Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1332

(03/2020)

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

Aplicaciones y servicios seguros (2) – Seguridad de los sistemas de transporte inteligentes (STI)

Directrices de seguridad para servicios de medición inteligentes en redes inteligentes

Recomendación UIT-T X.1332

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 aleatorios 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.1332

Directrices de seguridad para servicios de medición inteligentes en redes inteligentes

Resumen

El amplio despliegue mundial de servicios de medición inteligentes tiene como objetivo aumentar la eficacia y fiabilidad de las redes eléctricas mediante la recopilación de datos sobre el consumo eléctrico y su posterior distribución a los consumidores. Esta información permite obtener un cálculo de la demanda de electricidad de los consumidores, el cual puede utilizarse para impulsar desplazamientos de esa demanda o puede distribuirse a los usuarios para, junto con la información sobre el consumo eléctrico, modificar los patrones de consumo eléctrico de los clientes. Sin embargo, los servicios de medición inteligentes pueden presentar disfunciones en respuesta a diversas amenazas; por ejemplo, la información de medición no válida puede dar como resultado decisiones de gestión de la demanda erróneas y el uso excesivo de las funciones de control de la carga puede provocar daños físicos y económicos en los clientes. En la Recomendación UIT-T X.1332 se establecen directrices de seguridad para los servicios de medición inteligentes a fin de que los proveedores de servicios puedan poner en marcha medidas de seguridad adecuadas que garanticen la seguridad del servicio; se identifican las amenazas a la seguridad de los servicios de medición inteligentes y los métodos de ataque contra dichos servicios, y se especifican los requisitos y las capacidades en materia de seguridad para mitigar esas amenazas y ataques.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1332	26-03-2020	17	11.1002/1000/14086

Palabras clave

Infraestructura de medición avanzada, directrices de seguridad, red inteligente, servicio de medición inteligente.

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

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1332

Directrices de seguridad para servicios de medición inteligentes en redes inteligentes

1 Alcance

En la presente Recomendación se describen las directrices de seguridad para servicios de medición inteligentes en redes inteligentes. Se tratan los temas siguientes:

– determinación de las amenazas a la seguridad y los ataques contra servicios de medición inteligente;

– requisitos de seguridad de los servicios de medición inteligente; y

– directrices de seguridad de los servicios de medición inteligente en cumplimiento de los requisitos de seguridad.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

La presente Recomendación utiliza los términos siguientes definidos en otros documentos:

3.1.1 respuesta a la demanda (DR) [b-UIT-T Y.2071]: Característica de las redes inteligentes que permite que los consumidores reduzcan o alteren sus patrones de consumo eléctrico durante los picos de demanda, normalmente a cambio de un incentivo económico. La respuesta a la demanda proporciona mecanismos e incentivos para que los proveedores de servicios públicos, las empresas, las industrias y los clientes particulares abonados disminuyan el consumo eléctrico durante los picos de demanda o en situaciones de riesgo de la fiabilidad del suministro eléctrico. La respuesta a la demanda es necesaria para optimizar el equilibrio entre oferta y demanda de electricidad.

3.1.2 operador del sistema de energía eléctrica [b-CEI 60050-617]: Agente responsable del funcionamiento seguro y fiable de una parte del sistema de energía eléctrica en una zona concreta y de la conexión con otras partes del sistema de energía eléctrica.

3.1.3 sistema de gestión de energía (EMS) [b-UIT-T Y.2071]: Sistema informático formado por una plataforma *software* que ofrece servicios de soporte básicos y un conjunto de aplicaciones con la funcionalidad necesaria para utilizar con eficacia las instalaciones de generación y transmisión de electricidad, a fin de garantizar una seguridad adecuada del suministro eléctrico a un coste mínimo.

3.1.4 contador inteligente [b-UIT-T X.1331]: Dispositivo instalado en los locales para supervisar y controlar el consumo eléctrico de los dispositivos domésticos inteligentes basado en su información de respuesta a la demanda.

3.2 Términos definidos en la presente Recomendación

Esta Recomendación define los términos siguientes:

3.2.1 concentrador de datos: Dispositivo intermedio ubicado entre un contador inteligente y los sistemas de servicios públicos cuyo objetivo principal es recopilar y gestionar los datos recibidos del contador inteligente.

3.2.2 sistema de gestión de datos de medición (MDMS): Un sistema de gestión de datos de medición (MDMS) agrega, valida, calcula y permite editar datos de contadores, por ejemplo, del consumo y la generación de electricidad. Un MDMS almacena estos datos durante un plazo determinado antes de enviarlos a un almacén de datos y los pone a disposición de los sistemas autorizados.

NOTA – Adaptado de [b-UIT-T Y.2071]

3.2.3 servicio de medición inteligente: Servicio que recopila datos sobre el consumo eléctrico a través de contadores inteligentes y proporciona información analizada a los clientes y los servicios públicos. Los proveedores de servicios terceros que deseen utilizar datos sobre el consumo eléctrico para prestar un servicio o un conjunto de servicios a un cliente también pueden participar en este servicio.

4 Abreviaturas y acrónimos

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

CDMA Acceso múltiple por división de código (*code-division multiple access*)

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

DoS Denegación de servicio (*denial of service*)

EMS Sistema de gestión de la energía (*energy management system*)

EUIS Sistema de información sobre consumo eléctrico (*energy usage information system*)

HMAC Código de autentificación de mensajes basado en número generador (*hash-based message authentication code*)

IHD Pantalla doméstica (*in-home display*)

IIP Información de identificación personal

LTE Evolución a largo plazo (*long-term evolution*)

MDMS Sistema de gestión de datos de medición (*meter data management system*)

PLC Comunicación por la línea eléctrica (*power line communication*)

QoS Calidad de servicio (*quality of service*)

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

VPN Red privada virtual (*virtual private network*)

5 Convenios

Ninguno.

6 Resumen

El amplio despliegue mundial de servicios de medición inteligentes, que constituyen una de las características fundamentales de las redes inteligentes, tiene como objetivo aumentar la eficacia y fiabilidad de las redes eléctricas mediante la recopilación de datos sobre el consumo eléctrico y su posterior distribución a los consumidores.

Un contador inteligente mide, registra y comunica la cantidad de electricidad que ha utilizado un cliente. Los datos de las mediciones se transmiten de manera periódica, por ejemplo, cada 5 o 15 minutos. Los proveedores de servicios de medición inteligentes utilizan esta información para calcular la demanda de electricidad de los clientes y, sobre la base de esta estimación, reorientar la

demanda o modificar los patrones de consumo eléctrico de los usuarios a fin de aumentar la fiabilidad de la red eléctrica.

Los proveedores de servicios de medición inteligentes pueden facilitar a los clientes información sobre su consumo eléctrico, además de tarifas de la electricidad en tiempo real, facturas estimadas, datos estadísticos o tendencias de la demanda. Con estos datos, los consumidores pueden intentar reducir voluntariamente su consumo eléctrico. Por ejemplo, si el proveedor aplica la tarificación dinámica y cambia el precio de acuerdo con la demanda de electricidad, los usuarios pueden adelantar o posponer las actividades que consumen electricidad.

Sin embargo, existen amenazas que pueden provocar disfunciones en las redes inteligentes. Por ejemplo, la información de medición no válida puede dar como resultado decisiones de gestión de la demanda erróneas y el uso excesivo de las funciones de control de la carga puede provocar daños físicos y económicos en los clientes. Además, es importante tener en cuenta la protección de la información de identificación personal (IIP) cuando los proveedores de servicios terceros tienen acceso a la información de medición.

Asimismo, la información sobre consumo eléctrico, las estadísticas y la información sobre las tarifas se transmiten normalmente a dispositivos de los clientes conectados a internet, como teléfonos inteligentes u ordenadores de bolsillo. Por tanto, casi todas las amenazas que pueden afectar a los dispositivos móviles podrían afectar también a los servicios de medición inteligentes.

En esta Recomendación se investigan las amenazas a la seguridad de los servicios de medición inteligentes y se especifican los requisitos y las funcionalidades en materia de seguridad para garantizar la seguridad de los servicios de medición inteligentes.

7 Arquitectura de los servicios de medición inteligentes

Para poder describir la seguridad de los servicios de medición inteligentes, es importante definir previamente una arquitectura que identifique a todas las entidades relacionadas con el servicio de medición inteligente y aclarar sus relaciones.

Con miras a establecer una definición de un modelo general de servicio de medición, en esta Recomendación se consideran los casos de uso siguientes:

– recopilación de datos sobre el consumo eléctrico recogidos por dispositivos de medición;
– comunicación de las tendencias de consumo eléctrico a los consumidores;
– comunicación de la información sobre consumo eléctrico a los proveedores de servicios terceros; y
– comunicación de la información sobre consumo eléctrico a los operadores de sistemas de energía eléctrica.

En la Figura 7-1 se muestra un modelo de arquitectura de servicio de medición inteligente para estos casos de uso, con seis entidades principales: dispositivo de medición, operador del sistema de energía eléctrica, sistema de gestión de datos de medición (MDMS), servicio público (sistema), proveedor de servicios tercero y cliente.

El dispositivo de medición mide el consumo eléctrico del cliente y envía los datos al MDMS de un servicio público. Dicho servicio transmite los datos a un sistema de información sobre consumo eléctrico (EUIS), que presenta las tendencias de consumo eléctrico a los usuarios. Para generar la información estadística, el EUIS toma los datos de medición del MDMS. El sistema de facturación del servicio público también utiliza datos de medición. En esta arquitectura, el EUIS y el sistema de facturación se clasifican como sistemas de servicios públicos.

El operador del sistema de energía eléctrica utiliza los datos de medición para calcular la situación actual y futura del sistema de energía. El sistema de gestión de la energía (EMS) del operador recibe los datos de medición del MDMS, analiza las tendencias de la demanda de electricidad y, basándose en los resultados de este ejercicio, ajusta la cantidad de suministro eléctrico para que el sistema de energía pueda equilibrar la oferta y la demanda.

El cliente dispone de visualizadores de energía inteligentes o dispositivos inteligentes que muestran las estadísticas del consumo energético y controlan las cargas conectadas con las redes de las instalaciones de las que forman parte. Existen diferentes tipos de dispositivos, como teléfonos inteligentes, tabletas, TV inteligentes, ordenadores personales y pantallas domésticas (IHD) especializadas para acceder el EUIS del servicio público.

El proveedor de servicios tercero utiliza los datos de medición para mejorar la calidad del servicio. Por ejemplo, si una distribuidora de televisión por cable sabe que uno de sus clientes está haciendo la colada, puede emitir un anuncio comercial de un detergente específicamente para ese cliente.

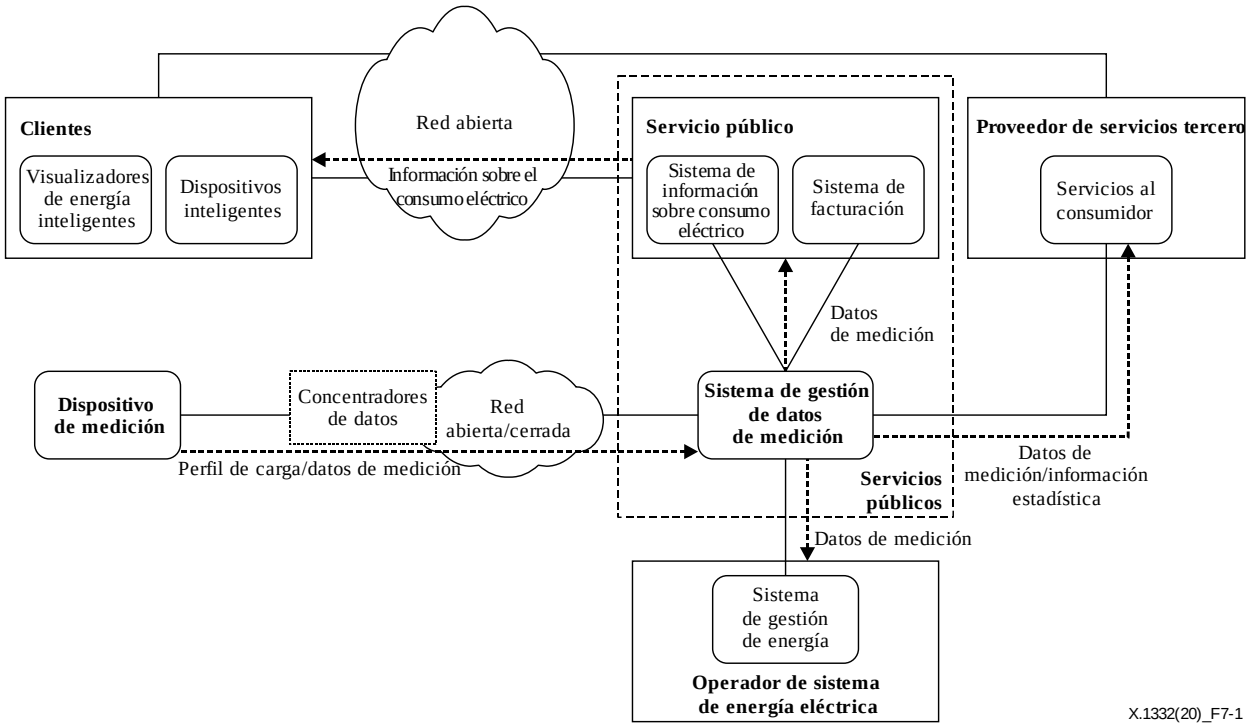

Figura 7-1 – Arquitectura del servicio de medición inteligente

En este modelo arquitectónico se contemplan seis relaciones entre entidades: dispositivo de medición y MDMS, MDMS y EMS, MDMS y sistema de servicios públicos, MDMS y proveedor de servicios terceros, cliente y sistema de servicios públicos, y cliente y proveedor de servicios terceros.

El dispositivo de medición se conecta al MDMS a través de una red, que puede ser abierta (por ejemplo, LTE o CDMA) o cerrada (por ejemplo, PLC o línea alquilada). Los concentradores de datos agregarán los datos de medición de una zona y los enviarán al MDMS, independientemente del tipo de red de que se trate.

El MDMS y el EMS se comunican entre sí a través de una red de telecomunicaciones con calidad de servicio (QoS) garantizada.

El MDMS y el sistema de servicios públicos suelen estar ubicados en la misma red. Si no están conectados en la misma red, normalmente se conectan con una red de telecomunicaciones con QoS garantizada.

El MDMS puede conectarse con proveedores de servicios terceros a través de una red de telecomunicaciones con QoS garantizada.

Dado que los clientes utilizan una red abierta, por ejemplo, Internet, tanto el sistema de servicios públicos como el proveedor de servicios tercero se conectan con el cliente a través de esa red abierta. Los clientes pueden acceder a las redes por Wi-Fi, LTE, Bluetooth, etc.

8 Amenazas a la seguridad en los servicios de medición inteligentes

8.1 Amenazas a la interfaz entre el dispositivo de medición y el MDMS

La interfaz entre el dispositivo de medición y el MDMS permite recopilar y procesar grandes volúmenes de información sobre el consumo eléctrico de los clientes, como datos de medición, perfiles de carga y mediciones de calidad de la electricidad, que constituyen el objetivo principal de los ataques. Los atacantes interceptan, falsifican y sustituyen los datos que se transmiten a través de esta interfaz y, en consecuencia, causan daños en los servicios de medición inteligentes.

Otro objetivo posible es la denegación de los servicios de medición inteligentes: los atacantes lanzan ataques de denegación de servicio distribuida (DDoS) contra el MDMS.

La interfaz entre el dispositivo de medición y el MDMS es vulnerable a las amenazas siguientes:

– Fuga de información: Los dispositivos de medición inteligentes, como el contador inteligente, envían periódicamente datos sobre la carga eléctrica (datos de medición) al MDMS a través de un concentrador de datos. En las redes inteligentes, la periodicidad de este proceso es mínima, por ejemplo, 5 minutos o menos. Por consiguiente, los atacantes pueden averiguar los hábitos de los clientes rebuscando en los datos de medición.

– Falsificación de datos de medición: Los atacantes pueden bloquear los datos de medición reales y enviar datos falsificados al MDMS. Al impedir que el MDMS y el EMS accedan a los datos de medición reales recopilados, pueden producirse fallos en la estimación de la demanda y puede desequilibrarse la oferta y la demanda y, por tanto, el suministro eléctrico puede llegar a interrumpirse.

– Falsificación de perfil de carga: Los atacantes pueden realizar modificaciones no autorizadas en el perfil de carga almacenado en los dispositivos de medición. Habida cuenta de que el sistema de facturación cobra a los clientes de acuerdo con su perfil de carga, esta amenaza podría provocar errores en la facturación de los usuarios.

– Denegación de servicio (DoS): Los atacantes pueden realizar un ataque de DoS para ejecutar código maligno en varios dispositivos de medición o concentradores de datos e inundar un objetivo (normalmente un MDMS) con grandes cantidades de datos o peticiones de servicio. Este ataque puede ralentizar o incluso detener un dispositivo de medición.

8.2 Amenazas a la interfaz entre el MDMS y el proveedor de servicios tercero

La interfaz entre el MDMS y el proveedor de servicios tercero permite compartir los datos de medición y posibilita la prestación de múltiples servicios personalizados del proveedor a cada cliente. Dado que la IIP se puede transmitir a través de esta interfaz, los atacantes se centran principalmente en estos datos, que interceptan y utilizan, causando daños en los servicios de medición inteligentes.

La interfaz entre el MDMS y el proveedor de servicios tercero es vulnerable a las amenazas siguientes:

– Fugas de IIP: Los atacantes pueden interceptar la IIP mediante un ataque de rastreo de paquetes o la ejecución de código maligno en sistemas del proveedor de servicios tercero conectados a Internet.

8.3 Amenazas a la interfaz entre el sistema de servicios públicos y el cliente

La interfaz entre el sistema de servicios públicos y el dispositivo ubicado en las instalaciones del cliente ofrece informaciones variadas que animan a los usuarios a participar en la respuesta a la demanda, por ejemplo, datos sobre las tendencias de consumo eléctrico del cliente, tarifas de la electricidad en tiempo real, tendencias de la demanda, facturas y datos estadísticos. Al falsificar la información transmitida, los atacantes pueden engañar a un cliente para que consuma demasiada electricidad. El ataque de DoS es otra amenaza grave contra el sistema de servicios públicos que está conectado con los dispositivos ubicados en las instalaciones del usuario.

La interfaz entre el sistema de servicios públicos y el dispositivo del cliente es vulnerable a las amenazas siguientes:

– Falsificación de la tarifa en tiempo real: Los atacantes pueden falsificar la tarifa en tiempo real comunicada a los clientes para engañarlos. Si la tarifa falsificada es menor que la real, los dispositivos de los clientes (como el visualizador de energía inteligente) pueden hacer aumentar el consumo de un dispositivo eléctrico (por ejemplo, vehículo eléctrico). En cambio, si la tarifa falsificada es mayor que la real, el cliente puede perder la oportunidad de almacenar electricidad con un coste más bajo.

– Denegación de servicio: Los atacantes pueden realizar un ataque de DoS para ejecutar código maligno en varios dispositivos de cliente e inundar un objetivo (normalmente un EUIS) con cantidades ingentes de peticiones de servicio. Este ataque podría ralentizar o incluso detener un servicio de medición inteligente.

– Fugas de IIP: Un atacante puede interceptar la IIP mediante un ataque de rastreo de paquetes o la ejecución de código maligno en un dispositivo del cliente conectado a Internet.

9 Requisitos de seguridad de los servicios de medición inteligentes

9.1 Requisitos de seguridad para la medición del consumo eléctrico

La medición del consumo eléctrico es la funcionalidad más importante de los servicios de medición inteligentes. Cuando funciona debidamente, el MDMS puede recopilar la información necesaria para elaborar tendencias del consumo eléctrico, el patrón de consumo individual de los clientes, facturas de electricidad, etc. Además, otras entidades del servicio de medición inteligente pueden utilizar esta información para desempeñar correctamente sus funciones. Por consiguiente, la integridad, la autenticidad y la confidencialidad de los datos de medición son los principales requisitos de seguridad del procedimiento de recopilación de datos.

Para responder adecuadamente a las amenazas contra la interfaz de comunicación entre el contador inteligente y el MDMS, hay que tener en cuenta los requisitos de seguridad siguientes.

– Se debe garantizar la confidencialidad de extremo a extremo de los datos transmitidos a través de la interfaz de comunicación entre un contador inteligente y el MDMS.

– Se debe garantizar la integridad de extremo a extremo de los mensajes de comunicación entre un contador inteligente y el MDMS para impedir la modificación no autorizada de los datos.

– Se deben proteger los datos de medición y la información de autenticación que se almacenan en los diferentes dispositivos, como contadores inteligentes, concentradores de datos y MDMS, frente a accesos no autorizados.

– Se debe garantizar la autenticidad del remitente en cada transacción de comunicación.

9.2 Requisitos de seguridad para la información utilizada por el cliente

Debido a su capacidad para acceder al sistema de servicios públicos conectado con el sistema interno de energía eléctrica, los dispositivos de cliente son el principal objetivo de los ataques contra los servicios de medición inteligentes. Por tanto, para garantizar la seguridad del servicio de medición inteligente, es necesario proteger los datos y las aplicaciones de los dispositivos de los clientes.

A fin de mitigar los posibles efectos colaterales de las amenazas contra la interfaz de comunicación entre el sistema de servicios públicos y el cliente, hay que tener en cuenta los requisitos de seguridad siguientes.

– Se debe garantizar la confidencialidad de los datos en la interfaz de comunicación entre el cliente y el sistema de servicios públicos.
– Se debe garantizar la integridad de los mensajes de comunicación entre el cliente y el sistema de servicios públicos para impedir la modificación no autorizada de los datos.
– Se debe garantizar la autenticidad del remitente en cada transacción de comunicación.
– Se debe proteger la información que se almacena en los dispositivos de los clientes y el sistema de servicios públicos frente a accesos no autorizados.
– Se debe tener en cuenta la integridad de las aplicaciones en los dispositivos de los clientes.

9.3 Requisitos de seguridad para la información utilizada por proveedores de servicios terceros

Los problemas principales en este ámbito son la manipulación de la IIP y las fugas de IIP durante la transmisión entre el proveedor de servicios tercero y el MDMS.

A fin de gestionar adecuadamente las amenazas contra la interfaz de comunicación entre el MDMS y el proveedor de servicios tercero, hay que tener en cuenta los requisitos de seguridad siguientes.

– Se debe garantizar la confidencialidad de los datos en la interfaz de comunicación entre el MDMS y el proveedor de servicios tercero.
– Se debe garantizar la integrar de los datos en los mensajes de comunicación entre el MDMS y el proveedor de servicios terceros para impedir la modificación no autorizada de los datos.
– Se debe garantizar la autenticidad del remitente en cada transacción de comunicación.
– Para proporcionar servicios personalizados, los datos de IIP deben gestionarse adecuadamente, únicamente conforme al propósito comunicado y con el consentimiento del cliente.
– En el caso de los servicios que no utilizan IIP, no se debe facilitar IIP relacionada con las mediciones.

9.4 Requisitos de seguridad para la información utilizada por el operador del sistema de energía eléctrica

Para prevenir adecuadamente las amenazas contra las interfaces de comunicación entre el MDMS y el operador del sistema de energía eléctrica, hay que tener en cuenta los requisitos de seguridad siguientes.

– Se debe garantizar la confidencialidad de los datos en la interfaz de comunicación entre el MDMS y el operador del sistema de energía eléctrica.
– Se debe garantizar la integridad de los mensajes de comunicación entre el MDMS y el operador del sistema de energía eléctrica para impedir la modificación no autorizada de los datos.
– Solo las entidades autorizadas deben tener permiso para acceder a la interfaz de comunicación entre el MDMS y el operador del sistema de energía eléctrica.

– No se debe facilitar IIP relacionada con la medición.

10 Directrices de seguridad para servicios de medición inteligentes

10.1 Controles de seguridad para los servicios de medición inteligentes

A fin de satisfacer los requisitos de seguridad aplicables a la medición del consumo eléctrico, todas las entidades de la medición de la electricidad deben incluir funcionalidades para los controles de seguridad siguientes.

– Se requieren control de acceso de los dispositivos de medición, los concentradores de datos y el MDMS a los datos de medición. Solo las entidades autorizadas tienen permiso para acceder a los datos sobre consumo eléctrico.
– A fin de garantizar la autenticidad del remitente, se debe utilizar un mecanismo de autenticación mutua entre el dispositivo de medición y el MDMS.
– Se deben adoptar medidas de autenticación de mensajes para proteger la integridad de los datos sobre el consumo eléctrico que se transmiten al MDMS, por ejemplo, el uso de códigos de autenticación de mensajes criptográficos como el HMAC.
– El cifrado de datos puede considerarse una medida de seguridad para proteger los datos relacionados con la facturación.
– La detección de los daños a la integridad de los datos y la descodificación de los datos encriptados deben ejecutarse en el MDMS.
– Para permitir la generación, la elección consensuada, el almacenamiento y la actualización de las claves criptográficas con seguridad, se debe adoptar un mecanismo de gestión segura de las claves en los dispositivos de medición, los concentradores de datos y el MDMS.
– Se debe utilizar un mecanismo de protección de datos para garantizar la confidencialidad e integridad de los datos de medición almacenados en el MDMS.
– Se pueden implantar en el MDMS medidas de seguridad para mitigar los ataques de DoS.

10.2 Controles de seguridad para la información utilizada por el cliente

A fin de satisfacer los requisitos de seguridad aplicables a la información utilizada por el cliente, todas las entidades deben incluir funcionalidades para los controles de seguridad siguientes.

– Se requieren medidas de comunicación segura, como TLS, para la comunicación entre el dispositivo del cliente y el sistema de servicios públicos. Se requiere autenticación mutua, autenticación de los datos de comunicación y cifrado entre el dispositivo del cliente y el sistema de servicios públicos.
– Se debe ejecutar autenticación y autorización del usuario para acceder a la información sobre el consumo eléctrico en las aplicaciones que proporcionan estos datos. El sistema de servicios públicos permitirá que los usuarios accedan solo a sus propios datos.
– Los datos de autenticación del usuario y las claves criptográficas para la autenticación del usuario y la comunicación segura, así como la IIP, deben almacenarse con seguridad en el dispositivo del cliente.
– Se deben poner en marcha medidas de comprobación de la integridad para detectar las falsificaciones de una aplicación cuando esta se ejecuta en el dispositivo del cliente.

10.3 Controles de seguridad para la información utilizada por el proveedor de servicios tercero

A fin de satisfacer los requisitos de seguridad aplicables a la información utilizada por el proveedor de servicios tercero, todas las entidades deben incluir funcionalidades para los controles de seguridad siguientes:

– Se puede utilizar una línea alquilada para evitar que usuarios no autorizados accedan a la conexión entre el MDMS y el proveedor de servicios tercero.

– Se requieren medidas de comunicación segura, como una red privada virtual (VPN, *virtual private network*), para la comunicación entre el dispositivo del cliente y el sistema de servicios públicos. Se requiere autenticación mutua, autenticación de los datos de comunicación y cifrado entre el dispositivo del cliente y el sistema de servicios públicos.

– La IIP a la que accede un proveedor de servicios debe estar sujeta a procesos de protección durante todo su ciclo de vida [b-GAO-08-343]. Si el proveedor de servicios tercero no necesita los datos, puede resultar conveniente ejecutar una desidentificación.

10.4 Controles de seguridad para la información utilizada por el operador del sistema de energía eléctrica

A fin de satisfacer los requisitos de seguridad aplicables la información utilizada por el operador del sistema eléctrico, todas las entidades deben incluir funcionalidades para los controles de seguridad siguiente:

– Se debe utilizar una línea alquilada para reducir el riesgo de acceso no autorizado a la conexión entre el MDMS y el operador del sistema de energía eléctrica.

– Se requieren medidas de comunicación segura, como VPN, para la comunicación entre el MDMS y operador del sistema de energía eléctrica. Se requiere autenticación mutua, autenticación de los datos de comunicación y cifrado entre el MDMS y el operador del sistema de energía eléctrica.

– Si el operador del sistema de energía eléctrica no necesita los datos de identificación, puede resultar conveniente ejecutar una desidentificación.

Bibliografía

[b-UIT-T X.1331] Recomendación UIT-T X.1331 (2018), *Directrices de seguridad para dispositivos de redes domésticas (HAN) en sistemas eléctricos inteligentes*

[b-UIT-T Y.2071] Recomendación UIT-T Y.2071 (2015), *Marco para una microrred eléctrica*

[b-GAO-08-343] United States Government Accountability Office, GAO-08-343:2008, *Information Security: Protecting Personally Identifiable Information.* https://www.gao.gov/new.items/d08343.pdf

[b-CEI 60050-617] CEI 60050-617:2009, *International Electrotechnical Vocabulary – Part 617: Organization/Market of electricity*

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 la 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, 2020