

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1209

(12/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Capabilities and their context scenarios for cybersecurity information sharing and exchange

Recommendation ITU-T X.1209

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.1209

Capabilities and their context scenarios for cybersecurity information sharing and exchange

Summary

Recommendation ITU-T X.1209 describes high level scenarios and supporting capabilities for cybersecurity information sharing and exchange. This Recommendation provides capabilities important for supporting interoperability between applications for the sharing and exchange of cybersecurity information.

Capabilities are described which may be used in scenarios/situations supporting previously independent acting entities to participate in various coordinated efforts, such as the prevention or halting of targeted behaviour or the coordination of analysis and determination efforts.

The goal of the capabilities listed and described is to support more efficient and effective security operations by supporting the interoperable sharing and exchange of information between trusted parties working together to monitor, maintain and generally manage the security of systems and networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1209	2010-12-17	17

Keywords

Cybersecurity information, information exchange, information sharing.

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 2011

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

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	Introduction	2
7	Capabilities scenarios	2
7.1	General scenario	3
7.2	Operational policies.....	3
7.3	Regional policies	3
7.4	Exchange format.....	3
7.5	Privacy protection.....	4
7.6	Access granularity	4
7.7	Source verification.....	4
7.8	Multichannel distribution	5
7.9	Backwards compatibility	5
8	Capabilities	5
8.1	Format/encoding capabilities.....	5
8.2	Transfer/exchange capabilities	5
8.3	Security capabilities.....	6
8.4	Policy capabilities.....	6
8.5	Vendor neutrality capabilities.....	6
9	Applicability of capabilities.....	7
9.1	Format/encoding capabilities.....	7
9.2	Transfer/exchange capabilities	7
9.3	Security capabilities.....	7
9.4	Policy capabilities.....	7
9.5	Vendor neutrality capabilities.....	7
	Appendix I – Introduction to cybersecurity information sharing and exchange.....	8
	Appendix II – Related activities.....	12
	II.1 Common security information.....	12
	II.2 Novel security information.....	12
	II.3 Related activities to share security information	13
	Appendix III – Related activities	14
	Bibliography.....	15

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

Recommendation ITU-T X.1209

Capabilities and their context scenarios for cybersecurity information sharing and exchange

1 Scope

This Recommendation provides capabilities important for supporting interoperability between applications for the sharing and exchange of cybersecurity information. Accordingly, clause 7 contains descriptions of high level use capabilities scenarios which are used to set the context for the capabilities found in clause 8. To further clarify the purpose of the capabilities, clause 9 contains descriptions of which capabilities are more likely to be needed in which situations.

The intended audience for this Recommendation are those involved in authorized security operations.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 cybersecurity [b-ITU-T X.1205]: 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 the following:

- availability
- integrity, which may include authenticity and non-repudiation
- confidentiality.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 cybersecurity information: Structured information or knowledge which may include but is not limited to: the "state" of equipment, software or network systems; forensics related to incidents or events; parties implementing the information exchange capabilities in terms of cybersecurity; specifications for the exchange of information in terms of cybersecurity, including modules, schemas and assigned numbers; identities and trust attributes for all of the preceding and implementation requirements, guidelines and practices.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDoS	Distributed Denial of Service
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol (HTTP over SSL)
IPS	Intrusion Prevention System

5 Conventions

None.

6 Introduction

Cyber attacks involving viruses, worms, etc., are shortening their propagation speeds through networks using various techniques, ever evolving into more threatening forms. Various kinds of security solutions including anti-virus, spyware detection, firewall, virtual private network, intrusion detection and protection, etc., have been developed, so that security incidents due to such threatening attacks may be countered by a rapid response system through the taking of effective countermeasures.

Security managers' most common line of defense against exploits, viruses, worms and botnets has primarily been in the form of various discussion forums that many security professionals subscribe to. Usually within a couple of days to a week, holes are plugged, vulnerabilities patched and things can return back to normal.

Unfortunately, the exploitation of vulnerabilities by viruses, worms and botnets could propagate across networks very quickly. Within seconds, entire networks can be significantly affected.

The exchange of cybersecurity information within a given organization may be accomplished quickly. However, the exchange of a broad range of information between organizations is not well supported using current methods. The lack of effective communication means may turn each organization into an island of security.

Therefore, it is important to share cybersecurity information among many organizations, including telecom operators, telecom service providers and centers of security operations. To make such an information exchange possible, what is needed are:

- trusted and secure methods for participants to exchange information more quickly,
- methods to ensure the protection of privacy.

This Recommendation provides considered scenarios and supporting capabilities for the exchange of cybersecurity information among participants in a secure, trusted and reliable manner.

7 Capabilities scenarios

To be able to put the capabilities listed in clause 8 into a proper context for the understanding of this Recommendation, high level usage scenarios are presented in five different settings to help explain the five logical groups of capabilities which follow.