segmentos de un nodo activo corre peligro o cuando el acceso a un segmento del equipo periférico se ignora o está mal configurado.
- **Utilización indebida de las herramientas de auditoría** [b-ENISA]: los operadores de red emplean herramientas de auditoria para supervisar la actividad de la red y obtener información para múltiples fines, por ejemplo, la optimización, le mejora de la seguridad y la explotación comercial. Con este tipo de herramientas de software, los atacantes maliciosos pueden ejecutar actividades de reconocimiento con miras a un ataque. Los atacantes maliciosos suelen recurrir a elementos internos del operador de red móvil (MNO) con acceso privilegiado a estas herramientas, a fin de obtener información sensible.
- **Fuga de datos sobre claves a largo plazo para autenticación/autorización de usuario** [b-ENISA]: esta amenaza está relacionada con la exposición de las claves a largo plazo de los controles de autenticación y seguridad realizados de forma interna o por un trabajador hostil o poco fiable de la red troncal.
- **Explotación de sistemas y/o redes configurados de manera incorrecta o inadecuada** [b-ENISA]: si la configuración de los sistemas y las redes es incorrecta o inadecuada, los atacantes pueden acceder a activos críticos. Los atacantes pueden utilizar un sistema con configuración accidentalmente incorrecta para llegar a activos críticos de la red. Los errores de configuración pueden referirse a diferentes etapas del ciclo de vida de aplicación de la solución, como la instalación y el mantenimiento de los productos.
- **El rastreo de tráfico** [b-ENISA] es un rastreador utilizado por los atacantes para interceptar, registrar y analizar el tráfico y los datos de red que son software o hardware. A través del rastreo, los atacantes también pueden acceder a los datos de ciertos elementos de red o conectar con información sensible y robarla. Se puede utilizar el rastreo en cualquier ubicación con tráfico constante.
- **Registro de funciones de red maliciosas** [b-ENISA]: esta amenaza consiste en desplegar funciones de red maliciosas en redes IMT-2020. Se puede instalar de manera indebida una función de red no autorizada o una función que incorpore un troyano introduciéndola en la red a través de un elemento interno (del MNO) o un vendedor/proveedor de servicios, para registrarla en la red troncal a través de una función de almacenamiento de funciones de red (NRF) con el objetivo de exponer otras API maliciosas. Al instalar o activar una función de red (NF) no autorizada, el atacante podría acceder a activos sensibles de la red para realizar otros tipos de ataque como DoS, distribución de software malicioso o robo de información sensible.
- **Exposición de NF inseguras a funciones de aplicación de terceros** [b-Ta-Hao Ting]: la exposición de funciones de red entre redes internas y externas permite el despliegue dinámico y flexible de las IMT-2020. Si se suplanta o manipula un mensaje, toda la red troncal resultará afectada.
- **Interfaz basada en servicios insegura** [b-TS 33.501]: se suplanta o manipula un mensaje entre elementos de red a través de la interfaz basada en servicios (SBI), con miras a su posible modificación y divulgación.

8.6 Amenazas a la segmentación de la red

Se han identificado las siguientes amenazas a la segmentación de la red:

- **Amenazas a la comunicación entre segmentos de la red** [b-Khan]: un atacante puede perturbar la comunicación entre segmentos para impedir la correcta gestión del ciclo de vida de los segmentos.
- **Ataque por suplantación de identidad** [b-Khan]: un atacante puede suplantar la identidad de una plataforma anfitriona física para asignar recursos no disponibles. Además, un atacante puede suplantar la identidad de un administrador de segmentos de red para robar un parámetro de creación de segmento de red.
- **Discordancia de políticas de seguridad** [b-Khan]: la variedad de políticas de seguridad y de protocolos de seguridad entre los distintos segmentos permite a los atacantes acceder al sistema de segmentación de la red y controlar las entidades a través del segmento menos seguro.
- **DoS** [b-Khan]: un atacante puede realizar un ataque de DoS en una plataforma virtualizada o en recursos físicos, a fin de agotar los recursos de red disponibles para otros segmentos.
- **Canal paralelo** [b-Khan]: un atacante obtiene acceso a un segmento y ataca a un conjunto de segmentos que comparten el mismo hardware principal.
- **Filtración de datos privados** [b-Khan]: los proveedores de infraestructuras o los proveedores de VNF roban la información de los usuarios a través de los segmentos.
- **Amenazas relativas al hipervisor** [b-Khan]: ataques contra el hipervisor para poner en peligro la virtualización de los recursos. Estos ataques consisten en errores de software en el hipervisor, entrada por la puerta trasera a través del sistema operativo anfitrión, ataques de DoS y ataques a los recursos de hardware.

8.7 Amenazas a la computación periférica de acceso múltiple

Se han identificado las siguientes amenazas a la computación periférica:

- **Pasarela MEC falsa o fraudulenta** [b-ENISA]: la naturaleza abierta de las pasarelas periféricas puede dar lugar a una situación de ataque en la que los atacantes pueden desplegar sus propios dispositivos pasarela. Esta amenaza tiene el mismo efecto que los ataques de intermediario.
- **Sobrecarga de nodo periférico** [b-ENISA]: si determinadas aplicaciones móviles o dispositivos de IoT comienzan a inundar el nodo periférico con peticiones o tráfico dirigido a ese componente, puede producirse una sobrecarga del nodo periférico a nivel local o de servicio. Este ataque procede de redes periféricas formadas por dispositivos IoT que perturban los nodos vecinos de la red afectada.
- **Abuso de API abiertas periféricas** [b-ENISA]: si se explotan las vulnerabilidades de las aplicaciones de tipo MEC, se puede abusar de las API de los nodos de la MEC. Se necesitan API abiertas en la MEC principalmente para dar soporte a los servicios federados y a las interacciones con distintos proveedores y creadores de contenido. Esta amenaza puede vincularse a la DoS, los ataques de intermediario, la filtración de datos privados y la manipulación de VM.
- **Manipulación física con dispositivos**: la manipulación física con dispositivos es más probable que sea posible, ya que los recursos informáticos de la arquitectura de computación periférica se encuentran más cerca de los atacantes. El atacante puede destruir los nodos periféricos y, a su vez, poner en peligro la eficacia de toda la red.

8.8 Amenazas a la virtualización de las funciones de red

Se han identificado las siguientes amenazas a la NFV:

- **Abuso del protocolo de interconexión de centros de datos (DCI)** [b-ENISA]: si se explotan las vulnerabilidades de los protocolos de DCI, un atacante podría crear tráfico falsificado. El despliegue de sistemas virtualizados en centros de datos puede generar amenazas para la seguridad de los centros de datos, que han de tenerse en cuenta.
- **Abuso de los recursos de computación en la nube** [b-ENISA]: si un atacante utiliza un simple proceso de registro en un proveedor de servicios de computación en la nube, puede abusar de una potente infraestructura informática, tanto de sus componentes de software como de hardware. Los atacantes se aprovechan de la capacidad informática existente en las redes en la nube y pueden iniciar ataques en muy poco tiempo. Por ejemplo, un atacante puede lanzar ataques de fuerza bruta y ataques de DoS abusando de la capacidad de la computación en la nube.
- **Elusión de la virtualización de la red** [b-ENISA]: los problemas relacionados con una mala ejecución y configuración de la segmentación de la red, o un aislamiento inadecuado, pueden provocar la pérdida de la confidencialidad/privacidad de los datos (datos/tráfico interceptado por entidades de otros segmentos). Una red utilizada por distintos arrendatarios debe asegurarse de que solo el tráfico legítimo entra o sale de un segmento de la red, y de que cualquier elemento de conmutación comprueba y ejecuta el aislamiento del tráfico, instalando reglas de flujo legítimo que impidan el acceso al segmento. A nivel de la red troncal, un atacante hostil explotaría las vulnerabilidades del hipervisor y de la configuración de las reglas de flujo para traspasar el aislamiento del segmento y divulgar datos pertenecientes a otros arrendatarios.
- **Abuso del anfitrión virtualizado** [b-ENISA]: la ejecución de aplicaciones en anfitriones virtualizados puede dar lugar a un abuso de los recursos compartidos en el entorno virtualizado. En los entornos virtualizados, en los que los recursos físicos se comparten entre los arrendatarios, puede haber un conjunto de comportamientos que den lugar a la divulgación de información sensible. Por ejemplo, la exposición a través de la búsqueda de residuos de datos en los entornos virtualizados es mayor que en los sistemas físicos. Aunque la interceptación es una amenaza común en los sistemas físicos (por ejemplo, los entornos de red), sus efectos se agravan aún más en los entornos virtuales porque estos permiten la inspección cruzada de flujos de datos de varios arrendatarios, así como interferencias relativas a la topología que podrían utilizarse para preparar un ataque de DoS.
- **Amenaza a la integridad de la infraestructura** [b-Alwakeel]: un atacante suplanta la identidad de un proveedor de servicios para aparecer como parte de los servicios reales de la NFV y obtener acceso a los datos de los usuarios.
- **Utilización indebida de los recursos** [b-Alwakeel]: un atacante libera algunos recursos y los utiliza en beneficio propio.
- **Cambio de la definición de función de NFV** [b-Alwakeel]: un atacante modifica algunas de las operaciones de la funcionalidad o definición de NFV, o incluso causa una DoS. Se suele hacer por infiltración.
- **Modificación de los privilegios** [b-Alwakeel]: un atacante modifica los privilegios de los usuarios mediante un ataque sin control de datos, en el que se mejora o degrada su acceso a las entidades del sistema, de forma no autorizada.
- **Ataque a la confidencialidad de los datos basado en recursos compartidos** [b-Alwakeel]: mediante un ataque de canal paralelo, los atacantes pueden extraer información privada de otros usuarios utilizando un servicio compartido de forma no autorizada.
- **Usuario interno malicioso** [b-Alwakeel]: los miembros de confianza de una organización se sirven de su autoridad para acceder a datos privados de los usuarios de forma no autorizada.

8.9 Amenazas a la gestión

Se han identificado las siguientes amenazas a la gestión:

- **Interfaz de gestión insegura** [b-TR 33.811]: esta amenaza existe cuando la interfaz no está protegida. Permite a los atacantes obtener acceso a las capacidades de gestión de red sin autorización y crear instancias de segmentos de red que requieren importantes recursos de red o un gran número de instancias de segmentos de red.
- **Divulgación de datos de supervisión y notificación relacionados con la función de gestión** [b-TR 33.811]: esta amenaza existe cuando los datos de supervisión y notificación no están protegidos de forma adecuada, lo que da lugar a que un atacante manipule los resultados de supervisión/notificación, e intercepte la transmisión de datos de supervisión y notificación y extraiga información sensible que puede usarse para ejecutar ataques en instancias de segmentos de redes en funcionamiento.
- **Acceso no autorizado a la interfaz de gestión de la exposición** [b-Ta-Hao Ting]: si la interfaz se ve comprometida por un acceso no autorizado, las funciones de red, incluidas la SDN, la NFV y la segmentación de redes, pueden sufrir anomalías de funcionamiento inadecuadas, como la introducción de cambios no autorizados en las funciones de red, el establecimiento de configuraciones de red inadecuadas y la modificación de las funciones de red.

9 Requisitos aplicables a las capacidades de seguridad relativas a los componentes y las funciones

9.1 Capacidades de seguridad relativas a los equipos de usuario

En el marco de los UE, se debería dar soporte a las siguientes capacidades de seguridad:

- **Capacidad de lucha contra el malware para proteger los UE**: los programas anti-malware están diseñados para evitar, detectar y suprimir programas informáticos maliciosos (malware) de los UE. A fin de proteger los UE frente a infecciones por programas maliciosos, se utilizan tres métodos: la detección de malware basada en firmas, la detección de malware basada en el comportamiento y la utilización de bancos de pruebas aislados.
- **Capacidad de seguridad IMSI para garantizar la seguridad de la identidad del abonado (IMSI) mediante encriptación**: la IMSI debería encriptarse mediante clave de encriptación efímera utilizando un algoritmo criptográfico simétrico. Como condición previa, el UE debe disponer de su propia IMSI y de la clave asimétrica pública de la red doméstica, y cada operador móvil (denominado aquí "red doméstica") debe disponer de un par público/privado de claves asimétricas. Se parte del supuesto de que la red doméstica mantiene en secreto la clave asimétrica privada de la red doméstica, mientras que la clave asimétrica pública de la red doméstica está preconfigurada en los dispositivos móviles, junto con las IMSI específicas del abonado.
- **Capacidad de verificación de la identidad**: verifica la identidad del usuario para los servicios de itinerancia y en la nube.
- **Capacidad de gestión de claves**: permite la verificación de la identidad del usuario y la autenticación mutua entre el UE y el elemento de red.
- **Capacidad de seguridad de la ubicación**: garantiza la seguridad de la ubicación del usuario.
- **Autenticación de la red de servicio**: el UE debería autenticar el identificador de la red de servicio mediante la autenticación de clave implícita, lo que significa que la autenticación ha de proporcionarse a través del uso correcto de las claves resultantes del acuerdo de autenticación y claves en los procedimientos subsiguientes.

- **Confidencialidad e integridad de los datos de usuario y los datos de señalización** [b-UIT-T X.1811]: el UE puede dar soporte tanto a la confidencialidad de los datos, mediante algoritmos de cifrado para el encriptado, como a la protección de la integridad y a la protección contra reproducción de los datos de usuario entre el UE y los nodos de la red.
- **Capacidad de almacenamiento y procesamiento seguro de las credenciales de abonado** [b-Craven]: el UE tiene la capacidad de proteger la integridad de las credenciales y sus claves a largo plazo mediante hardware resistente a la manipulación. No se debería poder acceder de las claves a largo plazo sin encriptar fuera del hardware resistente a la manipulación. El programa debería ejecutarse en el hardware resistente a la manipulación utilizando un algoritmo de autenticación y las credenciales de abonado.

9.2 Capacidades de seguridad relativas a la red de acceso

En el marco de las redes de acceso, se debería dar soporte a las siguientes capacidades de seguridad:

- **Capacidad de seguridad de los enlaces**: proporciona confidencialidad e integridad a las comunicaciones de los canales de control y los canales de tráfico de usuario con el UE.
- **Capacidad de autenticación del UE**: la red de servicio debería autenticar el identificador permanente de abonado en el proceso del acuerdo de autenticación y claves entre el UE y la red.
- **Capacidad de autorización del UE** [b-Craven]: la red de servicio debería autorizar al UE utilizando el perfil de abonado obtenido de la red doméstica.
- **Capacidad de la red doméstica para autorizar la red de servicio** [b-Craven]: debería asegurase de que el UE está conectado a una red de servicio autorizada por la red doméstica.
- **Capacidad para autorizar la red de acceso** [b-Craven]: la red de servicio debería autorizar a la red de acceso para la prestación de servicios al UE.
- **Capacidad de confidencialidad de los datos de usuario y de señalización** [b-Craven]: la red de acceso debería dar soporte al encriptado de los datos de usuario en tránsito y de la señalización de RRC.
- **Capacidad de integridad de los datos de usuario y de señalización** [b-Craven]: los nodos, al igual que el UE, deberían dar soporte a la protección de la integridad y la protección contra reproducción de los datos de los usuarios que circulan entre el UE y el siguiente nodo B.
- **Capacidad de instalación y configuración** [b-Craven]: cuando se instalan y configuran los sistemas de operaciones y gestión, el siguiente nodo B debería ser autenticado y autorizado por una autoridad de registro y una autoridad de certificación (RA/CA) para que los atacantes no puedan modificar las ajustes y las configuraciones de software del siguiente nodo B.
- **Capacidad de gestión de claves dentro del siguiente nodo B** [b-Craven]: es necesario proteger los distintos elementos de las claves de encriptación proporcionadas por la red troncal de IMT-2020 al siguiente nodo B.
- **Capacidad de gestión de datos del plano del usuario y del plano de control** [b-Craven]: la capacidad de gestión de claves es similar a la de la gestión de datos del plano de usuario y del plano de control para el siguiente nodo B.
- **Capacidad de entorno seguro** [b-Craven]: también existen requisitos para el entorno seguro en el que se ejecutan todos estos datos no encriptados. El entorno seguro debería dar soporte al almacenamiento seguro, mediante, por ejemplo, secretos criptográficos a largo plazo y datos de configuración esenciales.
- **Capacidad para hacer frente a las amenazas de interrupción de servicio de las solicitudes de conexión RRC**: para evitar la amenaza que plantean las solicitudes de conexión RRC manipuladas, las estaciones base deben mantener la conexión RRC con los usuarios existentes durante un periodo de tiempo más largo. En concreto, las estaciones base

deben mantener una conexión más larga que el temporizador de espera de la conexión RRC existente. Además, en dichas estaciones base, deberían utilizarse los parámetros de "límite de tiempo" y "cómputo de límite", y se debería añadir un proceso de supervisión para comprobar si se están produciendo dichos ataques. El escenario de ataque detallado se describe en el Apéndice II.

9.3 Capacidades de seguridad relativas a las redes definidas por software

En el marco de las SDN, se debería dar soporte a las siguientes capacidades de seguridad [UIT-T X.1038]:

- **Capacidad de autenticación** de la aplicación SDN para autenticar el controlador SDN/el usuario/el administrador.
- **Capacidad de autorización** de la aplicación SDN para autorizar al usuario y/o administrador a acceder a información del sistema.
- **Capacidad de confidencialidad de los datos** de la aplicación SDN para proteger la confidencialidad de la información del sistema almacenada en la plataforma de la aplicación y proteger la confidencialidad del transporte de datos a través de la interfaz de control de la aplicación.
- **Capacidad de gestión de claves/certificados** de la aplicación SDN para permitir la gestión de claves y/o certificados.
- **Capacidad de gestión de la seguridad** de la aplicación SDN para permitir el registro y la auditoría.
- **Capacidad de protección de las aplicaciones** de la aplicación SDN para permitir la defensa contra las vulnerabilidades de la aplicación.
- **Capacidad de integridad de los datos** de la aplicación SDN para permitir la protección de la integridad del transporte de datos a través de la interfaz de control de la aplicación.
- **Capacidad de autenticación** del controlador SDN para autenticar a los administradores/la aplicación SDN/el conmutador SDN.
- **Capacidad de autorización** del controlador SDN para autorizar a los administradores/la aplicación SDN a gestionar el controlador SDN.
- **Capacidad de autenticación y gestión de la seguridad** del controlador SDN para permitir la protección anti-DoS.
- **Capacidad de integridad de los datos del controlador SDN** para proteger la integridad de los datos de configuración almacenados en el controlador SDN; para proteger la integridad de los datos de usuario almacenados en el controlador SDN; para proteger la integridad del transporte de datos a través de la interfaz de control de la aplicación; y para proteger la integridad del transporte de datos a través de la interfaz de control de recursos.
- **Capacidad de gestión de claves y/o certificados** del controlador SDN para realizar la gestión de claves y/o certificados.
- **Capacidad de confidencialidad de los datos del controlador SDN** para ejecutar la protección de la confidencialidad de los datos de configuración almacenados en el controlador SDN; para ejecutar la protección de la confidencialidad de los datos de usuario almacenados en el controlador SDN; para ejecutar la protección de la confidencialidad del transporte de datos a través de la interfaz de control de la aplicación; y para ejecutar la protección de la confidencialidad del transporte de datos a través de la interfaz de control de recursos.
- **Capacidad de fortalecimiento del sistema operativo del controlador SDN** para permitir el fortalecimiento del sistema operativo.
- **Capacidad de autenticación de la capa de recursos SDN** para autenticar a los administradores y/o al controlador SDN.

- **Capacidad de autorización de la capa de recursos SDN** para autorizar a los administradores a gestionar los conmutadores SDN.
- **Capacidad de gestión de la seguridad de la capa de recursos SDN** para permitir el registro y la auditoría.
- **Capacidad de integridad de los datos de la capa de recursos SDN** para ejecutar la protección de la integridad de los datos de configuración almacenados en el conmutador SDN y para ejecutar la protección de la integridad del transporte de datos entre conmutadores SDN y/o para ejecutar la protección de la integridad del transporte de datos a través de la interfaz de control de recursos.
- **Capacidad de gestión de claves y/o certificados de la capa de recursos SDN** para realizar la gestión de claves y/o certificados.
- **Capacidad de confidencialidad de los datos de la capa de recursos SDN** para ejecutar la protección de la confidencialidad de los datos de configuración almacenados en el conmutador SDN; para ejecutar la protección de la confidencialidad del transporte de datos entre conmutadores SDN; y para ejecutar la protección de la confidencialidad del transporte de datos a través de la interfaz de control de recursos.
- **Capacidad de prevención del desbordamiento de la capacidad de la tabla de flujos de la capa de recursos SDN**. El controlador SDN debe procurar un mantenimiento dinámico de la tabla de flujos incorporando y eliminando entradas de flujo.

9.4 Funciones de seguridad relativas a la red troncal

Se debería dar soporte a las siguientes funciones de seguridad:

- **Capacidad de detección de DoS y DDoS** para proteger el punto de control centralizado de la SDN.
- **Capacidad de verificación de la configuración** para verificar las reglas de flujo del elemento de red SDN.
- **Capacidad de control para limitar el acceso** a la SDN y a los elementos de la red troncal.

También se debería dar soporte a las siguientes funciones de exposición de red y de interfaz basada en servicios:

- **Capacidades de exposición de las funciones de seguridad de la red** [b-TS 33.501]: la autenticación mutua basada en los certificados del cliente y el servidor debería realizarse entre la capacidad de exposición de red y la capacidad de aplicación de las funciones de aplicaciones de terceros fuera del dominio del operador IMT-2020, mediante un túnel seguro, como la TLS. El tráfico entre la capacidad de exposición de red (NEF) y la capacidad de aplicación debería utilizarse a efectos de la protección de la integridad, la protección contra reproducción y la protección de la confidencialidad.
- **Confidencialidad, integridad de los datos y autenticación de los elementos de red a través de una interfaz basada en servicios** [b-TS 33.501]: el tráfico entre los elementos de red, cursado a través de la SBI, debería facilitar la protección de la integridad, la protección contra reproducción y la protección de la confidencialidad de los datos, así como la autenticación de los elementos de red a través de un túnel seguro, como la TLS.

9.5 Capacidades de seguridad relativas a la segmentación de red

En lo que respecta al ciclo de vida de los segmentos, se debería dar soporte a las siguientes capacidades de seguridad [b-Olimid]:

- **Capacidad de seguridad del ciclo de vida de los segmentos**: se debería reforzar la seguridad en las cuatro fases, ya que una vulnerabilidad en una de ellas puede introducir vulnerabilidades en las otras.

- **Capacidad de registro y auditoría adecuados**: deberían implementarse diferentes niveles de registro en distintos segmentos de la red, en función de varios factores, como la normativa aplicable, el nivel de seguridad deseado para los servicios de consumo, los dispositivos específicos según el tipo de consumidor (por ejemplo, uso humano o por aparatos), etc. Se deberían proteger los resultados de los registros e informes, ya que su exposición conllevaría la filtración de información sensible.
- **Capacidad de seguridad de la plantilla de segmento de red**: se debería proteger la confidencialidad y la integridad de su transmisión y almacenamiento, y autenticar el origen de la plantilla.
- **Capacidad de orquestación de la seguridad**: se deberían orquestar y prestar servicios de seguridad personalizados en función de los requisitos de seguridad de las distintas industrias de carácter vertical [b-UIT-T X.1047].
- **Capacidad de aislamiento de segmento**: se debería proteger el aislamiento al crear el segmento, supervisarlo y, de ser necesario, actualizarlo durante el tiempo de ejecución [b-UIT-T X.1047].
- **Capacidad de seguridad de las API**: las API deberían estar protegidas en términos de derechos de acceso y explotación, y no deberían exponer los datos de tráfico; las API deberían admitir únicamente las capacidades y el acceso a los datos en los términos acordados entre las partes por medios jurídicos.
- **Capacidad de desmantelamiento**: en el momento del desmantelamiento, cabría destruir los datos sensibles (o, en su caso, almacenarlos de forma segura) y liberar los recursos y las funciones de red.

Dentro de los segmentos, se debería dar soporte a las siguientes capacidades de seguridad:

- **Capacidad de seguridad de extremo a extremo**: los segmentos son redes lógicas de extremo a extremo, por lo que debería tenerse en cuenta la seguridad de extremo a extremo [b-UIT-T X.1047].
- **Capacidad de utilización adecuada de los mecanismos de seguridad**: todas las comunicaciones (por ejemplo, entre los segmentos y las capas de recursos, entre los segmentos y sus gestores, entre los subsegmentos de cada segmento o entre el dispositivo del cliente y el punto de acceso a la red) deberían aplicar los mecanismos adecuados para garantizar el nivel de seguridad deseado; entre los requisitos mínimos deberían figurar la confidencialidad, la integridad y la autenticación de los datos y la autenticación mutua entre pares.
- **Capacidad de autenticación del UE**: los dispositivos de los clientes IMT-2020 deberían contar con un sólido sistema de autenticación, basado en técnicas de autenticación primaria y, preferiblemente, secundaria.
- **Capacidad de consumo seguro de funciones y recursos**: se deberían proteger todos los recursos y funciones de red consumidos por un segmento.
- **Capacidad de seguridad del arrendatario**: se deberían proteger las nuevas instalaciones introducidas por los arrendatarios (por ejemplo, funciones de red, configuraciones, servicios, etc.), así como su integración, para evitar debilidades que pueden ser explotadas posteriormente.
- **Capacidad de seguridad de la identidad**: se deberían proteger los identificadores sensibles y no se debería filtrar ninguna correlación entre los identificadores.
- **Interceptación legal**: debería ser posible tanto como en la capa de segmento como en la de servicio.
- **Capacidades de acceso, derechos y configuración de los arrendatarios**: deberían ajustarse a los acuerdos jurídicos entre las partes.

En el marco de la comunicación entre segmentos, se debería dar soporte a las siguientes capacidades de seguridad:

- Debería garantizar un nivel de seguridad mínimo para cada segmento.
- **Capacidad de aislamiento de segmento**: el aislamiento entre los segmentos debería ser lo suficientemente sólido como para impedir ataques a través de otros segmentos menos seguros [b-UIT-T X.1047].
- **Capacidad de seguridad mínima de la comunicación**: la comunicación entre los segmentos debería reducirse al mínimo, definirse mediante reglas estrictas y efectuarse a través de canales seguros.
- **Capacidad de gestión de claves**: no se deberían compartir las claves criptográficas (ni otros parámetros sensibles) entre segmentos.
- **Capacidad de asignación mínima de recursos**: la asignación de recursos debería garantizar un nivel mínimo de disponibilidad para cada segmento; en particular, los mecanismos de seguridad deberían poder ejecutarse independientemente del consumo de recursos.
- Los segmentos cuyos niveles de seguridad difieran notablemente no deberían compartir recursos ni funciones de red; en particular, no se deberían ejecutar nunca segmentos en modo prueba junto con segmentos en fase dinámica.
- **Capacidad de seguridad independiente**: cada segmento debería contar con sus propios mecanismos de autenticación, autorización y control del acceso.

9.6 Capacidades de seguridad relativas a la computación periférica de acceso múltiple

Se debería dar soporte a las siguientes funciones de seguridad:

- **Capacidad de mitigación de DDoS** para proteger los servicios web en la nube.
- **Capacidad de control del acceso** para limitar el acceso a los elementos de red en el marco de la computación periférica de acceso múltiple.
- **Capacidad de verificación de la integridad** para proteger los datos y el sistema de almacenamiento en el marco de la computación en la nube.
- **Capacidad de control de acceso a los servicios** para limitar el elemento de computación en la nube basado en servicios.
- **Capacidad de seguridad física**: se debería proporcionar seguridad física a cualquier nodo periférico que no esté situado en un centro de datos periférico de alta seguridad, como los que emplean técnicas de protección física adicionales durante la fase de fabricación o implementan mecanismos de bloqueo y otras protecciones físicas sobre el terreno.

9.7 Capacidades de seguridad relativas a la función de virtualización de red

Se debería dar soporte a las siguientes funciones de seguridad:

- **Capacidad de aislamiento del tráfico**: para garantizar las funciones de los segmentos virtuales y de la red virtual.
- **Capacidad de prevención de ataques de DoS** [b-Alwakeel]: deberían utilizarse elementos de red, tales como cortafuegos y equilibradores de cargas, para mitigar los ataques de DoS/DDoS.
- **Capacidad de integridad de la infraestructura** [b-Alwakeel]: debería utilizarse una cadena de confianza y un módulo de plataforma de confianza (TPM) para velar por la seguridad de los distintos proveedores de servicios VNF.
- **Capacidad de mitigación del uso indebido de los recursos** [b-Alwakeel]: se debería proporcionar un planificador avanzado del hipervisor que permita una asignación justa entre los procesos y limite la cantidad máxima permita para cada servicio virtual.

- **Capacidad de protección contra cambios en la definición de funciones NFV** [b-Alwakeel]: se debería conservar una copia de los servicios virtuales del usuario en un lugar de almacenamiento separado, para evitar ataques por infiltración de malware. En estos casos, se utiliza un cuadro de atribución de archivos (FAT) que contiene información sobre los servicios y el software que el usuario está ejecutando.
- **Capacidad de prevención de modificación de los privilegios** [b-Alwakeel]: se debería proteger la entidad de virtualización de los accesos no autorizados incorporando políticas de restricción del acceso a los recursos.
- **Capacidad de mitigación de los recursos compartidos** [b-Alwakeel]: se debería recurrir a una capacidad de mitigación de los ataques de canal paralelo para limitar el acceso a las imágenes de las VM y los componentes de la infraestructura de virtualización de las funciones de red (NFVI), y controlar la utilización de los recursos. A tal efecto, se puede utilizar un cortafuegos virtual que evite los accesos no autorizados al sistema.
- **Capacidad de mitigación de los usuarios internos maliciosos** [b-Alwakeel]: se pueden mitigar los ataques de usuarios internos recurriendo a varias capacidades, entre ellas el registro de los accesos al entorno de NFV, lo que puede utilizarse después para auditorías internas con miras a detectar actividades sospechosas. Otro mecanismo consiste en establecer políticas estrictas de autenticación y autorización para los usuarios que disponen de acceso.

9.8 Capacidades de seguridad relativas a la función de gestión

Se debería dar soporte a las siguientes capacidades de seguridad [b-TR 33.811]:

- **Capacidad de autenticación mutua** entre el consumidor del servicio de gestión y el productor del servicio de gestión utilizando un túnel seguro, como la TLS, basado en 1) los certificados del cliente y el servidor, o 2) claves compartidas previamente (PSK) con TLS-PSK.
- **Capacidad de protección de la integridad, protección contra reproducción y protección de la confidencialidad** para la interfaz entre el productor del servicio de gestión y el consumidor del servicio de gestión que resida fuera de la TLS del dominio de confianza del operador 3GPP.
- **Capacidad de seguridad de las PI de la interfaz de gestión**: las API deberían estar protegidas en términos de derechos de acceso y explotación, y no deberían exponer los datos de tráfico; las API de la interfaz de gestión deberían admitir únicamente las capacidades y el acceso a los datos en los términos acordados entre las partes por medios jurídicos.

Anexo A

Arquitectura de seguridad de los sistemas de comunicaciones IMT-2020

(El presente anexo es parte integrante de la Recomendación.)

La Figura 4-1 en [b-TS 33.501] ilustra una visión de conjunto de la arquitectura de seguridad de los sistemas de comunicaciones IMT-2020.

La Figura 4-1 en [b-TS 33.501] comprende los siguientes dominios de seguridad:

– Seguridad del acceso a la red (I): abarca el conjunto de funciones de seguridad que permite la autenticación de los UE y su acceso a los servicios a través de la red de forma segura, entre otras cosas a través de las redes de acceso 3GPP y las redes de acceso no 3GPP, y garantizar un cierto nivel de protección contra los ataques a las interfaces (radioeléctricas). Además, incluye la comunicación del contexto de seguridad de la red de servicio (SN) a la red de acceso (AN) para afianzar la seguridad del acceso.

– Seguridad del dominio de red (II): abarca el conjunto de funciones de seguridad que permite el intercambio seguro de datos de señalización y datos del plano de usuario entre los nodos de la red.

– Seguridad del dominio del usuario (III): abarca el conjunto de funciones de seguridad que protege el acceso de los usuarios a los equipos móviles.

– Seguridad del dominio de aplicación (IV): abarca el conjunto de funciones de seguridad que permite a las aplicaciones del dominio de usuario y del dominio de proveedor intercambiar mensajes de forma segura. La seguridad del dominio de aplicación queda fuera del alcance del presente Recomendación.

– Seguridad del dominio SBA (V): abarca el conjunto de funciones de seguridad que permite a las NF de la arquitectura SBA comunicarse de forma segura dentro del dominio de la SN y con otros dominios de red. Dichas funciones incluyen aspectos de seguridad relacionados con el registro, el descubrimiento y la autorización de las funciones de red, así como la protección de las interfaces basadas en servicios. La seguridad del dominio SBA constituye una nueva función de seguridad en comparación con [b-TS 33.401].

– Visibilidad y capacidad de configuración de la seguridad (VI): abarca el conjunto de funciones de seguridad que permite comunicar al usuario si una función de seguridad se halla en funcionamiento o no.

Apéndice I

Arquitectura de seguridad de red genérica para la provisión de capacidades de seguridad de red de extremo a extremo

(Este apéndice no forma parte integrante de la presente Recomendación.)

En el presente apéndice se describe un tipo de arquitectura de seguridad de red genérica capaz de garantizar la seguridad de la red de extremo a extremo que se describe en [b-UIT-T X.805], en cuyo contenido se basa esta Recomendación.

En [b-UIT-T X.805] se define una arquitectura que garantiza la seguridad de las redes de extremo a extremo. Esta arquitectura puede aplicarse a distintas clases de red en las que hay que garantizar la seguridad de extremo a extremo y funciona de manera independiente a la tecnología de red subyacente. En la Recomendación [b-UIT-T X.805] se definen los elementos arquitectónicos generales que guardan relación con la seguridad y que son necesarios para garantizar la seguridad de extremo a extremo. El objetivo de la norma en cuestión es servir de base para la redacción de Recomendaciones detalladas en favor de la seguridad de las redes de extremo a extremo.

En la Recomendación [b-UIT-T X.805] se definen ocho dimensiones de seguridad:

1) control de acceso;
2) autenticación;
3) no repudio;
4) confidencialidad de datos;
5) seguridad de la comunicación;
6) integridad de los datos;
7) disponibilidad; y
8) privacidad.

En la Recomendación [b-UIT-T X.805] también se definen tres capas de seguridad que se complementan entre sí para proporcionar soluciones basadas en la red, estas son:

1) la capa de seguridad de la infraestructura;
2) la capa de seguridad de los servicios; y
3) la capa de seguridad de las aplicaciones.

Por último, en [b-UIT-T X.805] se definen tres planos de seguridad:

1) el plano de gestión;
2) el plano de control; y
3) el plano de usuario de extremo.

Apéndice II

Amenaza de interrupción del servicio a partir de una solicitud de conexión de control de recursos radioeléctricos (RRC) manipulada y su capacidad

(Este apéndice no forma parte integrante de la presente Recomendación.)

II.1 Generalidades

Una solicitud de conexión RRC es un mensaje que se transmite cuando un UE accede a una red y se envía en texto sin formato. Incluye la identidad temporal única global (GUTI) o S-TMSI, que es un tipo de información de identificación temporal del UE. Existen diversas formas de averiguar la información de identificación temporal de un usuario concreto. Una vez interceptada la solicitud de conexión RRC y modificado el mensaje transmitido en texto sin formato en el paso anterior, el atacante puede utilizar la información de identificación temporal de la víctima para bloquear continuamente su conexión de red.

II.2 Hipótesis de ataque

Un atacante puede interceptar un mensaje de solicitud de conexión RRC transmitido en texto sin formato e identificar el GUTI o S-TMSI, es decir, la información de identificación temporal de la víctima. Al enviar un mensaje de solicitud de conexión RRC manipulado, el atacante utiliza indebidamente la información de identificación temporal y su mensaje se confunde con el enviado por el UE de la víctima. Aunque la conexión RRC del atacante se libera debido a un fallo de autenticación MAC (código de autenticación de mensajes) durante la señalización NAS (capa de no acceso), el atacante puede bloquear continuamente la conexión de la víctima enviando una vez más el mismo mensaje manipulado. Por otro lado, la información de identificación temporal se renueva a intervalos regulares, con arreglo a unas normas específicas basadas en la IMSI. Si se modifica la S-TMSI, el atacante puede detectar el cambio y volver a enviar un mensaje de ataque. Para bloquear el acceso radioeléctrico del UE víctima, el atacante ha de enviar un mensaje de solicitud de conexión RRC manipulado. A tal efecto, debe cumplir dos requisitos previos: 1) el atacante necesita ubicar su dispositivo móvil en la misma célula en que se halle el UE de la víctima, para capturar el tráfico radioeléctrico; y 2) el atacante debe disponer de un UE capaz de enviar mensajes manipulados.

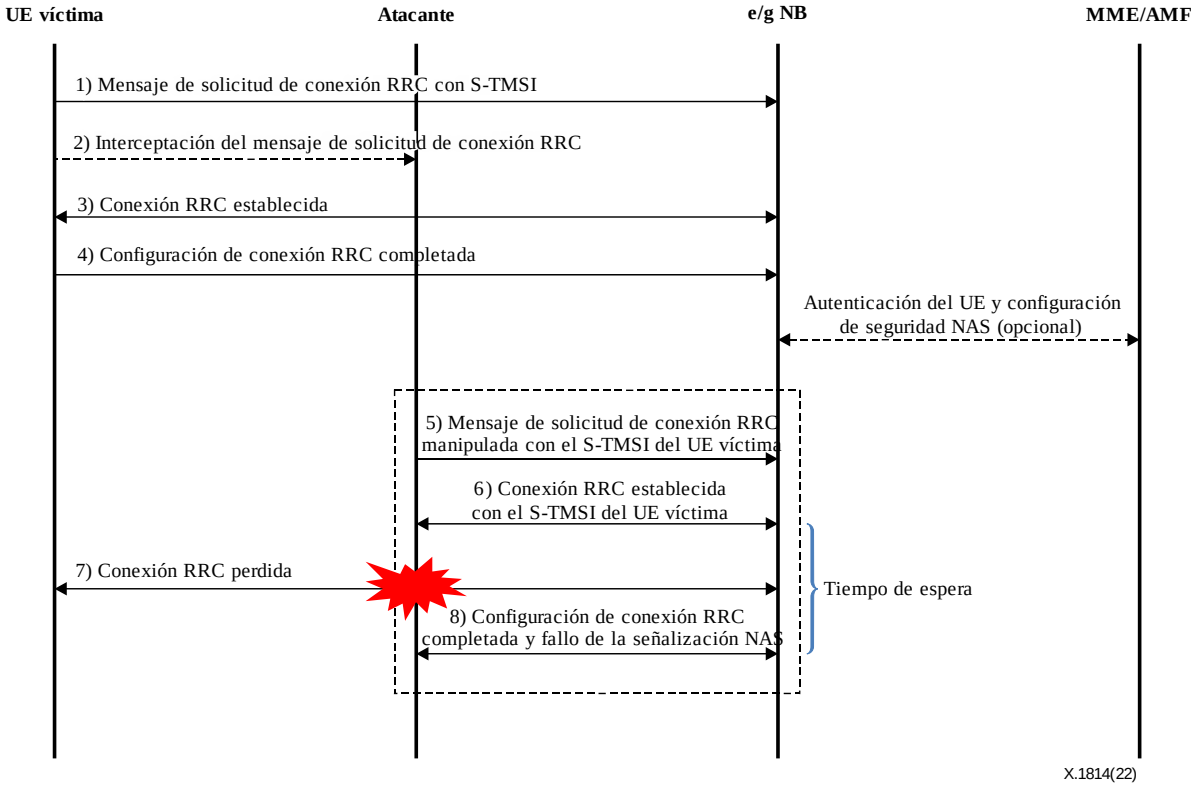

Figura II.1 – Hipótesis de ataque a partir de una solicitud de conexión RRC manipulada

II.3 Consecuencias

Debido a esta vulnerabilidad, a raíz de la cual no se comprueba si el mensaje ha sido manipulado, el equipo de red radioeléctrica (e/gNodeB) desconecta la conexión existente con el UE de la víctima, de acuerdo con el mensaje enviado por el atacante, y se conecta con el UE del atacante. En consecuencia, el equipo de la víctima puede verse privado de la capacidad de acceder a la red con normalidad.

II.4 Contramedidas

La contramedida más sencilla y eficaz consiste en que la estación base mantenga la conexión RRC con el usuario existente durante un periodo de tiempo determinado. Aunque el atacante establezca una conexión RRC utilizando el ID robado de la víctima, la conexión se libera en el momento en que el proceso de señalización NAS falla. En consecuencia, si se logra mantener la conexión previa de la víctima hasta que la conexión RRC del atacante se libere, la conexión radioeléctrica puede mantenerse. Normalmente, el tiempo que transcurre desde que un atacante intenta establecer una conexión RRC hasta que dicha conexión se libera debido a un fallo en el proceso de señalización NAS equivale al tiempo que tarda la estación base en transmitir los datos de configuración de la conexión RRC y esperar a que ésta se complete. Por tanto, cabe la posibilidad de implementar un "temporizador de espera"[1] en el e/gNodeB, a fin de calcular el tiempo que transcurre entre el envío de los datos de configuración de la conexión RRC al UE y la recepción de la configuración de conexión RRC completa. Además, conviene añadir un procedimiento que permita a la estación base mantener una conexión más larga que la establecida por el temporizador de espera para la conexión RRC existente, enviar a continuación una solicitud con un ID duplicado y mantener la conexión existente cuando se libere la nueva conexión dentro del plazo establecido. El tiempo de mantenimiento debe minimizarse, dadas sus repercusiones en los servicios de comunicaciones y la calidad de funcionamiento de los equipos.

[1] Por ejemplo, el sistema T352, definido en la especificación técnica TS 25.331 de 3GPP.

Por otro lado, un atacante puede enviar repetidas solicitudes de conexión RRC a la estación base para mantener el estado de interrupción del servicio a una víctima. Para mitigar esta situación, conviene establecer parámetros de "límite de tiempo" y "límite de repeticiones" en el e/gNodeB, que permitan detectar la reiteración del establecimiento y la liberación de conexiones RRC dentro de un plazo de tiempo determinado y por encima de un umbral concreto. De esta forma, la estación base podrá alertar al operador de red para que este realice un seguimiento de los ataques.

Bibliografía

[b-UIT-T Q.700] Recomendación UIT-T Q.700 (1993), *Introducción al sistema de señalización N.° 7 del CCITT*.

[b-UIT-T X.509] Recomendación UIT-T X.509 (2019), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

[b-UIT-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*.

[b-UIT-T X.1047] Recomendación UIT-T X.1047 (2021), *Requisitos y arquitectura de seguridad para la gestión y orquestación de la segmentación de red*.

[b-UIT-T X.1401] Recomendación UIT-T X.1401 (2019), *Amenazas a la seguridad de tecnología de libro mayor distribuido*.

[b-UIT-T X.1406] Recomendación UIT-T X.1406 (2021), *Amenazas de seguridad para la votación en línea mediante la tecnología de libro mayor distribuido*.

[b-UIT-T X.1408] Recomendación UIT-T X.1408 (2021), *Amenazas y requisitos de seguridad para el acceso y la compartición de datos basados en la tecnología de libro mayor distribuido*.

[b-UIT-T X.1811] Recomendación UIT-T X.1811 (2021), *Directrices de seguridad para la aplicación de algoritmos de seguridad cuántica en sistemas IMT-2020*.

[b-UIT-T Y.3100] Recomendación UIT-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-UIT-T Y.3101] Recomendación UIT-T Y.3101 (2018), *Requisitos de la red IMT-2020.*

[b-UIT-T Y.3150] Recomendación UIT-T Y.3150 (2020), *Características técnicas de alto nivel de informatización de la red para las IMT-2020*.

[b-UIT-T Y.4807] Recomendación UIT-T Y.4807 (2020): *Agilidad por diseño para la seguridad de sistemas de telecomunicaciones/TIC utilizados en la Internet de las cosas*.

[b-UIT taller] Tercer taller y jornada anual de demostración IMT-2020/5G de la UIT (18 de julio de 2018), *Actividades relacionadas con la seguridad de la 5G y planes de futuro de la CE 17 del UIT-T*.

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers*.

[b-ISO 81001-1] ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts.*

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/TS 21719-2] ISO/TS 21719-2: 2018, *Electronic fee collection – Personalization of on-board equipment (OBE) – Part 2: Using dedicated short-range communication*.

[b-RFC 3588] IETF RFC 3588 (2003), *Diameter base protocol*.

[b-TR 33.811] 3GPP TR 33.811 (2018), *Study on security aspects of 5G network slicing management*.

[b-TS 33.401] 3GPP TS 33.401 (2021), *3GPP System Architecture Evolution (SAE); Security architecture*.

[b-TS 33.501] 3GPP TS 33.501 (2022), *Security architecture and procedures for 5G System*.

[b-Alwakeel] Alwakeel, A.M., Alnaim, A., and Fernández, E.B., *A Survey of Network Function Virtualization Security*, IEEE Southeast Conf. 2018. https://www.researchgate.net/publication/328146655_A_Survey_of_Network_Function_Virtualization_Security

[b-Craven] Craven, C., *5G Security Standards: What Are They?* 10 June 2020. https://www.sdxcentral.com/5g/definitions/5g-security-standards/

[b-ENISA] European Union Agency for Cybersecurity (ENISA) (2019), *ENISA Threat Landscape for 5G Networks*.

[b-Goodin] Goodin, D. (2013), *Lucky Thirteen attack snarfs cookies protected by SSL encryption* Ars Technica. https://arstechnica.com/security/2013/02/lucky-thirteen-attack-snarfs-cookies-protected-by-ssl-encryption/

[b-Khan] Khan, R., Kumar, P., Jayakody, D.N.K, and Liyanage, M. (2019), *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions*, IEEE Communications Surveys and Tutorials, Vol. 22, No. 1, July, pp. 196-248.

[b-Möller] Möller, B, Duong, T, and Kotowicz, K. (2014), *This POODLE Bites: Exploiting The SSL 3.0 Fallback*. https://www.openssl.org/~bodo/ssl-poodle.pdf

[b-NGMN] The Next Generation Mobile Networks Alliance (NGMN Alliance) (2016), *5G security recommendations package*.

[b-Olimid] Olimid, R., and Nencioni, G. (2020) *5G Network Slicing: A Security Overview*, IEEE Access, Vol. 8, June, 99999-100009.

[b-SQL] OWASP, *SQL injection.* https://owasp.org/www-community/attacks/SQL_Injection

[b-Ta-Hao Ting] Ta-Hao Ting, Tsung-Nan Lin, Shan-Hsiang Shen, and Yu-Wei Chang (2019), *Guidelines for 5G end to end architecture and security issues*. https://arxiv.org/abs/1912.10318

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2023