International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1541

(09/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Event/incident/heuristics exchange

Incident object description exchange format version 2

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed legder technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
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.1541

Incident object description exchange format version 2

Summary

Recommendation ITU-T X.1541 describes the information model for the incident object description exchange format (IODEF) version 2 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 7970 and showing whether they are normative or informative.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1541	2012-09-07	17	11.1002/1000/11375
2.0	ITU-T X.1541	2017-09-06	17	11.1002/1000/13264

* 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

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) 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 version 2

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 IODEF and provides an associated data model specified with XML schema.

A 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 7970] IETF RFC 7970 (2016), *The Incident Object Description Exchange Format Version 2*.
<https://datatracker.ietf.org/doc/rfc7970/>

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) version 2 as, with direct references to [IETF RFC 7970] sections, with alignment of the clauses with the section numbers. Thus, for example, clause 6.x aligns with [IETF RFC 7970] section x, including with matching titles.

6.1 Introduction

[IETF RFC 7970] section 1 is informative.

6.1.1 Terminology

[IETF RFC 7970] section 1.1 is informative.

6.1.2 Notations

[IETF RFC 7970] section 1.2 is informative.

6.1.3 About the IODEF data model

[IETF RFC 7970] section 1.3 is informative.

6.1.4 Changes from RFC 5070

[IETF RFC 7970] section 1.4 is informative.

6.2 IODEF data types

[IETF RFC 7970] section 2 is informative, but its subsections, i.e., sections 2.1-2.15 are normative. They define the following data types:

- Integers ([IETF RFC 7970] section 2.1 defines this)
- Real numbers ([IETF RFC 7970] section 2.2 defines this)
- Characters and strings ([IETF RFC 7970] section 2.3 defines this)
- Multilingual strings ([IETF RFC 7970] section 2.4 defines this)
- Binary strings ([IETF RFC 7970] section 2.5 defines this)
  - Base64 bytes ([IETF RFC 7970] section 2.5.1 defines this)
  - Hexadecimal bytes ([IETF RFC 7970] section 2.5.2 defines this)
- Enumerated types ([IETF RFC 7970] section 2.6 defines this)
- Date-Time string ([IETF RFC 7970] section 2.7 defines this)
- Timezone string ([IETF RFC 7970] section 2.8 defines this)
- Port lists ([IETF RFC 7970] section 2.9 defines this)
- Postal address ([IETF RFC 7970] section 2.10 defines this)
- Telephone number ([IETF RFC 7970] section 2.11 defines this)
- Email string ([IETF RFC 7970] section 2.12 defines this)
- Uniform resource locator strings ([IETF RFC 7970] section 2.13 defines this)
- Identifiers and identifier references ([IETF RFC 7970] section 2.14 defines this)
- Software ([IETF RFC 7970] section 2.15 defines this)

  - SoftwareReference class ([IETF RFC 7970] section 2.15.1 defines this)
- Extension ([IETF RFC 7970] section 2.16 defines this)

6.3 The IODEF information model

[IETF RFC 7970] section 3 is informative, but its subsections, i.e., sections 3.1-3.29 are normative. They define the following data models

- IODEF-Document class ([IETF RFC 7970] section 3.1 defines this)
- Incident class ([IETF RFC 7970] section 3.2 defines this)
- Common attributes ([IETF RFC 7970] section 3.3 defines this)
  - restriction attribute ([IETF RFC 7970] section 3.3.1 defines this)
  - observable-id attribute ([IETF RFC 7970] section 3.3.2 defines this)
- IncidentID class ([IETF RFC 7970] section 3.4 defines this)
- AlternativeID class ([IETF RFC 7970] section 3.5 defines this)
- RelatedActivity class ([IETF RFC 7970] section 3.6 defines this)
- ThreatActor class ([IETF RFC 7970] section 3.7 defines this)
- Campaign class ([IETF RFC 7970] section 3.8 defines this)
- Contact class ([IETF RFC 7970] section 3.9 defines this)
  - RegistryHandle class ([IETF RFC 7970] section 3.9.1 defines this)
  - PostalAddress class ([IETF RFC 7970] section 3.9.2 defines this)
  - Email class ([IETF RFC 7970] section 3.9.3 defines this)
  - Telephone class ([IETF RFC 7970] section 3.9.4 defines this)
- Discovery class ([IETF RFC 7970] section 3.10 defines this)
  - DetectionPattern class ([IETF RFC 7970] section 3.10.1 defines this)
- Method class ([IETF RFC 7970] section 3.11 defines this)
  - Reference class ([IETF RFC 7970] section 3.11.1 defines this)
- Assessment class ([IETF RFC 7970] section 3.12 defines this)
  - SystemImpact class ([IETF RFC 7970] section 3.12.1 defines this)
  - BusinessImpact class ([IETF RFC 7970] section 3.12.2 defines this)
  - TimeImpact class ([IETF RFC 7970] section 3.12.3 defines this)
  - MonetaryImpact class ([IETF RFC 7970] section 3.12.4 defines this)
  - Confidence class ([IETF RFC 7970] section 3.12.5 defines this)
- History class ([IETF RFC 7970] section 3.13 defines this)
  - HistoryItem class ([IETF RFC 7970] section 3.13.1 defines this)
- EventData class ([IETF RFC 7970] section 3.14 defines this)
  - Relating the incident and EventData classes ([IETF RFC 7970] section 3.14.1 defines this)
  - Recursive definition of EventData ([IETF RFC 7970] section 3.14.2 defines this)
- Expectation class ([IETF RFC 7970] section 3.15 defines this)
- Flow class ([IETF RFC 7970] section 3.16 defines this)
- System class ([IETF RFC 7970] section 3.17 defines this)
- Node class ([IETF RFC 7970] section 3.18 defines this)
  - Address class ([IETF RFC 7970] section 3.18.1 defines this)

  - NodeRole class ([IETF RFC 7970] section 3.18.2 defines this)
  - Counter class ([IETF RFC 7970] section 3.18.3 defines this)
- DomainData class ([IETF RFC 7970] section 3.19 defines this)
  - Nameservers class ([IETF RFC 7970] section 3.19.1 defines this)
  - DomainContacts class ([IETF RFC 7970] section 3.19.2 defines this)
- Service class ([IETF RFC 7970] section 3.20 defines this)
  - ServiceName class ([IETF RFC 7970] section 3.20.1 defines this)
  - ApplicationHeader class ([IETF RFC 7970] section 3.20.2 defines this)
- EmailData class ([IETF RFC 7970] section 3.21 defines this)
- Record class ([IETF RFC 7970] section 3.22 defines this)
  - RecordData class ([IETF RFC 7970] section 3.22.1 defines this)
  - RecordPattern class ([IETF RFC 7970] section 3.22.2 defines this)
- WindowsRegistryKeysModified class ([IETF RFC 7970] section 3.23 defines this)
  - Key class ([IETF RFC 7970] section 3.23.1 defines this)
- CertificateData class ([IETF RFC 7970] section 3.24 defines this)
  - Certificate class ([IETF RFC 7970] section 3.24.1 defines this)
- FileData class ([IETF RFC 7970] section 3.25 defines this)
  - File class ([IETF RFC 7970] section 3.25.1 defines this)
- HashData class ([IETF RFC 7970] section 3.26 defines this)
  - Hash class ([IETF RFC 7970] section 3.26.1 defines this)
  - FuzzyHash class ([IETF RFC 7970] section 3.26.2 defines this)
- SignatureData class ([IETF RFC 7970] section 3.27 defines this)
- IndicatorData class ([IETF RFC 7970] section 3.28 defines this)
- Indicator class ([IETF RFC 7970] section 3.29 defines this)
  - IndicatorID class ([IETF RFC 7970] section 3.29.1 defines this)
  - AlternativeIndicatorID class ([IETF RFC 7970] section 3.29.2 defines this)
  - Observable class ([IETF RFC 7970] section 3.29.3 defines this)
  - IndicatorExpression class ([IETF RFC 7970] section 3.29.4 defines this)
  - Expressions with IndicatorExpression ([IETF RFC 7970] section 3.29.5 defines this)
  - ObservableReference class ([IETF RFC 7970] section 3.29.6 defines this)
  - IndicatorReference class ([IETF RFC 7970] section 3.29.7 defines this)
  - AttackPhase class ([IETF RFC 7970] section 3.29.8 defines this)

6.4 Processing Considerations

[IETF RFC 7970] section 4 is normative, though some of its subsections are informative, as clarified in the following subsections.

6.4.1 Encoding

[IETF RFC 7970] section 4.1 is normative.

6.4.2 IODEF Namespace

[IETF RFC 7970] section 4.2 is normative.

6.4.3 Validation

[IETF RFC 7970] section 4.3 is normative.

6.4.4 Incompatibilities with v1

[IETF RFC 7970] section 4.4 is informative.

6.5 Extending the IODEF

[IETF RFC 7970] section 5 is informative.

[b-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 (ITU-T X.1541). This Recommendation (ITU-T X.1541) provides the base format for the exchange of incident information but that does not cover all use cases in accordance with [b-ITU-T X.1500]. Extensions to meet necessary use cases may be developed.

6.5.1 Extending the enumerated values of attributes

[IETF RFC 7970] section 5.1 and its subsections are normative.

6.5.2 Extending classes

[IETF RFC 7970] section 5.2 and its subsections are normative.

6.6 Internationalization issues

[IETF RFC 7970] section 6 is normative.

6.7 Examples

[IETF RFC 7970] section 7 and its subsections, which describe the example IODEF documents are informative.

6.8 The IODEF data model (XML schema)

[IETF RFC 7970] section 8 is normative.

6.9 Security considerations

[IETF RFC 7970] section 9 and its subsections are 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 7970] section 10 and its subsections are normative.

6.11 References

6.11.1 Normative references

[IETF RFC 7970] section 11.1 is informative.

This ITU-T Recommendation has identified [IETF RFC 7970] section 11.1 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 7970].

6.11.2 Informative references

[IETF RFC 7970] section 11.2 is informative.

Bibliography

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017