Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1582

(01/2014)

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

Intercambio de información de ciberseguridad – Intercambio asegurado

Protocolos de transporte para el intercambio de información de ciberseguridad

Recomendación UIT-T X.1582

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/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

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

Recomendación UIT-T X.1582

Protocolos de transporte para el intercambio de información de ciberseguridad

Resumen

En la Recomendación UIT-T X.1582 se presenta los protocolos de transporte que se han adoptado para el intercambio de información de ciberseguridad (CYBEX) y que se han adaptado al mismo. Se describen las aplicaciones de transporte, las características de los protocolos de transporte y los aspectos relativos a la seguridad.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1582	2014-01-24	17	11.1002/1000/12037

Palabras clave

Información de ciberseguridad, protocolos de intercambio de información, transferencia de información.

* 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

Introducción

Para el intercambio de información de ciberseguridad ya existen y se utilizan diversos mecanismos y protocolos de intercambio. Sin embargo, muchos de ellos, si no la mayoría, son privados y no se conocen bien o no están suficientemente documentados, por lo que resulta difícil utilizarlos para el intercambio mundial de información de ciberseguridad. Del mismo modo, la mayoría de aplicaciones de intercambio actuales sólo se ejecutan entre un número de partes limitado, ya sea en número o en ámbito de las operaciones de ciberseguridad.

Para que el intercambio de información de ciberseguridad adopte un carácter más global y sea compatible con el mayor número de espacios de aplicación posible, el "*Intercambio de información de ciberseguridad*" (CYBEX) presenta una familia de especificaciones de protocolos que soportan la globalización del intercambio de información de ciberseguridad bilateral o multilateral entre el mayor número de espacios de aplicación posible.

Recomendación UIT-T X.1582

Protocolos de transporte para el intercambio de información de ciberseguridad

1 Alcance

En esta Recomendación se presentan los protocolos de transferencia e intercambio que se han normalizado para su uso en el espacio de aplicación de la transferencia e intercambio de información de ciberseguridad, y/o que ya se utilizan en él, y que se han adoptado y adaptado para su utilización con las Recomendaciones de la serie UIT-T X.1500.

Esta Recomendación está principalmente dirigida a los diseñadores e implementadores cuya responsabilidad es habilitar la transferencia e intercambio de información de ciberseguridad a escala local, regional o mundial.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[UIT-T X.1500] Recomendación UIT-T X.1500 (2011), *Aspectos generales del intercambio de información de ciberseguridad.*

3 Definiciones

3.1 Términos definidos en otros documentos:

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

3.1.1 ciberseguridad [b-UIT-T X.1205]: Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen la disponibilidad, integridad (que puede incluir la autenticidad y el no repudio) y la confidencialidad.

NOTA – (no forma parte de [b-ITU-T X.1205]) Determinadas legislaciones y reglamentaciones nacionales pueden exigir la implementación de mecanismos para la protección de información de identificación personal.

3.1.2 protocolo de intercambio [UIT-T X.1500]: Conjunto de reglas técnicas y formatos que rige el intercambio de información entre dos o más entidades.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen el siguiente término:

3.2.1 entidad de ciberseguridad: Toda entidad que posee o busca información de ciberseguridad.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

BEEP Protocolo de intercambio extensible de bloques (*blocks extensible exchange protocol*)

CAPEC Enumeración y clasificación de pautas de ataques comunes (*common attack pattern enumeration and classification*)

CYBEX Intercambio de información de ciberseguridad (*cybersecurity information exchange)*

DDoS Ataque de denegación de servicio distribuido (*distributed denial of service*)

EVCERT Certificado de validación extendida (*extended validation certificate*)

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)

HSTS Seguridad estricta de transporte del protocolo de transferencia de hipertexto (*hypertext transfer protocol strict transport security*)

IODEF Formato de intercambio de descripciones de objetos incidentes (*incident object description exchange format*)

MIME Ampliaciones multifunción del correo Internet (*multipurpose Internet mail extensions*)

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

RSS Sindicación muy sencilla (*really simple syndication)*

SCTP Protocolo de transmisión de control de trenes (*stream control transmission protocol)*

SOAP Protocolo simple de acceso a objetos (*simple object access protocol*)

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

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

UDP Protocolo de datagrama de usuario (*user datagram protocol)*

URI Identificador uniforme de recursos (*uniform resource identifier*)

XML Lenguaje de marcaje extensible (*extensible markup language*)

5 Convenios

Ninguno.

6 Protocolos de transporte para el intercambio de información de seguridad

6.1 Aplicación de transporte

El intercambio de información de ciberseguridad puede llevarse a cabo en muy distintas circunstancias y utilizando diversos protocolos de transporte, que tienen cada uno de ellos sus propias características. A fin de contrastar esas características, se describen a continuación cuatro aplicaciones de transporte representativas.

6.1.1 Divulgación de información

Las entidades de ciberseguridad pueden divulgar información de manera indiscriminada gracias a protocolos ampliamente disponibles para comunicación de datos, como RSS. Cuando el objetivo es divulgar información, ésta puede facilitarse a cualquiera sin filtrar o adaptar los datos a una parte específica.

6.1.2 Abono a publicaciones

Una entidad de ciberseguridad puede abonarse a un determinado proveedor de información mediante un acuerdo bilateral, y el proveedor de información facilitará a esa parte específica los datos adaptados a sus intereses. En este caso, el proveedor de información es un intermediario entre el editor de la información (por ejemplo, fabricante de software) y el abonado. Estos servicios de abono a publicaciones exigen un filtrado por parte del intermediario, para lo que a su vez hay que proceder a una enumeración y una búsqueda, por ejemplo, enumeración de activos o búsqueda de la información pertinente.

6.1.3 Intercambio de información garantizado

Las entidades de ciberseguridad con capacidades similares pueden intercambiar información entre ellas a fin de aumentar la cobertura o acelerar la respuesta ante incidentes. El formato para el intercambio de descripciones de objetos de incidentes (IODEF) [b-UIT-T X.1541] y la defensa entre redes en tiempo real (RID) [b-UIT-T X.1580] son dos protocolos adaptados a la comunicación de detalles. Las entidades de ciberseguridad identificarán a los puntos extremos comunicantes y les exigirán que se autentifiquen y garanticen mutuamente. Cuando el objetivo son intercambios garantizados, es posible que cada entidad de ciberseguridad tenga que iniciar la comunicación con otras entidades, lo que se puede conseguir con protocolos de transporte bidireccional.

6.1.4 Prueba de posesión de información

Puede haber entidades de ciberseguridad que quieran comunicar con partes que hayan participado o sido testigos de un evento o incidente concreto, sin divulgar los detalles a otras partes no concernidas. Esto puede hacerse gracias a una determinada clase de protocolo criptográfico, por ejemplo, la intersección de conjuntos con preservación de la privacidad [b-Kissner]. En pocas palabras, estos intercambios con protocolos criptográficos demuestran la posesión de la información sin intercambiar la información misma, garantizando así la confidencialidad de la información sensible. Estos protocolos criptográficos pueden utilizarse por encima de los protocolos de transporte bidireccional.

6.2 Consideraciones sobre el protocolo de transporte

En función de las funciones asignadas a las entidades de ciberseguridad, los puntos extremos comunicantes pueden funcionar asimétricamente o como pares.

En un caso típico, donde los puntos extremos funcionan de manera asimétrica, se consideran adecuados los protocolos de pregunta-respuesta, pues la comunicación la inicia siempre un extremo. Cuando los puntos extremos funcionan como pares, ambos extremos inician la comunicación, por lo que conviene utilizar protocolos bidireccionales.

6.2.1 Protocolos de pregunta-respuesta

En los protocolos de pregunta-respuesta, el cliente inicia la conexión y el servidor responde. En este caso el flujo de información no sirve para establecer la distinción entre cliente y servidor, pues los clientes pueden facilitar la información o consumirla, en función de la división de funciones.

Con los protocolos de pregunta-respuesta, es posible que los servidores no puedan divulgar la información a los clientes de manera puntual, a menos que los clientes interroguen continuamente a los servidores. Dicho de otro modo, los clientes inician el intercambio de información y los servidores responden.

En el Cuadro 1 se resumen los protocolos de pregunta-respuesta disponibles.

Cuadro 1 – Protocolos de pregunta-respuesta disponibles para la transferencia y el intercambio

Nombre del protocolo	Características	Referencias
Protocolo de transferencia de hipertexto (HTTP)	El HTTP ofrece mecanismos básicos para extraer información de la entidad interrogada o facilitársela. HTTP puede utilizarse para intercambiar información de cualquier tipo que pueda identificarse con un identificador uniforme de recursos (URI) y cuyo tipo pueda especificarse con tipos de ampliaciones polivalentes de correo de Internet (MIME)	[b-IETF RFC 2616]
Protocolo simple de acceso a objetos (SOAP)	El SOAP se superpone al HTTP para facilitar la comunicación de pares atributo-valor. Se utiliza el esquema Lenguaje de marcaje extensible (XML) para especificar el tipo de atributos y valores	[b-SOAP]

6.2.2 Protocolos bidireccionales

Con los protocolos bidireccionales cualquiera de los extremos puede iniciar el intercambio de información. Estos protocolos pueden ser asimétricos, es decir, que se considera que uno de los extremos es el cliente y ha de iniciar la conexión. También pueden ser simétricos y, en ese caso, ambos extremos pueden iniciar la conexión cuando deseen.

Con los protocolos bidireccionales, se puede efectuar un intercambio puntual de información sin imponer una tara importante a la interrogación periódica. Los protocolos bidireccionales no sólo son convenientes cuando son simétricos y múltiples entidades de ciberseguridad intercambian información entre ellas, sino que también ofrecen la ventaja de la adaptabilidad cuando se necesita divulgar información a través de un gran número de nodos cliente.

También es posible establecer una conexión bidireccional entre un par de conexiones pregunta-respuesta independientes, para lo que se requiere que ambos puntos extremos ejerzan de cliente y de servidor, lo que puede plantear problemas de aplicación de software adicionales.

En el Cuadro 2 se presentan los protocolos bidireccionales disponibles.

Cuadro 2 – Protocolos bidireccionales disponibles para la transferencia y el intercambio

Nombre del protocolo	Características	Referencias
Protocolo de intercambio extensible de bloques (BEEP)	El BEEP acepta puntos extremos simétricos y asimétricos. Ambos extremos pueden iniciar la conexión y responder a ella	[b-IETF RFC 3080]
WebSocket	El protocolo WebSocket se superpone a HTTP, por lo que siempre son los clientes los que inician la conexión. Aunque se distingue entre cliente y servidor, el servidor puede iniciar la interacción del protocolo mediante una conexión iniciada por el cliente	[b-IETF RFC 6455]

6.3 Consideraciones de seguridad

De entre los protocolos de transporte CYBEX, los soportados por navegadores web requieren un cuidadoso análisis antes de su adopción, pues algunos navegadores web ofrecen un nivel rudimentario de separación entre las líneas de programación que se ejecutan en distintos sitios web, que por lo general tienen niveles de fiabilidad variables. Si bien una entidad de ciberseguridad válida puede emplear navegadores web para intercambiar información, esa misma instancia del navegador puede utilizarse para navegar por sitios web no fiables, que pueden albergar códigos perjudiciales para un punto extremo CYBEX concreto. Entre esas amenazas, falsificación de petición desde otro sitio (CSRF) (CAPEC ID 62) e inyección de código a través de scripts ejecutados en otros sitios (XSS) (CAPEC ID 63) son manifestaciones actualmente conocidas que efectivamente violan el principio de separación entre sitios web con distintos niveles de fiabilidad.

Contra estas amenazas existen, en forma de extensiones de HTTP, las contramedidas que se presentan en el Cuadro 3. La marca y versión de los navegadores web determinarán las extensiones soportadas.

Cuadro 3 – Extensiones HTTP disponibles para mejorar la seguridad

Nombre del protocolo	Características	Referencias
Política de seguridad de contenido (CSP)	La CSP puede restringir las fuentes de objetos incorporados, incluidas las líneas de programación ejecutadas dinámicamente, a una serie de sitios web predefinidos	[b-CSP]
Seguridad de transporte estricta HTTP (HSTS)	La HSTS puede restringir las interacciones de protocolo subsiguientes a canales seguros como seguridad en la capa de transporte (TLS) durante un periodo determinado de tiempo	[b- IETF RFC 6797]
HttpOnly	HttpOnly impide que los programas ejecutados dentro de los navegadores web accedan a las credenciales de autentificación, por ejemplo, cookies	[b- IETF RFC 6265]
Origin cookies	Origin cookies impide que otros sitios web modifiquen las cookies configuradas por el servidor web de origen. Las cookies originales sólo se pueden modificar desde el sitio en que se generaron	[b-Bortz]

Otros protocolos de capa de aplicación pueden ser objeto de amenazas semejantes, pues los navegadores web modernos pueden ejecutar programas arbitrarios dentro de plug in de navegación, como la programación Java y Flash, que a su vez pueden utilizarse para falsificar interacciones de protocolo. Por tanto, los puntos extremos CYBEX deberían evitar albergar y ejecutar software procedentes de fuentes no fiables, incluidos los de los sitios web. En caso de que esa medida no pueda imponerse al otro punto extremo CYBES, a causa de la naturaleza indiscriminatoria de una aplicación concreta, se habrá de medir y controlar el riesgo incurrido.

6.4 Consideraciones de capa de transporte y sesión

Dado que los puntos extremos CYBEX necesitan proteger la integridad del canal de comunicación, se alienta la utilización de TCP o SCTP [b-IETF RFC 4960]. Además, los implementadores de puntos extremos CYBEX deben considerar la protección contra la denegación de servicios por diversos medios, por ejemplo, mediante SYN cookies [b-IETF RFC 4987] y otras contramedidas contra los ataques de denegación de servicio distribuido (DDoS) [b-Mirkovic]. También pueden reforzar la integridad del canal de comunicación con códigos de autentificación de mensaje, como se define en la opción de autentificación del protocolo de control de transmisión (TCP) [b-IETF RFC 5925] y en authenticated chunks del protocolo de transmisión de control de trenes (SCTP) [b-IETF RFC 4895].

Las amenazas conocidas contra SCTP están documentadas en [b-IETF RFC 5062], donde además se indican las contramedidas pertinentes. No debe utilizarse UDP a fin de minimizar el riesgo de ataques reflejo [b-Paxson].

Para lograr la confidencialidad de la comunicación, se alienta la utilización de TLS [b-IETF RFC 5246] [b-IETF RFC 3436]. Si se considera necesario garantizar la identidad del punto extremo, conviene utilizar certificados de validación extendida (EVCERT) [b-EVCERT].

Bibliografía

[b-UIT-T X.1205] Recomendación UIT-T X.1205 (2008), *Aspectos generales de la ciberseguridad.*

[b-UIT-T X.1541] Recomendación UIT-T X.1541 (2012), *Formato para el intercambio de descripciones de objetos de incidentes.*

[b-UIT-T X.1544] Recomendación UIT -T X.1544 (2013), *Enumeración y clasificación de pautas de ataques comunes*

[b-UIT-T X.1580] Recomendación UIT-T X.1580 (2012), *Defensa entre redes en tiempo real*.

[b-CSP] W3C, Content Security Policy 1.0.
http://www.w3.org/TR/CSP/

[b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol* – HTTP/1.1.

[b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*.

[b-IETF RFC 3436] IETF RFC 3436 (2002), *Transport Layer Security over Stream Control Transmission Protocol*.

[b-IETF RFC 4895] IETF RFC 4895 (2007), *Authenticated Chunks for the Stream Control Transmission Protocol*.

[b-IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

[b-IETF RFC 4987] IETF RFC 4987 (2007), *TCP SYN Flooding Attacks and Common Mitigations*.

[b-IETF RFC 5062] IETF RFC 5062 (2007), *Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures*.

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

[b-IETF RFC 5925] IETF RFC 5925 (2010), *The TCP Authentication Option*.

[b-IETF RFC 6265] IETF RFC 6265 (2011), *HTTP State Management Mechanism*.

[b-IETF RFC 6455] IETF RFC 6455 (2011), *The WebSocket Protocol*.

[b-IETF RFC 6797] IETF RFC 6797 (2012), *HTTP Strict Transport Security*.

[b-Kissner] Lea Kissner and Dawn Song, *Privacy-Preserving Set Operations*, CRYPTO 2005.

[b-Mirkovic] Jelena Mirkovic and Peter Reiher, *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, ACM SIGCOMM Computer Communication Review, 34(2), April 2004.

[b-Paxson] Vern Paxson, *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*, ACM SIGCOMM Computer Communication Review, 31(3), July 2001.

[b-SOAP] W3C, *Simple Object Access Protocol*.
SOAP Version 1.2 Part 1: Messaging Framework (2007).

SOAP Version 1.2 Part 2: Adjuncts (2007).

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, 2014