

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1570

(09/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Identification and
discovery

Discovery mechanisms in the exchange of cybersecurity information

Recommendation ITU-T X.1570



International
Telecommunication
Union
Documents

Document Sharing Hub

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.1570

Discovery mechanisms in the exchange of cybersecurity information

Summary

Recommendation ITU-T X.1570 provides a framework for discovering cybersecurity information and the mechanism that enables this. Discovery can be seen as a stage of the cybersecurity information lifecycle adjacent to information publishing and acquisition, which are integral and necessary stages for discovery. Thus, the framework covers how to publish cybersecurity information, obtain the candidate list, and acquire the needed information. A discovery scheme may be implemented with arbitrary mechanisms so long as they comply with the framework. Among these mechanisms are object identifier (OID)-based discovery and resource description framework (RDF)-based discovery, which are also elaborated in this Recommendation.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1570	2011-09-02	17

Keywords

Cybersecurity information, information discovery, source discovery.

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	2
5 Conventions	2
6 Framework to identify and locate the source of cybersecurity information.....	3
7 Types and level of details of discovered cybersecurity information	3
8 Cybersecurity information identifier	4
9 Types of discovery mechanisms	5
9.1 OID-based discovery mechanisms in the exchange of cybersecurity information	5
9.2 RDF-based discovery mechanisms in cybersecurity information exchange..	6
10 Methods available for access to discovered information.....	7
Appendix I – Cybersecurity operational information ontology	8
I.1 Cybersecurity operation domains	8
I.2 Roles	8
I.3 Cybersecurity information.....	9
Appendix II – Specifications describing databases and knowledge bases.....	12
Appendix III – An illustrated implementation of RDF-based discovery	13
III.1 RDF-based discovery implementation example.....	13
III.2 Class hierarchy of cybersecurity information.....	13
Bibliography.....	15

Introduction

Greater importance than ever is being placed on the exchange of cybersecurity information. An international standard for exchanging cybersecurity information, called CYBEX, is drawing particularly significant attention. CYBEX discovery, which provides a scheme for finding the source of cybersecurity information, is among CYBEX's various technical specifications. This Recommendation explains its framework and techniques.

Recommendation ITU-T X.1570

Discovery mechanisms in the exchange of cybersecurity information

1 Scope

This Recommendation provides a framework for discovering cybersecurity information and the mechanism that enables this. Discovery can be seen as a stage of the cybersecurity information lifecycle adjacent to information publishing and acquisition, which are integral and necessary stages for discovery. Thus, the framework covers how to publish cybersecurity information, obtain the candidate list, and acquire the needed information. A discovery scheme may be implemented with arbitrary mechanisms so long as they comply with the framework. Among these mechanisms are object identifier (OID)-based discovery and resource description framework (RDF)-based discovery, which are also elaborated on in this Recommendation.

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.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*.

[W3C RDF] W3C Recommendation (2004), *Resource Description Framework (RDF): Concepts and Abstract Syntax*.
<<http://www.w3.org/TR/rdf-concepts/>>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 object identifier [ITU-T X.660]: An ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node.

3.1.2 ontology [b-Gruber]: An explicit specification of a conceptualization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cybersecurity information: Structured information or knowledge concerning:

1. the "state" of equipment, software or network-based systems as related to cybersecurity, especially vulnerabilities;
2. forensics related to incidents or events;
3. heuristics and signatures gained from experienced events;

4. parties who implement cybersecurity information exchange capabilities within the scope of this framework;
5. specifications for the exchange of cybersecurity information, including modules, schemas, policies and assigned numbers;
6. the identities and trust attributes of all of the above;
7. implementation requirements, guidelines and practices.

NOTE – This definition is based on the description given for cybersecurity information in [b-ITU-T X.1500].

3.2.2 exchange (cybersecurity information): The transfer of cybersecurity information between two or more cybersecurity entities. This transfer may be uni-directional, bi-directional, or multi-directional, i.e., many-to-many.

3.2.3 discovery: The act or process of discovering the target, i.e., obtaining knowledge of the target for the first time.

3.2.4 retriever: An entity retrieving cybersecurity information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CCE	Common Configuration Enumeration
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
CYBEX	CYBersecurity information EXchange
HTTP	Hypertext Transfer Protocol
IODEF	Incident Object Description Exchange Format
MAEC	Malware Attribute Enumeration and Characterization
OID	Object Identifier
OVAL	Open Vulnerability and Assessment Language
RDF	Resource Description Framework
SCAP	Security Content Automation Protocol
SNMP	Simple Network Management Protocol
XCCDF	eXtensible Configuration Checklist Description Format

5 Conventions

None.