

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1500

Amendment 12

(03/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Overview of
cybersecurity

Overview of cybersecurity information exchange

Amendment 12

Recommendation ITU-T X.1500 (2011) –
Amendment 12

ITU-T

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 ledger 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.1500

Overview of cybersecurity information exchange

Amendment 12

Summary

Recommendation ITU-T X.1500 describes techniques for exchanging cybersecurity information. These techniques can be used individually or in combinations, as desired or appropriate, to enhance cybersecurity through coherent, comprehensive, global, timely and assured information exchange. No obligations to exchange information are implied, nor are the means of acquisition or ultimate use of the information treated. Cybersecurity information exchange (CYBEX) is one of the elements providing confidence and security in the use of ICTs.

Amendment 12 provides a list of structured cybersecurity information techniques that have been created to be continually updated as these techniques evolve, expand, are newly identified or are replaced. The list follows the outline provided in the body of the Recommendation. This amendment reflects the situation of recommended techniques as of March 2017, including bibliographical references.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1500	2011-04-20	17	11.1002/1000/11060
1.1	ITU-T X.1500 (2011) Amd. 1	2012-03-02	17	11.1002/1000/11574
1.2	ITU-T X.1500 (2011) Amd. 2	2012-09-07	17	11.1002/1000/11751
1.3	ITU-T X.1500 (2011) Amd. 3	2013-04-26	17	11.1002/1000/11942
1.4	ITU-T X.1500 (2011) Amd. 4	2013-09-04	17	11.1002/1000/12041
1.5	ITU-T X.1500 (2011) Amd. 5	2014-01-24	17	11.1002/1000/12159
1.6	ITU-T X.1500 (2011) Amd. 6	2014-09-26	17	11.1002/1000/12334
1.7	ITU-T X.1500 (2011) Amd. 7	2015-04-17	17	11.1002/1000/12446
1.8	ITU-T X.1500 (2011) Amd. 8	2015-09-17	17	11.1002/1000/12596
1.9	ITU-T X.1500 (2011) Amd. 9	2016-03-23	17	11.1002/1000/12851
1.10	ITU-T X.1500 (2011) Amd. 10	2016-09-07	17	11.1002/1000/13071
1.11	ITU-T X.1500 (2011) Amd. 11	2017-03-30	17	11.1002/1000/13263
1.12	ITU-T X.1500 (2011) Amd. 12	2018-03-29	17	11.1002/1000/13590

* 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/>.

© ITU 2018

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.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Basic concept – Cybersecurity information exchange (CYBEX)	3
7	Structured cybersecurity information exchange techniques	4
	7.1 Weakness, vulnerability and state – exchange cluster.....	5
	7.2 Event, incident, and heuristics – exchange cluster	5
	7.3 Information exchange policy – exchange cluster	6
	7.4 Identification, discovery, and query cluster	6
	7.5 Identity assurance cluster	7
	7.6 Exchange protocol cluster	7
	Appendix I – Structured cybersecurity information exchange techniques	8
	Appendix II – A cybersecurity information exchange ontology.....	19
	II.1 Operation domains.....	20
	II.2 Cybersecurity entities	20
	II.3 Cybersecurity operational information.....	21
	Appendix III – CYBEX examples of security automation schemas.....	23
	III.1 Example: USA Federal Desktop Core Configuration/United States Government Configuration Baseline	24
	III.2 Example: Japan vulnerability information portal site, JVN	24
	Bibliography.....	28

Introduction

This Recommendation is intended to be adaptable, extensible, and non-prescriptive to allow a wide range of techniques – some of which are continuously evolving and in varying stages of completion – to be applied in different instantiations to enhance the exchange of cybersecurity information about telecommunication/ICT infrastructure, devices, and services. It will be revised periodically as those techniques evolve – those that are appropriate will be published as ITU-T Recommendations in the ITU-T X.1500 series.

The expectation for the techniques embodied in this Recommendation is that telecommunication/ ICT organizations, including computer incident response teams (CIRTs), both within and between jurisdictions, will:

- a) have information to enable decision making and action to substantially enhance the confidentiality, integrity and availability of global telecommunication/ICT facilities and services;
- b) have information to facilitate secure collaborative processes and controls which improve the level of assurance in the information exchanges between organizations;
- c) enable a coherent approach to manage and exchange cybersecurity information on a global basis;
- d) improve security awareness and collaboration to diminish cyberthreats, cyberattacks and malware.

The techniques include:

- structuring cybersecurity information for exchange purposes;
- identifying and discovering cybersecurity information and entities;
- establishment of trust and policy agreement between exchanging entities;
- requesting and responding with cybersecurity information;
- assuring the integrity of the cybersecurity information exchange;

and are organized into "clusters":

- Weakness, vulnerability and state.
- Event, incident, and heuristics.
- Information exchange policy.
- Identification, discovery, and query.
- Identity assurance.
- Exchange protocols.

Recommendation ITU-T X.1500

Overview of cybersecurity information exchange

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T X.1500 (2011). Amendments 1 to 11 have been superseded.

1 Scope

This Recommendation presents a cybersecurity information exchange (CYBEX) model and discusses techniques that can be used to facilitate the exchange of cybersecurity information. These techniques can be used individually or in combinations, as desired or appropriate, to enhance cybersecurity through coherent, comprehensive, global, timely and assured information exchange. No obligations to exchange information are implied, nor are the means of acquisition or ultimate use of the information treated. The techniques include the structured global discovery and interoperability of cybersecurity information in such a way as to allow for continual evolution to accommodate the significant activities and specification evolution occurring in numerous cybersecurity forums. CYBEX is one of the elements providing confidence and security in the use of ICTs.

This Recommendation has the following basic functions that can be used separately or together as appropriate:

- structuring cybersecurity information for exchange purposes;
- identifying and discovering cybersecurity information and entities;
- establishment of trust and policy agreement between exchanging entities;
- requesting and responding with cybersecurity information;
- assuring the integrity of the cybersecurity information exchange.

Subject to agreed policies and applicable laws and regulations, the means of acquiring information as well as the uses made of the information are specifically out of scope and not treated in this Recommendation. Some specific national and regional regulations and legislations may require implementation of mechanisms to protect personally identifiable information. Neither the techniques described in this Recommendation nor the exchange of related cybersecurity information are mandated by this Recommendation.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cybersecurity [b-ITU-T X.1205]: The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant

security risks in the cyber environment. The general security objectives comprise availability, integrity (which may include authentication and non-repudiation) and confidentiality.

NOTE – Some specific national regulations and legislations may require implementation of mechanisms to protect personally identifiable information.

3.1.2 security incident [b-ITU-T E.409]: Any adverse event whereby some aspect of security could be threatened.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 assurance: The degree of confidence that the process or deliverable meets defined characteristics or objectives.

3.2.2 exchange protocol: A set of technical rules and format governing the exchange of information between two or more entities.

3.2.3 information exchange policy: The terms and conditions associated with the use and sharing of cybersecurity information.

3.2.4 system state: The current status of a system or entity, including such information as its configuration, memory usage, or other data relevant to cybersecurity.

3.2.5 vulnerability (aligned with [b-ITU-T X.800]): Any weakness that could be exploited to violate a system or the information it contains.

3.2.6 weakness: A shortcoming or imperfection that, while not itself being recognized as a vulnerability, could, at some point become a vulnerability, or could contribute to the introduction of other vulnerabilities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ARF	Assessment Results Format or Asset Reporting Format (depending on the context)
BEEP	Blocks Extensible Exchange Protocol
CA	Certification Authority
CAPEC	Common Attack Pattern Enumeration and Classification
CCE	Common Configuration Enumeration
CEE	Common Event Expression
CEEE	Common Event Expression Exchange
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
CYIQL	Cybersecurity Information Query Language
DDoS	Distributed Denial of Service

EVC	Extended Validation Certificates
EVCERT	Extended Validation Certificate
HTTP	HyperText Transfer Protocol
IC	Integrated Circuit
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IODEF	Incident Object Description Exchange Format
IPS	Intrusion Prevention System
IT	Information Technology
MAEC	Malware Attribute Enumeration and Characterization
OID	Object Identifier
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
RID	Real-time Inter-network Defense
SCAP	Security Content Automation Protocol
SOAP	Simple Object Access Protocol
TLP	Traffic Light Protocol
TLS	Transport Layer Security
TNC	Trusted Network Connect
TPM	Trusted Platform Module
XCCDF	eXtensible Configuration Checklist Description Format

5 Conventions

When the term "standard" or "standards" is used in this Recommendation in the generic sense, it should be interpreted to include: standards; specifications and Recommendations.

6 Basic concept – Cybersecurity information exchange (CYBEX)

This cybersecurity information exchange (CYBEX) Recommendation is intended to accomplish a simple, limited objective – describe techniques by which cybersecurity entities can exchange cybersecurity information using methods which provide a suitable level of assurance. Such entities typically consist of organizations, persons, devices, or processes possessing or seeking cybersecurity information. Most frequently, these entities are CIRTs and the operators or vendors of equipment, software or network-based systems.

Cybersecurity information exchange is valuable for achieving enhanced cybersecurity and infrastructure protection, as well as contributing to the principal functions performed by CIRTs.

The exchange of cybersecurity information can occur within highly compartmentalized trust communities adhering to need-to-know principles based on previously agreed-upon policies, as well as within the public domain. Knowledge of threats, vulnerabilities, incidents, risks, and mitigations and their associated remedies are typical examples of the types of cybersecurity information exchanged between entities. The related techniques included in this Recommendation are intended to facilitate this information exchange and thereby enhance cybersecurity.

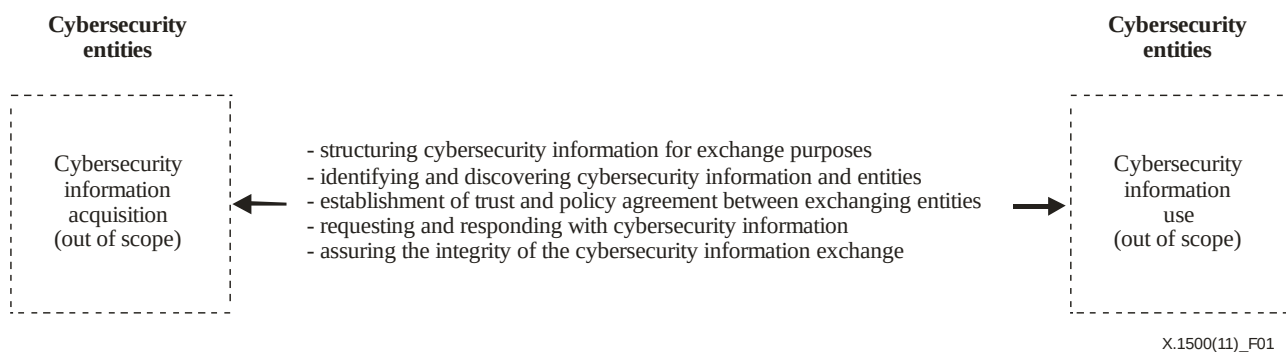


Figure 1 – CYBEX model

The general cybersecurity information exchange model used in this Recommendation, as shown in Figure 1, consists of basic functions that can be used separately or together as appropriate, and extended as needed in order to facilitate assured cybersecurity information exchanges. These are:

- structuring cybersecurity information for exchange purposes;
- identifying and discovering cybersecurity information and entities;
- establishment of trust and information exchange policy agreements between exchanging entities;
- requesting and responding with cybersecurity information;
- assuring the integrity of the cybersecurity information exchange.

Clause 7 describes techniques for accomplishing these functions.

The exchange of cybersecurity information may be bidirectional. This bidirectionality allows for verified information requests and responses to facilitate required levels of assurance between the parties or to provide certification of delivery.

Subject to agreed policies and applicable laws and regulations, the means of acquiring information as well as the uses made of the information are specifically out of scope and not treated in this Recommendation. For example, some specialized cybersecurity information exchange implementations such as traceback of attack sources may require application-specific mechanisms that allow for a recursive series of requests and responses to obtain required information. However, other implementations such as making cybersecurity measureable and manageable through the use of security automation capabilities are in scope. These and other types of use-cases may be facilitated by the techniques included in this Recommendation. Neither the included techniques nor the exchange of related cybersecurity information are mandated by this Recommendation, and other techniques may be appropriate.

7 Structured cybersecurity information exchange techniques

For the exchange of cybersecurity information to occur between any two entities, the exchange must be structured and described in some consistent manner that is understood by both of those entities. The goal of CYBEX is to make it easier to share cybersecurity information that includes "common enumerations," that is, ordered lists of well-established information values for the same data type. Common enumeration allows distributed databases and other capabilities to be linked together, and facilitates cybersecurity-related comparisons.

For the purposes of accomplishing these exchanges, cybersecurity information includes structured information or knowledge concerning:

- the "state" of equipment, software, or network-based systems as related to cybersecurity, especially vulnerabilities;

- forensics related to incidents or events;
- heuristics and signatures gained from experienced events;
- cybersecurity entities involved;
- specifications for the exchange of cybersecurity information, including modules, schemas, terms and conditions, and assigned numbers;
- the identities and assurance attributes of all cybersecurity information;
- implementation requirements, guidelines and practices.

As a means of describing at a general level the desired attributes of cybersecurity information exchange, the structured information capabilities are organized into six "clusters" of techniques for distinct cybersecurity information exchange groups. These are:

- weakness, vulnerability and state;
- event, incident, and heuristics;
- information exchange policy;
- identification, discovery, and query;
- identity assurance;
- exchange protocol.

These clusters are broad classifications, and capabilities in one cluster may actually be used in one or more other clusters, depending on the application.

Each of the clusters listed above is described in detail in the subclauses below. Each cluster description provides an overview of its role in CYBEX, and lists techniques for its realization. None of the identified techniques are intended to be prescriptive; rather, they simply illustrate techniques considered consistent with the purposes of the relevant cluster. The choice of treatment has primarily to do with the degree of specialization of the "owning" user community and the global benefits derived from importation.

The CYBEX techniques in this Recommendation identify an array of complementary techniques that enable and facilitate these and other instantiations.

The remainder of this clause and the associated Appendix I describe each cluster, including an overview of the role of each within CYBEX, and lists techniques for the realization of each cluster. The references are non-normative and further detailed in the Bibliography.

Implementers and users of the cluster techniques shall comply with all applicable national and regional laws, regulations and policies.

7.1 Weakness, vulnerability and state – exchange cluster

The enabling capabilities associated with the weakness, vulnerability, and state exchange cluster support the exchange of weakness and vulnerability information and assessment of the state of systems and applications.

Table I.1 provides a list of enabling capabilities that are representative of the types that can facilitate the support of exchange of weakness, vulnerability, and state information.

7.2 Event, incident, and heuristics – exchange cluster

The enabling capabilities associated with the event, incident, and heuristics exchange cluster support the exchange of information pertaining to observed events, incidents, or heuristics.

Table I.2 provides a list of enabling capabilities that are representative of the types that can facilitate the exchange of observed event, incident or heuristic information in a structured fashion among CIRTs and others. This exchanged information may be used to create comprehensive responses to attacks as well as reduce existing weaknesses and vulnerabilities.

7.3 Information exchange policy – exchange cluster

The enabling capabilities associated with the information policy exchange cluster supports the sharing and use of cybersecurity information between entities concerning the terms and conditions associated with the information being shared. This understanding may be bound to the specific information being shared, or to the broad class of information to which it belongs, or be associated with the entities involved. To the extent it is necessary under the circumstances, it is desirable to provide notice of these policies to the entities involved. This notice may take many forms, and be conveyed together with the information or independently provided through a query-response mechanism.

Table I.3 provides a list of enabling capabilities that are representative of the types that can facilitate the exchange of policy information between cybersecurity entities. Note that requirements and protocols for policy exchange continue to emerge within information security exchange forums, and care should be taken to ensure their proper implementation.

7.4 Identification, discovery, and query cluster

The enabling capabilities associated with the identification, discovery, and query cluster supports identification, discovery and query processes.

Common interests exist among cybersecurity communities regarding cybersecurity identifiers and their creation, administration, discovery, verification, and use. Some of those interests include:

- Enhancing the value of the cybersecurity information by enabling widespread exchange of the related event information and analysis of events over long periods of time.
- Enhancing the security of cybersecurity information exchanges by enabling identifier information to be obtained for verification and the related policies to be known.
- Enhancing the flexibility of cybersecurity information exchanges by enabling new or additional information associated with the message to be obtained, e.g., information status.

Different cybersecurity organizations may desire to implement common cybersecurity protocols for the capture and exchange of system state, vulnerability, incident forensics, and incident heuristics information in operational applications. As this information is becoming available from many different sources, implementers should harmonize how they identify cybersecurity organizations, trust and information exchange policies, and the information itself that is exchanged or distributed. That a globally unique identifier used for global cybersecurity information exchange may exist necessarily implies that it has the following characteristics:

- simplicity, usability, flexibility, extensibility, scalability, and deployability;
- distributed management of diverse identifier schemes;
- long-term reliability of identifier registrars, and the availability of high-performance tools for discovering information associated with any given identifier.

Table I.4 provides a list of enabling capabilities that are representative of the types that can facilitate identification of cybersecurity organizations, and discovering and querying for cybersecurity information processes.