Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1580

(09/2012)

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

Intercambio de información de ciberseguridad – Intercambio asegurado

Defensa entre redes en tiempo real

Recomendación UIT-T X.1580

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	
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	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	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
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/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	**X.1580–X.1589**

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

Recomendación UIT-T X.1580

Defensa entre redes en tiempo real

Resumen

Esta Recomendación sobre defensa entre redes en tiempo real (RID, *real-time inter-network defense*) resume un método proactivo de comunicación entre redes para facilitar la automatización de la compartición de información sobre tratamiento de incidentes. Las implementaciones pueden integrarse con sistemas de gestión de incidentes existentes y con mecanismos de detección, identificación de fuente y mitigación para una solución más completa de tratamiento de incidentes. La RID especifica un método de comunicación seguro de información sobre incidentes, permitiendo el intercambio de documentos de lenguaje de marcaje extensible (XML) en formato de intercambio de descripciones de objetos de incidentes (IODEF). La RID proporciona un medio técnico para transmitir controles de seguridad, política y privacidad para permitir el intercambio de información potencialmente confidencial. Las capacidades técnicas se pueden mapear con las políticas apropiadas para permitir que los proveedores de servicio u organizaciones tomen decisiones apropiadas conforme a sus políticas.

Esta Recomendación especifica la RID enumerando las cláusulas pertinentes de RFC 6545 e indicando si son normativas o informativas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1580	2012-09-07	17

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

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en esta Recomendación 1
4 Abreviaturas y acrónimos 1
5 Convenios 2
6 Defensa entre redes en tiempo real (RID) 2
6.1 Introducción 2
6.2 Características de incidentes 2
6.3 Comunicaciones entre CSIRT y proveedores de servicio 2
6.4 Formatos de mensaje 3
6.5 Esquema IODEF-RID 3
6.6 Mensajes RID 3
6.7 Intercambios de comunicación RID 4
6.8 Definición de esquema RID 4
6.9 Requisitos de seguridad 4
6.10 Consideraciones de seguridad 5
6.11 Internacionalización 5
6.12 Consideraciones de IANA 5
6.13 Resumen 5
6.14 Referencias 5
Bibliografía 6

Introducción

La Recomendación X.1500, Aspectos generales del intercambio de información de ciberseguridad, proporciona una serie de orientaciones para el intercambio de información de ciberseguridad, incluida la relativa a incidentes e indicadores, tal y como se proporciona en esta Recomendación del UIT-T. Las organizaciones pueden mejorar su sensibilización sobre situaciones y beneficiarse de la asistencia de otras organizaciones por medio del intercambio de información sobre incidentes. El intercambio de información sobre incidentes permite a las organizaciones compartir recursos para identificar incidentes, mitigar actividades maliciosas dirigidas a sus recursos informáticos y comprender bien las posibles amenazas.

El tratamiento de incidentes puede entrañar la detección, información y mitigación de incidentes, ya sean cuestiones de configuración benignas, incidentes TI, infracciones a un acuerdo de nivel de servicio (SLA), ataque contra sistemas mediante la manipulación de personas, ataques de denegación de servicio (DoS), etc. Cuando se detecta un incidente, la respuesta puede consistir en rellenar un informe, enviar ese informe al origen del incidente, dirigirse a un proveedor de servicio para solicitar asistencia sobre una posible solución/mitigación, o una solicitud de buscar la fuente.

La defensa entre redes en tiempo real (RID) da una idea general de un método de comunicación proactivo entre redes para facilitar la divulgación de información sobre el tratamiento de incidentes. La RID puede estar integrada en mecanismos existentes de gestión, detección, identificación de origen y mitigación de incidentes para una solución completa de tratamiento de incidentes. La RID ofrece un medio técnico para transmitir controles de seguridad, política y privacidad a fin de permitir el intercambio de información potencialmente confidencial. La RID permite el intercambio seguro y automatizado de documentos en lenguaje de marcaje extensible (XML) en formato de intercambio de descripción de objeto de incidente (IODEF). Esto ofrece a los proveedores de servicios u organizaciones la posibilidad de adoptar decisiones adecuadas conformes a sus políticas haciendo corresponder políticas y acuerdos con los controles técnicos proporcionados. La RID comprende disposiciones sobre secreto, confidencialidad, integridad y autenticación para el intercambio de información sobre incidentes.

Los datos en mensajes RID se representan en un documento XML utilizando el IODEF y una envolvente RID. Siguiendo este modelo, IODEF y RID forman una interfaz de programación de aplicación para la integración con otros instrumentos de tratamiento de incidentes. Se proporcionan marcadores de datos y valores de enumeración XML para indicar qué acciones se recomienda adoptar para detener o mitigar los efectos del incidente o ataque. La RID está destinada a proporcionar un método para comunicar la información pertinente. Como la RID y el protocolo de transporte asociado se limitan a proporcionar una interfaz para automatizar la comunicación entre herramientas, permite la interoperabilidad con diversos planteamientos de detección y respuesta existentes y posiblemente futuros. Los incidentes pueden comprender seguridad informática y otros tipos de incidentes.

Las consideraciones de seguridad y privacidad son muy importantes porque podría intercambiarse información potencialmente confidencial en mensajes RID. La mensajería RID aprovecha técnicas existentes tales como funciones de seguridad XML además de marcadores de datos XML para indicar requisitos de privacidad y política a través del esquema RID. El esquema RID es una envolvente XML utilizada para comunicar documentos IODEF. La RID se define en IETF RFC 6545. Mensajes RID pueden en capsular separa transporte seguro. El transporte RID se define en una recomendación aparte, UIT-T X.1581. Las características combinadas de autenticación, integridad y autorización de RID y transporte RID se pueden utilizar para lograr el nivel de seguridad necesario.

Numerosas consideraciones de procedimiento, confianza, políticas y jurídicas pueden limitar o impedir el intercambio de información.

Recomendación UIT-T X.1580

Defensa entre redes en tiempo real

1 Alcance

Esta Recomendación especifica la defensa entre redes en tiempo real (RID) y proporciona un método para el intercambio seguro de información sobre incidentes. Esta Recomendación proporciona el conjunto de mensajes de coordinación sobre incidentes necesario para comunicar documentos IODEF con seguridad entre entidades. La RID es esencialmente una envolvente para documentos en lenguaje de marcaje extensible (XML) en IODEF, incluidas cualesquiera extensiones de IODEF. Los formatos normalizados de mensajes e intercambio comprenden opciones/consideraciones de seguridad, privacidad y política que son necesarias en un esquema global de coordinación de incidentes. La RID es la capa de seguridad entre documentos IODEF y el protocolo de transporte, proporcionada a través de las opciones de esquema IODEF-RID XML y los requisitos de seguridad de los flujos de comunicación RID.

Las implementaciones que permiten el intercambio de información de incidente deben proporcionar las capacidades para cumplir todas las legislaciones, normativas y políticas nacionales y regionales aplicables.

Los implementadores y usuarios de todas las recomendaciones del UIT-T, incluida la Recomendación UIT-T X.1580 y las técnicas subyacentes, cumplirán todas las legislaciones, normativas y políticas nacionales y regionales aplicables.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios a que estudien la posibilidad de utilizar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente en vigor. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[IETF RFC 6545] IETF RFC 6545 (2012), *Real-time Inter-network Defense (RID)*.
<https://datatracker.ietf.org/doc/rfc6545/>

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Abreviaturas y acrónimos

CSIRT Equipo encargados de incidentes informáticos (*computer security incident response team*)

DoS Negación de servicio (*denial of service*)

IODEF Formato de intercambio de descripción de objeto de incidente (*incident object description exchange format*)

IT Tecnología de la información (*information technology*)

RID Defensa entre redes en tiempo real (*real-time inter-network defense*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

5 Convenios

Los siguientes términos se consideran equivalentes:

- En la UIT, los requisitos obligatorios se expresan con el futuro simple del verbo principal (futuro de mandato) u otras expresiones con significado de obligación y sus equivalentes negativos.
- En la UIT, el uso de la palabra inglesa "shall" es equivalente al uso que se hace en el IETF de la palabra "MUST".
- En la UIT, el uso de la expresión inglesa "shall not" es equivalente al uso que se hace en el IETF de la expresión "MUST NOT".

NOTA – En el IETF las palabras inglesas "shall" y "must" (en minúsculas) se utilizan en textos informativos.

6 Defensa entre redes en tiempo real (RID)

La cláusula 6 define la mensajería de defensa entre redes en tiempo real (RID) especificada en IETF RFC6545. Esta cláusula proporciona referencias directas a IETF RFC 6545 mediante la alineación de las cláusulas con los números de sección de modo que la cláusula 6.x se alinea con la sección x de IETF RFC6 545 con los mismos títulos.

6.1 Introducción

La sección 1 de [b-IETF RFC 6545] es informativa.

6.1.1 Cambios con respecto a RFC 6045

La sección 1.1 de [b-IETF RFC 6545] es informativa.

6.1.2 Normativa e informativa

La sección 1.2 de [b-IETF RFC 6545] es informativa.

6.1.3 Terminología

La sección 1.3 de [b-IETF RFC 6545] es normativa.

6.2 Características de incidentes

La sección 2 de [b-IETF RFC 6545] es informativa.

6.3 Comunicaciones entre CSIRT y proveedores de servicio

La sección 3 de [b-IETF RFC 6545] es informativa.

6.3.1 Mensajería RID de proveedor entre redes

La sección 3.1 de [b-IETF RFC 6545] es informativa.

6.3.2 Topología de comunicación RID

La sección 3.2 de [b-IETF RFC 6545] es informativa.

6.4 Formatos de mensaje

La sección 4 de [IETF RFC 6545] es normativa.

6.4.1 Tipos de datos RID

La sección 4.1 de [IETF RFC 6545] es normativa.

6.4.1.1 Booleano

La sección 4.1.1 de [IETF RFC 6545] es normativa.

6.4.2 Tipos de mensaje RID

La sección 4.2 de [IETF RFC 6545] es normativa.

6.5 Esquema IODEF-RID

La sección 5 de [IETF RFC 6545] es normativa.

6.5.1 Clase RIDPolicy

La sección 5.1 de [IETF RFC 6545] es normativa.

6.5.1.1 ReportSchema

La sección 5.1.1 de [IETF RFC 6545] es normativa.

6.5.2 RequestStatus

La sección 5.2 de [IETF RFC 6545] es normativa.

6.5.3 IncidentSource

La sección 5.3 de [IETF RFC 6545] es normativa.

6.5.4 Espacios de nombre RID

La sección 5.4 de [IETF RFC 6545] es normativa.

6.5.5 Codificación

La sección 5.5 de [IETF RFC 6545] es normativa.

6.5.6 Inclusión de IODEF u otros documentos XML

La sección 5.6 de [IETF RFC 6545] es normativa.

6.5.6.1 Inclusión de documentos XML en RID

La sección 5.6.1 de [IETF RFC 6545] es normativa.

6.6 Mensajes RID

La sección 6 de [b-IETF RFC 6545] es normativa.

6.6.1 Petición

La sección 6.1 de [IETF RFC 6545] es normativa.

6.6.2 Acuse de recibo

La sección 6.2 de [IETF RFC 6545] es normativa.

6.6.3 Resultado

La sección 6.3 de [IETF RFC 6545] es normativa.

6.6.4 Informe

La sección 6.4 de [IETF RFC 6545] es normativa.

6.6.5 Búsqueda

La sección 6.5 de [IETF RFC 6545] es normativa.

6.7 Intercambios de comunicación RID

La sección 7 de [b-IETF RFC 6545] es normativa.

6.7.1 Flujo de comunicación de traza en sentido ascendente

La sección 7.1 de [IETF RFC 6545] es normativa.

6.7.1.1 Ejemplo de TraceRequest de RID

La sección 7.1.1 de [b-IETF RFC 6545] es normativa.

6.7.1.2 Ejemplo de mensaje de acuse de recibo

La sección 7.1.2 de [b-IETF RFC 6545] es informativa.

6.7.1.3 Ejemplo de mensaje de resultado

La sección 7.1.3 de [b-IETF RFC 6545] es informativa.

6.7.2 Flujo de comunicación de petición de investigación

La sección 7.2 de [IETF RFC 6545] es normativa.

6.7.2.1 Ejemplo de petición de investigación

La sección 7.2.1 de [b-IETF RFC 6545] es informativa.

6.7.2.2 Ejemplo de mensaje de acuse de recibo

La sección 7.2.2 de [b-IETF RFC 6545] es informativa.

6.7.3 Flujo de comunicación de informe

La sección 7.3 de [b-IETF RFC 6545] es normativa.

6.7.3.1 Ejemplo de informe

La sección 7.3.1 de [b-IETF RFC 6545] es informativa.

6.7.4 Flujo de comunicación de búsqueda

La sección 7.4 de [IETF RFC 6545] es normativa.

6.7.4.1 Ejemplo de búsqueda

La sección 7.4.1 de [b-IETF RFC 6545] es informativa.

6.8 Definición de esquema RID

La sección 8 de [IETF RFC 6545] es normativa.

6.9 Requisitos de seguridad

La sección 9 de [b-IETF RFC 6545] es normativa.

6.9.1 Firmas y encriptado digital XML

La sección 9.1 de [IETF RFC 6545] es normativa.

6.9.2 Transporte de mensaje

La sección 9.2 de [IETF RFC 6545] es normativa.

6.9.3 Infraestructura de clave pública

La sección 9.3 de [IETF RFC 6545] es normativa.

6.9.3.1 Autenticación

La sección 9.3.1 de [IETF RFC 6545] es normativa.

6.9.3.2 Autenticación de solicitud de varios saltos

La sección 9.3.2 de [IETF RFC 6545] es normativa.

6.9.4 Consorcios e infraestructura de clave pública

La sección 9.4 de [IETF RFC 6545] es normativa.

6.9.5 Inquietudes de privacidad y directrices de utilización de sistema

La sección 9.5 de [IETF RFC 6545] es normativa.

6.9.6 Compartición de perfiles y políticas

La sección 9.6 de [IETF RFC 6545] es normativa.

6.10 Consideraciones de seguridad

La sección 10 de [b-IETF RFC 6545] es normativa.

6.11 Internacionalización

La sección 11 de [IETF RFC 6545] es normativa.

6.12 Consideraciones de IANA

La sección 12 de [IETF RFC 6545] es normativa.

6.13 Resumen

La sección 13 de [b-IETF RFC 6545] es informativa.

6.14 Referencias

6.14.1 Referencias normativas

La sección 14.1 de [b-IETF RFC 6545] es informativa.

Esta Recomendación del UIT-T ha identificado la sección 14.1 de RFC 6545 como informativa porque el UIT-T no desarrolló una posición sobre ninguna de esas referencias con respecto a esta Recomendación. No obstante, se reconoce que el IETF ha identificado un conjunto de referencias normativas para RFC 6545.

6.14.2 Referencias informativas

La sección 14.2 de [b-IETF RFC 6545] es informativa.

Bibliografía

[b-UIT-T X.1500] Recomendación UIT-T X.1500, *Aspectos generales del intercambio de información de ciberseguridad*.

[b-ITU-T X.1541] Recommención ITU-T X.1541 (2012), *Incident object description exchange format*.

[b-ITU-T X.1581] Recommención ITU-T X.1581 (2012), *Transport of real-time inter-network defence messages*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2012