ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1815 (03/2023)

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

Seguridad en las redes IMT-2020

Directrices y requisitos de seguridad para los servicios de computación periférica de las IMT-2020

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PUBLICAS 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 INTERCONEXION 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.1815

Directrices y requisitos de seguridad para los servicios de computación periférica de las IMT-2020

Resumen

La red IMT-2020 permitirá una gran variedad de servicios, incluidos los servicios de banda ancha móvil mejorada (eMBB), los servicios basados en comunicaciones masivas de tipo máquina (mMTC) y los servicios basados en comunicaciones ultrafiables y de baja latencia (URLLC), en una infraestructura de recursos de red y computación. A tenor de las características clave y de los requisitos identificados para la red IMT-2020, es necesario que sea más eficiente, personalizada, inteligente, fiable y flexible.

A fin de dar soporte a los servicios típicos de la red IMT-2020, especialmente a los servicios de eMBB y a los servicios basados en las URLLC, la computación periférica está reconocida como una de las tecnologías clave para cumplir los exigentes indicadores fundamentales de rendimiento (IFR) de la red IMT-2020, especialmente en lo que respecta a la baja latencia y a la eficiencia del ancho de banda.

La computación periférica permite al operador y al proveedor de servicios de terceros desplegar los servicios cerca del punto de acceso del usuario, logrando así una prestación de servicios de alta eficiencia gracias a la reducción de la latencia de extremo a extremo y de la carga en la red de transporte.

Con el fin de garantizar la seguridad del despliegue y la aplicación de los servicios de computación periférica, es necesario analizar las amenazas a la seguridad y los requisitos de seguridad pertinentes específicos de los servicios de computación periférica y establecer el marco de seguridad general.

El objetivo del presente proyecto de Recomendación es analizar los métodos de despliegue y los escenarios de aplicación típicos de los servicios de computación periférica, especificar las amenazas y los requisitos de seguridad específicos de los servicios de computación periférica en las IMT-2020 y, por lo tanto, establecer las capacidades de seguridad para que el operador pueda salvaguardar sus aplicaciones.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1815	03-03-2023	17	11.1002/1000/15113

Palabras clave

Directrices de seguridad, red IMT-2020, servicios de computación periférica.

* 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, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1815

Directrices y requisitos de seguridad para los servicios de computación periférica de las IMT-2020

1 Alcance

En la presente de Recomendación se proporcionan posibles métodos de despliegue y los escenarios de aplicación típicos de los servicios de computación periférica, se especifican las amenazas y los requisitos de seguridad específicos de los servicios de computación periférica en las IMT-2020 y, por consiguiente, se facilitan las directrices sobre capacidades de seguridad para que el operador pueda salvaguardar sus aplicaciones.

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 alienta a los usuarios de esta Recomendación a que 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 la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

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

[3GPP TS 23.501] 3GPP TS 23.50 (2022), *5G; Arquitectura del sistema 5G (5GS) (versión 17.4.0 publicación 17).*

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 IMT-2020 [b-UIT-T Y.3100]: (Basado en [b-UIT-R M.2083]) Sistemas, componentes de sistemas y tecnologías conexas que ofrecen capacidades mucho más avanzadas que las descritas en [b-UIT-R M.1645].

3.1.2 caballo de Troya [b-UIT-T E.800]: Parte de un software que parece benigno o incluso útil, pero que esconde el verdadero objetivo del software, que consiste en dañar el sistema o robar información.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 servicio de computación periférica IMT-2020: Un servicio prestado a través del sistema IMT-2020 que permite alojar un servicio cerca del punto de acceso del equipo del usuario, con el fin de lograr una prestación eficiente del servicio gracias a la reducción de la latencia de extremo a extremo y de la carga en la red de transporte.

3.2.2 sistema IMT-2020: Sistema 3GPP compuesto por la red de acceso IMT-2020 (AN), la red medular IMT-2020 y los equipos de usuario (UE).

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siglas y los acrónimos siguientes:

AF Función de aplicación (*application function*)

AMF Función de gestión de acceso y movilidad (*access and mobility management function*)

AN Red de acceso (*access network*)

CDN Red de entrega de contenidos (*content delivery network*)

DC Centro de datos (*data centre*)

DDoS Denegación de servicio distribuida (*distributed denial of service*)

DN Red de datos (*data network*)

DNN Nombre de la red de datos (*data network name*)

DNS Sistema de nombres de dominio (*domain name system*)

EASDF Función de descubrimiento del servidor periférico de aplicaciones (*edge application server discovery function*)

EHE Entorno de alojamiento periférico (*edge hosting environment*)

eMBB Banda ancha móvil mejorada (*enhanced mobile broadband*)

GW-C Plano de control de la pasarela (*gateway-control plane*)

GW-U Plano de usuario de la pasarela (*gateway-user plane*)

IFR Indicador fundamental de rendimiento (*key performance indicator*)

IMS Subsistema multimedios del protocolo Internet (*Internet protocol multimedia subsystem*)

IP Protocolo Internet (*Internet protocol*)

MEC Computación móvil periférica (*mobile edge computing*)

mMTC Comunicaciones masivas de tipo máquina (*massive Machine Type Communications*)

NAT Conversión de dirección de red (*network address translation*)

NB IoT Internet de las cosas de banda estrecha (*narrow-band Internet of Things*)

NEF Función exposición de red (*network exposure function*)

NFVO Orquestador de virtualización de funciones de red (*network functions virtualization orchestrator*)

NRF Función de repositorio de red (*network repository function*)

OSS Sistemas de apoyo a las operaciones (*operation support systems*)

PDU Unidad de datos de protocolo (*protocol data unit*)

PSA Ancla de sesión de unidad de datos de protocolo (*protocol data unit session anchor*)

QoS Calidad de servicio (*quality of service*)

RAN Red de acceso radioeléctrico (*radio access network*)

SBA Arquitectura basada en servicios (*service based architecture*)

SIM Módulo de identificación de abonado (*subscriber identification module*)

SMF Función de gestión de sesiones (*session management function*)

TLS Seguridad de la capa de transporte (*transport layer security*)

UE Equipo de usuario (*user equipment*)

UPF Función de plano de usuario (*user plane function*)

URLLC Comunicaciones ultrafiables de baja latencia (*ultra-reliable low latency communications*)

V2X Vehículo a su entorno (*vehicle to everything*)

VNFM Gestor de funciones de red virtualizadas (*virtualized network function manager*)

5 Convenios

En la presente Recomendación:

La expresión "**se requiere**" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con este documento.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. Su cumplimiento no es indispensable para alegar la conformidad con la presente Recomendación.

6 Síntesis de la computación periférica IMT-2020

La red IMT-2020 permitirá una gran variedad de servicios, incluidos los servicios de banda ancha móvil mejorada (eMBB), los servicios basados en comunicaciones masivas de tipo máquina (mMTC) y los servicios basados en comunicaciones ultrafiables y de baja latencia (URLLC) [UIT-T Y.3101], en una infraestructura de recursos de red y computación. A tenor de las características clave y de los requisitos identificados en la red IMT-2020, es necesario que sea una red más eficiente, personalizada, inteligente, fiable y flexible.

A fin de dar soporte a los servicios típicos de la red IMT-2020, especialmente a los servicios de eMBB y a los servicios basados en las URLLC, la computación periférica está reconocida como una de las tecnologías clave para cumplir los exigentes indicadores fundamentales de rendimiento (IFR) de la red IMT-2020, especialmente en lo que respecta a la baja latencia y a la eficiencia del ancho de banda.

La computación periférica IMT-2020 permite al operador y al proveedor de servicios de terceros desplegar los servicios cerca del punto de acceso del usuario a través del sistema IMT-2020, logrando así una prestación de servicios de alta eficiencia gracias a la reducción de la latencia de extremo a extremo y de la carga en la red de transporte.

6.1 Métodos de despliegue

La arquitectura del sistema IMT-2020 especificada por el 3GPP en el sistema IMT-2020 dispone de dos opciones, una basada en el método tradicional de punto de referencia e interfaz y otra en la que las funciones de la red medular interactúan entre sí utilizando una arquitectura basada en servicios (SBA).

La Figura 6-1 representa una arquitectura del sistema IMT-2020 basada en [3GPP TS 23.501].

Desde la perspectiva del operador, el método de despliegue de los servicios de computación periférica IMT-2020 con SBA puede incluir las siguientes funciones de red IMT-2020:

– UPF (Función de plano de usuario): La UPF es una de las funciones de red (NF) de la red medular de las IMT-2020. Es responsable del encaminamiento y el reenvío de paquetes, la inspección de paquetes, la gestión de la calidad de servicio (QoS) y la sesión de la unidad de datos de protocolo (PDU) externa para la interconexión con la red de datos (DN), en la arquitectura IMT-2020.

– AMF (Función de gestión de acceso y movilidad): La AMF recibe toda la información relacionada con la conexión y la sesión del equipo de usuario (UE) a través de N1 y de la red de acceso (radioeléctrico) ((R)AN) a través de la interfaz N2 (véase la Figura 1), pero sólo se encarga de gestionar las tareas de conexión y movilidad.

– SMF (Función de gestión de sesión): La SMF es un elemento fundamental de la SBA de las IMT-2020. Es la principal responsable de interactuar con el plano de datos disociado, de crear, actualizar y eliminar sesiones de la PDU y de gestionar el contexto de la sesión con la UPF.

– EASDF (Función de descubrimiento del servidor periférico de aplicaciones): La EASDF incluye una o más de las siguientes funcionalidades: registro en la función de repositorio de red (NRF) para el descubrimiento y la selección de la EASDF y gestión de los mensajes DNS según las instrucciones de la SMF. La EASDF tiene conectividad directa en el plano de usuario (es decir, sin conversión de dirección de red (NAT)) con la UPF del ancla de sesión de PDU (PSA) a través de la interfaz N6 para la transmisión de la señalización del sistema de nombres de dominio (DNS) intercambiada con el UE.

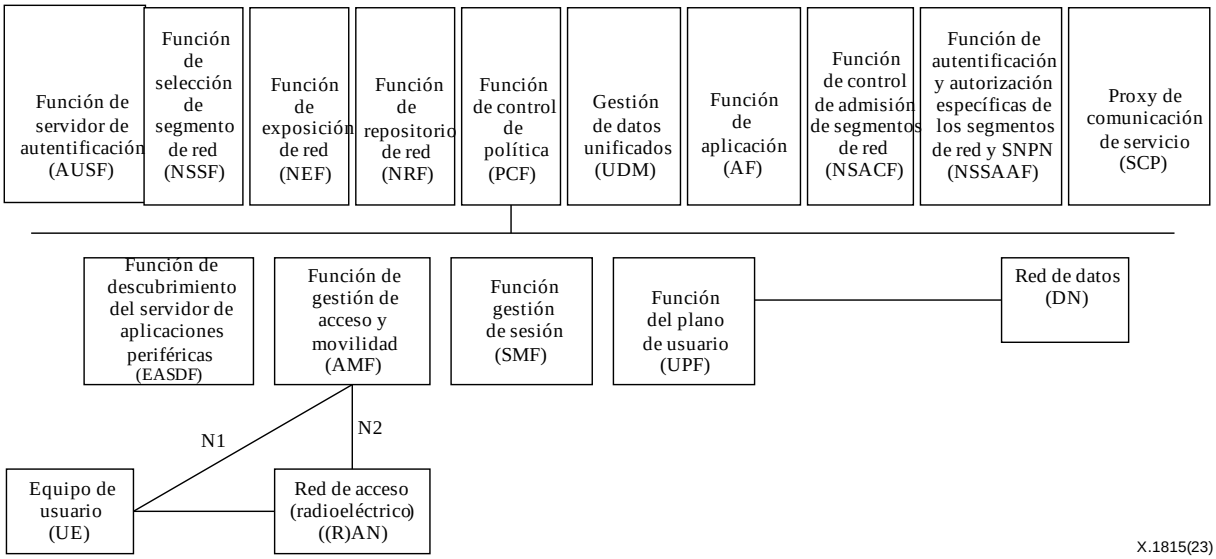

Figura 6-1 – Arquitectura del sistema IMT-2020

La Figura 6-2 describe un método de despliegue de los servicios de computación periférica IMT-2020.

El sistema IMT-2020 soporta el entorno de alojamiento periférico (EHE) desplegado en la DN más allá de la UPF del PSA. Un EHE puede estar bajo el control del operador o de terceros [b-3GPP TS 23.548]. La parte local de la DN en la que se despliega el EHE puede tener conectividad en el plano de usuario tanto con un PSA desplegado centralmente como con un PSA desplegado localmente del mismo DNN.

Desde el punto de vista del operador, el método de despliegue de los servicios de computación periférica IMT-2020 es el que se muestra en la Figura 6-2.

– DC periférico: Proporciona la funcionalidad de computación móvil periférica (MEC) que permite los servicios de computación periférica IMT-2020 y las funcionalidades del plano de usuario de la pasarela (GW-U) y UPF.

– DC local: Proporciona las funcionalidades del GW-U, red de entrega de contenidos (CDN) y UPF.

– DC zonal: Proporciona funcionalidades de plano de control de la pasarela (GW-C), AMF/SMF, NB IoT e IMS, etc.

– Gestión del dominio: Incluye la plataforma de gestión en la nube, el orquestador de virtualización de funciones de red (NFVO) y el gestor de funciones de red virtualizadas (VNFM).

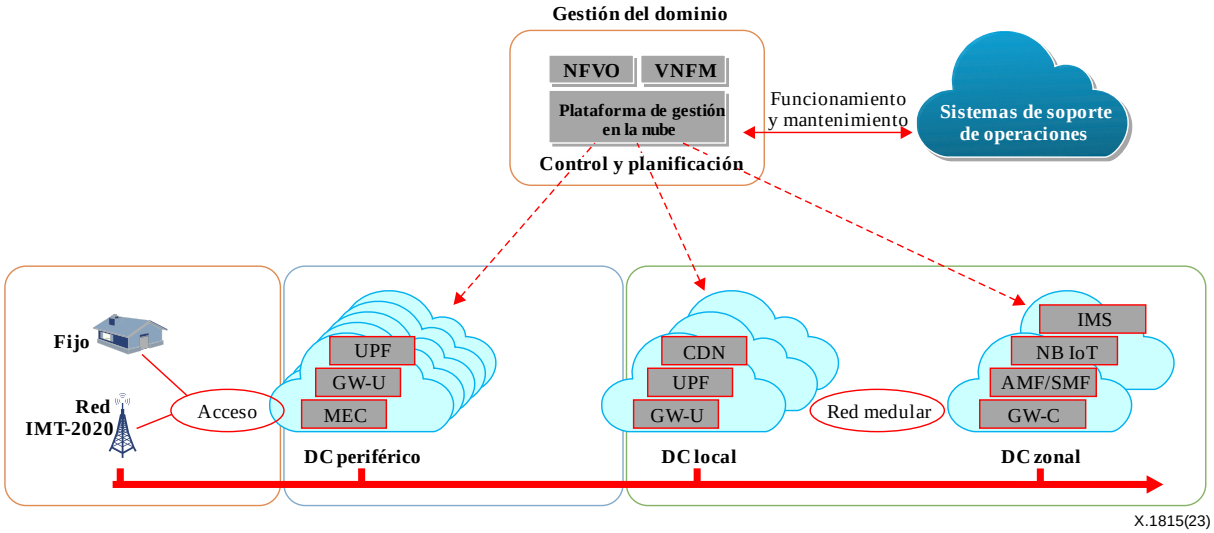

Figura 6-2 – Método de despliegue de los servicios de computación periférica IMT-2020

6.2 Escenario típico de aplicación

6.2.1 Vehículo a su entorno (V2X)

En el escenario de V2X, el volumen de dispositivos conectados con múltiples aplicaciones conlleva un aumento de los requisitos de transferencia de datos al lado red. La red debe ofrecer una banda ancha mejorada y capacidades de computación para el uso y almacenamiento de datos.

Al aplicar la tecnología de computación periférica IMT-2020 en escenarios V2X, es posible desplegar las aplicaciones en el nodo periférico, reduciendo así el retardo de extremo a extremo y aumentando la fiabilidad conforme a los requisitos específicos de los distintos servicios V2X (por ejemplo, el servicio de conducción segura tiene requisitos estrictos de latencia y de fiabilidad), lo que permite beneficiarse de la ruta de transmisión más corta y ofrecer recursos de computación y almacenamiento más potentes.

Los servicios V2X basados en la tecnología de computación periférica IMT-2020 son, entre otros, los siguientes:

– Servicio de información: El servicio de computación periférica ofrece funciones de carga y actualización de mapas, audio y vídeo recreativos, y detección remota para el vehículo. Estas funciones requieren un servicio de computación periférica que ofrezca una capacidad de banda ancha móvil mejorada, por ejemplo, al menos 25 Mbps para el servicio de vídeo de alta definición 4K.

– Servicio de conducción segura: El servicio de computación periférica ayuda al conductor a tomar decisiones de control del vehículo (por ejemplo, avisando de una colisión) mediante la obtención de información del vehículo, de los peatones y de la unidad vial. Es necesario que el servicio de computación periférica ofrezca baja latencia y alta fiabilidad (generalmente, el retardo es inferior a 20 ms y la fiabilidad de las telecomunicaciones es de al menos el 99%).

– Servicio de mejora de la eficiencia en la conducción: El servicio de computación periférica optimiza la eficiencia de las instalaciones de tráfico basándose en las tecnologías IMT-2020 de análisis de macrodatos y V2X, por ejemplo, el control de los semáforos u orientaciones sobre la velocidad de los vehículos.

6.2.2 Internet de las Cosas (IoT)

Al aplicar la tecnología de computación periférica IMT-2020 a la IoT, es posible desplegar las aplicaciones en el nodo periférico, reduciendo así el retardo de extremo a extremo, lo que permite beneficiarse de la ruta de transmisión más corta y ofrecer un servicio más eficiente a través de la computación de datos locales.

Los escenarios de servicio en la tecnología de computación periférica IMT-2020 basada en la IoT son, entre otros, los siguientes:

– la ciudad inteligente;

– el edificio inteligente;

– el hogar inteligente.

6.2.3 Internet industrial

La tecnología de computación periférica IMT-2020 soporta los servicios de Internet industrial (en particular en el caso de las aplicaciones de IoT en tiempo real, donde el procesamiento de datos suele realizarse lejos de un centro de datos centralizado y una baja latencia es un requisito obligatorio) coordinando la red IMT-2020 con el controlador periférico, la pasarela periférica y la nube periférica.

El controlador periférico se encarga de la orquestación de tareas, el despliegue de aplicaciones y la gestión del ciclo de vida desde la pasarela periférica, y controla los dispositivos industriales, etc.

La pasarela periférica implementa la orquestación de tareas, el registro de dispositivos industriales, el despliegue de aplicaciones y la gestión del ciclo de vida desde la nube periférica, y analiza los datos periféricos, etc.

La nube periférica se encarga de la orquestación de tareas, el registro de dispositivos industriales, el despliegue de aplicaciones y la gestión del ciclo de vida desde la pasarela periférica, y coordina los servidores periféricos y analiza los datos periféricos, etc.

7 Amenazas contra la seguridad

Desde el punto de vista de la estratificación, la prestación de un servicio de computación periférica IMT-2020 requiere una capa de infraestructura, una capa de red y una capa de aplicación, por lo que las amenazas contra la seguridad deben considerarse desde todas esas perspectivas. Conviene señalar que, aunque la MEC tiene características de seguridad y protección de la privacidad porque la transmisión de datos se efectúa directamente a los servidores MEC, en lugar de a servidores centrales, reduciendo así el riesgo de fuga de datos en el proceso de transmisión de datos en la red, la explotación de un gran número de dispositivos móviles y el despliegue de servidores de nube periférica genera nuevos retos de seguridad. Concretamente, es posible que las soluciones de seguridad de computación en la nube tradicionales no sean adecuadas para la MEC, pues los entornos de los dispositivos IoT en la periferia afrontan nuevas amenazas que distan bastante de las que se encuentran en la gestión tradicional de la nube. En la práctica es imposible aplicar los métodos de seguridad de datos actuales en los dispositivos periféricos porque la mayoría de ellos tienen limitaciones de recursos y la red se vuelve vulnerable a causa del elevado dinamismo del entorno MEC. ENISA (Agencia para la Ciberseguridad de la Unión Europea) [b-ENISA] efectuó una evaluación exhaustiva de las vulnerabilidades de la MEC considerando las especificaciones 5G de 3GPP Publicación 16. Por consiguiente, aún debe seguir investigándose la manera de desarrollar un entorno MEC para las futuras aplicaciones 5G garantizando al mismo tiempo la seguridad.

7.1 Capa de infraestructura

7.1.1 Plataforma de gestión en la nube

El despliegue de un servicio de computación periférica IMT-2020 puede requerir una plataforma de gestión en la nube. Además de las amenazas generales contra la seguridad de dicha plataforma, un

atacante puede utilizar la interfaz entre la plataforma de gestión en la nube y la red IMT-2020 para lanzar un nuevo ataque a la red IMT-2020.

7.1.2 Infraestructura virtualizada

La infraestructura virtualizada puede no estar disponible si los recursos físicos son atacados o se corrompen. Esta posible vulnerabilidad del sistema puede ser utilizada por un atacante para obtener acceso de administración no autorizado al sistema de gestión de recursos virtuales y modificar la información de configuración.

7.1.3 Inyecciones de hardware/software maligno

Los componentes de software y hardware no autorizados, conocidos como caballos de Troya, pueden inyectarse en la infraestructura para degradar la eficacia de los servidores y dispositivos periféricos existentes e incluso permitir la explotación de los proveedores de servicios [b-Daniel]. En consecuencia, las entidades que proporcionan soluciones de software y hardware para el servicio de computación periférica pueden ejecutar involuntariamente actividades malignas en nombre de un atacante.

7.1.4 Manipulación física de dispositivos

La manipulación física de los dispositivos es más probable cuando los recursos informáticos de la arquitectura de computación periférica se encuentran más cerca de los posibles atacantes. Un atacante puede destruir los nodos periféricos y, en consecuencia, poner en peligro la eficacia de toda la red.

7.2 Capa de red

7.2.1 Análisis del flujo de red

Un atacante puede vigilar y/o robar los datos de los enlaces y analizar las características de los flujos para obtener información sobre los servicios y, de este modo, proceder a un nuevo ataque a la red.

7.2.2 Inspección de la topología de red

Un atacante puede poner en peligro el nodo de servicio desplegado en entornos abiertos para lanzar un ataque que inspeccione la topología de la red.

7.2.3 Ataque por denegación de servicio distribuida (DDoS)

Un atacante puede poner en peligro a los usuarios suscritos y/o los nodos de servicio que estén desplegados en entornos abiertos para lanzar un ataque por DDoS. Cuando se producen ataques por DDoS, un recurso de red existente se ve saturado de tráfico de otros recursos afectados dentro de la red, lo que constituye otro riesgo de seguridad de la computación periférica.

7.2.4 Intercepción o manipulación de datos de la comunicación

Los servicios que utilizan la computación periférica IMT-2020 se basan en la red inalámbrica abierta. Un atacante puede interceptar o manipular los datos de la comunicación; en algunos escenarios, por ejemplo, la industria y la fabricación, la ciudad inteligente, los datos de comunicación pueden incluir información de suma importancia, como los identificadores y credenciales de los usuarios, información comercial e información de seguridad pública.

7.2.5 Ataque entre dominios

Dado que el servicio de computación periférica en la red IMT-2020 requiere coordinar las funcionalidades entre la red de acceso, la red medular y la plataforma de gestión en la nube, el único punto amenazado puede dar lugar a un ataque entre dominios que deje la red y el servicio inoperativos.

7.2.6 Acceso no autorizado

Para que el equipo de usuario pueda conectarse al mejor servicio de computación periférica, se necesitan interacciones de señalización entre el equipo de usuario y la red medular IMT-2020. Si un atacante manipula la señalización, puede posibilitar el acceso no autorizado al servicio de computación periférica e incluso un ataque por DDoS.

7.2.7 Exposición de la red a la aplicación periférica

La red IMT-2020 podría exponer la información de la red a la función de aplicación local (AF) con posibles escenarios como la UPF del PSA local, exponiendo la información de la red a la AF local a través de la función de exposición de la red local (NEF) o directamente.

7.2.8 Ataques contra la información de encaminamiento

Un ataque contra la información de encaminamiento, o simplemente un ataque de encaminamiento, se produce en la capa de red de una red periférica. Los ataques de encaminamiento interfieren en la forma en que se transfiere el tráfico dentro de una red, lo que puede afectar al rendimiento, a la latencia y a los trayectos de datos.

7.2.9 Apropiación de la sesión

El ciberatacante intercepta y se apropia de una sesión de usuario para obtener acceso a los datos y servicios del usuario.

7.3 Capa de aplicación

7.3.1 Vulnerabilidad del marco técnico

En los servicios de computación periférica de las IMT-2020, dado que una gran cantidad de nodos utilizan el mismo marco técnico entre diferentes escenarios e industrias verticales, si un nodo sufre un ataque, repercutirá en los demás.

7.3.2 Uso no autorizado

La amenaza del uso no autorizado se produce cuando un usuario ilegal o no suscrito accede a los servicios de computación periférica de las IMT-2020 haciéndose pasar por una entidad autorizada.

7.3.3 Troyanos y virus

Los ataques con troyanos y virus se producen cuando un atacante o un servicio malintencionado de computación periférica IMT-2020 se hace pasar por un proveedor de servicios legales e inyecta en una aplicación troyanos o virus que pueden ser perjudiciales para los dispositivos y los datos de los usuarios, e incluso lanzar un ataque posterior a la red de telecomunicaciones móviles.

7.3.4 Divulgación de datos

La divulgación de datos se produce cuando los atacantes se hacen pasar por una entidad jurídica para obtener datos durante los procesos de migración, transmisión, almacenamiento, compartición y destrucción de datos de la aplicación de un servicio de computación periférica.

8 Requisitos de seguridad

8.1 Capa de infraestructura

Una plataforma de gestión en la nube debe cumplir, entre otros, los siguientes requisitos de seguridad:

a) Que la plataforma de gestión en la nube admita la autentificación y la autorización para la pasarela del plano de datos, la gestión de la plataforma de computación periférica y la aplicación de computación periférica.

b) Que proteja los datos sensibles para impedir el acceso no autorizado y la manipulación de datos (por ejemplo, en escenarios industriales los datos de producción sensibles deben protegerse a fin de efectuar correctamente los procesos industriales y evitar interrupciones por ataques a la red).

c) Que la plataforma de gestión en la nube esté aislada de forma segura con los elementos de la red medular IMT-2020 (por ejemplo, NEF, UPF).

d) Que se realicen análisis de canales laterales para detectar troyanos de hardware mediante análisis de temporización, potencia y temperatura espacial. Básicamente, este método detecta el firmware o software malicioso instalado en los nodos periféricos mediante la identificación de comportamientos inusuales del sistema, como el aumento del tiempo de ejecución y el consumo de energía.

e) Que se utilicen métodos de detección de hardware troyano que comparen el hardware afectado por troyanos con el que no lo está para detectar ataques maliciosos.

f) Que se refuerce la seguridad física de los nodos periféricos que no estén ubicados en centros de datos periféricos de alta seguridad, por ejemplo, empleando técnicas de protección física adicionales durante la fabricación o implementando mecanismos de bloqueo y otras salvaguardas físicas *in situ*.

g) Que, independientemente de lo que antecede, las partes del sistema periférico que traten con material criptográfico deben estar protegidas contra los ataques por canal lateral utilizando, por ejemplo, tarjetas SIM endurecidas y resistentes.

La infraestructura virtualizada debe cumplir, entre otros, los siguientes requisitos de seguridad:

a) Que, si la infraestructura del servicio de computación periférica IMT-2020 se despliega mediante una máquina virtual, la vCPU, la memoria y la E/S de la máquina virtual estén aisladas de forma segura.

b) Que la infraestructura virtualizada soporte un aislamiento seguro entre contenedores.

c) Que la infraestructura virtualizada soporte la réplica de los repositorios y la firma.

d) Que la segmentación de la red separe el tráfico y aísle los recursos de computación [b-ENISA].

8.2 Capa de red

La red de telecomunicaciones debe cumplir, entre otros, los siguientes requisitos de seguridad:

a) Que admita la protección de la confidencialidad e integridad de la transmisión de datos.

b) Que utilice un protocolo de seguridad (por ejemplo, TLS v1.2) para establecer un canal seguro entre los elementos de la red.

c) El uso del cifrado del tráfico de datos entre las partes mediante un protocolo de transporte seguro de extremo a extremo, el uso de un número o cadena aleatoria larga como clave de sesión y la regeneración del identificador de sesión después de cada inicio de sesión efectivo.

d) Que soporte la capacidad de protección contra DDoS filtrando cuidadosamente el tráfico para que no se permitan las solicitudes no legítimas, mientras que las legítimas se aprueben sin retardos significativos.

La gestión de red debe cumplir, entre otros, los siguientes requisitos de seguridad:

a) Que los sistemas de apoyo a las operaciones (OSS) soporten la autentificación y autorización para la interacción con la plataforma de gestión en la nube.

b) Que las funciones entre la gestión de servicios de computación periférica y los OSS estén aisladas de forma segura.

c) Que se controle continuamente si la red es lenta o presenta algún fallo, y que se notifiquen a tiempo las alarmas de los ataques y problemas de la red.

d) Que se establezcan protocolos de encaminamiento fiables.

8.3 Capa de aplicación

La aplicación periférica debe cumplir, entre otros, los siguientes requisitos de seguridad:

a) Que se realice una evaluación de la seguridad, incluyendo una comprobación del cumplimiento de las medidas de seguridad, la gestión de activos, la búsqueda de virus, etc.

b) Que la aplicación periférica soporte la autentificación y autorización para las interacciones entre la plataforma de gestión en la nube y otras aplicaciones periféricas.

c) Que proteja los datos sensibles para impedir el acceso no autorizado y la manipulación de datos.

d) Que admita la verificación de la integración para la aplicación periférica.

e) Que verifique la identidad y la autoridad del administrador durante la carga e instanciación de la aplicación periférica.

f) Que soporte la confidencialidad y la protección de la integración para los procesos de migración, transmisión, almacenamiento, intercambio y destrucción de datos.

g) Que soporte una función de identificación automática y endurecimiento de la seguridad basada en la extensión de la seguridad del lenguaje del programa y el análisis estático del programa.

h) Que admita funciones de supervisión, análisis y alarma en tiempo real con respecto al rendimiento de las aplicaciones, el tráfico, el canal de origen y el entorno cliente.

i) Que admita la auditoría de aplicaciones, que recopile regularmente los registros de seguridad de los dispositivos y aplicaciones periféricos, que los almacene y analice, y que luego notifique y rastree las violaciones, los casos de superación de las atribuciones y los comportamientos anormales de las aplicaciones.

9 Directrices sobre capacidades de seguridad del servicio de computación periférica

9.1 Capa de infraestructura

A fin de satisfacer los requisitos de seguridad de la capa de infraestructura, las capacidades de seguridad necesarias que deben proporcionarse son las siguientes:

a) Supervisión de los riesgos de seguridad de los datos y alerta temprana para evitar la manipulación y la fuga de datos.

b) Almacenamiento de seguridad de datos, incluyendo las capacidades de almacenamiento cifrado y encapsulado de datos sensibles.

c) Capacidades de protección de la seguridad para la plataforma de virtualización, mediante el refuerzo de la seguridad del sistema, el aislamiento de la seguridad, el control de la seguridad, el cifrado de datos y otras capacidades que refuercen la seguridad de los datos en la red de virtualización.

d) Funciones de seguridad que refuercen la seguridad de las NF de virtualización, en particular:
   - controles de autentificación;
   - controles de acceso;
   - verificación remota de la seguridad del sistema;
   - seguridad de las comunicaciones;
   - atestado;

- espejo;
- firma;
- aislamiento de seguridad;
- enclaves de ejecución por hardware;
- núcleo de confianza basado en hardware;
- cifrado por hardware;
- entorno de ejecución fiable;
- almacenamiento autocifrado;
- acceso directo a la memoria;
- módulos de seguridad de hardware;
- protección y verificación de la integridad del software.

9.2 Capa de red

Las capacidades de seguridad que deben proporcionarse para la capa de red son, entre otras, las siguientes:

a) Capacidades para proteger la confidencialidad e integridad de la transmisión de datos, como la indicación de tiempo, el número de serie, el cifrado de enlaces y otros mecanismos.

b) Soporte de capacidades para evitar el secuestro de la sesión, como el cifrado del tráfico de datos entre las partes, el uso de un número aleatorio largo o una cadena como clave de sesión, y la regeneración del identificador de sesión después de un inicio de sesión efectivo.

c) Control de la seguridad de los datos en los nodos periféricos, incluida la autentificación de la identidad, el aislamiento de la seguridad, la supervisión continua y la alerta temprana, el cifrado de datos, la desensibilización de los datos y las copias de seguridad.

d) Protocolos de encaminamiento fiables.

9.3 Capa de aplicación

Las capacidades de seguridad que deben proporcionarse para la capa de aplicación son, entre otras, las siguientes:

a) Control de los permisos de aplicación de los diferentes usuarios y escenarios, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos y servicios de la capa de aplicación.

b) Protección contra ataques de virus y actualización oportuna de la base de datos de virus para evitar la fuga o el robo de datos.

c) Identificación y evaluación de datos sensibles, incluida la autorización de desensibilización, el almacenamiento cifrado, la supervisión y el seguimiento, la alarma anormal, la gestión de auditorías, la destrucción y otras capacidades.

d) Autentificación de la identidad, supervisión continua y alerta temprana.

Bibliografía

[b-UIT-T E.800] Recomendación UIT-T E.800 (2008), *Definiciones de términos relativos a la calidad de servicio.*

[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), *Condiciones y definiciones relativas a las redes IMT-2020.*

[b-UIT-R M.1645] Recomendación UIT-R M.1645 (2006), *Marco y objetivos generales del desarrollo futuro de las IMT-2000 y de los sistemas posteriores*.

[b-UIT-R M.2083] Recomendación UIT-R M.2083 (2015), *Concepción de las IMT – Marco y objetivos generales del futuro desarrollo de las IMT para 2020 y en adelante*.

[b-3GPP TS 23.548] 3GPP 23.548 (2021), 5*G system enhancements for edge computing (version 17.2.0 release 17).*

[b-Daniel] B. Daniel, *Is edge computing secure? Here are 4 security risks to be aware of* 9 December 2020.
https://www.trentonsystems.com/blog/is-edge-computing-secure.

[b-ENISA] ENISA (Agencia para la Ciberseguridad de la Unión Europea), *ENISA Threat Landscape For 5G Networks*, diciembre de 2020. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

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

Publicado en Suiza
Ginebra, 2023