Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1368

(01/2021)

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

Aplicaciones y servicios seguros (2) – Seguridad en la Internet de las cosas (IoT)

Actualización segura del firmware o software para dispositivos de Internet de las cosas

Recomendación UIT-T X.1368

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.1368

Actualización segura del firmware o software para dispositivos de Internet de las cosas

Resumen

En la Recomendación UIT-T X.1368 se especifican: 1) modelos y procedimientos básicos para actualizar con seguridad el firmware o el software (FW/SW) de los dispositivos de Internet de las cosas (IoT); y 2) requisitos y capacidades para actualizar el FW de la IoT.

También se especifica un procedimiento de actualización seguro común con unos requisitos generales. Este procedimiento permite que las actualizaciones comunes del SW/FW de IoT se apliquen de manera segura entre las partes interesadas en el entorno de la IoT, como son los desarrolladores de dispositivos de IoT y los proveedores de sistemas/servicios de IoT.

Esta Recomendación se centra en la actualización del FW, pero es aplicable a la actualización de cualquier otro SW de dispositivos de IoT.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1368	07-01-2021	17	11.1002/1000/14445

Palabras clave

Actualización de software, IoT; seguridad.

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

ÍNDICE

Introducción

Los ciberataques contra dispositivos o sistemas de Internet de las cosas (IoT) son cada vez más sofisticados, inteligentes y variados. Antes, las funciones de la mayoría de dispositivos de IoT estaban determinadas por los fabricantes durante su fase de comercialización inicial. Sin embargo, en los últimos tiempos los dispositivos se conectan a Internet para prestar una serie de servicios de IoT mejorados. Por consiguiente, los dispositivos de IoT en uso corren el riesgo de sufrir ciberamenazas o ciberataques. Hay que saber que es necesario actualizar de manera segura el firmware o software (FW/SW) integrado en los dispositivos de IoT para eliminar sus vulnerabilidades y puntos débiles. Algunos fabricantes ya han empezado a prestar un servicio de actualización FW dentro de sus propios planes.

En esta Recomendación se exponen los modelos y procedimientos básicos de actualización segura del SW/FW de IoT, así como los requisitos y capacidades conexos. Gracias a los modelos básicos y al procedimiento de actualización común, las partes interesadas pueden intercambiar de forma segura el SW/FW de IoT en el entorno de la IoT, lo que los incita a actualizar el SW/FW de IoT obsoleto.

Recomendación UIT-T X.1368

Actualización segura del firmware o software para dispositivos de Internet de las cosas

1 Alcance

En esta Recomendación se especifican los modelos y procedimientos básicos para la actualización segura del firmware o software (FW/SW) de dispositivos de IoT. También se describen los requisitos y capacidades necesarios para la actualización del FW/SW de IoT. Esta Recomendación se centra en la actualización del FW, pero es aplicable a la actualización otro SW de dispositivos de IoT.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 autor: Entidad que produce imágenes de firmware (FW) y software (SW) para dispositivos de Internet de las cosas. Puede tratarse de personas individuales o grupos, como una empresa o una organización de otro tipo. El autor puede cargar la imagen a uno o más servidores FW, no necesariamente fiables.

3.2.2 consumidor de firmware: Entidad que almacena, verifica y ejecuta imágenes de firmware (FW) en un dispositivo de Internet de las cosas (IoT). Debe decidir si se han de ejecutar las imágenes de FW vigentes. Un dispositivo de IoT tiene uno o más consumidores de FW.

3.2.3 servidor de firmware: Entidad que distribuye imágenes de firmware (FW). Puede aceptar imágenes de FW de múltiples autores; puede servir de depósito para un fabricante concreto o ser el depósito de varios fabricantes. En una configuración ideal, el servidor FW es fiable, pero puede no serlo y puede intentar ver o modificar los lotes de FW recibidos de los autores.

3.2.4 manifiesto: Registro que contiene los metadatos de una imagen de firmware (FW).

3.2.5 rastreador de estado: Entidad que verifica y hace un seguimiento del estado de las imágenes de firmware (FW) dentro de uno o más consumidores de FW e inicia la actualización del FW, según sea necesario. Se incluye aquí la supervisión detallada de los cambios del dispositivo, por ejemplo, la versión de las imágenes de FW que se ejecutan y el estado del ciclo de actualización de FW en que se encuentra el dispositivo. El rastreador de estado puede residir en el dispositivo de Internet de las cosas, en la Intranet o en la Internet.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

DLT Tecnología de libro mayor distribuido (*distributed ledger technology*)

FW Firmware

IoT Internet de las cosas (*internet of things*)

SW Software

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

5 Convenios

En esta Recomendación se siguen los siguientes convenios, armonizados con los de [b-IETF RFC 2119].

"Debe(n)" Esta palabra significa que el elemento en cuestión es un requisito absoluto de esta Recomendación.

"No debe(n)" Esta expresión significa que el elemento es una prohibición absoluta de esta Recomendación.

"Debería(n)" Esta palabra significa que en determinadas circunstancias pueden existir motivos válidos para hacer caso omiso del elemento de que se trate, pero que deberían tenerse en cuenta todas las implicaciones y ponderar cuidadosamente el caso antes de decidir optar por una vía diferente.

"No debería(n)" Esta expresión significa que pueden existir motivos válidos en determinadas circunstancias en las que el comportamiento indicado sea aceptable o incluso de utilidad, pero que deberían tenerse en cuenta todas las implicaciones y ponderar cuidadosamente el caso antes de implementar cualquier comportamiento descrito con esta etiqueta.

"Puede(n)" Esta palabra significa que el elemento es verdaderamente facultativo. Un fabricante puede optar por incluir el elemento porque así se exige en un determinado mercado o porque mejora el producto, por ejemplo; otro fabricante puede omitir el mismo elemento.

6 Modelo básico

Los dispositivos de IoT pueden utilizar arquitecturas de interconexión de redes diferentes, pero en todos los casos deberá haber las siguientes cuatro entidades funcionales: consumidor de FW (véase la cláusula 3.2.2), rastreador de estado (véase la cláusula 3.2.5), autor (véase la cláusula 3.2.1) y servidor de FW (véase la cláusula 3.2.3). Ha de tenerse en cuenta que en un nodo pueden residir múltiples entidades funcionales. Por ejemplo, un dispositivo cámara web contiene múltiples consumidores de FW y un rastreador de estado, mientras que un servidor web contiene un rastreador de estado y un servidor de FW. Dentro de una red puede haber múltiples consumidores de FW, que son supervisados por el rastreador de estado implementado en la pasarela. Los diseños pueden variar en función de las restricciones impuestas a los dispositivos de IoT. En la cláusula 8 se describen los modelos típicos.

En el modelo básico estas entidades desempeñan un papel fundamental en la actualización del SW/FW de IoT. La situación básica en este modelo es simple: *un rastreador de estado reconoce la necesidad de actualizar el SW/FW de IoT e inicia el procedimiento de actualización del SW/FW que permite a los consumidores de FW recibir una imagen de SW/FW de un autor a través de un servidor de FW*.

7 Procedimiento de actualización

En la Figura 1 se ilustra el procedimiento básico de actualización del FW. Antes de iniciar el procedimiento de actualización del FW, el autor debe cargar una nueva imagen de FW en un servidor de FW. Conviene que la imagen vaya acompañada de una firma digital y esté encriptada por el autor.

Cuando un rastreador de estado recibe una solicitud de actualización de una imagen de FW con su localización [por ejemplo, su localizador uniforme de recursos (URL, *uniform resource locator*)], verifica la solicitud y, si ésta es válida, verifica el estado del FW mediante comunicación con el consumidor de FW para confirmar la necesidad de esa actualización. En la cláusula 9 se enumeran algunas de las formas comunes de envío de solicitudes.

Una vez verificada la necesidad de actualizar el FW, el consumidor de FW inicia la actualización comunicando la localización del FW disponible. A continuación, el consumidor de FW solicita la imagen de FW actualizada al servidor de FW. El servidor de FW proporciona la imagen de FW al consumidor de FW siempre y cuando éste esté legitimado para recibir la actualización. En caso contrario, el servidor envía un mensaje de actualización con un código de error.

Al recibir el mensaje de actualización, el consumidor de FW verifica la imagen. De no encontrarse errores, el consumidor de FW instala el FW y envía la información de estado al rastreador de estado. Téngase en cuenta que las cardinalidades de las cuatro entidades funcionales citadas son muchas a muchas, es decir, que múltiples rastreadores de estado pueden comunicar con múltiples consumidores de FW, que pueden comunicarse con múltiples servidores de FW, que puede comunicarse con múltiples autores.

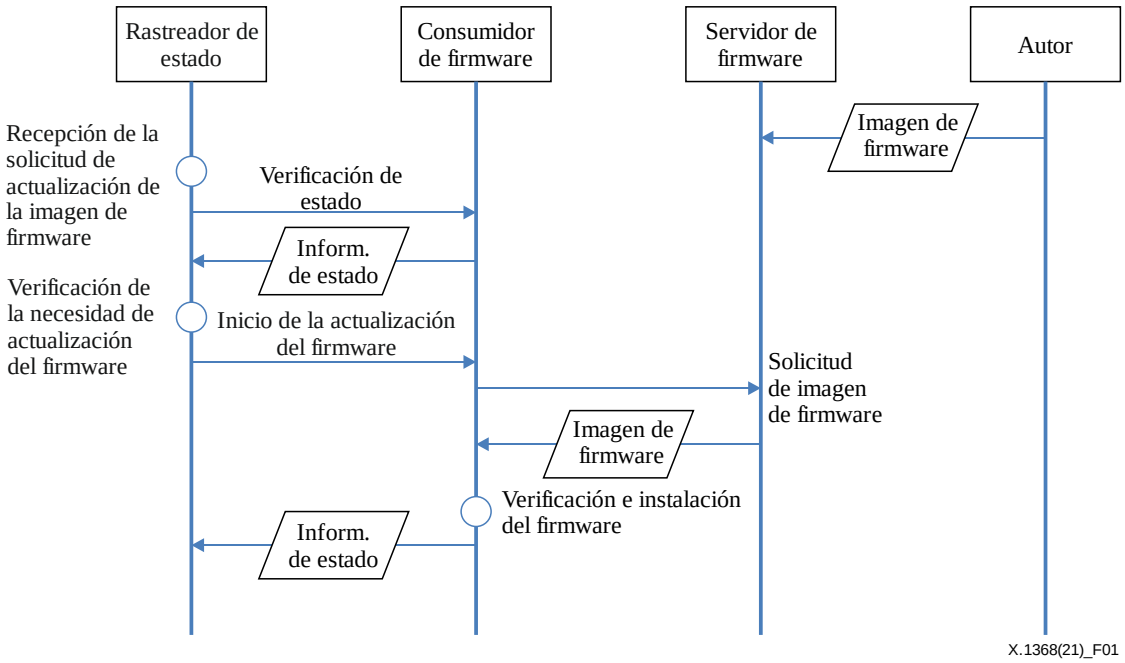

Figura 1 – Procedimiento protocolo

8 Configuraciones de despliegue

Como se menciona en la cláusula 6, múltiples entidades funcionales pueden residir en un nodo y múltiples entidades pueden actuar como una entidad funcional. Las configuraciones de despliegue pueden variar en función de cada caso. En esta cláusula se ilustran distintas configuraciones de despliegue.

8.1 Entidades funcionales dentro de los dispositivos de IoT

En la Figura 2 se muestran cuatro tipos de dispositivos de IoT. Un dispositivo de IoT contendrá, al menos, un consumidor de FW, pues es natural que un dispositivo de IoT contenga múltiples imágenes de FW.

Un dispositivo de IoT contendrá, al menos, un rastreador de estado. Puede contener múltiples rastreadores de estado para manejar múltiples consumidores de FW, pero también puede haber un sólo rastreador de estado que maneje todos los consumidores de FW.

Un dispositivo de IoT con limitaciones de recursos puede optar por minimizar la funcionalidad del rastreador de estado. En tal caso, la funcionalidad de rastreador de estado se divide en un módulo cliente y un módulo servidor, desplegado fuera del dispositivo de IoT. La funcionalidad mínima, por ejemplo, la interacción con un consumidor de FW, se deja en el lado cliente, mientras que las demás funcionalidades se exportan al lado servidor. Un módulo servidor puede ocuparse de múltiples módulos cliente y éste suele ser la configuración de despliegue preferida.

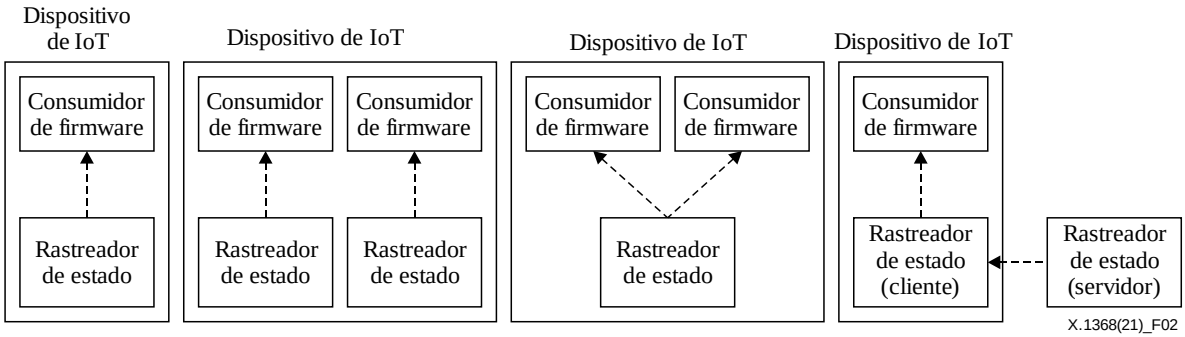

Figura 2 – Distintos tipos de dispositivos de IoT

8.2 Configuraciones de despliegue del rastreador de estado

Los recursos de los dispositivos de IoT pueden ser muy diferentes. Un rastreador de estado puede residir en un dispositivo de IoT, pero los dispositivos de IoT con limitación de recursos pueden optar por un rastreador aparte y minimizar su consumo de recursos. Además, puede ocurrir que se prefiera, por comodidad, gestionar los dispositivos de IoT con una entidad centralizada.

Para dar cabida a todas esas opciones, se puede dividir el rastreador de estado en varios módulos e implementarlos de manera jerárquica. En ese caso, se pueden poner en cascada varios módulos para que un módulo superior pueda juzgar la necesidad de actualizar el FW e iniciar el procedimiento conexo a través de los módulos inferiores.

En las cláusulas 8.2.1 a 8.2.3 se analizan casos en los que: (1) un rastreador de estado dentro de un dispositivo de IoT se comunica directamente con un servidor de FW; (2) un rastreador de estado dentro de un dispositivo de IoT se comunica directamente con un servidor de FW a través de otro rastreador de estado que resida en la Intranet; y (3) un rastreador de estado dentro de un dispositivo de IoT se comunica con un servidor de FW a través de múltiples rastreadores de estado.

8.2.1 Modelo de rastreador de estado dentro del dispositivo

En la Figura 3 se muestra el modelo de rastreador dentro del dispositivo, donde dentro del dispositivo IoT residen un consumidor de FW y un rastreador de estado. Cuando el rastreador de estado detecta la necesidad de actualizar el FW (véase la cláusula 9),, pide al consumidor de FW que reciba las imágenes de FW del servidor FW. Téngase en cuenta que en esta cláusula se omiten los canales de comunicación, pero que la conexión puede hacerse a través de Internet, de otros protocolos, o de una combinación de protocolos que exija la existencia de puentes de comunicación entre entidades. En la Figura 3 se muestra Internet, pero las técnicas indicadas en esta Recomendación pueden aplicarse a todo tipo de redes.

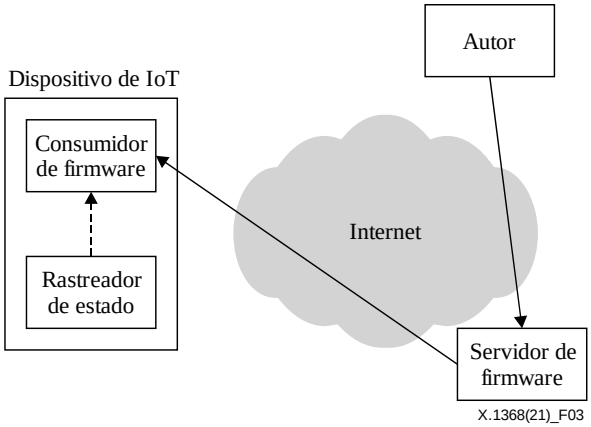

Figura 1 – Ilustración del modelo de rastreador de estado dentro del dispositivo

8.2.2 Modelo de rastreador de estado cliente-servidor

En la Figura 4 se muestra el modelo de rastreador de estado cliente-servidor. En este modelo, el rastreador de estado se divide en un módulo cliente y un módulo servidor. El módulo cliente reside en los dispositivos IoT, mientras que el módulo servidor reside en una red. El módulo servidor supervisa varios dispositivos de IoT comunicándose con los módulos cliente. Los módulos cliente simplemente verifican el mensaje del módulo servidor y actúan en consecuencia. El módulo servidor inicia el procedimiento de actualización del FW.

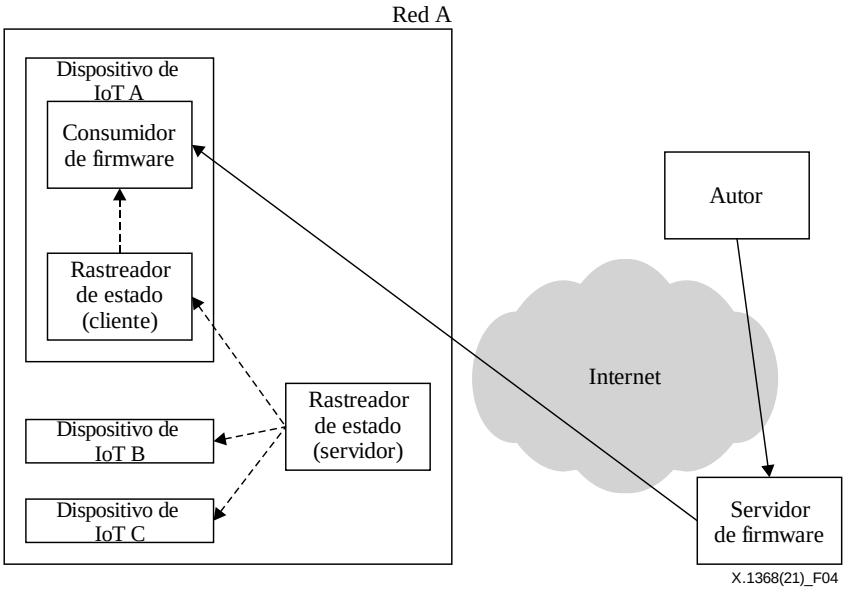

Figura 4 – Ilustración del modelo de rastreador de estado cliente-servidor

8.2.3 Modelo de rastreador de estado jerárquico

En la Figura 5 se muestra el modelo de rastreador de estado jerárquico. En este modelo el rastreador de estado se divide en varios módulos: módulo cliente, módulos intermedios y módulo servidor. El módulo cliente reside en los dispositivos de IoT, el módulo servidor y los módulos intermedios residen en las redes. Los módulos intermedios supervisan varios dispositivos IoT y, mediante comunicación con los módulos cliente, el módulo servidor supervisa todos los módulos cliente comunicándose con los módulos intermedios. Téngase en cuenta que es posible poner los módulos intermedios en cascada para generar una jerarquía más definida. Los módulos cliente simplemente verifican el mensaje del módulo servidor y actúan en consecuencia. El módulo servidor inicia el procedimiento de actualización del FW. El módulo servidor inicia el procedimiento de actualización del FW.

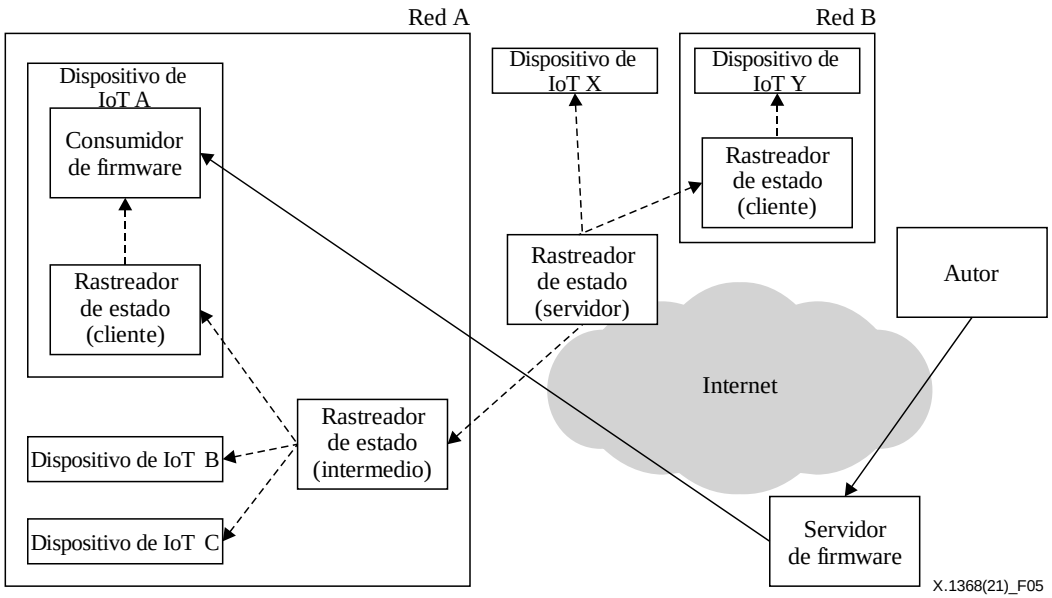

Figura 5 – Ilustración del modelo de rastreador de estado jerárquico

9 Descubrimiento de nuevas imágenes de firmware disponibles e inicio del procedimiento

El rastreador de estado inicia todo el proceso al recibir una solicitud de actualización de la imagen de FW. Este tipo de solicitud puede adoptar distintas formas:

a) un autor que publica nuevas versiones de imágenes de FW puede enviar la solicitud;

b) un servidor de FW que recibe una nueva versión de una imagen de FW puede enviar la solicitud;

c) un administrador de dispositivo de IoT reconoce la publicación de una nueva versión de imágenes de FW y puede enviar la solicitud;

d) un rastreador de estado o uno de sus rastreadores de estado superiores descubre la nueva versión de las imágenes de FW sondeando periódicamente el servidor de FW;

e) un rastreador de estado o uno de sus rastreadores de estado superiores reconoce la existencia de una nueva versión de una imagen de FW observando el procedimiento de actualización de FW de otro dispositivo de IoT del que se ocupa.

Diversos otros eventos pueden dar lugar a la solicitud, pero ésta debe dar información sobre el URL de las imágenes de FW o sus versiones al rastreador de estado. Si el rastreador de estado considera que la información es fiable y fidedigna, puede iniciar el procedimiento indicado en la cláusula 7.

10 Requisitos

En esta cláusula se enumeran los requisitos funcionales para la actualización de SW de IoT. Por motivos de limitación de recursos, es posible que no todos los procedimientos de actualización de SW sean aplicables en un entorno ilimitado. Suele pasar que no haya un usuario u operador humano cerca de los dispositivos de IoT, por lo que, al diseñar el procedimiento de actualización segura concreto, se han de tener en cuenta esas diferencias. Téngase en cuenta que se ha de preservar la confidencialidad, integridad y disponibilidad de las cuatro entidades funcionales como requisitos *sine qua non* para la actualización del SW, motivo por el que se omiten en la lista siguiente.

a) No se distribuirá SW/FW maligno:

   i) se han de identificar las imágenes malignas antes de cargarlas o intercambiarlas;

   ii) deberá poderse verificar la integridad de las imágenes de FW;

iii) deberá poder verificarse el proveedor de las imágenes de FW.

b) No se dejarán SW/FW vulnerables sin las medidas adecuadas:

i) deben detectarse las versiones obsoletas del SW/FW;

ii) debe detectarse el SW/FW vulnerable.

c) Deberán poderse recuperar los fallos causados durante el proceso de actualización:

i) si falla la actualización de un SW/FW, debe haber un medio para notificar la situación;

ii) debe haber un medio de restitución o un medio de protección en caso de fallo del proceso de actualización.

d) Sólo se procederá a la actualización deseada y necesaria:

i) sólo deberán poder instalarse las versiones del SW/FW de IoT más recientes;

ii) sólo deberán poder instalarse imágenes de SW/FW de IoT fiables.

e) Deberán tenerse en cuenta las limitaciones de recursos:

i) no se procederá a la actualización si no es necesaria para minimizar recursos de red;

ii) las funciones del rastreador de estado pueden ponerse en cascada para minimizar la carga en dispositivos de IoT con limitación de recursos.

f) Deberán preservarse los derechos de propiedad intelectual de los autores:

i) las imágenes de SW/FW deberán estar encriptadas por los autores;

ii) deberán preservarse la confidencialidad, integridad y disponibilidad de las imágenes de SW/FW de IoT;

iii) las imágenes de SW/FW deberán transferirse de forma segura desde el autor hasta el destino final.

11 Capacidades

De acuerdo con los requisitos indicados en la cláusula 10, en esta cláusula se enumeran las capacidades de las entidades funcionales.

11.1 Capacidades del consumidor de firmware

a) Un consumidor de FW debe poder:

i) verificar si la anterior actualización del FW se llevó a cabo satisfactoriamente;

ii) compartir información sobre sus imágenes de SW/FW vigentes (por ejemplo, número de versión) con las partes que soliciten esa información y estén legitimadas para hacerlo;

iii) implementar un medio de restitución o un medio de protección en caso de fallo del proceso de actualización;

iv) notificar al rastreador de estado la necesidad de actualizar el FW;

v) confirmar la autenticidad e integridad de las imágenes de FW verificando sus certificados por sí mismo o recurriendo a otros medios (véase la delegación del proceso de verificación en otras entidades);

vi) optar por no instalar las nuevas versiones de imágenes de SW/FW.

b) Se recomienda que el consumidor de FW pueda ejecutarse en un "modo seguro" en el dispositivo de IoT con una funcionalidad mínima y que, al menos, ofrezca un medio para instalar, restaurar o actualizar FW manualmente.

11.2 Capacidades del rastreador de estado

Un rastreador de estado debe poder:

a) mantener listas de consumidores de FW, aquellos con imágenes de FW actualizadas y aquellos con imágenes obsoletas:
   i) esas listas deben contener, como mínimo, sus identificadores exclusivos,
   ii) un rastreador de estado debe poder identificar los consumidores de FW con FW obsoleto;

b) conocer el estado de los consumidores de FW que administra y disponer de medios para:
   i) confirmar si el consumidor de FW (y el dispositivo de IoT que contiene ese consumidor de FW) está activo mediante la comunicación con el consumidor de FW y mediante verificación de los registros de comunicación con el consumidor de FW,
   ii) confirmar si la anterior actualización del FW de un consumidor de FW se llevó a cabo satisfactoriamente,
   iii) conocer las versiones del FW que ejecuta el consumidor de FW;

c) juzgar si es necesario actualizar el SW/FW e iniciar un procedimiento de actualización del FW cuando sea necesario;

d) verificar la autenticidad de un rastreador de estado superior cuando se implemente de manera jerárquica.

Cuando la funcionalidad de un rastreador de estado se divida en más de un módulo, cada módulo deberá poder:

a) mantener la confidencialidad e integridad de las comunicaciones entre ellos;

b) verificar la autenticidad de las señales enviadas entre ellos;

c) mantener su información de accesibilidad.

11.3 Capacidades del servidor de firmware

Un servidor de FW debe poder:

a) aceptar la presentación de imágenes de SW/FW de IoT de los autores;

b) facilitar las imágenes de SW/FW que contiene a los consumidores de FW;

c) identificar imágenes de SW/FW malignas y tomar las medidas convenientes, como eliminarlas de su almacén interno y prohibir las presentaciones de autores que han presentado esas imágenes;

d) gestionar la lista de autores y de consumidores de FW que lo utilizan;

e) gestionar las versiones de las imágenes de SW/FW de IoT;

f) mantener la lista de consumidores de FW y de las imágenes de SW/FW que han descargado en el pasado;

g) notificar a los dispositivos de IoT la disponibilidad de nuevas versiones de las imágenes de SW/FW de IoT que descargaron en el pasado y han quedado obsoletas;

h) verificar el emplazamiento geográfico o lógico de los dispositivos de IoT y permitirles o denegarles la descarga de imágenes de SW/FW para evitar su distribución en emplazamientos prohibidos por políticas u otros medios.

11.4 Capacidades del autor

Un autor debe poder mantener la autenticidad, la confidencialidad y la integridad de las imágenes de FW que produce.

a) El FW no debe ser sustituido o puesto en peligro por terceros (autenticidad e integridad).

b) Debe preservarse la propiedad intelectual de los fabricantes en el FW (confidencialidad).

c) Un autor debe aplicar medidas de seguridad para proteger la imagen de FW que carga en servidores de FW, pues éstos no han de ser necesariamente fiables.

Apéndice I

Actividades conexas fuera del UIT-T

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

Entre las actividades relacionadas con la actualización de SW de IoT que se llevan a cabo fuera del UIT-T pueden citarse las siguientes:

1) Taller IOTSU [b-ISOC IoTSU].

2) Grupo de Trabajo SUIT del IETF [b-IETF suit]:
   - sobre el archivo manifiesto [b-IETF manifest],
   - sobre la arquitectura de actualización de FW [b-IETF architecture];

3) oneM2M: Normas sobre M2M e IoT [b-oneM2M], etc.

Apéndice II

Ejemplo de actualización de software de IoT con tecnología de libro mayor distribuido

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

II.1 Aspectos generales

La infraestructura de IoT contiene numerosos dispositivos que ha de gestionar un administrador. Un dispositivo de IoT puede ser objeto de diversas revisiones, en función de las características del hardware, y también pueden aplicarse distintos FW de acuerdo con la placa de sensores adicional. Además, en función del hardware, pueden ser distintas las versiones del SW soportadas. Del mismo modo, las diferencias entre los lotes de SW instalados pueden crear problemas de dependencia, que se pueden solventar con tecnología de libro mayor distribuido (DLT).

La DLT dispone de un contrato inteligente que permite la actualización del FW o SW de hardware en función de los contratos preestablecidos por el administrador. Además, las soluciones a las vulnerabilidades de seguridad que pueden surgir durante el proceso de actualización pueden basarse en algoritmos de consenso y en la capa criptográfica.

En este ejemplo se muestra cómo proceder a la actualización de FW/SW segura con DLT en entornos con distintas revisiones de hardware y distintas versiones de SW, como puede ser la infraestructura de IoT.

II.2 Procedimiento de actualización de software

Véase el Cuadro II.1 y las Figuras II.1 y II.2.

Cuadro II.1 – Estructura de bloques para la actualización de SW

Encabezamiento de bloque	– Tamaño de bloque, versión – Aleatorización de encabezamiento de bloque previa
Datos de bloque	– Raíz Merkle – Nombre del proveedor, hora de publicación, número de versión, código de aleatorización del archivo, enlace del archivo, nombre del archivo, tamaño del archivo, hardware soportado, dependencia de SW

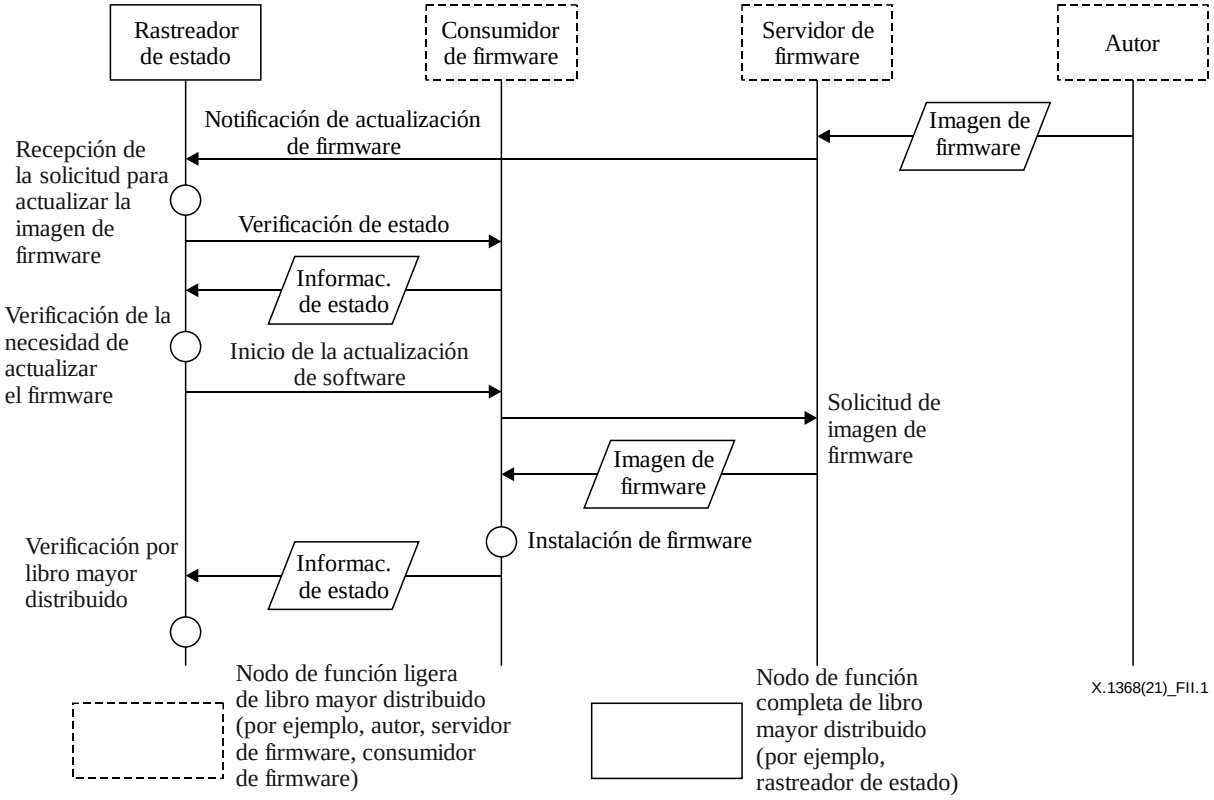

Figura II.1 – Procedimiento de actualización de software basada en la tecnología de libro mayor distribuido

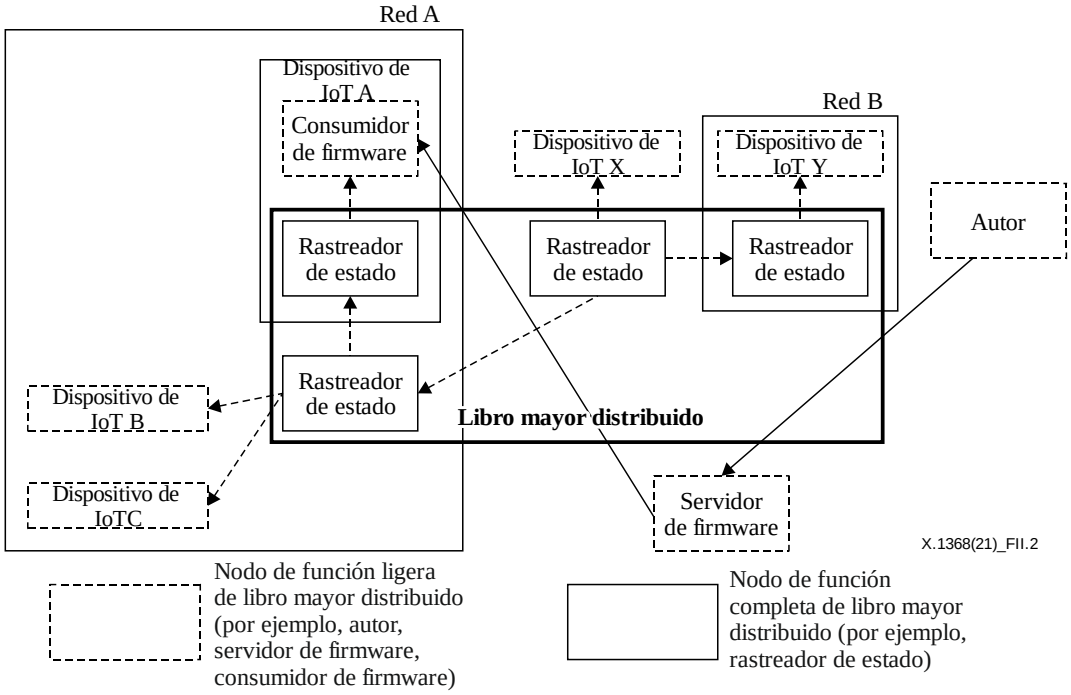

Figura II.2 – Actualización de software basada en la tecnología de libro mayor distribuido para múltiples redes

Bibliografía

[b-IETF RFC 2119] IETF RFC 2119 (1997), *Key words for use in RFCs to indicate requirement levels.*

[b-IETF architecture] IETF SUIT (2019), *A firmware update architecture for Internet of things.*, Wilmington, DE: Internet Engineering Task Force. Disponible en: https://tools.ietf.org/html/draft-ietf-suit-architecture-08 [consultado el 19-02-2021]

[b-IETF manifest] Moran, B., Tschofenig, H., Birkholz, H. (2019), *Firmware updates for Internet of things devices – An information model for manifests.* Wilmington, DE: Internet Engineering Task Force. Disponible en: https://tools.ietf.org/id/draft-ietf-suit-information-model-02.html [consultado el 19-02-2021]

[b-IETF suit] IETF (2021), *Software updates for the internet of things (suit)*, version 7.26.0. Wilmington, DE: Internet Engineering Task Force. Disponible en: https://datatracker.ietf.org/wg/suit/about/ [consultado el 19-02-2021]

[b-ISOC iotsu] Internet Architecture Board (Internet), *Internet of things software update workshop (IoTSU) 2016*. Reston, VA: Internet Society. Disponible en: https://www.iab.org/activities/workshops/iotsu/ [consultado el 20-02-2021]

[b-oneM2M] oneM2M (2017), *Standards for M2M and the Internet of things*. oneM2M. Disponible en: http://www.onem2m.org/technical/published-drafts [consultado el 20-02-2021]

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