Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1606

(09/2020)

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

Seguridad de la computación en nube – Diseño de la seguridad de la computación en nube

Requisitos de seguridad para el entorno de aplicación Comunicaciones como servicio

Recomendación UIT-T X.1606

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	X.1140–X.1149
Protocolos de seguridad (1)	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.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
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
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
SEGURIDAD DE 5G	X.1800–X.1819

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

Recomendación UIT-T X.1606

Requisitos de seguridad para el entorno de aplicación Comunicaciones como servicio

Resumen

En la Recomendación UIT-T X.1606 se identifican las amenazas de seguridad y se recomiendan requisitos de seguridad para el entorno de aplicación Comunicaciones como servicio (CaaS). En esta Recomendación se describen las hipótesis de aplicación y las características de CaaS con capacidades multicomunicación. A continuación se identifican las amenazas específicas que plantean las características únicas de CaaS y se recomiendan los requisitos de seguridad de CaaS correspondientes.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1606	2020-09-03	17	11.1002/1000/14265

Palabras clave

CaaS, computación en la nube, requisito de seguridad, riesgo.

* 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.1606

Requisitos de seguridad para el entorno de aplicación Comunicaciones como servicio

1 Alcance

Esta Recomendación se centra en los requisitos de seguridad para el entorno de aplicación Comunicaciones como servicio (CaaS), que difieren de los definidos para Software como servicio (SaaS) en [UIT-T X.1602]. La CaaS de las organizaciones de telecomunicación fusiona las capacidades de las telecomunicaciones y de Internet. Esta convergencia hace que la CaaS tenga unas características únicas que plantean riesgos concretos. En esta Recomendación se identifican esos riesgos y se recomiendan los requisitos de seguridad correspondientes.

Los requisitos toman en consideración las obligaciones impuestas por la legislación y la reglamentación nacionales a cada Estado Miembro. El texto se basa en la metodología especificada en la cláusula 10 de [UIT-T X.1601].

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.1601] Recomendación UIT-T X.1601 (2015), *Marco de seguridad para la computación en la nube.*

[UIT-T X.1602] Recomendación UIT-T X.1602 (2016), *Requisitos de seguridad para el entorno de aplicación Software como servicio.*

[UIT-T Y.3501] Recomendación UIT-T Y.3501 (2016), *Marco de la computación en nube y requisitos de alto nivel.*

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 autentificación [UIT-T X.1601]: Verificación de la identidad de un usuario, proceso o dispositivo, que suele ser condición necesaria para acceder a recursos de un sistema de información.

3.1.2 capacidad [b-ISO 15531-1]: Cualidad de poder realizar una determinada actividad.

3.1.3 computación en la nube [b-UIT-T Y.3500]: Paradigma para dar acceso a la red a un conjunto elástico y ampliable de recursos físicos o virtuales compartibles con administración y configuración en autoservicio previa solicitud.

NOTA – Como ejemplos de recursos pueden citarse los servidores, sistemas operativos, redes, software, aplicaciones y equipos de almacenamiento, entre otros.

3.1.4 servicio en la nube [b-UIT-T Y.3500]: Una o varias capacidades que se ofrecen mediante computación en la nube a las que se accede con una interfaz declarada.

3.1.5 cliente de servicio en la nube [b-UIT-T Y.3500]: Parte que mantiene una relación comercial a los efectos de utilizar servicios en la nube.

NOTA – Una relación comercial no implica necesariamente un acuerdo financiero.

3.1.6 asociado del servicio en la nube [b-UIT-T Y.3500]: Parte que colabora o asiste en actividades del proveedor de servicios en la nube o del cliente del servicio en la nube, o en ambas.

3.1.7 proveedor de servicios en la nube [b-UIT-T Y.3500]: Parte que ofrece servicios en la nube.

3.1.8 usuario de servicios en la nube [b-UIT-T Y.3500]: Persona física, o entidad que la represente, asociada a un cliente del servicio en la nube, que utilice servicios en la nube.

NOTA – Como ejemplos de tales entidades pueden citarse los dispositivos y aplicaciones, entre otros.

3.1.9 comunicaciones como servicio (CaaS) [b-UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube una capacidad de comunicación y colaboración en tiempo real.

NOTA – CaaS puede ofrecer los tipos de capacidad de plataforma y de aplicación.

3.1.10 multiarrendamiento [b-UIT-T Y.3500]: Atribución de recursos físicos y virtuales mediante los cuales varios arrendatarios y sus cálculos y datos están aislados y son inaccesibles para terceros.

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

3.1.12 software como servicio (SaaS) [b-UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube un tipo de capacidades de aplicación.

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y acrónimos siguientes:

CaaS Comunicaciones como servicio (*communications as a service*)

CSC Cliente del servicio en la nube (*cloud service customer*)

CSN Asociado del servicio en la nube (*cloud service partner*)

CSP Proveedor de servicios en la nube (*cloud service provider*)

CSU Usuario del servicio en la nube (*cloud service user*)

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

GSM Sistema Mundial para Comunicaciones Móviles (*Global System for Mobile*)

IaaS Infraestructura como servicio (*infrastructure as a service*)

IAM Gestión de identidad y de acceso (*identity and access management*)

ID Identificador (*identifier*)

MMS Servicio de mensajería multimedios (*multimedia messaging service*)

NaaS Red como servicio (*network as a service*)

OS Sistema operativo (*operating system*)

PaaS Plataforma como servicio (*platform as a service*)

PC Computador personal (*personal computer*)

QR Respuesta rápida (*quick response*)

SaaS Software como servicio (*software as a service*)

SDK Herramienta de creación de software (*software development kit*)

SIM Módulo de identificación del abonado (*subscriber identity module*)

SMS Servicio de mensajes breves (*short message service*)

URL Localizador uniforme de recursos (*uniform resource locator*)

(U)SIM Módulo de identificación del abonado (universal) (*(universal) subscriber identity module*)

VoLTE Voz por evolución a largo plazo (*voice over long-term evolution*)

VPN Red privada virtual (*virtual private network*)

5 Convenios

En esta Recomendación no se distingue entre servidor y servidor virtual.

6 Aspectos generales de la CaaS

La definición de Comunicaciones como servicio (CaaS, *communications as a service*) puede encontrarse en la cláusula 3.1.9. Se ha recomendado que los requisitos generales de la CaaS sean capacidades de comunicación abiertas, soporte de software de comunicación y comunicación unificada (véase la cláusula 11 de [UIT-T Y.3501]).

De acuerdo con las prácticas de la industria, la CaaS suele implementar o soportar las siguientes capacidades:

– combinación de servicios de telecomunicaciones y servicios Internet;
– comunicación en tiempo real;
– sincronización multidispositivo;
– aislamiento de recursos de comunicación;
– actualización de presencia de usuarios;
– conversaciones o reuniones grupales;
– integración por otros SaaS;
– aceptación o rechazo explícitos del usuario;
– personalización del proceso de servicio;
– compartición de datos o ficheros;
– gestión de identidad y acceso (IAM, identity and access management).

En la Figura 6-1 se ilustra el modelo de servicio CaaS general. En la Figura 6-1 hay cuatro capas, a saber, usuario, acceso, servicio y recursos.

– La capa de usuario contiene los terminales de usuario de servicio en la nube (CSU, *cloud service user*) que pueden ejecutar algunos clientes CaaS y pueden acceder a Internet e incluso a las redes de telecomunicaciones.
– La capa de acceso ofrece diversos tipos de túneles, generalmente para permitir el acceso de los terminales al servicio CaaS objetivo.
– La capa de servicio, que también es la capa CaaS, pertenece a un proveedor de servicios en la nube (CSP, *cloud service provider*), que depende de los recursos internos y externos

necesarios para completar el funcionamiento del servicio. La capa de servicio personaliza los procesos de servicio y atribuye recursos a los clientes del servicio en la nube (CSC, *cloud service customers*), mantiene una red de servicio (virtualmente) dinámica para los CSC y sus CSU, y aísla los recursos de cálculo y las redes de comunicaciones de cualquier CSC.

– La capa de recursos ofrece los recursos infraestructurales fundamentales relacionados con el procesamiento de datos y la comunicación, parte de los cuales pueden ser Infraestructura como servicio (IaaS, *infrastructure as a service*), Plataforma como servicio (PaaS, *platform as a service*) y Red como servicio (NaaS, *network as a service*).

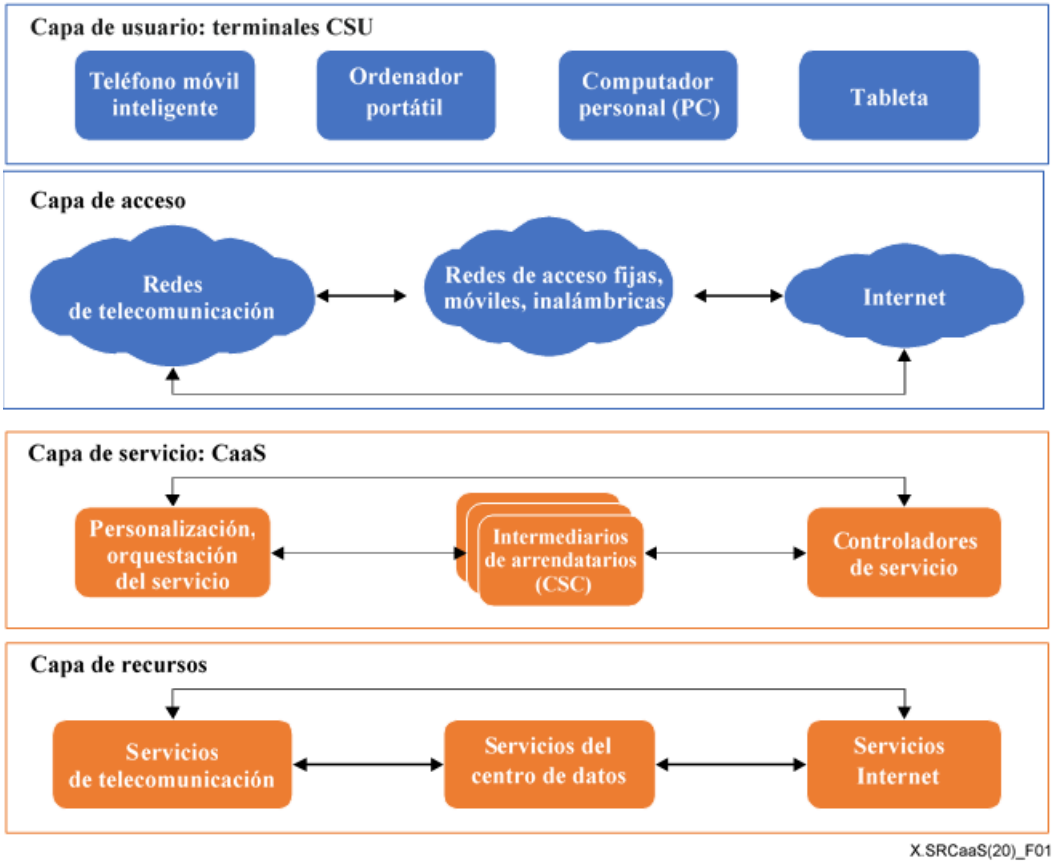

Figura 1 – Modelo general del servicio CaaS

A continuación:

– En la cláusula 7 se analizan las amenazas a la seguridad de la CaaS que afectan a una o más de las cuatro capas.

– En la cláusula 8 se recomiendan requisitos de seguridad para contrarrestar las amenazas a tres capas de la CaaS:

- capa de terminal CSU;
- capa de CaaS;
- capa de recursos de servicio.

No se contempla aquí la capa de acceso porque la CaaS no controla sus capacidades de seguridad, aunque tanto la CaaS como el CSU pueden evaluar y supervisar el nivel de seguridad de la capa de acceso.

7 Amenazas a la seguridad de la CaaS

Las amenazas y retos a la seguridad de la computación en la nube identificados en [UIT-T X.1601] (también enumerados en el Apéndice I) son de aplicación a las diversas hipótesis de aplicación de la CaaS. Además, en las cláusulas 7.1 a 7.8 se identifican las amenazas específicas a la CaaS.

7.1 Amenazas a la identidad

El núcleo de la CaaS son las capacidades de comunicación unificadas, que difieren ligeramente de otros SaaS. La CaaS integra y mejora las capacidades de comunicación entre terminales gracias a la computación en la nube. CaaS soporta la mayoría de terminales o sistemas operativos (OS, *operating system*) habituales, como los teléfonos inteligentes o los computadores personales (PC, *personal computer*).

Por consiguiente, dentro del modelo de comunicación multipunto a multipunto, la CaaS puede verse amenazada en caso de problemas con la identidad.

7.1.1 Robo de credenciales de identidad

Para comodidad de los CSU, muchas CaaS adoptan una solución de autentificación que soporta la autentificación por número móvil (es decir, el identificador móvil (ID, *mobile identifier*)), la autentificación por nombre de usuario y contraseña o ambas. En este caso, el nombre de usuario por defecto utilizado puede configurarse como el ID móvil. Además, algunas CaaS soportan que un CSU con un ID acceda al servicio desde varios terminales al mismo tiempo o soportan la sincronización del historial de comunicación entre varios terminales.

La seguridad de la autentificación por número móvil depende en gran medida de la confianza en la autentificación, la encriptación del operador de red móvil y la tarjeta de módulo de identidad de abonado universal ((U)SIM, *(universal) subscriber identity module*) que contiene las credenciales. Las redes móviles tienen algunas vulnerabilidades (demostradas en la práctica), en particular la red de la Global System for Mobile Communications Alliance (GSMA), que debilitan la confianza y pueden dar pie a un robo (temporal) de las credenciales de identidad. Por ejemplo, es posible duplicar físicamente algunos tipos de tarjetas de módulo de identidad del abonado (SIM, *subscriber identity module*) y en las redes del sistema mundial para comunicaciones móviles (GSM, *global system for mobile*) es posible interceptar los códigos de autentificación dinámica transferidos por el servicio de mensajes breves (SMS, *short message service)*.

Además, la autentificación por nombre de usuario y contraseña puede dar al infractor una oportunidad de utilizar ese tipo de autentificación con otros terminales cualificados para (simultáneamente) vigilar a un CSU. Por ejemplo, si un infractor puede acceder a un terminal móvil CSU con una tarjeta (U)SIM o una SIM electrónica, puede obtener el nombre de usuario en la memoria cache y utilizar el mecanismo de reinicio para crear una nueva contraseña y guardarla en la memoria cache del terminal. Es posible así que el CSU no se dé cuenta de que se ha reinicializados la contraseña y que el infractor puede vigilar en silencio todo el contenido de las comunicaciones en curso e incluso su historial de comunicación.

7.1.2 Falsificación de identidad

Una vez robada u obtenida por medios fraudulentos la credencial de identidad del CSU, ésta puede utilizarse indebidamente para acceder al servicio perteneciente a un CSC a que está asociado el CSU. Mientras tanto, el infractor puede obtener también una entidad social respaldada por la credencial de identidad del CSU o incluso falsificar otras entidades sociales o crear una nueva, que la función de presencia muestre en primer lugar.

La presencia es una característica común de la CaaS, que suele utilizar un autorretrato del CSU de pequeño tamaño y un texto breve. Gracias a la presencia los CSU asociados al mismo CSC pueden adquirir rápidamente un conocimiento somero de los otros CSU. Sin embargo, es posible falsificar la presencia de una identidad intervenida e implicarla en actividades fraudulentas. Por ejemplo, un

infractor puede obtener datos financieros confidenciales del contable de una empresa falsificando su presencia como miembro de la Junta.

La conversación por vídeo en tiempo real es una configuración normalizada de la CaaS. También se puede falsificar el fondo mostrado por la identidad falsificada en el flujo de vídeo para aumentar la autenticidad de la entidad social y la actividad fraudulenta.

7.2 Amenazas a la gestión del ciclo de vida de las cuentas

Tanto un CSU, como un CSC o un CSP, puede tener derecho a solicitar la supresión de una cuenta sobre la que tiene autoridad. A lo largo del ciclo de vida de la cuenta, cuando ésta se ha de suprimir será necesario acordar con antelación lo que se supone que el CSP debe hacer con la comunicación de contenido y la información de la cuenta en todo su servicio CaaS, si el CSC puede conservar esos datos en su espacio lógico o si el CSU puede conservarlos en su terminal.

La destrucción o robo de un terminal puede implicar también la obligación de supresión de toda información de la cuenta en la memoria cache y de cualquier otro dato relacionado.

7.3 Amenaza a la orquestación

Gracias a la función de orquestación (véase [b-UIT-T Y.3100]), un CSC puede personalizar sus procesos y capacidades de servicio por sí mismo o a través del CSP. Por ejemplo, un CSC puede ajustar el proceso y los privilegios de gestión de los miembros de una conversación grupal, así como aumentar o reducir las limitaciones del ámbito en que un CSU puede buscar un contacto.

En términos de requisitos del cliente, un CSP puede permitir que dos o más CSC compartan sus contactos e incluso comuniquen mutuamente, y también puede fusionar más de un CSC en uno más grande.

Además, para implementar una nueva característica de servicio, el CSP puede aumentar o reducir las condiciones previas de seguridad de las redes a las que tiene acceso el CSU.

Toda orquestación que no tenga plenamente en cuenta la seguridad puede menoscabar el aislamiento de la información y los servicios. Por ejemplo, si la CaaS de un CSC está orquestada para integrar los servicios de mensajería y voz de una red GSM, será prácticamente imposible implementar el aislamiento de extremo a extremo, porque las entidades de red GSM adoptaron tecnologías antiguas y no pueden soportar ningún tipo de aislamiento. Si la orquestación permite que un tipo de red inseguro soporte una característica de servicio más flexible, puede aumentarse el nivel de riesgo de la CaaS para más de un CSC. Por ejemplo, si el requisito de acceso por red privada virtual (VPN, *virtual private network*) como método de aislamiento se reconfigura de obligatorio a optativo, a fin de garantizar la calidad de la conversación por vídeo en la CaaS, aumentará el riesgo de escuchas ilegales.

7.4 Amenazas al contexto de los terminales

El contexto de seguridad de los terminales CaaS puede ser incierto, en particular cuando se trata de teléfonos inteligentes o dispositivos portátiles. Si esos terminales se consideran propiedad privada, el contexto puede ser más complejo. Los parientes o amigos del CSU podrán utilizar esos terminales. Es posible proyectar la pantalla de un terminal o compartirla con otra pantalla, por lo que la grabación clandestina de la pantalla es posible. Las vulnerabilidades de un terminal pueden ser más directamente visibles para un atacante en las redes inseguras. El contenido de las comunicaciones por CaaS puede no estar encriptado y puede almacenarse en terminal. Todas esas hipótesis pueden dar pie a una fuga de datos.

Si un atacante puede controlar un terminal (a distancia o localmente), puede abusar de él para explotar las vulnerabilidades de la CaaS e incluso del CSU. Si controla muchos terminales simultáneamente gracias a un botnet, el atacante puede lanzar también un ataque de denegación de servicio distribuida (DDoS, *distributed denial of service*).

7.5 Amenazas de comunicaciones masivas no solicitadas (spam) y distribución de software maligno (malware)

Un CSU puede sufrir acoso, e incluso peska, a través de un ataque de spam lanzado por otros CSU por CaaS. De hecho, en muchos casos resulta difícil para el CSU identificar racionalmente si puede confiar en la información de un localizador uniforme de recursos (URL, *uniform resource locator*) breve o un código de respuesta rápida (QR, *quick response*), que puede dirigirlo hacia un sitio web de peska o hacerle descargar un malware.

7.6 Amenazas de complementos

Es natural que la CaaS facilite complementos a su servicio básico, por ejemplo, compartición de ficheros, navegador web incorporado, sistema de gestión del contenido o, incluso, negocio-e. En la mayoría de los casos, esos complementos son bastante ligeros.

Las vulnerabilidades de esos complementos pueden suponer una importante amenaza para la CaaS misma. Por ejemplo, hacer clic en un URL breve inseguro puede invocar extensiones del navegador web incapaces de contrarrestar una dirección peligrosa, por lo que aumenta considerablemente la probabilidad de poner en peligro la seguridad del CSU e incluso de la CaaS.

Algunos complementos pueden provocar que el CSU abandone su CaaS actual y se pase a un servicio maligno. Si el CSU desconoce ese cambio, no podrá ajustar oportuna y adecuadamente sus parámetros de confianza y sufrirá un amplio abanico de daños (explotación de más vulnerabilidades, extorsión, etc.).

7.7 Amenaza a la herramienta de creación de software

La CaaS puede ofrecer una herramienta de creación de software (SDK, *software development kit*) para fomentar la integración por otras aplicaciones o SaaS. La integración implica básicamente la existencia de un determinado vínculo de confianza entre la CaaS y el usuario de la SDK. Por consiguiente, las vulnerabilidades del usuario de la SDK pueden aumentar el nivel de amenaza de ataque o abuso de la CaaS.

Dado que un terminal puede tener diversas credenciales de identidad para distintos CSC, un usuario de SDK CaaS puede utilizar indebidamente esas credenciales sin permiso para acceder ilícitamente a otros CSC.

7.8 Amenazas causadas por vulnerabilidades de las redes de telecomunicaciones

Además del acceso a Internet, si la CaaS incorpora otras capacidades del operador de redes de telecomunicaciones, como el SMS, la voz por evolución a largo plazo (VoLTE, *voice over long-term evolution*), las llamadas en modo circuito, el servicio de mensajería multimedios (MMS, *multimedia messaging service*) y la ubicación, la seguridad de la red de telecomunicaciones puede influir directamente en la CaaS.

Todo abuso de las vulnerabilidades de la red de telecomunicaciones que se lleve a cabo con éxito puede provocar una fuga de datos de la CaaS. Del mismo modo, todo ataque ejecutado con éxito en la red de telecomunicaciones, en particular en los nodos conectados a servidores CaaS, puede ampliar la superficie vulnerable de la CaaS.

Además, dado que los terminales comercializados modernos pueden conmutar activamente entre las redes de acceso y las VPN de diversos proveedores, de acuerdo con políticas predefinidas que apenas tienen en consideración la confianza y autenticidad de la red de acceso, es posible que el CSU no sepa que utiliza un entorno de red inseguro, lo que puede causar una fuga de información confidencial.

8 Requisitos de seguridad para CaaS

Los requisitos de seguridad para SaaS identificados en [UIT-T X.1602] son aplicables a la CaaS. Además, en esta cláusula se establecen otros requisitos de seguridad para hacer frente a las amenazas identificadas en la cláusula 7.

8.1 Gestión de identidad y acceso

8.1.1 Gestión de identidad

La CaaS debe fijar un límite al número de terminales que pueden compartir simultáneamente la misma credencial de identidad. La CaaS puede verificar un terminal con el hardware necesario y la identificación de servicio como controlador primario, que puede autorizar las solicitudes de acceso de otros terminales.

La CaaS puede supervisar los terminales concurrentes con la misma credencial de identidad y mantener informados a todos los terminales (o, al menos, al controlador primario) del estado más reciente de los demás terminales concurrentes. El CSU puede utilizar el controlador primario o un método de autentificación más seguro (como la autentificación por derivación) para forzar la desconexión de un terminal específico, prohibirle todo futuro acceso e, incluso, suprimir la información residual que contiene.

La CaaS puede considerar la posibilidad de orientar al CSU hacia la utilización de distintas credenciales (y, como poco, distintas contraseñas) para distintos CSC, reduciendo así el riesgo de que se utilice una sola credencial robada para acceder a muchos CSC.

8.1.2 Control de acceso

Si la concurrencia de terminales con una credencial de identidad es una capacidad común de CaaS, convendría permitir que la CaaS adquiriese y actualizase la situación geográfica de los terminales a fin de poder describir toda anomalía en acceso de cualquier terminal. Dado que un terminal puede acceder a muchas redes al mismo tiempo, la CaaS puede considerar la posibilidad de utilizar información multidimensional para la verificación cruzada de la autenticidad de la ubicación.

Si no se puede garantizar la seguridad de la red, las VPN son una buena opción para mejorar la seguridad infraestructural. La CaaS debe considerar la posibilidad de exigir al CSU o el CSC la utilización de un servicio VPN obligatorio y prohibir al CSU o el CSC la adopción de otro servicio VPN como salto o enlace para acceder al servicio VPN obligatorio. Una VPN optativa o no fiable podría ocultar la ubicación de un terminal y aumentar el riesgo de sufrir un ataque por intermediario.

Además, si el CSC no puede aceptar el riesgo de intercepción de SMS GSM, la CaaS debe considerar la posibilidad de supervisar el tipo de red al que accede cualquier CSU y rechazar la utilización del SMS como método de autentificación, si el CSU se encuentra en una red GSM. La CaaS también puede simplemente excluir el recurso SMS GSM para el CSC.

8.1.3 Verificación de identidad

Dado que un CSU puede utilizar información oculta, inexacta o, incluso, falsificada para su autorretrato, la CaaS debe alertar a todos los CSU de si una identidad social de sus contactos está verificada por un tercero fiable. El tercero puede ser un CSC, una CaaS o cualquier otra autoridad independiente. La verificación puede ser obligatoria u optativa, pero en este último caso será necesario alertar al CSU de que el CSP o el CSC no pueden considerarse responsables de la autenticidad de las identidades sociales en el CSC.

Dado que la identidad social o profesional de un CSC utilizada como cliente de la CaaS puede ser completamente distinta de la utilizada en público, se sugiere que la CaaS considere la posibilidad de considerar la identidad declarada de un CSC en público con la información disponible para evitar posibles fraudes públicos o profesionales. Por ejemplo, un CSC maligno puede pretender ser una organización caritativa y falsificar algunas donaciones para engañar al CSU.

8.1.4 Gestión de cuentas

Dado que un CSU puede tener, como mínimo, una cuenta en un CSC y que el CSC también puede tener, como mínimo, una cuenta en CaaS, la CaaS debe otorgar todos los privilegios de acceso a los datos de una cuenta al CSU o el CSC, en función de la propiedad de los datos. Además, cuando se debe cancelar o suprimir una cuenta, la CaaS deberá facilitar una capacidad fiable de destrucción física de los datos de la cuenta en el lado terminal, el lado servicio y el lado red de acuerdo con los términos de la autorización legal dada por el propietario de los datos.

8.2 Seguridad del terminal

8.2.1 Seguridad interna

La CaaS debe facilitar medidas técnicas, como una herramienta de seguridad o un módulo de seguridad integrado en los terminales CSU, para llevar a cabo verificaciones de seguridad cíclicas o a la demanda. La verificación de seguridad puede evaluar si el contexto de un terminal CSU cumple los requisitos de seguridad obligatorios antes de acceder a la CaaS. Si el terminal CSU no supera con éxito la verificación de seguridad, la CaaS puede considerar la posibilidad de denegar (parcialmente) la prestación de servicios. Al mismo tiempo, la CaaS debe orientar al CSU para resolver los riesgos de seguridad descubiertos o resolver las vulnerabilidades directamente con autorización del CSU.

8.2.2 Seguridad externa

La CaaS debe facilitar el software utilizado en los terminales CSU, así como una plataforma o fuentes de distribución de software seguras, oficiales o autorizadas. La CaaS también debe declarar el mecanismo de verificación para que los terminales lo puedan utilizar para verificar la autenticidad y la integridad antes de la actualización. El OS o el software mismo de los terminales CSU deben tener capacidad de reversión en caso de fallo de la actualización.

La mayoría de las veces la actualización de seguridad del software terminal es optativa. Sin embargo, de haber una vulnerabilidad que pudiera causar un gran daño a la CaaS, el CSC o incluso otro CSU, y que una actualización de seguridad del software terminal pudiera resolver esa vulnerabilidad, la CaaS podría considerar la posibilidad de denegar temporalmente el acceso al servicio al terminal CSU hasta que se efectúe con éxito la actualización conforme al acuerdo de usuario.

En la mayor parte de los casos, la distribución de software terminal de la CaaS es pública. No obstante, en ocasiones un CSC puede necesitar un software terminal personalizado y exigir una distribución de software limitada, por ejemplo, sólo a través del personal CSC. La distribución deberá entonces ser privada y se necesitará una autentificación bidireccional entre el CSU y la CaaS antes de poder descargar o actualizar el software.

8.3 Seguridad del servicio

8.3.1 Seguridad de la orquestación

Antes de aplicar o configurar un cambio de orquestación, será necesario evaluar si ese cambio puede afectar los límites de seguridad, reducir el nivel de seguridad o influir en la relación de confianza. De poder haber efectos negativos, será necesario volver a negociar y acordar los requisitos o acuerdos de seguridad de la CaaS entre el CSP, el CSC e incluso el CSU.

8.3.2 Lucha contra el spam

La CaaS puede considerar la posibilidad de ofrecer al CSC, como capacidad optativa, una función de lucha contra el spam. También el CSP puede considerar la posibilidad de permitir al CSC que integre una función de lucha contra el spam tercera en su propia CaaS. Los CSP, CSC y CSU podrán concluir acuerdos de servicio y usuario distintos con distintas restricciones en cuando a la eventual utilización de una función de lucha contra el spam y sus modalidades de aplicación.

Por ejemplo, si todos los CSU son empleados de un CSC y la CaaS correspondiente está destinada exclusivamente a la utilización en beneficio del CSC, basta con un acuerdo entre el CSP y el CSC para utilizar la función de lucha contra el spam.

En caso contrario, si los CSU son clientes del CSC, será necesario que esos CSU autoricen al CSC (junto con el CSP) a ayudarlos a luchar contra el spam.

En términos generales, la función de lucha contra el spam debe estar en el lado terminal, el lado nube o en ambos. Pueden verse las tecnologías alternativas utilizadas para esta función en [b-UIT-T X.1244] y [b-UIT-T X.1246].

8.4 Coordinación de seguridad

8.4.1 Seguridad de complementos y SDK

La CaaS sólo debe permitir los complementos que han superado la verificación de seguridad de su servicio. El software terminal debe ayudar a la CaaS a supervisar y analizar toda anomalía de los complementos. Una lista blanca ayudaría a la CaaS a limitar la capacidad de los complementos a acceder a enlaces o nombres de dominio externos.

Si un complemento necesita acceder a los datos del cliente para prestar el servicio, se impondrá como condición previa la autorización inequívoca del CSU. Para auditorías posteriores convendría llevar un registro claro del acceso de los complementos a los datos de los clientes.

Una SDK para CaaS debe poder supervisar y analizar anomalías de las aplicaciones o el SaaS que integra la SDK. La SDK debe encriptar y aislar las credenciales de identidad para evitar todo acceso indebido. Por ejemplo, la aplicación A y la aplicación B tienen integrada la misma SDK y existen en el mismo terminal, pero ninguna de ellas tiene acceso a las credenciales de identidad de la otra.

8.4.2 Seguridad de la infraestructura

La CaaS debe conocer las amenazas que plantea la infraestructura, por ejemplo, cuando integra las capacidades de servicio de las redes de telecomunicaciones, como el SMS y las llamadas de voz. La CaaS debe considerar la posibilidad de imponer una pasarela entre ella y la red de telecomunicaciones para supervisar, contrarrestar o filtrar el spam y evitar la difusión de fraudes de identidad de los servicios telecomunicaciones. Convendría que la CaaS alertase a los CSU de los tipos de canales de comunicación o servicios en uso.

Apéndice I

Breve guía de las amenazas y retos a la seguridad previstos en la Recomendación UIT-T X.1601

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

Como se indica en la cláusula 7, las amenazas y retos a la seguridad de la computación en la nube identificados en [UIT-T X.1601] pueden aplicarse a las diversas hipótesis de aplicación de CaaS. En este apéndice se enumeran todas las amenazas y retos a la seguridad de [UIT-T X.1601] para facilitar su consulta. Puede encontrarse información más detallada al respecto en [UIT-T X.1601].

– Amenazas de seguridad en la computación en la nube
  a) Amenazas de seguridad al CSC
    1) Pérdida y filtración de datos
    2) Acceso inseguro al servicio
    3) Amenazas internas
  b) Amenazas de seguridad al CSP
    1) Acceso con derechos de administración no autorizado
    2) Amenazas internas
– Problemas de seguridad en la computación en la nube
  a) Problemas de seguridad al CSC
    1) Ambigüedad en las responsabilidades
    2) Pérdida de confianza
    3) Pérdida de gobernanza
    4) Pérdida de confidencialidad
    5) Indisponibilidad del servicio
    6) Dependencia del CSP
    7) Apropiación indebida de propiedad intelectual
    8) Pérdida de integridad del software
  b) Problemas de seguridad para los CSP
    1) Ambigüedad en las responsabilidades
    2) Contexto compartido
    3) Incoherencia y conflictos en los mecanismos de protección
    4) Conflictos jurisdiccionales
    5) Evolución de los riesgos
    6) Migración e integración deficientes
    7) Discontinuidad de actividades
    8) Dependencia del asociado de servicios en la nube (CSN)
    9) Vulnerabilidad en la cadena de suministro
    10) Dependencias del software

c) Problemas de seguridad para los CSN
   1) Ambigüedad en las responsabilidades
   2) Apropiación indebida de propiedad intelectual
   3) Pérdida de integridad del software

Apéndice II

Correspondencia entre las amenazas a la seguridad y los requisitos de seguridad

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

Este apéndice vincula las amenazas de la cláusula 7 con los requisitos de la cláusula 8 (véase el Cuadro I.1).

Cuadro I.1 – Correspondencia entre las amenazas a la seguridad y los requisitos de seguridad de esta Recomendación

Amenazas de la cláusula 7	Requisitos de la cláusula 8 correspondientes
7.1 Amenazas a la identidad	8.1 Gestión de identidad y acceso
7.1.1 Robo de credenciales de identidad	8.1.1 Gestión de identidad 8.1.2 Control de acceso 8.1.4 Gestión de cuentas
7.1.2 Falsificación de identidad	8.1.3 Verificación de identidad 8.1.4 Gestión de cuentas
7.2 Amenazas a la gestión del ciclo de vida de las cuentas	8.1.4 Gestión de cuentas
7.3 Amenaza a la orquestación	8.3.1 Seguridad de la orquestación
7.4 Amenazas al contexto de los terminales	8.2Seguridad del terminal
7.5 Amenazas de comunicaciones masivas no solicitadas (spam) y distribución de software maligno (malware)	8.2 Seguridad del terminal 8.3.2 Lucha contra el spam
7.6 Amenazas de complementos	8.4.1 Seguridad de complementos y SDK
7.7 Amenaza a la herramienta de creación de software	8.4.1 Seguridad de complementos y SDK
7.8 Amenazas causadas por vulnerabilidades de las redes de telecomunicaciones	8.4.2 Seguridad de la infraestructura

Bibliografía

[b-UIT-T X.1244] Recomendación UIT-T X.1244 (2008), *Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP*.

[b-UIT-T X.1246] Recomendación UIT-T X.1246 (2015), *Tecnologías implicadas en la lucha contra el spam de voz en las organizaciones de telecomunicaciones*.

[b-UIT-T Y.3100] Recomendación UIT-T Y.3100 (2017), *Condiciones y definiciones relativas a las redes IMT-2020*.

[b-UIT-T Y.3500] Recomendación UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Tecnología de la información – Computación en la nube – Descripción general y vocabulario.*

[b-ISO 15531-1] ISO 15531-1:2004, *Industrial automation systems and integration – Industrial manufacturing management data – Part 1: General overview*.

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, 2021