International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1581

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Assured exchange

Transport of real-time inter-network defence messages

Recommendation ITU-T X.1581

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**

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

Recommendation ITU-T X.1581

Transport of real-time inter-network defence messages

Summary

Recommendation ITU-T X.1581 specifies a transport protocol for real-time inter-network defence (RID) based upon the passing of RID messages over hypertext transfer protocol/transport layer security (HTTP/TLS). This is achieved by listing the relevant clauses of IETF RFC 6546 and showing whether they are normative or informative.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1581	2012-09-07	17

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

Recommendation ITU-T X.1500, Overview of cybersecurity information exchange, provides guidance for the exchange of cybersecurity information including that for incidents and indicators as provided through this Recommendation. The incident object description exchange format (IODEF) defines a common extensible markup language (XML) data model representation for computer security incident information exchange, and real-time inter-network defence (RID) provides a secure communication method for IODEF documents intended for the cooperative handling of security incidents between interested parties. This Recommendation specifies a transport protocol for RID based upon the exchange of RID messages over hypertext transfer protocol/transport layer security (HTTP/TLS).

Clause 6 specifies a method for the transport of real-time inter-network defence (RID) messages.

Recommendation ITU-T X.1581

Transport of real-time inter-network defence messages

1 Scope

This Recommendation specifies a transport protocol for the exchange of real-time inter-network defence (RID) messages over hypertext transfer protocol/transport layer security (HTTP/TLS).

Implementations enabling the exchange of incident information must provide the capabilities to comply with all applicable national and regional laws, regulations and policies.

Implementers and users of all ITU-T Recommendations, including this Recommendation and the underlying techniques, shall comply with all applicable national and regional laws, regulations and policies.

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.

[IETF RFC 6546] IETF RFC 6546 (2012), *Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS.*
<https://datatracker.ietf.org/doc/rfc6546/>

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
RID	Real-time Inter-network Defence
TLS	Transport Layer Security
XML	eXtensible Markup Language

5 Conventions

The following terms are considered equivalent:

- In ITU use of the word 'shall' and 'must' and their negatives are considered equivalent.
- In ITU use of the word 'shall' is equivalent to the IETF use of the word 'MUST'.
- In ITU use of the phrase 'shall not' is equivalent to the IETF use of the term 'MUST NOT'.

NOTE – In the IETF use of the words 'shall' and 'must' (in lower case) are used for informative text.

6 Transport of real-time inter-network defence

This clause defines transport of real-time inter-network defence (RID) messaging as specified in [IETF RFC 6546]. This clause provides direct references to [IETF RFC 6546] through alignment of the clauses with the section numbers such that clause 6.x aligns with [IETF RFC 6546] section x with matching titles.

6.1 Introduction

[IETF RFC 6546] section 1 is informative.

6.1.1 Changes from RFC 6046

[IETF RFC 6546] section 1 is informative.

6.2 Terminology

[IETF RFC 6546] section 2 is normative.

6.3 Transmission of RID messages over HTTP/TLS

[IETF RFC 6546] section 3 is normative.

6.4 Security considerations

[IETF RFC 6546] section 4 is normative.

6.5 IANA considerations

[IETF RFC 6546] section 5 is normative.

6.6 Acknowledgements

[IETF RFC 6546] section 6 is informative.

6.7 References

6.7.1 Normative references

[IETF RFC 6546] section 7.1 is informative.

This Recommendation has identified [IETF RFC 6546] section 7.1 as being informative because the ITU-T did not develop a position on any of these references with respect to this Recommendation. However, it is recognized that the IETF has identified a set of normative references for [IETF RFC 6546].

6.7.2 Informative references

[IETF RFC 6546] section 7.2 is informative.

Bibliography

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

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

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

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, 2012