International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1582

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Assured exchange

Transport protocols supporting cybersecurity information exchange

Recommendation ITU-T X.1582

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	**X.1580–X.1589**
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1582

Transport protocols supporting cybersecurity information exchange

Summary

Recommendation ITU-T X.1582 provides an overview of transport protocols that have been adopted and adapted for use within the Cybersecurity Information Exchange (CYBEX). The Recommendation outlines applications of transport, transport protocol characteristics, as well as security considerations.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1582	2014-01-24	17	11.1002/1000/12037

Keywords

Cybersecurity information, information exchange protocols, information transfer.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

A number of exchange mechanisms and protocols already exist and are in use in the exchange of cybersecurity information. However, many, if not most of them, are either in private use and not well documented or not widely known, thus making their use in the global exchange of cybersecurity information difficult. Also, most current exchange applications are among limited exchange partners, limited either in number or area of cybersecurity operations.

To support a more global and interoperable exchange of cybersecurity information among a wider array of application spaces possible, "*Cybersecurity Information Exchange*" (CYBEX) provides an overview of a family of protocol specific specifications supporting the globalization of cybersecurity information exchange among and between as wide range of application spaces as possible.

Recommendation ITU-T X.1582

Transport protocols supporting cybersecurity information exchange

1 Scope

This Recommendation provides an overview of transfer and exchange protocols that have been standardized for and/or in current usage within the application space of cybersecurity information transfer and exchange and that have been adopted and adapted for use within the ITU-T Recommendations in the X.1500 series.

This Recommendation is most applicable to application designers and implementers whose responsibility is to enable the transfer and exchange of cybersecurity information on local, regional or global scales.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange (CYBEX).*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cybersecurity [b-ITU-T X.1205]: The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise availability, integrity (which may include authentication and non-repudiation) and confidentiality.

NOTE – (not part of [b-ITU-T X.1205]) Some specific national regulation and legislation may require implementation of mechanisms to protect personally identifiable information.

3.1.2 exchange protocol [ITU-T X.1500]: A set of technical rules and format governing the exchange of information between two or more entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 cybersecurity entity: Any entity possessing or seeking cybersecurity information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BEEP	Blocks Extensible Exchange Protocol
CAPEC	Common Attack Pattern Enumeration and Classification
CYBEX	Cybersecurity information Exchange
DDoS	Distributed Denial of Service
EVCERT	Extended Validation Certificate
HTTP	Hypertext Transfer Protocol
HSTS	Hypertext transfer protocol Strict Transport Security
IODEF	Incident Object Description Exchange Format
MIME	Multi-purpose Internet Mail Extensions
RID	Real-time Inter-network Defence
RSS	Really Simple Syndication
SCTP	Stream Control Transmission Protocol
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
XML	extensible Markup Language

5 Conventions

None.

6 Transport protocols supporting cybersecurity information exchange

6.1 Application of transport

Cybersecurity information exchange encompasses wide variety of usage scenarios that can be implemented with several transport protocols, each with unique characteristics. In order to contrast their characteristics, four representative applications of transport are described here.

6.1.1 Information dissemination

Cybersecurity entities may disseminate information on a non-discriminatory basis. This can be accomplished through widely available protocols for feeding data, such as RSS. In such information dissemination purposes, the same set of information can be provided to anyone without filtering or tailoring the data to specific party.

6.1.2 Publish-subscribe

A cybersecurity entity may subscribe to a certain information provider on a bilateral basis, and the information provider may feed custom-tailored data that are relevant to the specific requesting party. In such scenario, the information provider can act as intermediary between information publisher (e.g., software vendors) and subscriber. Such publish-subscribe services require filtering at the intermediary that, in turn, necessitates enumeration and query, e.g., enumeration of assets or query for relevant information.

6.1.3 Assured exchange of information

Cybersecurity entities with similar capabilities may exchange information among themselves, in order to increase coverage or to expedite incident response. Incident object description exchange format (IODEF) [b-ITU-T X.1541] and real-time inter-network defence (RID) [b-ITU-T X.1580] are two such protocols for communicating details. Cybersecurity entities will identify communicating endpoints, and they will require authentication and assurance with each other. In such assured exchange purposes, each cybersecurity entity may need to initiate communication to other entities. This can be accomplished through bidirectional transport protocols.

6.1.4 Proof of information possession

Cybersecurity entities may wish to communicate with involved parties that observed particular event or incident, without disclosing details to other unaffected neighbours. This can be accomplished through certain class of cryptographic protocol, e.g., through privacy-preserving set intersection [b-Kissner]. Essentially, such cryptographic protocol exchanges proof of information possession without exchanging information itself, thus guaranteeing confidentiality of sensitive information. Such cryptographic protocols can be implemented on top of bidirectional transport protocols.

6.2 Transport protocol considerations

Depending on the roles assigned to cybersecurity entities, communication endpoints may operate asymmetrically or as peers.

In a typical case where roles of both endpoints are fixed in asymmetric fashion, request-response protocols are considered appropriate, as one end always initiates communication. When both endpoints work as peers, both ends may initiate communication, thus bidirectional protocols are considered appropriate.

6.2.1 Request-response protocols

In request-response protocols, the client is the initiator of connection and the server is the responder. Here, the flow of information is irrelevant from the client-server distinction; clients may provide information, or clients may consume information, depending on the separation of roles.

With request-response protocols, servers may not be able to disseminate information to clients in a timely manner, unless clients keep polling servers. In other words, clients are the initiator of information exchange, and servers are the responders of information exchange.

Available request-response protocols are summarized in Table 1.

Table 1 – Available request-response protocols for transfer and exchange

Protocol name	Characteristics	References
Hypertext transfer protocol (HTTP)	HTTP provides basic mechanisms to retrieve information from, or submit information to the responder. HTTP can be used to exchange any type of information that can be identified by a uniform resource identifier (URI) and whose type can be specified with multi-purpose Internet mail extensions (MIME) types.	[b-IETF RFC 2616]
Simple object access protocol (SOAP)	SOAP is built on top of HTTP to facilitate communication of attribute-value pairs. An extensible markup language (XML) Schema is used to specify the type of attributes and values.	[b-SOAP]

6.2.2 Bidirectional protocols

In bidirectional protocols, both ends can be the initiator of information exchange. Such protocols may be asymmetric, i.e., one end is considered to be a client and is required to initiate the connection. Another such protocol may be symmetric, i.e., both ends can initiate connection at their own will.

With bidirectional protocols, timely exchange of information is made possible without incurring significant overhead in the periodic polling. The benefits of bidirectional protocols are not limited to symmetric use cases where multiple cybersecurity entities exchange information among themselves; there are benefits in terms of scalability when information dissemination across a large number of client nodes are required.

It is also possible to compose a bidirectional connection from a pair of independent request-response connections. Such combination requires both endpoints to act as client and server, which may introduce additional software implementation issues.

Available bidirectional protocols are summarized in Table 2.

Table 2 – Available bidirectional protocols for transfer and exchange

Protocol name	Characteristics	References
Blocks extensible exchange protocol (BEEP)	BEEP is capable of accommodating both symmetric and asymmetric endpoints. Both ends can be connection initiator and responder.	[b-IETF RFC 3080]
WebSocket	The WebSocket protocol is built on top of HTTP, thus clients are always connection initiators. Although client and server are distinguished, the server can initiate protocol interaction through a client-initiated connection.	[b-IETF RFC 6455]

6.3 Security considerations

Among the CYBEX transport protocols, protocols supported by web browsers require careful security analysis before adoption, as some Web browsers provide rudimentary level of separation among scripts being executed across websites, often with varying level of trustworthiness. While valid cybersecurity entity may employ Web browsers to exchange information, the same web browser instance can be used to navigate across untrusted websites, which may be hosting potentially harmful code against particular CYBEX endpoint. Among such threats, cross-site request forgery (CSRF) (CAPEC ID 62) and cross site scripting (XSS) (CAPEC ID 63) are currently known manifestations that effectively break the separation principle between websites with different trust levels.

Countermeasures against such threats are available as extensions to HTTP, as summarized in Table 3. Depending on the brand and version of web browsers, supported extensions may vary.

Table 3 – Available extensions to HTTP for improving security

Name	Characteristics	References
Content security policy (CSP)	CSP can restrict sources of embedded objects, including dynamically running scripts, to a predefined set of websites.	[b-CSP]
HTTP strict transport security (HSTS)	HSTS can restrict subsequent protocol interactions to secure channel such as transport layer security (TLS) for certain period of time.	[b-IETF RFC 6797]
HttpOnly	HttpOnly restricts programs running within Web browsers from accessing authentication credentials, e.g., cookies.	[b-IETF RFC 6265]
Origin cookies	Origin cookies restrict other websites from clobbering cookies set by the originating web server; origin cookies are only modifiable from an exact origin.	[b-Bortz]

Other application-layer protocols can be susceptible to similar threats. As modern web browsers can execute arbitrary programs within browser plug-ins, such as Java and Flash scripts, they can be used to forge protocol interactions. Hence, CYBEX endpoints should avoid hosting and running software from untrusted sources, including those from websites. In case such enforcement to the other CYBEX endpoint is not considered realistic due to non-discriminatory nature of particular application, measurement and control of on-going risk is required.

6.4 Transport and session layer considerations

As CYBEX endpoints need to protect integrity of communication channel, use of TCP or SCTP [b-IETF RFC 4960] is encouraged. In addition, implementers of CYBEX endpoints should consider protection against denial of services through variety of means, e.g., through SYN cookies [b-IETF RFC 4987] and other distributed denial of service (DDoS) countermeasures [b-Mirkovic]. Implementers may further strengthen integrity of communication channel through message authentication codes, as defined in the transmission control protocol (TCP) authentication option [b-IETF RFC 5925] and stream control transmission protocol (SCTP) authenticated chunks [b-IETF RFC 4895].

Known threats against SCTP are documented in [b-IETF RFC 5062], along with their countermeasures. UDP should not be used, in order to minimize the risk of reflection attacks [b-Paxson].

In order to achieve confidentiality of communication, use of TLS is encouraged [b-IETF RFC 5246] [b-IETF RFC 3436]. If assurance of endpoint identity is considered necessary, use of extended validation certificate (EVCERT) [b-EVCERT] is encouraged.

Bibliography

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

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

[b-ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification.*

[b-ITU-T X.1580] Recommendation ITU-T X.1580 (2012), *Real-time inter-network defense*.

[b-Bortz] Andrew Bortz, Adam Barth and Alexei Czeskis, Origin Cookies: Session Integrity for Web Applications, W2SP 2011.

[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 OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014