International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1541

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Event/incident/heuristics exchange

Incident object description exchange format

Recommendation ITU-T X.1541

ITU-T

International Telecommunication Union

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.1541

Incident object description exchange format

Summary

Recommendation ITU-T X.1541 describes the information model for the incident object description exchange format (IODEF) and provides an associated data model specified with XML schema. The IODEF specifies a data model representation for sharing commonly exchanged information about computer security or other incident types. This is achieved by listing the relevant clauses of IETF RFC 5070 and showing whether they are normative or informative.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1541	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 ITU-T Recommendation. The incident object description exchange format (IODEF) is a data model for representing commonly exchanged information regarding computer security. It specifies an XML data model representation for conveying incident information between entities that have an operational responsibility for instituting proactive defences, remediation activities, or a watch-and-warning over a defined constituency. The data model provides a method to encode information about hosts, networks and the services running on these systems; exploitation methodology and associated data; impact of the incident; and limited approaches for documenting workflow.

The overriding purpose of the IODEF is to enhance operational capabilities and improve situational awareness. Community adoption of the IODEF provides an improved ability to resolve incidents and convey situational awareness of the threat landscape by simplifying collaboration and information sharing. The IODEF structured format allows for:

- increased automation in the processing of incident information through the exchange of structure incident information, eliminating the need for security analysts to parse free-form textual documents;
- decreased effort in correlating similar data (even when highly structured) from different sources enhancing situational awareness;
- a common format on which to provide interoperability between tools for incident handling and analysis, specifically when information comes from multiple entities.

Numerous procedural, trust, policy and legal considerations may restrict or prevent the exchange of information. The IODEF is a technical specification and does not attempt to address these issues. However, operational implementations of the IODEF and associated formats and protocols should consider this broader context when forming information sharing agreements.

Recommendation ITU-T X.1541

Incident object description exchange format

1 Scope

The incident object description exchange format (IODEF) specifies a data model representation for sharing commonly exchanged information about computer security or other incident types. This Recommendation describes the information model for the IODEF and provides an associated data model specified with XML schema.

Any data model representation or framework enabling the sharing of information about computer security or other incident types 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 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format*. <http://datatracker.ietf.org/doc/RFC 5070/>

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:

IANA Internet Assigned Numbers Authority

IODEF Incident Object Description Exchange Format

5 Conventions

The following terms are considered equivalent:

- In ITU, the use of the word 'shall' and 'must', and their negatives, are considered equivalent.
- In ITU, the use of the word 'shall' is equivalent to the IETF use of the word 'MUST'.
- In ITU, the 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 Incident object description and exchange format

Clause 6 defines the incident object description exchange format (IODEF). This clause provides direct references to [IETF RFC 5070] through alignment of the clauses with the section numbers so that clause 6.x aligns with [IETF RFC 5070] section x with matching titles.

NOTE – An Errata to [b-IETF RFC 5070] is available in [b-Errata ID3333].

6.1 Introduction

[b-IETF RFC 5070] section 1 is informative.

6.1.1 Terminology

[b-IETF RFC 5070] section 1.1 is informative.

6.1.2 Notations

[b-IETF RFC 5070] section 1.2 is informative.

6.1.3 About the IODEF data model

[b-IETF RFC 5070] section 1.3 is informative.

6.1.4 About the IODEF implementation

[b-IETF RFC 5070] section 1.4 is informative.

6.2 IODEF data types

[b-IETF RFC 5070] section 2 is informative.

6.2.1 Integers

[IETF RFC 5070] section 2.1 is normative.

6.2.2 Real numbers

[IETF RFC 5070] section 2.2 is normative.

6.2.3 Characters and strings

[IETF RFC 5070] section 2.3 is normative.

6.2.4 Multilingual strings

[IETF RFC 5070] section 2.4 is normative.

6.2.5 Bytes

[IETF RFC 5070] section 2.5 is normative.

6.2.6 Hexadecimal bytes

[IETF RFC 5070] section 2.6 is normative.

6.2.7 Enumerated types

[IETF RFC 5070] section 2.7 is normative.

6.2.8 Date-time strings

[IETF RFC 5070] section 2.8 is normative.

6.2.9 Timezone string

[IETF RFC 5070] section 2.9 is normative.

6.2.10 Port lists

[IETF RFC 5070] section 2.10 is normative.

6.2.11 Postal address

[IETF RFC 5070] section 2.11 is normative.

6.2.12 Person or organization

[IETF RFC 5070] section 2.12 is normative.

6.2.13 Telephone and fax numbers

[IETF RFC 5070] section 2.13 is normative.

6.2.14 Email string

[IETF RFC 5070] section 2.14 is normative.

6.2.15 Uniform resource locator strings

[IETF RFC 5070] section 2.15 is normative.

6.3 The IODEF data model

[b-IETF RFC 5070] section 3 is informative.

6.3.1 IODEF-document class

[IETF RFC 5070] section 3.1 is normative.

6.3.2 Incident class

[IETF RFC 5070] section 3.2 is normative.

6.3.3 IncidentID class

[IETF RFC 5070] section 3.3 is normative.

6.3.4 AlternativeID class

[IETF RFC 5070] section 3.4 is normative.

6.3.5 RelatedActivity class

[IETF RFC 5070] section 3.5 is normative.

6.3.6 AdditionalData class

[IETF RFC 5070] section 3.6 is normative.

6.3.7 Contact class

[IETF RFC 5070] section 3.7 is normative.

6.3.7.1 RegistryHandle class

[IETF RFC 5070] section 3.7.1 is normative.

6.3.7.2 PostalAddress class

[IETF RFC 5070] section 3.7.2 is normative.

6.3.7.3 Email class

[IETF RFC 5070] section 3.7.3 is normative.

6.3.7.4 Telephone and fax classes

[IETF RFC 5070] section 3.7.4 is normative.

6.3.8 Time classes

[IETF RFC 5070] section 3.8 is normative.

6.3.8.1 StartTime

[IETF RFC 5070] section 3.8.1 is normative.

6.3.8.2 EndTime

[IETF RFC 5070] section 3.8.2 is normative.

6.3.8.3 DetectTime

[IETF RFC 5070] section 3.8.3 is normative.

6.3.8.4 ReportTime

[IETF RFC 5070] section 3.8.4 is normative.

6.3.8.5 DateTime

[IETF RFC 5070] section 3.8.5 is normative.

6.3.9 Method class

[IETF RFC 5070] section 3.9 is normative.

6.3.9.1 Reference class

[IETF RFC 5070] section 3.9.1 is normative.

6.3.10 Assessment class

[IETF RFC 5070] section 3.10 is normative.

6.3.10.1 Impact class

[IETF RFC 5070] section 3.10.1 is normative.

6.3.10.2 TimeImpact class

[IETF RFC 5070] section 3.10.2 is normative.

6.3.10.3 MonetaryImpact class

[IETF RFC 5070] section 3.10.3 is normative.

6.3.10.4 Confidence class

[IETF RFC 5070] section 3.10.4 is normative.

6.3.11 History class

[IETF RFC 5070] section 3.11 is normative.

6.3.11.1 HistoryItem class

[IETF RFC 5070] section 3.11.1 is normative.

6.3.12 EventData class

[IETF RFC 5070] section 3.12 is normative.

6.3.12.1 Relating the incident and EventData classes

[IETF RFC 5070] section 3.12.1 is normative.

6.3.12.2 Cardinality of EventData

[IETF RFC 5070] section 3.12.2 is normative.

6.3.13 Expectation class

[IETF RFC 5070] section 3.13 is normative.

6.3.14 Flow class

[IETF RFC 5070] section 3.14 is normative.

6.3.15 System class

[IETF RFC 5070] section 3.15 is normative.

6.3.16 Node class

[IETF RFC 5070] section 3.16 is normative.

6.3.16.1 Counter class

[IETF RFC 5070] section 3.16.1 is normative.

6.3.16.2 Address class

[IETF RFC 5070] section 3.16.2 is normative.

6.3.16.3 NodeRole class

[IETF RFC 5070] section 3.16.3 is normative.

6.3.17 Service class

[IETF RFC 5070] section 3.17 is normative.

6.3.17.1 Application class

[IETF RFC 5070] section 3.17.1 is normative.

6.3.18 OperatingSystem class

[IETF RFC 5070] section 3.18 is normative.

6.3.19 Record class

[IETF RFC 5070] section 3.19 is normative.

6.3.19.1 RecordData class

[IETF RFC 5070] section 3.19.1 is normative.

6.3.19.2 RecordPattern class

[IETF RFC 5070] section 3.19.2 is normative.

6.3.19.3 RecordItem class

[IETF RFC 5070] section 3.19.3 is normative.

6.4 Processing considerations

[b-IETF RFC 5070] section 4 is informative.

6.4.1 Encoding

[IETF RFC 5070] section 4.1 is normative.

6.4.2 IODEF namespace

[IETF RFC 5070] section 4.2 is normative.

6.4.3 Validation

[IETF RFC 5070] section 4.3 is normative

6.5 Extending the IODEF

[b-IETF RFC 5070] section 5 is informative.

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 throughout this Recommendation. This Recommendation provides the base format for the exchange of incident information but that does not cover all use cases in accordance with Recommendation ITU-T X.1500. Extensions to meet necessary use cases may be developed.

6.5.1 Extending the enumerated values of attributes

[IETF RFC 5070] section 5.1 is normative.

6.5.2 Extending classes

[IETF RFC 5070] section 5.2 is normative.

6.6 Internationalization issues

[IETF RFC 5070] section 6 is normative.

6.7 Examples

[b-IETF RFC 5070] section 7 is informative.

6.7.1 Worm

[b-IETF RFC 5070] section 7.1 is informative.

6.7.2 Reconnaissance

[b-IETF RFC 5070] section 7.2 is informative.

6.7.3 Bot-net reporting

[b-IETF RFC 5070] section 7.3 is informative.

6.7.4 Watch list

[b-IETF RFC 5070] section 7.4 is informative.

6.8 The IODEF schema

[IETF RFC 5070] section 8 is normative.

6.9 Security considerations

[IETF RFC 5070] section 9 is normative.

In ITU-T compliant implementations, the underlying messaging format and protocol used to exchange instances of the IODEF shall provide appropriate guarantees of confidentiality, integrity, and authenticity.

NOTE – In the IETF use of the word 'must' (in lower case) is used for informative text.

6.10 IANA considerations

[IETF RFC 5070] section 10 is normative.

6.11 Acknowledgements

[b-IETF RFC 5070] section 11 is informative.

6.12 References

6.12.1 Normative

[b-IETF RFC 5070] section 12.1 is informative.

This ITU-T Recommendation has identified [IETF RFC 5070] section 12 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 5070].

6.12.2 Informative

[b-IETF RFC 5070] section 12.2 is informative.

Bibliography

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

[b-Errata ID3333] IETF RFC Errata ID: 3333, *IETF RFC5070, "The Incident Object Description Exchange Format", December 2007; Status: Held for Document Update; Type: Editorial; Date Reported: 2012-09-02.* <http://www.rfc-editor.org/errata_search.php?eid=3333>

[b-IETF RFC 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format (IODEF).* <https://datatracker.ietf.org/doc/RFC 5070/>

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, 2013