Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1127

(09/2017)

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

Aplicaciones y servicios con seguridad (1) – Seguridad en las redes móviles

Requisitos de seguridad y arquitecturas funcionales para las medidas de lucha contra el robo de teléfonos móviles

Recomendación UIT-T X.1127

UIT-T

Unión Internacional de Telecomunicaciones

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.1319

Recomendación UIT-T X.1127

Requisitos de seguridad y arquitecturas funcionales para las medidas de lucha contra el robo de teléfonos móviles

Resumen

La Recomendación UIT-T X.1127 se centra en los requisitos funcionales de seguridad y la arquitectura funcional para los mecanismos contra el robo de teléfonos inteligentes basados en los requisitos generales descritos por la Global System Mobile Association (GSMA).

Los teléfonos inteligentes están expandiéndose rápidamente y se han convertido en una parte casi indispensable de la vida diaria. Lamentablemente, muchos usuarios de teléfonos inteligentes han visto cómo robaban sus teléfonos. Una medida contra el robo de los teléfonos inteligentes, es decir una herramienta de desactivación que se utilice en caso de pérdida o robo del teléfono, debería ofrecer la capacidad para:

– eliminar a distancia los datos del usuario autorizado presentes en el teléfono inteligente;

– hacer que el teléfono sea inutilizable para un usuario no autorizado;

– evitar la reactivación sin el permiso del usuario autorizado, en la medida en que sea posible desde el punto de vista tecnológico; y

– cancelar la desactivación en caso de que el teléfono inteligente sea recuperado por el usuario autorizado, y restablecer en la medida de lo posible los datos del usuario en el mismo.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1127	2017-09-06	17	11.1002/1000/13259

Palabras clave

Medidas contra el robo, requisitos de seguridad, teléfono móvil.

* 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 [ha recibido/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

Página

Recomendación UIT-T X.1127

Requisitos de seguridad y arquitecturas funcionales para las medidas de lucha contra el robo de teléfonos móviles

1 Alcance

En esta Recomendación se abordan los requisitos funcionales de seguridad y la arquitectura funcional para las medidas contra el robo de teléfonos inteligentes (es decir, una herramienta de desactivación), que permite a los usuarios eliminar a distancia sus datos personales o inutilizar los dispositivos telefónicos perdidos o robados.

Se considera que los requisitos funcionales de seguridad y la arquitectura funcional indicados en esta Recomendación pueden aplicarse a los teléfonos móviles que tienen la capacidad de proporcionar medidas contra el robo, respondiendo a las demandas de los usuarios de teléfonos móviles, los fabricantes de teléfonos móviles y los operadores de servicios móviles.

Esta Recomendación se centra en los requisitos funcionales de seguridad, la arquitectura funcional y los mecanismos contra el robo. Utiliza un modelo de referencia constituido por el propietario del dispositivo, el servidor autorizado, el servidor de copia de seguridad y dispositivos robados o perdidos. Las amenazas específicas que afectan a las medidas contra el robo se describen en el Apéndice III. Esta Recomendación no modifica los requisitos generales para medidas contra el robo de teléfonos móviles inteligentes elaborados por la GSMA [b-GSMA].

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.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de la autentificación de entidades*.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 limpieza de datos [b-NIST SP 800-88]: acciones realizadas para asegurar que los datos grabados en medios no pueden recuperarse tanto por métodos ordinarios como extraordinarios. (A veces llamado sanitización).

3.1.2 garantía de autentificación de entidad (EAA, *entity authentication assurance*) [UIT-T X.1254]: grado de confianza que se alcanza con el proceso de autentificación de que la entidad es lo que afirma ser o se espera que sea (esta definición está basada en la definición de "garantía de autentificación" contemplada en [b-UIT-T X.1252]).

NOTA – La confianza se basa en el grado de confianza de la relación que existe entre la entidad y la identidad presentada.

3.1.3 identidad [b-UIT-T X.1250]: representación de una entidad bajo la forma de uno o más elementos de información que permiten distinguir suficientemente a la(s) entidad(es) dentro del contexto. A los efectos de la gestión de identidad, se entiende que el término identidad es una identidad contextual (subconjunto de atributos), es decir que la diversidad de atributos está limitada por un marco con fronteras definidas (el contexto) en el cual existe e interactúa la entidad.

NOTA – Cada entidad está representada por una identidad holística, que comprende todos los posibles elementos de información que caracterizan a dicha entidad (los atributos). Sin embargo, la identidad holística es una cuestión teórica y elude cualquier descripción y utilización práctica, dado que el número de todos los atributos posibles es indefinido.

3.1.4 herramienta de desactivación [b-GSMA]: manera de desactivar funciones esenciales de un dispositivo móvil.

NOTA – Es una función esencial dentro de un dispositivo móvil, que puede ser activada, por ejemplo, cuando un mensaje con un cierto formato es enviado al dispositivo, para que deje de funcionar como es debido y que solo pueda ser reactivado o reutilizado si el propietario del dispositivo autoriza su reactivación.

3.1.5 teléfono móvil [b-UIT-T X-Sup.19]: dispositivo electrónico utilizado para realizar llamadas telefónicas y enviar mensajes de texto por una amplia zona geográfica mediante acceso radioeléctrico a redes móviles públicas, que permite ser móvil al usuario.

3.1.6 teléfono inteligente [b-UIT-T X-Sup.19]: teléfono móvil con gran capacidad de cálculo, conectividad heterogénea y sistema operativo avanzado que constituye una plataforma para aplicaciones de terceros.

3.1.7 amenaza [b-ISO/IEC 27000]: causa potencial de un incidente indeseado, que puede infringir daño a un sistema u organización.

3.1.8 túnel [b-ISO/IEC 27033-1]: un túnel es un trayecto de datos entre dispositivos conectados en red, que se establece dentro de una infraestructura de red existente.

NOTA – Los túneles pueden establecerse utilizando técnicas como protocolos de encapsulado, conmutación por etiquetas o circuitos virtuales.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 hardware del dispositivo: los componentes físicos que forman conjuntamente un dispositivo móvil que funciona, y que incluyen la pantalla, las teclas, la tarjeta de circuito impreso, los circuitos integrados, la tarjeta SIM, el almacenamiento extraíble, etc.

3.2.2 software del dispositivo: todos los programas de software en el dispositivo y la tarjeta SIM, incluidas las aplicaciones, el sistema operativo, el cargador de arranque, la memoria ROM de arranque y el firmware.

3.2.3 usuario de dispositivo: el usuario autorizado del dispositivo móvil.

3.2.4 tunelización segura: protocolo que permite la transferencia segura de datos o mensajes de una ubicación de red a otra.

NOTA – La tunelización segura soporta generalmente autentificación de entidad, integridad del mensaje y confidencialidad del mensaje.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y acrónimos siguientes:

ATM Cajero automático (*automated teller machine*)

CRL Lista de revocación de certificados (*certificate revocation list*)

DER Normas de codificación distinguida (*distinguished encoding rules*)

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

DM Gestión de dispositivos (*device management*)

EAA Garantía de autentificación de entidad (*entity authentication assurance*)

GPS Sistema de posicionamiento global (*global positioning system*)

GSMA Asociación GSM (*Global System Mobile Association*)

HTTP Protocolo de transferencia de hipertexto *(hyper text transfer protocol)*

MAC Código de autenticación de mensaje *(message authentication code)*

NdG Nivel de garantía

OCSP Protocolo en línea de estado de certificados *(online certificate status protocol)*

OMA Alianza móvil abierta *(open mobile alliance)*

OTP Contraseña de uso único *(one time password)*

PII Información de identificación personal *(personally identifiable information)*

PKI Infraestructura de clave pública *(public-key infrastructure)*

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

SMS-SC Servicio de mensajes breves – centro de servicio (*short message service – service centre*)

SSL Capa de zócalo segura *(secure socket layer)*

TCP Protocolo de control de la transmisión *(transmission control protocol)*

TFA Autentificación de tres factores *(three-factor authentication)*

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

U Universal

UICC Tarjeta con circuito integrado universal (*universal integrated circuit card*)

USSD Datos de servicio suplementario no estructurados (*unstructured supplementary service data*)

2FA Autentificación de dos factores (*2-factor authentication*)

5 Convenios

La presente Recomendación se ajusta a las siguientes formas verbales de expresión de disposiciones:

a) "deberá" indica una obligación;

b) "debería" denota una recomendación;

c) "podría" significa que se da permiso;

d) "puede" indica posibilidad y capacidad.

6 Resumen de las medidas contra el robo de teléfonos móviles

6.1 Medidas contra el robo

El número de teléfonos inteligentes está creciendo rápidamente y se han convertido en una parte indispensable del día a día. Sin embargo, a millones de usuarios de teléfonos móviles les han robado sus teléfonos. Una medida contra el robo de teléfonos móviles, como por ejemplo una herramienta de desactivación debería proporcionar la capacidad de:

– borrar a distancia los datos personales de usuario que se encuentran en el teléfono inteligente en caso de robo o pérdida;
– dejar inoperable un teléfono inteligente para una persona no autorizada;
– almacenar, en caso de necesidad, los datos personales de usuario en el servidor de copia de seguridad gestionado por los operadores de servicio celular o los fabricantes de dispositivos;
– impedir la reactivación sin la autorización del usuario; y
– anular la inutilización cuando el usuario autorizado recupere el teléfono inteligente y volver a cargar los datos personales de usuario en el teléfono inteligente en la medida de lo posible desde el servicio de copia de seguridad.

El software contra el robo, instalado en el dispositivo móvil, puede desactivar un teléfono robado o perdido.

Cuando el propietario de un dispositivo se da cuenta de que su teléfono ha sido robado o ha desaparecido, existen dos escenarios para iniciar la ejecución de las funciones de desactivación:

1) el propietario del dispositivo contacta con el operador de su servicio celular, que ejecuta la operación de desactivación del dispositivo móvil; y
2) el propietario del dispositivo ejecuta una aplicación en otro dispositivo móvil o accede a una herramienta de desactivación que deja inoperable el dispositivo móvil perdido/robado.

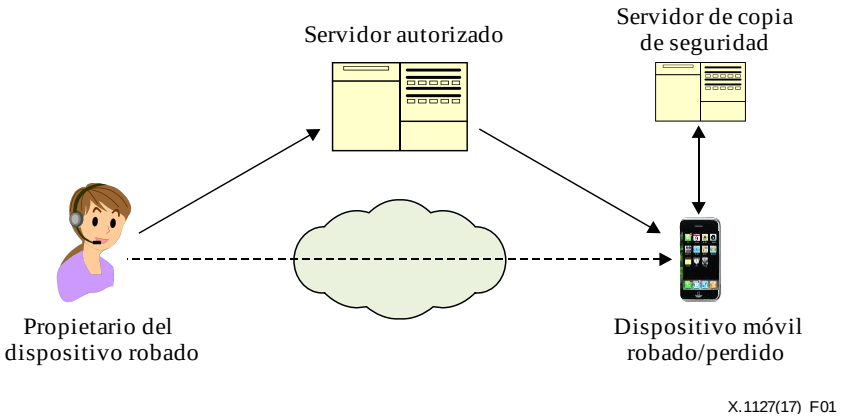


Figura 1 – Modelo de referencia para las medidas contra el robo

En la Figura 1, se describe el modelo de referencia para las medidas contra el robo de dispositivos móviles. El servidor autorizado soporta la función de desactivación de los dispositivos móviles, robados o perdidos, y los operadores del servicio celular o los fabricantes de dispositivos lo gestionan. El servidor autorizado envía una instrucción de desactivación al dispositivo móvil robado o perdido. El servidor de copia de seguridad recarga los datos personales del usuario a petición del propietario del dispositivo.

La comunicación entre el dispositivo móvil perdido/robado y el servidor autorizado debería protegerse mediante la utilización de un túnel seguro (por ejemplo, mediante una capa de zócalo segura (SSL, *secure socket layer*)). Además, la comunicación entre el dispositivo móvil perdido/robado y el servidor de copia de seguridad debería protegerse mediante un túnel seguro (por ejemplo SSL).

Esta Recomendación se ha elaborado basándose en el marco de la garantía de autentificación de entidad (EAA, *entity authentication assurance*) descrita en [UIT-T X.1254]. La EAA define cuatro niveles de garantía (NdG). Cada NdG describe el grado de confianza en los procesos que conducen a la autentificación, incluido el proceso de autentificación propiamente dicho, lo que garantiza que

la entidad que utiliza una determinada identidad es en realidad la entidad a la que se asignó dicha identidad.

Algunas legislaciones pueden requerir que el software contra el robo esté instalado o disponible para su descarga. Por ejemplo, en los Estados Unidos, California exige que se instale un software contra el robo en los nuevos teléfonos pero, aunque venga activado por defecto, los usuarios tendrán la posibilidad de desactivar esta prestación. Al tener la prestación contra el robo con un consentimiento por defecto (opt-out) en vez de explícito (opt-in), se prevé que muchos clientes utilicen las medidas contra el robo y, en consecuencia, la probabilidad de que un dispositivo móvil esté protegido será mayor.

6.2 Requisitos de alto nivel de las medidas contra el robo

Los requisitos de seguridad de alto nivel para las medidas contra el robo cuando se transfieren mensajes del sistema contra el robo entre el servidor autorizado y el dispositivo móvil son:

– autentificación de la entidad;
– integridad del mensaje;
– detección de repetición e integridad de secuencia;
– prueba de recepción y prueba de ejecución;
– confidencialidad de mensaje; e
– indicación del mecanismo de seguridad utilizado.

7 Arquitectura funcional para las medidas contra el robo de teléfonos móviles

7.1 Amenazas que afectan a las medidas contra el robo de teléfonos móviles

En esta sección se describe un conjunto de amenazas identificadas de seguridad, contempladas en algunos requisitos o mecanismos de la presente Recomendación. El modelo de amenaza contra la seguridad y otros aspectos fundamentales se han tratado de acuerdo con las siguientes Recomendaciones UIT-T:

– [b-UIT-T X.800] define los elementos de la arquitectura relativos a la seguridad en general que pueden aplicarse de manera adecuada en el caso de que se requiera una protección de la comunicación entre sistemas abiertos.
– [b-UIT-T X.805] define la arquitectura de seguridad de la red para proporcionar una seguridad de red extremo a extremo.

En [b-UIT-T X.800] y [b-UIT-T X.805], se identifican las siguientes amenazas contra las redes:

– destrucción de información y/o de otros recursos;
– corrupción o modificación de la información;
– robo, eliminación o perdida de información y/o de otros recursos;
– divulgación de información;
– interrupción de servicios.

Esta Recomendación identifica las siguientes amenazas específicas de las medidas contra el robo de teléfonos móviles:

– petición no autorizada de borrado de datos en un teléfono móvil desactivado;
– petición no autorizada de desactivación de un teléfono móvil;
– divulgación no autorizada de datos sensibles de un teléfono móvil;
– perdida de datos de usuario en un teléfono móvil;

– acceso no autorizado y/o modificación de las funciones de un dispositivo desactivado, o de los datos que contiene;
– divulgación no autorizada de datos de usuario y del intercambio de software entre el dispositivo y el operador de red y/o desactivación de la herramienta de medidas contra el robo.

Los riesgos son los siguientes:

– los piratas informáticos podrían encontrar una manera de piratear una instrucción de desactivación y apagar el móvil;
– podrían divulgarse los datos personales almacenados en la copia de seguridad o en tránsito entre e dispositivo móvil y el servidor de seguridad.

7.2 Funciones de seguridad esenciales para las medidas contra el robo de teléfonos móviles

La función de desactivación de un dispositivo móvil deberá ejecutarse únicamente desde un servidor autorizado o una herramienta de desactivación que soporte la función de desactivación. Con el fin de cumplir ese requisito, son necesarias las cinco funciones siguientes:

1) una comunicación segura entre el dispositivo y el servidor;
2) autentificación de la entidad del dispositivo efectuada por el servidor;
3) autentificación de la entidad del servidor por el dispositivo y autorización al servidor para realizar la función;
4) seguimiento de la ubicación del dispositivo robado; y
5) copia de seguridad/borrado seguro de los datos de un teléfono móvil desactivado.

Debería proporcionarse un mecanismo a través del sitio web personal para permitir a los propietarios de los dispositivos gestionar la información de identificación personal (PII) que debe almacenarse. La aplicación instalada en el móvil puede proporcionarse al propietario del dispositivo. La aplicación contra el robo puede permitir que los propietarios de los dispositivos seleccionen los datos, incluida la PII, para las medidas contra el robo, e incluye la realización de copias de seguridad de los datos, incluida la PII, en una solución de almacenamiento en la nube. El procedimiento para esta gestión se compone de tres pasos:

1) instalación de las aplicaciones en el dispositivo móvil;
2) inscripción en el sitio web por el operador del servicio móvil o el fabricante del dispositivo;
3) gestión (es decir, borrado, descarga y carga remota) de la PII almacenada en el servidor de copia de seguridad a través del sitio web personal.

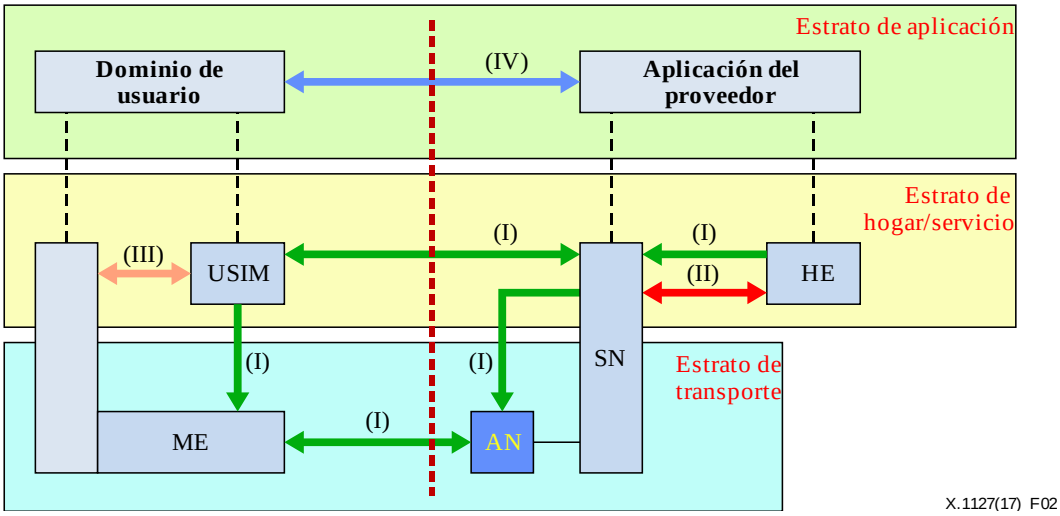
7.3 Arquitectura funcional para las medidas contra el robo de teléfonos móviles

La arquitectura funcional para las medidas contra el robo de dispositivos móviles se basa en la arquitectura de seguridad descrita en [b-3GPP TS 33.102]. La Figura 2 muestra la arquitectura de seguridad que comprende los cinco grupos de seguridad siguientes:

1) seguridad de acceso a la red (I): El conjunto de funciones de seguridad que proporciona a los usuarios un acceso seguro a los servicios 3G y que, en particular, protege de los ataques contra el enlace (radioeléctrico) de acceso;
2) seguridad del dominio de red (II): El conjunto de funciones de seguridad que permite a nodos del dominio del proveedor intercambiar datos de señalización de manera segura y proteger de los ataques contra la red cableada;
3) seguridad del dominio de usuario (III): El conjunto de funciones de seguridad que protege el acceso a las estaciones móviles;

4) seguridad del dominio de aplicación (IV): El conjunto de funciones de seguridad que permite a las aplicaciones de los dominios de usuario y de proveedor intercambiar mensajes de manera segura;

5) visibilidad y capacidad de configuración de la seguridad (V): El conjunto de funciones que permite al usuario obtener información sobre si una función de seguridad está funcionando o no y si la utilización y prestación de servicios debería depender de la función de seguridad.



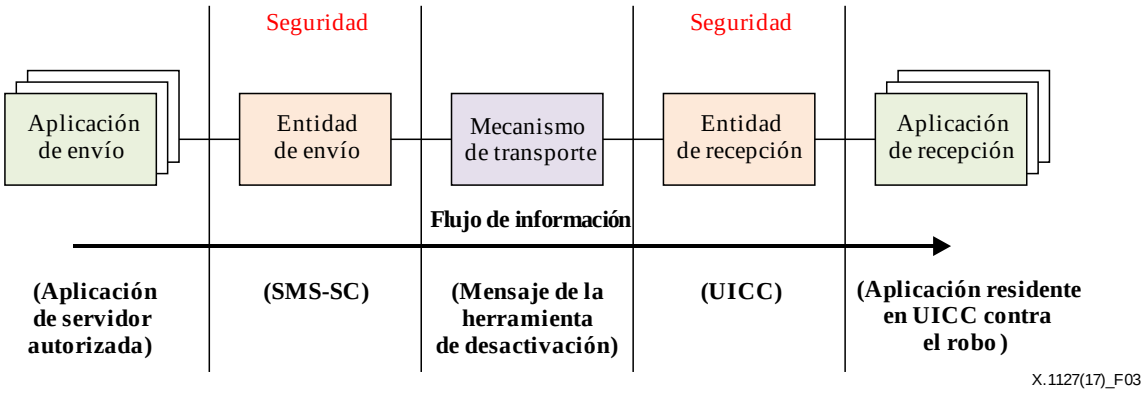
NOTA – La Figura 2 se ha tomado de [b-3GPP TS 33.102].

Figura 2 – Arquitectura de seguridad

La aplicación de medidas contra el robo en el dispositivo móvil forma parte del conjunto de aplicaciones que residen en el dominio de usuario, mientras que la función contra el robo en la parte del proveedor de servicio forma parte del conjunto de aplicaciones que residen en la aplicación del proveedor.

El modelo de referencia de seguridad para las medidas contra el robo se basa en una arquitectura descrita en [b-3GPP TS 22.048]. La aplicación de envío es una entidad que genera un mensaje de aplicación que se envía, mientras que la entidad de envío es la entidad de origen del paquete seguro (por ejemplo el centro de servicio de mensajes SMS (SMS-SC), la tarjeta de circuito integrado universal (UICC), el punto de entrada de datos de servicio suplementario no estructurados (USSD) o el servidor del juego de herramientas (U) SIM del módulo de identidad del abonado (universal) dedicado donde se invocan los mecanismos de seguridad. La entidad de envío genera los paquetes seguros para su envío. Los paquetes seguros se envían a través del túnel seguro del nivel de transporte o el túnel seguro del nivel de aplicación.

La aplicación de recepción es la entidad de destino del mensaje de la aplicación mientras que la entidad de recepción es la entidad donde se recibe el paquete seguro (por ejemplo el SMS-SC, la UICC, el punto de entrada de USSD o el juego de herramientas dedicado (U) SIM).



NOTA – La Figura 3 se ha tomado de [b-3GPP TS 22.048].

Figura 3 – Modelo de referencia de seguridad

En esta Recomendación, la arquitectura de seguridad se basa en el modelo de referencia de la Figura 1, la arquitectura de seguridad de la Figura 2 y el modelo de referencia de seguridad de la Figura 3.

7.4 Mecanismos para las medidas contra el robo de teléfonos móviles

7.4.1 Mecanismos para la comunicación segura

El dispositivo perdido o robado debería actuar como un servidor de autentificación del cliente de un túnel seguro.

El canal de comunicación entre el cliente y el servidor debería cumplir los seis requisitos siguientes:

1) Confidencialidad: El túnel seguro debería asegurar que las entidades no autorizadas no puedan leer los datos. Esto se realiza mediante la encriptación de los datos utilizando un algoritmo criptográfico y una clave secreta, es decir un valor conocido únicamente por las dos entidades que intercambian datos. Solo una entidad que tiene la clave secreta puede desencriptar los datos.

2) Integridad: El túnel seguro debería determinar si se han modificado los datos (de manera intencional o no) durante el tránsito. La integridad de los datos deberá garantizarse generando un valor de código de autentificación de mensaje (MAC), que es un código de verificación de los datos encriptado con clave. Si se modifican los datos y se recalcula el MAC, el antiguo y el nuevo MAC difieren.

3) Autentificación de pares: Cada punto extremo deberá confirmar la identidad del otro punto extremo con el cual desea comunicarse para asegurar que el tráfico de red y los datos se envían desde el servidor esperado. La autentificación de túnel seguro se realiza normalmente de manera unidireccional, autentificando el servidor al cliente; sin embargo, un túnel seguro necesita una autentificación de ambos puntos extremos.

4) Protección contra repeticiones: Los mismos datos no deberán entregarse múltiples veces y los datos no deberán entregarse burdamente de manera desordenada. Se podría utilizar un número de secuencia o un contador en el emisor del mensaje. El emisor del mensaje añade un número de secuencia a su paquete empezando por 0 y lo incrementa cada vez que envía un mensaje.

5) Protección contra el análisis de tráfico: Una persona que vigile el tráfico de red no deberá poder determinar el contenido del tráfico de red y la cantidad de información intercambiada. Un túnel seguro también puede ocultar qué partes están comunicando, mientras que SSL deja esta información expuesta. También puede protegerse, dependiendo de la implementación, la frecuencia de las comunicaciones. Sin embargo, se puede contar el número de paquetes intercambiados.

6) Control de acceso: Los puntos extremos del túnel seguro deberán realizar un filtrado para asegurar que únicamente los usuarios autorizados pueden acceder a recursos de red concretos. Los puntos extremos del túnel seguro también pueden permitir o bloquear cierto tipo de tráfico de red, como permitir el acceso a servidores web y denegar la compartición de ficheros.

Para cumplir los requisitos anteriores, se recomienda la utilización de la seguridad de la capa de transporte (TLS) para garantizar la seguridad de las comunicaciones entre el dispositivo móvil y el servidor autorizado. TLS es un protocolo que proporciona un túnel seguro de comunicación en las redes. Permite a las aplicaciones cliente/servidor comunicar de un modo diseñado para prevenir las escuchas, la manipulación o la falsificación de mensajes. TLS está posicionado entre los mejores protocolos de transporte fiables (por ejemplo, el protocolo de control de la transmisión (TCP), y se utiliza para la encapsulación de varios protocolos de alto nivel (por ejemplo, el protocolo de transferencia de hipertexto (HTTP)).

TLS se compone de tres fases básicas:

1) negociación entre pares para soporte del algoritmo;
2) intercambio de claves y autentificación;
3) encriptación de cifrado simétrico y mensajes de autentificación.

El perfil detallado para TLS se muestra en el Apéndice V.

Además, esta Recomendación también recomienda la utilización del canal seguro de comunicación basado en el protocolo de la Alianza Móvil Abierta (OMA).

7.4.2 Mecanismos de autentificación mutua

La autentificación sirve para confirmar las identidades de las entidades que comunican. Existen tres tipos de factores de autentificación:

1) factor de conocimiento ("algo que solo el usuario conoce"), como las contraseñas;
2) factor de posesión ("algo que solo el usuario posee"), como las tarjetas de los cajeros automáticos; y
3) factor inherente ("algo que solo el usuario es"), como los datos biométricos.

En [b-UIT-T X.1158] se describen tres tipos de métodos de autentificación:

1) autentificación de factor único (SFA), es el método tradicional que requiere solo un nombre de usuario y una contraseña antes de facilitar el acceso al usuario;
2) autentificación de dos factores (2FA), basada en la utilización de una combinación de dos factores de autentificación diferentes. Estos factores pueden ser algo que el usuario sabe, algo que el usuario posee o algo que el usuario es. En el día a día, un buen ejemplo es un usuario que quiere extraer dinero del cajero automático, solo la combinación correcta de una tarjeta bancaria (algo que el usuario posee) y de un número de identificación personal (PIN), es decir, algo que el usuario conoce, permite la realización de la transacción;
3) autentificación de tres factores (TFA) basada en la utilización de una combinación de tres factores diferentes independientes: Lo que el usuario sabe (contraseña), lo que el usuario posee (testigo de seguridad) y lo que el usuario es (verificación biométrica).

Las autentificaciones de múltiples factores se basan en la utilización de una combinación de dos o más factores diferentes independientes. Las autentificaciones de 2FA y TFA son una parte de las autentificaciones de múltiples factores.

7.4.3 Mecanismos para el borrado seguro de datos

La limpieza se refiere al proceso que impide el acceso a los datos objetivo en un medio, para un nivel de esfuerzo dado [b-NIST SP 800-88]. [b-NIST SP 800-88] proporciona las tres categorías de limpieza siguientes:

1) operación de borrado: aplica técnicas lógicas para la limpieza de los datos en todas las posiciones de almacenamiento accesibles por el usuario, como protección contra las técnicas simples no invasivas de recuperación de datos; se realizan normalmente a través de los comandos normalizados Escribir y Leer en el dispositivo de almacenamiento, como puede ser reescribir un nuevo valor o utilizar una opción de menú para reiniciar el dispositivo en su estado de fabricación (cuando no se soporta la reescritura);
2) operación de purga: aplica técnicas físicas o lógicas que impiden que se recuperen los datos objetivo mediante la utilización de las últimas técnicas de laboratorio;
3) operación de destrucción: impide la recuperación de los datos objetivo mediante la utilización de las últimas técnicas de laboratorio y tiene como resultado la imposibilidad de utilizar el medio para almacenar datos.

La operación de borrado sobrescribe el medio utilizando programas informáticos aprobados por la organización y realiza una verificación de los datos sobrescritos. El patrón de borrado debería tener al menos una pasada de escritura simple con un valor fijo de escritura, como todos ceros. Múltiples pasadas de escritura o valores más complejos son opciones que también pueden utilizarse.

8 Requisitos funcionales de seguridad

8.1 Resumen

– la arquitectura funcional debe basarse en el marco EAA descrito en [UIT-T X.1254];
– la arquitectura funcional debe proporcionar un túnel seguro (por ejemplo, TLS descrito en [b-IETF RFC 6460] o una canal seguro de comunicación basado en el protocolo OMA) para las comunicaciones entre componentes;
– la arquitectura funcional debe proporcionar una gestión segura de claves (por ejemplo, basada en la infraestructura de clave pública (PKI) descrita en [b-UIT-T X.509]) para soportar túneles seguros;
– la arquitectura funcional debe soportar al menos el mecanismo de autentificación de entidades con un nivel de garantía 2 (NdG2) descrito en [UIT-T X.1254];
– la arquitectura funcional debe soportar al menos la afiliación de entidades con un NdG2 descrita en [UIT-T X.1254];
– la arquitectura funcional debe soportar al menos la gestión de credenciales de entidad con un NdG2 descrita en [UIT-T X.1254];
– la arquitectura funcional debe soportar la autentificación de mensajes para los mensajes transferidos;
– la arquitectura funcional debe soportar la protección contra un ataque por repetición para los mensajes transferidos;
– la arquitectura funcional debe soportar la capacidad de realizar una copia de seguridad de los datos del dispositivo en el servidor seguro de red;
– la arquitectura funcional debe proporcionar una autorización robusta (control de acceso);
– la arquitectura funcional debe soportar mecanismos de seguridad descritos en [b-3GPP TS 22.048];
– la arquitectura funcional debe proporcionar una gestión de identidades para el propietario del dispositivo móvil, el servidor autorizado y los dispositivos móviles robados.

8.2 Requisitos funcionales de seguridad para el propietario del dispositivo móvil

– el propietario del dispositivo móvil debe ser autentificado en el servidor autorizado mediante una autentificación de al menos 2FA (por ejemplo, identificación/contraseña y una contraseña de uso único (OTP) como se describe en [UIT-T X.1254]);

– el propietario del dispositivo móvil debe identificarse utilizando al menos un procedimiento de afiliación de entidades con un NdG2 descrito en [UIT-T X.1254];

– la arquitectura funcional del propietario del dispositivo debe autentificar el servidor de autorización utilizando al menos un mecanismo de autentificación con un NdG2 descrito en [UIT-T X.1254];

– la arquitectura funcional del propietario del dispositivo debe soportar un túnel seguro (por ejemplo, TLS descrito en [b-IETF RFC 6460] o un canal seguro de comunicación basado en el protocolo OMA) para la comunicación de mensajes transferidos con el servidor autorizado.

8.3 Requisitos funcionales de seguridad para el servidor autorizado

– la arquitectura funcional del servidor autorizado debe autentificar el propietario del dispositivo utilizando al menos un mecanismo de autentificación 2FA (por ejemplo, las autentificaciones de NdG3 descritas en [UIT-T X.1254]);

– la arquitectura funcional del servidor autorizado debe ser autentificada por el dispositivo móvil robado utilizando al menos un mecanismo de autentificación 2FA (por ejemplo, las autentificaciones de NdG3 descritas en [UIT-T X.1254]);

– la arquitectura funcional del servidor autorizado debe soportar un túnel seguro (por ejemplo, TLS descrito en [b-IETF RFC 6460] o un canal seguro de comunicación basado en el protocolo OMA) para la comunicación de mensajes con el propietario del dispositivo móvil robado;

– la arquitectura funcional del servidor autorizado debe soportar un túnel seguro para la comunicación del mensaje transferido con el dispositivo móvil robado.

8.4 Requisitos funcionales de seguridad para el dispositivo móvil robado

– la arquitectura funcional del dispositivo móvil robado debe soportar un túnel seguro (por ejemplo, TLS descrito en [b-IETF RFC 6460] o un canal seguro de comunicación basado en el protocolo OMA) para la comunicación del mensaje transferido con el servidor autorizado;

– la arquitectura funcional del dispositivo móvil robado debe ser autentificado en el servidor autorizado utilizando al menos un mecanismo de autentificación 2FA (por ejemplo, las autentificaciones de NdG3 descritas en [UIT-T X.1254]);

– la arquitectura funcional del dispositivo móvil robado debe autentificar el servidor autorizado utilizando un mecanismo de autentificación 2FA (por ejemplo, las autentificaciones de NdG3 descritas en [UIT-T X.1254]);

– la arquitectura funcional del dispositivo móvil robado debe invocar una función para realizar una copia de seguridad de todos los datos del dispositivo que pertenecen al propietario a un servidor seguro de la red;

– la arquitectura funcional del dispositivo móvil robado debe implementar los mecanismos de control de acceso para lanzar la ejecución de las instrucciones recibidas del servidor autorizado;

– la arquitectura funcional del dispositivo móvil robado debe proteger los datos o las funciones frente al acceso y utilización por una entidad no autorizada;

– la arquitectura funcional del dispositivo móvil robado debe soportar la operación de borrado para la eliminación segura de los datos descrita en la sección 7.4.3, una vez recibida en el dispositivo móvil la instrucción de borrado enviada desde el servidor autorizado.

8.5 Requisitos funcionales de seguridad para el servidor de copia de seguridad

– la arquitectura funcional del servidor de copia de seguridad debe soportar un túnel seguro para la transferencia de mensajes con el dispositivo móvil;

– la arquitectura funcional del servidor de copia de seguridad debe autentificar el dispositivo móvil utilizando un mecanismo de autentificación robusta, que es la copia de seguridad de los datos del dispositivo, en caso de necesidad;

– la arquitectura funcional del servidor de copia de seguridad debe ser autentificada por el dispositivo móvil utilizando un mecanismo de autentificación robusto;

– la arquitectura funcional del servidor de copia de seguridad debe tener capacidad para realizar una copia de seguridad, desde el dispositivo móvil, de los datos apropiados del dispositivo;

– la arquitectura funcional del servidor de copia de seguridad debe proporcionar suficientes recursos (es decir, almacenamiento) al dispositivo móvil.

Apéndice I

Requisitos generales para las medidas contra el robo

(Este apéndice no forma parte integrante de esta Recomendación.)

La norma [b-GSMA] describe los requisitos generales de información para las medidas contra el robo. Este Apéndice describe esos requisitos.

I.1 Propietario del dispositivo

– Confirmar que el dispositivo está irremediablemente perdido o robado (por ejemplo, las coordenadas del sistema de posicionamiento global (GPS) del dispositivo muestran el dispositivo en una ubicación desconocida por el propietario), el propietario debe iniciar el procedimiento para la desactivación del servicio después de realizar las acciones siguientes:
  - activar el dispositivo para que emita un fuerte tono durante un periodo prolongado (30 segundos a 3 minutos) para permitir al propietario localizarlo, siempre y cuando esté al alcance del oído;
  - mostrar un mensaje en la pantalla principal o la pantalla de bloqueo del dispositivo pidiendo la devolución del mismo;
  - encontrar la ubicación del dispositivo utilizando el GPS (o cualquier otra función de localización soportada por el dispositivo) y mostrarla en un mapa.
– Es necesario que el propietario cancele explícitamente (opted-out) la función de desactivación del dispositivo que, por defecto, debe estar activada.
– En el arranque inicial y configuración del dispositivo móvil, se recomienda presentar al propietario del dispositivo una breve guía para informarle sobre los comportamientos seguros en la utilización y almacenamiento del nuevo dispositivo. Debería ser necesario completar la presentación de la guía antes de la activación del servicio.
– Se recomienda que el propietario del dispositivo pueda acceder e invocar una función de desactivación del dispositivo a través de la utilización de capacidades de autoservicio, sin la necesidad de involucrar al operador de red.
– Se recomienda que el propietario del dispositivo no pueda reactivar el dispositivo cuando ha sido desactivado por el operador.
– El propietario puede invocar una función para realizar una copia de seguridad de todos los datos del dispositivo que pertenecen al propietario (datos personales) en un servidor seguro de la red.
– El propietario debe tener la posibilidad de bloquear a distancia el acceso a todos los datos del dispositivo.
– El propietario debe poder borrar a distancia los datos de usuario (es decir, fotos, videos, agenda de contactos, correos electrónicos) del dispositivo. En el caso de que los datos de usuario estén fuertemente encriptados, entonces eliminar del dispositivo la clave de encriptación es suficiente.
– En el caso de los dispositivos perdidos o robados en una red visitada (itinerancia), puede avisarse al propietario de cualquier coste adicional cuando intente invocar funciones de copia de seguridad de los datos, desactivación del dispositivo o reactivación del dispositivo.
– Un usuario no autorizado no debe poder acceder a las funciones o a los datos de un dispositivo desactivado.
– Debería facilitarse al usuario una función para poder mostrar un mensaje en la pantalla principal o en la pantalla de bloqueo del dispositivo, pidiendo la devolución del mismo cuando el dispositivo no está a disposición del propietario.

I.2 Servidor

– Un operador de red debe autentificar una solicitud de un propietario de dispositivo para iniciar la desactivación del dispositivo.

– Una solicitud de un propietario para la desactivación de un dispositivo debe autentificarse y solo se requiere para controlar el dispositivo registrado por ese propietario.

– La ubicación y el acceso a los servidores que soportan la función de desactivación deben ser seguros.

– Se recomienda autorizar solo a personal con suficiente formación el acceso a las funciones de desactivación y la invocación de las mismas.

– El servidor debe generar y mantener registros de todas las solicitudes de desactivación recibidas.

– Cuando se restablezca el servicio en un dispositivo reactivado que haya sido previamente desactivado, es necesario restablecer los datos de la copia de seguridad y las aplicaciones en el dispositivo.

– Los datos de propietario de la copia de seguridad deben almacenarse de manera segura y debe garantizarse la confidencialidad e integridad de los mismos.

– Una vez que el propietario ha solicitado la desactivación de su dispositivo, cabe esperar que la función finalice su ejecución en menos de 15 minutos, siempre y cuando se realice correctamente la autentificación.

– Un reinicio a los valores de fábrica no puede servir como método para evitar las medidas contra el robo.

I.3 Dispositivo móvil

– Debe verificarse la autenticidad de la solicitud de desactivación de un dispositivo antes de efectuar los siguientes pasos del proceso de desactivación.

– El mecanismo para desactivar un dispositivo móvil debe ejecutarse desde un servidor autorizado que soporta la función de desactivación. Para cumplir ese requisito, es necesario:

  • una conexión segura entre el dispositivo y el servidor;

  • la autentificación del dispositivo por el servidor;

  • la autentificación del servidor por el dispositivo y que el servidor disponga de la autorización de realizar la función.

– El dispositivo móvil, en el arranque inicial y configuración, debe guiar explícitamente al propietario a través de la configuración de las capacidades contra el robo y de cualquier otra función de seguridad relevante como los mecanismos de control de acceso al dispositivo.

– El dispositivo debe tener la capacidad de que el propietario legítimo reactive el servicio después de que se haya desactivado. No debe ser capaz de ser reactivado por alguien que no sea su propietario legítimo.

– Se recomienda que la función de desactivación del dispositivo pueda ejecutarse cuando el dispositivo no está conectado a una red móvil terrestre pública pero está conectado a Internet.

– Para los dispositivos perdidos o robados en una red visitada (itinerancia), todas las funciones de copia de seguridad de los datos, desactivación del dispositivo o reactivación del servicio deben funcionar adecuadamente.

I.4 Fabricación del dispositivo

– Se recomienda que los fabricantes de dispositivos sigan implementando y evolucionando las medidas para impedir y prevenir la reconfiguración no autorizada de un dispositivo perdido o robado a un estado en el cual pueda utilizarlo alguien que no es el propietario.

Apéndice II

Requisitos adicionales de seguridad para las medidas contra el robo

(Este apéndice no forma parte integrante de esta Recomendación.)

II.1 Requisitos para el servido de copia de seguridad

– El mecanismo debe ejecutarse desde un servidor de copia de seguridad que soporte el almacenamiento de la PII de los dispositivos móviles perdidos o robados. Para cumplir ese requisito se necesita:

- una conexión segura entre el dispositivo y el servidor de copia de seguridad;
- la autentificación del dispositivo móvil por el servidor de copia de seguridad;
- la autentificación del servidor de copia de seguridad por el dispositivo.

Apéndice III

Amenazas específicas que afectan a las medidas contra el robo

(Este apéndice no forma parte integrante de esta Recomendación.)

III.1 Amenazas entre el propietario del dispositivo móvil y el servidor autorizado

– Suplantación del propietario del dispositivo. Un atacante que suplanta el propietario del dispositivo envía una instrucción de desactivación indebida al servidor autorizado. El ataque que explota esa amenaza puede provocar la desactivación de dispositivos móviles inocentes.

– Manipulación, escucha y reproducción de un mensaje. Se envía una instrucción de desactivación indebida al servidor autorizado; el contenido del mensaje de la instrucción es revelado al atacante que es capaz de acceder a la comunicación o se envía una enorme cantidad de tráfico que provoca un ataque de denegación de servicio distribuido (DDoS) al servidor autorizado.

– Suplantación del servidor autorizado. Se divulgan las credenciales de autentificación del propietario legítimo del dispositivo o se envía una instrucción de desactivación del propietario legítimo del dispositivo al servidor autorizado suplantado. El ataque que explota esta amenaza puede provocar la desactivación de dispositivos móviles inocentes.

III.2 Amenazas entre el servidor autorizado y el agente de desactivación contra el robo

– Suplantación del servidor de autentificación. Se envía una instrucción de desactivación indebida al dispositivo móvil robado.

– Manipulación, escucha y reproducción de un mensaje. Se envía una instrucción de desactivación indebida al agente de desactivación contra el robo; el contenido del mensaje de la instrucción es revelado al atacante que es capaz de acceder a la comunicación o se envía una enorme cantidad de tráfico que provoca un ataque distribuido de denegación de servicio DDoS al agente de desactivación.

– Suplantación del agente de desactivación. Se divulgan las credenciales de autentificación del servidor autorizado legítimo o se envía una instrucción de desactivación del propietario legítimo del dispositivo al agente de desactivación suplantado.

III.3 Amenazas entre el agente de desactivación contra el robo y el servidor de copia de seguridad

– Suplantación del agente de desactivación contra el robo. El mensaje de copia de seguridad almacenado en el servidor de copia de seguridad es revelado al agente de desactivación suplantado.

– Manipulación, escucha y reproducción de un mensaje. La información de copia de seguridad es modificada y revelada al atacante que es capaz de acceder a la comunicación.

– Suplantación del servidor de copia de seguridad. La información de copia de seguridad es revelada al servidor de copia de seguridad suplantado.

Apéndice IV

Entorno para las medidas contra el robo

(Este apéndice no forma parte integrante de esta Recomendación.)

IV.1 Tipo de funciones de desactivación de los dispositivos móviles

Existen dos tipos de funciones de desactivación:

1) una función de desactivación "dura" que provoca la inutilización permanente del dispositivo móvil robado;
2) una función de desactivación "suave" que solo provoca que un "usuario no autorizado" no pueda utilizar el dispositivo móvil.

IV.2 Permiso de los dispositivos móviles robados/perdidos

Las prestaciones contra el robo necesitan una participación activa del propietario del dispositivo móvil. Cuando el propietario de un dispositivo compra un nuevo dispositivo, y se abona a un proveedor celular, debería configurar el dispositivo móvil para permitir las funciones contra el robo.

IV.3 Escenario de desactivación de un dispositivo móvil robado/perdido

Cuando un teléfono móvil es robado o se pierde, el propietario del dispositivo contacta con su proveedor celular o utiliza un sitio web operado por el operador celular, identificado como un servidor autorizado, para enviar una instrucción de "desactivación del dispositivo" al dispositivo móvil. La instrucción bloqueará el dispositivo móvil y, si lo selecciona el propietario, podría borrar algunos datos personales del dispositivo móvil o permitir el almacenamiento de algunos datos personales en el servidor de copia de seguridad.

La instrucción de desactivación del dispositivo provocará que el dispositivo no pueda funcionar en la red de ningún proveedor de servicios móviles comerciales o de servicios de datos móviles comerciales en todo el mundo, incluso si se apaga el dispositivo y se extrae la memoria de almacenamiento de datos.

La única manera de reactivar un dispositivo bloqueado será una contraseña proporcionada por el propietario del dispositivo.

Apéndice V

Perfil TLS para las medidas contra el robo

(Este apéndice no forma parte integrante de esta Recomendación.)

En este apéndice se proporciona un perfil TLS mínimo para las medidas contra el robo. En [b-IETF RFC 6460] y [b-ISO/IEC 20648] se describe un ejemplo típico de perfil TLS.

V.1 Requisito del protocolo TLS

– Se recomienda que el sistema contra el robo actúe como servidor para la implementación del protocolo TLS; sin embargo, su utilización por los clientes es opcional. Se requiere la utilización de la versión 1.2 de TLS (especificada en [b-IETF RFC 5246]).

V.2 Conjuntos de cifrado TLS para la interoperabilidad

– El sistema contra el robo no deberá utilizar MD5 o SHA-1 como el código de autentificación de mensajes mediante troceo con clave (HMAC) por defecto.

– El sistema contra el robo no deberá utilizar RC4 como el algoritmo criptográfico por defecto.

NOTA – [b-IETF RFC 7465] prohíbe la utilización de RC4.

– El sistema contra el robo debe soportar: selección y utilización de pares de algoritmos de firma/troceo, utilizando los algoritmos de firma soportados en TLS 1.2 y la utilización de algoritmos de troceo SHA-256 o de mayor resistencia.

– El sistema contra el robo debe utilizar conjuntos de cifrado con una resistencia de al menos 112 bits. Además es necesario soportar los siguientes conjuntos de cifrado:

  • TLS_RSA_WITH_AES_128_CBC_SHA256 {0x00, 0x3C}.

V.3 Certificados digitales

El sistema contra el robo debe soportar los certificados de clave pública [b-UIT-T X.509] versión 3 conformes con el perfil de certificado y de extensión de certificado definidos en la sección 4 de [b-IETF RFC 5280].

– El servidor TLS del sistema contra el robo debe soportar certificados de servidor.

– Se recomienda que el cliente TLS del sistema contra el robo soporte los certificados de cliente.

– El sistema contra el robo debe soportar un tamaño de claves de 2048 bits o más, para los certificados [b-UIT-T X.509] de servidor RSA/DSA.

– El sistema contra el robo debe soportar los formatos de certificados: [b-UIT-T X.509] codificado según las normas de codificación distinguida (DER), [b-UIT-T X.509] con codificación Base64 y PKCS#12 [b-IETF RFC 7292].

– El sistema contra el robo debe soportar la validación de certificados según se describe en la sección 6 de la norma [IETF RFC 5280], que se presentan como certificados digitales. Además, se deberá utilizar uno de los dos siguientes enfoques para determinar si un certificado ha sido revocado:

  • Opción 1: utilización de listas de revocación de certificados (CRL): CRL soportadas en formato [b-UIT-T X.509] con codificación DER, [b-UIT-T X.509] con codificación Base64 y CRL válidas almacenadas localmente (la distribución no está soportada en esta norma) o recuperadas de una fuente externa (por ejemplo, un punto de distribución de CRL (CRLDP)).

- Opción 2: utilización de un protocolo de estado de certificados como el protocolo en línea de estado de certificados (OCSP), de uno de los modos siguientes: utilización directa del OSCP según se describe en [b-IETF RFC 6960] o utilización indirecta de OSCP a través de la extensión de petición del estado de certificados del protocolo TLS descrita en la sección 8 de [b-IETF RFC 6066].

Apéndice VI

Visión general de la gestión de dispositivos OMA

(Este apéndice no forma parte integrante de esta Recomendación.)

En este apéndice, se describe una visión general del protocolo de gestión de dispositivos (DM) definido por OMA [b-OMA-DM].

VI.1 Especificación de la gestión de dispositivos OMA

La especificación DM de OMA se ha diseñado para la gestión de dispositivos móviles como teléfonos móviles, PDA y tabletas informáticas. La gestión de dispositivos tiene como fin soportar las siguientes utilizaciones:

– Puesta en servicio: configuración del dispositivo (incluida la primera utilización), activación y desactivación de funciones.

– Configuración del dispositivo: permite cambios en los ajustes y parámetros del dispositivo.

– Actualizaciones de software: proporciona nuevo software y/o corrección de errores para cargar en el dispositivo, incluidas aplicaciones y software del sistema.

– Gestión de fallos: informa de errores en el dispositivo, consulta sobre el estado del dispositivo.

La especificación DM de OMA soporta todas las funciones descritas anteriormente, y un dispositivo puede implementar opcionalmente todas estas funcionalidades o un subconjunto de ellas. Como la especificación DM de OMA está enfocada a los dispositivos móviles, está diseñada con atención especial a los siguientes puntos:

– Dispositivos con una baja huella de carbono, donde la memoria y el espacio de almacenamiento pueden estar limitados.

– Limitaciones sobre el ancho de banda de las comunicaciones, como en la conectividad inalámbrica.

– Seguridad ajustada, pues los dispositivos son vulnerables a los ataques software; la autentificación y los retos forman parte de las especificaciones.

Bibliografía

[b-UIT-T X.509] Recomendación UIT-T X.509 (2012), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

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

[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.1158] Recomendación UIT-T X.1158 (2014), *Mecanismo de autentificación multifactorial utilizando un dispositivo móvil*

[b-UIT-T X.1250] Recomendación UIT-T X.1250 (2009), *Capacidades básicas para una mejor gestión y compatibilidad de identidades a escala mundial*.

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[b-UIT-T X-Sup.19] Recomendaciones UIT-T de la serie X – Suplemento 19 (2013), *Supplement on security aspects of smartphones*.

[b-ISO/IEC 20648] ISO/CEI 20648:2016, *Information technology – TLS specification for storage systems*.

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

[b-ISO/IEC 27033-1] ISO/CEI 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-3GPP TS 22.048] 3GPP TS 22.048 (2003), *Security mechanisms for the (U)SIM Application Toolkit*, junio de 2003.

[b-3GPP TS 33.102] 3GPP TS 33.102 (2009), *3G Security; Security architecture (Release 9)*, diciembre de 2009.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[b-IETF RFC 6066] IETF RFC 6066 (2011), *Transport Layer Security (TLS) Extensions: Extension Definitions.*

[b-IETF RFC 6460] IETF RFC 6460 (2012), *Suite B Profile for Transport Layer Security (TLS)*.

[b-IETF RFC 6960] IETF RFC 6960 (2013), *ITU-T X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[b-IETF RFC 7292] IETF RFC 7292 (2015), *PKCS #12 Personal Information Exchange Syntax v1.1*.

[b-IETF RFC 7465] IETF RFC 7465 (2015), *Prohibiting RC4 Cipher Suites*.

[b-GSMA] GSMA, *SG.24 Anti-Theft Device Feature Requirements v3.0*, 17 de mayo de 2016.

[b-OMA-DM] Open Mobile Alliance, *OMA Device Management V1.2*, abril de 2013.

[b-NIST SP 800-88] NIST, *NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization*, diciembre de 2014.

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, 2018