International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1500

Amendment 11

(03/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Overview of cybersecurity

---

Overview of cybersecurity information exchange

Amendment 11: Revised structured cybersecurity information exchange techniques

Recommendation ITU-T X.1500 (2011) – Amendment 11

--`,,```,,,,````-`-`,,`,,`,`,,`---

Documents
Document Sharing Hub

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Full document details: ITU-T X.1500 AMD 11 2017

Licensee=/, User=,
Not for Resale,

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
PKI related Recommendations	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1379
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.

Documents
Document Sharing Hub

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1500 AMD 11 2017

Recommendation ITU-T X.1500

Overview of cybersecurity information exchange

Amendment 11

Revised structured cybersecurity information exchange techniques

Summary

Amendment 11 to Recommendation ITU-T X.1500 (2011) 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

Keywords

Cybersecurity information exchange, CYBEX, security, trust and assurance.

* 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.

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1500 AMD 11 2017

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 2017

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

Documents
Document Sharing Hub
Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1500 AMD 11 2017

Recommendation ITU-T X.1500

Overview of cybersecurity information exchange

Amendment 11

Revised structured cybersecurity information exchange techniques

1) *Replace Appendix I with the appendix below*.

Appendix I

Structured cybersecurity information exchange techniques

(This appendix does not form an integral part of this Recommendation.)

Table I.1 – Techniques in the weakness, vulnerability and state exchange cluster

Technique	Description	References
Common vulnerabilities and exposures (CVE)	Common vulnerabilities and exposures is a method for identifying and exchanging information security vulnerabilities and exposures, and provides common identifiers for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories and services) with this "common enumeration". CVE is designed to allow vulnerability databases and other resources to be linked together, and to facilitate the comparison of security tools and services. As such, CVE does not contain information such as risk, impact, fix information, or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description and references to related vulnerability reports and advisories. The intention of CVE is to be comprehensive with respect to all publicly known vulnerabilities and exposures. While CVE is designed to contain mature information, the primary focus is on identifying vulnerabilities and exposures that are detected by security tools, as well as identifying any new problems that become public, and then addressing any older security problems that require validation.	[b-ITU-T X.1520]
Common vulnerability scoring system (CVSS)	The common vulnerability scoring system process provides for an open framework for communicating the characteristics and impacts of ICT vulnerabilities. CVSS consists of three groups: base, temporal and environmental. Each group produces a numeric score ranging from 0 to 10, and a vector, a compressed textual representation that reflects the values used to derive the score. The base group represents the intrinsic qualities of a vulnerability. The temporal group reflects the characteristics of a vulnerability that change over time. The environmental group represents the characteristics of a vulnerability that are unique to the environment of the user. CVSS enables ICT managers,	[b-ITU-T X.1521]

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Full document details: ITU-T X.1500 AMD 11 2017
Licensee=/, User=,
Not for Resale,
Documents
Document Sharing Hub

Table I.1 – Techniques in the weakness, vulnerability and state exchange cluster

Technique	Description	References
	vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting a common language of scoring ICT vulnerabilities.	
Common weakness enumeration (CWE)	Common weakness enumeration is a process for identifying and exchanging unified, measurable sets of software weaknesses. CWE enables more effective discussion, description, selection and use of software security tools and services that can find these weaknesses in source code and operational systems. It also provides for better understanding and management of software weaknesses related to architecture and design. CWE implementations are compiled and updated by a diverse, international group of experts from business, academia and government agencies, ensuring breadth and depth of content. CWE provides standardized terminology, allows service providers to inform users of specific potential weaknesses and proposed resolutions, and allows software buyers to compare similar products offered by multiple vendors.	[b-ITU-T X.1524]
Common weakness scoring system (CWSS)	The common weakness scoring system (CWSS) provides an open framework for communicating the characteristics and impacts of information and communication technology (ICT) weaknesses during development of software capabilities. The goal of CWSS is to enable ICT software developers, managers, testers, security vendors and service suppliers, buyers, application vendors and researchers to speak from a common language of scoring ICT weaknesses that could manifest as vulnerabilities when the software is used.	[b-ITU-T X.1525]
Critical Security Controls for Effective Cyber Defence (CSC)	The Critical Security Controls and associated compendiums describe a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks. The measures reflect the combined knowledge of actual attacks and effective defences	[b-CSC]
Open vulnerability and assessment language (OVAL)	The language for the open definition of vulnerabilities and for the assessment of a system state (also known as Open vulnerability and assessment language) is an international specification effort to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode endpoint details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of endpoints for testing, analysing the endpoint for the presence of the specified machine state (vulnerability, configuration, patch state, etc.), and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language. OVAL schemas written in XML have been developed to serve as the framework and vocabulary of the OVAL language. These schemas correspond to the three steps of the assessment	[b-ITU-T X.1526]

Copyright International Telecommunication Union/ITU Telcommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS
Licensee=/, User=,
Not for Resale,
Full document details: ITU-T X.1500 AMD 11 2017