

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 20
(04/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

**ITU-T X.1205 – Supplement on framework of
security information sharing negotiation**

ITU-T X-series Recommendations – Supplement 20

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.

Supplement 20 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on framework of security information sharing negotiation

Summary

This Supplement to Recommendation ITU-T X.1205 provides a framework for negotiating agreement on security information sharing between cybersecurity entities such as information requester and information provider. This Supplement defines functional capabilities and a reference model for security information sharing negotiation, conceptual data modelling of security information sharing agreement (SSA), security information sharing policy (SSP) and the SSA negotiation process.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 20	2013-04-26	17

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 publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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 2013

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 Supplement	1
4	Abbreviations and acronyms	1
5	Conventions	2
6	Introduction	2
	6.1 Concept of security information sharing negotiation	2
	6.2 Relationship with other CYBEX Recommendations	3
7	Functional capabilities for security information sharing negotiation	4
	7.1 Negotiation capabilities	4
	7.2 Agreement capabilities	4
	7.3 Security capabilities.....	4
8	Reference model of security information negotiation	5
9	Life cycle and data model of SSA	6
	9.1 Life cycle of SSA	6
	9.2 Structure of SSA.....	7
10	Process of SSA negotiation	8
	10.1 SSA negotiating messages.....	8
	10.2 SSA negotiating scenarios.....	9
	Appendix I – The example of security information sharing negotiation	14
	I.1 Negotiation between the security management server and security agent	14
	Bibliography.....	16

Supplement 20 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on framework of security information sharing negotiation

1 Scope

This Supplement provides a framework for security information sharing negotiation to develop cybersecurity information exchange contracts between entities. The scope of the negotiation framework includes the functional capabilities and reference model for security information sharing negotiation, conceptual data modelling of a security information sharing agreement (SSA), security information sharing policy (SSP) and a SSA negotiation process.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 cybersecurity [b-ITU-T X.1205]: Cybersecurity is 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 authenticity and non-repudiation) and Confidentiality.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 security information sharing agreement (SSA): A service contract on security information sharing between entities. SSA is translated into a security information sharing policy (SSP) to be applied to the corresponding cybersecurity entities.

3.2.2 security information sharing policy (SSP): A policy for cybersecurity entities to observe when sharing security information with each other. The SSP is made based on an SSA.

3.2.3 SSA negotiation: Interaction for entities to negotiate SSA before starting cybersecurity information sharing.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

CYBEX	Cybersecurity Information Exchange
EMS	Enterprise Management System
IDMEF	Intrusion Detection Message Exchange Format
IODEF	Incident Object Description and Exchange Format

SSA	Security information Sharing Agreement
SSP	Security information Sharing Policy
TMS	Threat Management System

5 Conventions

None.

6 Introduction

6.1 Concept of security information sharing negotiation

[b-ITU-T X.1500] defines a cybersecurity information exchange (CYBEX) model and techniques that can be used to facilitate the exchange of cybersecurity information between entities. An entity in the context of this Supplement is an information requester or information provider. Entities may be an independent organization or person, and as such, they have individual requirements on cybersecurity information sharing.

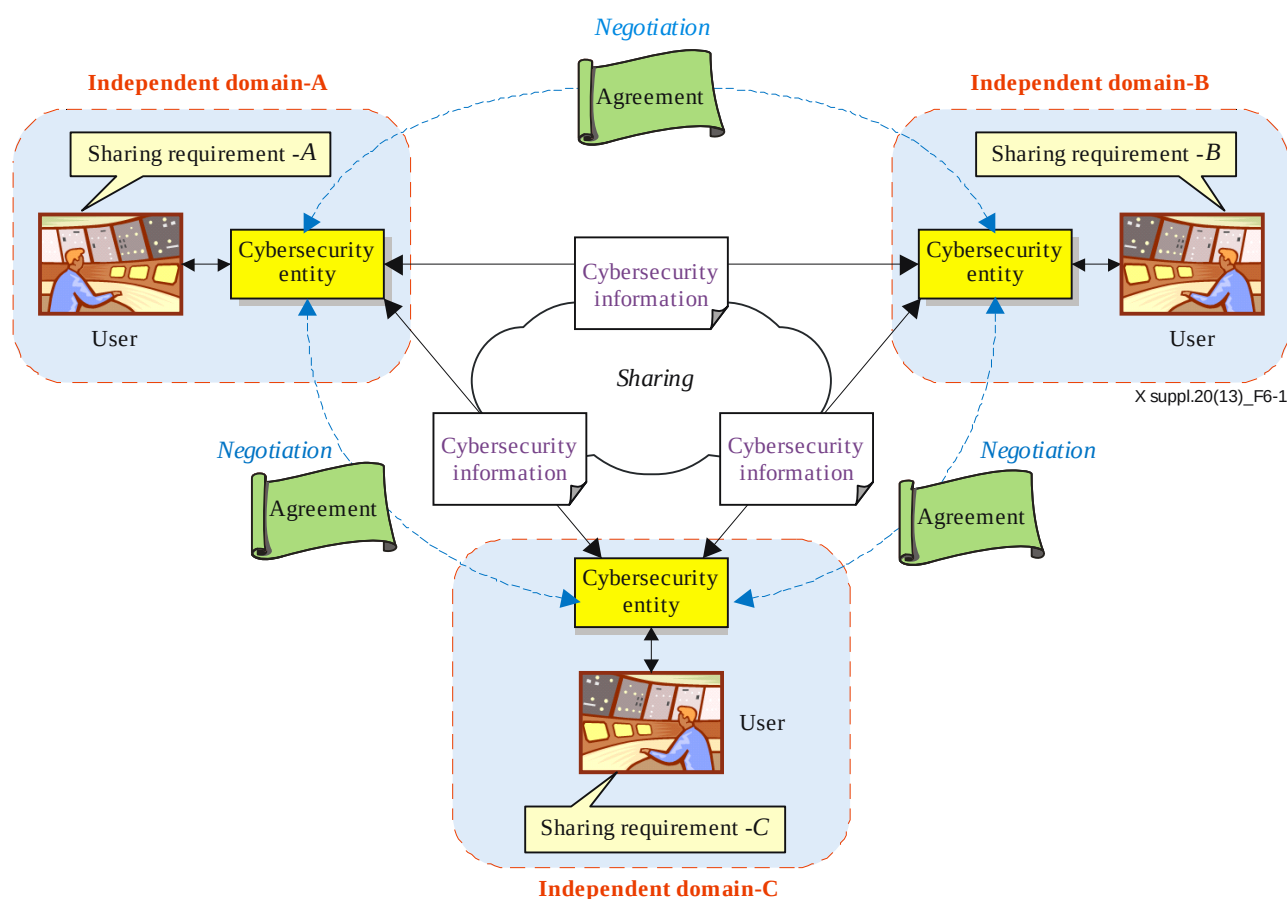


Figure 6-1 – Basic concept of security information sharing negotiation

Examples of requirements and restrictions on cybersecurity information sharing include:

- when to start and stop cybersecurity information sharing;
- what cybersecurity information to share (e.g., DoS detection log, botnet alert, black list, computer security incident, network traffic);
- what sharing level is appropriate (e.g., raw data sharing or statistical data sharing);