

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1580

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Assured exchange

Real-time inter-network defence

Recommendation ITU-T X.1580

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.1580

Real-time inter-network defence

Summary

Recommendation ITU-T X.1580 on real-time inter-network defence (RID) outlines a proactive inter-network communication method to facilitate the automation of sharing incident handling information. Implementations may integrate with existing incident management systems as well as detection, source identification, and mitigation mechanisms for a more complete incident handling solution. RID specifies a method to securely communicate incident information, enabling the exchange of incident object description exchange format (IODEF) extensible markup language (XML) documents. RID provides a technical means to convey security, policy, and privacy controls to enable the exchange of potentially sensitive information. The technical capabilities can be mapped to the appropriate policies to enable service providers or organizations the option to make appropriate decisions according to their policies.

This Recommendation specifies RID by listing the relevant clauses of IETF RFC 6545 and showing whether they are normative or informative.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1580	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/>.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	1
4 Abbreviations and acronyms	1
5 Conventions	2
6 Real-time inter-network defence	2
6.1 Introduction	2
6.2 Characteristics of incidents.....	2
6.3 Communications between CSIRTs and service providers	2
6.4 Message formats	2
6.5 IODEF-RID schema	3
6.6 RID messages	3
6.7 RID communication exchanges.....	3
6.8 RID schema definition.....	4
6.9 Security requirements	4
6.10 Security considerations.....	5
6.11 Internationalization.....	5
6.12 IANA considerations	5
6.13 Summary.....	5
6.14 References	5
Bibliography.....	6

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 ITU-T Recommendation. Organizations can improve their situational awareness and benefit from the assistance of other organizations through the exchange of incident information. The exchange of incident information enables organizations to share resources in identifying incidents, mitigating malicious activity targeting their computing resources, and gaining insight into potential threats.

Incident handling may involve the detection, reporting, and mitigation of an incident, whether it be a benign configuration issue, an IT incident, an infraction to a service level agreement (SLA), a socially engineered system compromise, or a denial-of-service (DoS) attack, etc. After detecting an incident, the response may include filing a report, sending that report to the source of the incident, a request for assistance in a possible resolution/mitigation, or a request to trace to the source.

Real-time inter-network defence (RID) outlines a proactive inter-network communication method to facilitate sharing incident handling information. RID may be integrated with existing incident management, detection, source identification, and mitigation mechanisms for a complete incident handling solution. RID provides a technical means to convey security, policy, and privacy controls to enable the exchange of potentially sensitive information. RID enables the secure and automated exchange of incident object description exchange format (IODEF) extensible markup language (XML) documents. This gives service providers or organizations the option to make appropriate decisions according to their policies by mapping policies and agreements to the provided technical controls. RID includes provisions for secrecy, confidentiality, integrity and authentication for the exchange of incident information.

The data in RID messages is represented in an XML document using the IODEF and an RID envelope. By following this model, IODEF and RID form an application programming interface for the integration with other tools for incident handling. Data markers and XML enumeration values are provided to indicate what actions are recommended to be taken in order to halt or mitigate the effects of the incident or attack. RID is intended to provide a method to communicate the relevant information. Since RID and the associated transport protocol merely provide an interface to automate communication between tools, it enables interoperability with a variety of existing and possible future detection and response approaches. Incidents may include computer security or other incident types.

Security and privacy considerations are of high concern since potentially sensitive information may be exchanged through RID messages. RID messaging takes advantage of existing techniques including XML security functions in addition to XML data markers to indicate privacy and policy requirements through the RID schema. The RID schema is an XML envelope used to communicate IODEF documents. RID is defined in IETF RFC 6545. RID messages may be encapsulated for secure transport. RID transport is defined in a separate Recommendation, ITU-T X.1581. The combined authentication, integrity, and authorization features of RID and RID transport may be used to achieve the necessary level of security.

Numerous procedural, trust, policy and legal considerations may restrict or prevent the exchange of information.

Recommendation ITU-T X.1580

Real-time inter-network defence

1 Scope

This Recommendation specifies real-time inter-network defence (RID) and provides a method for the secure exchange of incident information. This Recommendation provides the set of incident coordination messages necessary to communicate IODEF documents securely between entities. RID is essentially an envelope for IODEF extensible markup language (XML) documents, including any extensions of IODEF. The standard messages and exchange formats include security, privacy and policy options/considerations that are necessary in a global incident coordination scheme. RID is the security layer between IODEF documents and the transport protocol, provided through both the IODEF-RID XML schema options and the security requirements of the RID communication flows.

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

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:

CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
IODEF	Incident Object Description Exchange Format
IT	Information Technology

RID	Real-time Inter-network Defence
SLA	Service Level Agreement

5 Conventions

The following terms are considered equivalent:

- In ITU use of the words '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 Real-time inter-network defence

This clause defines real-time inter-network defence (RID) messaging as specified in [IETF RFC 6545]. This clause provides direct references to [IETF RFC 6545] through alignment of the clauses with the section numbers such that clause 6.x aligns with section x of [IETF RFC 6545] with matching titles.

6.1 Introduction

[IETF RFC 6545] section 1 is informative.

6.1.1 Changes from RFC 6045

[IETF RFC 6545] section 1.1 is informative.

6.1.2 Normative and informative

[IETF RFC 6545] section 1.2 is informative.

6.1.3 Terminology

[IETF RFC 6545] section 1.3 is normative.

6.2 Characteristics of incidents

[IETF RFC 6545] section 2 is informative.

6.3 Communications between CSIRTs and service providers

[IETF RFC 6545] section 3 is informative.

6.3.1 Inter-network provider RID messaging

[IETF RFC 6545] section 3.1 is informative.

6.3.2 RID communication topology

[IETF RFC 6545] section 3.2 is informative.

6.4 Message formats

[IETF RFC 6545] section 4 is normative.

6.4.1 RID data types

[IETF RFC 6545] section 4.1 is normative.

6.4.1.1 Boolean

[IETF RFC 6545] section 4.1.1 is normative.

6.4.2 RID message types

[IETF RFC 6545] section 4.2 is normative.

6.5 IODEF-RID schema

[IETF RFC 6545] section 5 is normative.

6.5.1 RIDPolicy class

[IETF RFC 6545] section 5.1 is normative.

6.5.1.1 ReportSchema

[IETF RFC 6545] section 5.1.1 is normative.

6.5.2 RequestStatus

[IETF RFC 6545] section 5.2 is normative.

6.5.3 IncidentSource

[IETF RFC 6545] section 5.3 is normative.

6.5.4 RID name spaces

[IETF RFC 6545] section 5.4 is normative.

6.5.5 Encoding

[IETF RFC 6545] section 5.5 is normative.

6.5.6 Including IODEF or other XML documents

[IETF RFC 6545] section 5.6 is normative.

6.5.6.1 Including XML Documents in RID

[IETF RFC 6545] section 5.6.1 is normative.

6.6 RID messages

[IETF RFC 6545] section 6 is normative.

6.6.1 Request

[IETF RFC 6545] section 6.1 is normative.

6.6.2 Acknowledgement

[IETF RFC 6545] section 6.2 is normative.

6.6.3 Result

[IETF RFC 6545] section 6.3 is normative.

6.6.4 Report

[IETF RFC 6545] section 6.4 is normative.

6.6.5 Query

[IETF RFC 6545] section 6.5 is normative.

6.7 RID communication exchanges

[IETF RFC 6545] section 7 is normative.

6.7.1 Upstream trace communication flow

[IETF RFC 6545] section 7.1 is normative.

6.7.1.1 RID TraceRequest example

[IETF RFC 6545] section 7.1.1 is normative.

6.7.1.2 Acknowledgement message example

[IETF RFC 6545] section 7.1.2 is informative.

6.7.1.3 Result message example

[IETF RFC 6545] section 7.1.3 is informative.

6.7.2 Investigation request communication flow

[IETF RFC 6545] section 7.2 is normative.

6.7.2.1 Investigation request example

[IETF RFC 6545] section 7.2.1 is informative.

6.7.2.2 Acknowledgement message example

[IETF RFC 6545] section 7.2.2 is informative.

6.7.3 Report communication flow

[IETF RFC 6545] section 7.3 is normative.

6.7.3.1 Report example

[IETF RFC 6545] section 7.3.1 is informative.

6.7.4 Query communication flow

[IETF RFC 6545] section 7.4 is normative.

6.7.4.1 Query example

[IETF RFC 6545] section 7.4.1 is informative.

6.8 RID schema definition

[IETF RFC 6545] section 8 is normative.

6.9 Security requirements

[IETF RFC 6545] section 9 is normative.

6.9.1 XML digital signatures and encryption

[IETF RFC 6545] section 9.1 is normative.

6.9.2 Message transport

[IETF RFC 6545] section 9.2 is normative.

6.9.3 Public key infrastructure

[IETF RFC 6545] section 9.3 is normative.

6.9.3.1 Authentication

[IETF RFC 6545] section 9.3.1 is normative.

6.9.3.2 Multi-hop request authentication

[IETF RFC 6545] section 9.3.2 is normative.

6.9.4 Consortiums and public key infrastructure

[IETF RFC 6545] section 9.4 is normative.

6.9.5 Privacy concerns and system use guidelines

[IETF RFC 6545] section 9.5 is normative.

6.9.6 Sharing profiles and policies

[IETF RFC 6545] section 9.6 is normative.

6.10 Security considerations

[IETF RFC 6545] section 10 is normative.

6.11 Internationalization

[IETF RFC 6545] section 11 is normative.

6.12 IANA considerations

[IETF RFC 6545] section 12 is normative.

6.13 Summary

[IETF RFC 6545] section 13 is informative.

6.14 References

6.14.1 Normative references

[IETF RFC 6545] section 14.1 is informative.

This Recommendation has identified section 14.1 of [IETF RFC 6545] 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 6545].

6.14.2 Informative references

[IETF RFC 6545] section 14.2 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.1581] Recommendation ITU-T X.1581 (2012), *Transport of real-time inter-network defence messages*.

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