

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1039

(10/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Network security

Technical security measures for implementation of ITU-T X.805 security dimensions

Recommendation ITU-T X.1039

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	
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
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.1039

Technical security measures for implementation of ITU-T X.805 security dimensions

Summary

Many organizations in developing countries as well as developed countries may have difficulties in implementing the high-level dimensions described in Recommendation ITU-T X.805. Recommendation ITU-T X.1039 is aimed at providing a set of security measures to implement the high-level dimensions. It also provides technical implementation guidance for security measures that can be used to improve organizations' security response capabilities. A set of security measures described in this Recommendation could assist organizations in managing information security risks and implementing technical dimensions. The audience of this Recommendation includes, but is not limited to, those individuals responsible for implementing an organization's information security dimensions.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1039	2016-10-14	17	11.1002/1000/13059

Keywords

Security dimension, security measures, technical implementation guidance.

* 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 2017

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	Overview of information security measures.....	3
7	Information security measures.....	4
	7.1 Access control	4
	7.2 Authentication	4
	7.3 Non-repudiation.....	5
	7.4 Data confidentiality	6
	7.5 Communication security.....	6
	7.6 Data integrity.....	8
	7.7 Availability	8
	7.8 Privacy.....	9
	Annex A – Additional technical implementation guidance	10
	A.1 Secure configuration.....	10
	A.2 Malware protection.....	10
	A.3 Patch management.....	11
	A.4 Vulnerability management	11
	A.5 Information security incidents management	11
	A.6 System development security	12
	A.7 Authentication for information systems and applications	12
	A.8 Data leakage prevention	13
	A.9 Operations security	13
	A.10 Backup and disaster recovery	13
	A.11 Desktop PC and mobile device protection	13
	Appendix I – Organizational implementation guidance	15
	I.1 Information security policies	15
	I.2 Organization of information security.....	15
	I.3 Human resources security	16
	I.4 Asset management	17
	I.5 Physical and environment security	17
	I.6 Supplier relationship	18
	Appendix II – Level of security assurance.....	19

	Page
II.1 Level of assurance for entity authentication [b-ITU-T X.1254]	19
II.2 Level of security assurance	19
Appendix III – Guidance on assigning specific level of security assurance from the final index	20
III.1 Methodology for level of security assurance.....	20
Appendix IV – SGSN specific implementation guideline	21
IV.1 Overview	21
IV.2 Access control dimension for module 1	21
IV.3 Availability dimension for module 1.....	21
IV.4 Non repudiation dimension for module 1.....	22
IV.5 Authentication dimension for module 1	22
IV.6 Data integrity dimension for module.....	22
IV.7 Privacy and data confidentiality dimension for module 1	22
IV.8 Communication security dimension for module 1	22
Bibliography.....	23

iv

Recommendation ITU-T X.1039

Technical security measures for implementation of ITU-T X.805 security dimensions

1 Scope

This Recommendation provides technical security measures for the implementation of [ITU-T X.805] security dimensions, which includes access control, communication security, authentications, and data confidentiality. It also provides examples for applying the set of technical security measures to the organizations with practical levels of information security dimensions, etc. in the appendices. It is not intended to cover all security measures, but to focus on several technical issues.

This Recommendation is applicable to all type of telecommunication organizations, including those in the developing countries.

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.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authentication [b-ITU-T X.1254]: Provision of assurance in the identity of an entity.

3.1.3 authorization [b-ITU-T X.1254]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.6 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.7 firewall [b-ISO/IEC 27033-1]: Type of security barrier placed between network environments – consisting of a dedicated device or a composite of several components and techniques – through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass.

3.1.8 intrusion detection [b-ISO/IEC 27039]: Formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns, as well as what, how, and which vulnerability has been exploited to include how and when it occurred.

3.1.9 intrusion detection system [b-ISO/IEC 27039]: Information systems used to identify that an intrusion has been attempted, is occurring, or has occurred.

3.1.10 intrusion prevention system [b-ISO/IEC 27039]: Variant on intrusion detection systems that are specifically designed to provide an active response capability.

3.1.11 privacy [b-ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

NOTE – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

3.1.12 security gateway [b-ISO/IEC 27033-1]: Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy.

3.1.13 repudiation [b-ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.14 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2FA	Two-Factor Authentication
ACL	Access Control Lists
AES	Advanced Encryption Standard
ATM	Automatic Teller Machine
CEO	Chief Executive Officer
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
FTP	File Transfer Protocol
GGSN	Gateway General packet radio service (GPRS) Support Node
GPRS	General Packet Radio Service
HIDS	Host Based Intrusion Detection System
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
ICT	Information Communication Technology
IDPS	Intrusion Detection and Prevention System

IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security
IPSG	IP Source Guard
ISP	Internet Service Provider
MFA	Multi-Factor Authentication
NIDS	Network Based Intrusion System
OS	Operating system
OSI	Open System Interconnection
PC	Personal Computer
PII	Personally Identifiable Information
PIN	Personal Identification Number
RPC	Remote Procedure Call
SFA	Single Factor Authentication
SGSN	Serving GPRS Support Node
SMB	Server Message Block
SNMP	Simple Network Management Protocol
TFA	Three-Factor Authentication
TLS	Transport Layer Security
VPN	Virtual Private Network

5 Conventions

None.

6 Overview of information security measures

A security measures is a means of managing risk, and includes policies, procedures, guidelines, practices or organisational structures, which can be of an administrative, technical, management, or legal nature.

A security dimension is a set of security measures designed to address a particular aspect of the network security. The security dimensions, defined in [ITU-T X.805] are:

- access control;
- authentication;
- non-repudiation;
- data confidentiality;
- communication security;
- data integrity;
- availability; and
- privacy.

A set of technical implementation guidance for each dimension should be defined and implemented by organizations.

This Recommendation presents a technical implementation guideline, which provides a set of security measures for each dimension, for mitigating the most common threats.

Deploying these security measures can assist an organisation in protecting against the most common forms of cyber-attack emanating from the external network.

Organisations implementing these security measures can benefit by gaining confidence that basic technical security measures are in place and that important steps are being taken to protect its information and system. The technical implementation guidance can be used to:

- improve organizations' security capabilities and posture;
- allow organizations to effectively and consistently evaluate security capabilities;
- share knowledge, best practices, and relevant documents across organizations as a means to improve security capabilities; and
- allow organizations to prioritize security measures and their associated activities and investment resources to improve security.

7 Information security measures

7.1 Access control

Access control protects against unauthorized use of network resources. User accounts, particularly those with special access privileges (e.g., administrative accounts) should be assigned only to authorized individuals, managed effectively and provide the minimum level of access to applications, computers and networks. User accounts should be managed through robust access control. The following information security measures should be considered regarding access control:

- Organizations should create user account according to a provisioning and approval process.
- Organization should allow special access privileges to a limited number of authorized individuals.
- Organizations should document details about special access privileges (e.g., the individual and purpose), keep them in a secure location and review them on a regular basis (e.g., quarterly).
- Organizations should use administrative accounts to perform authorized administrative activities, and should not grant access to the Internet.
- Organization should change password for administrative accounts on a regular basis (e.g., at least every 60 days).
- Organization should allow each user to be authenticated using a unique username and strong password before being granted access to applications, computers and network devices.
- Organizations should remove or disable user accounts and special access privileges when no longer required (e.g., when an individual changes role or leaves the organization) or after a pre-defined period of inactivity (e.g., 3 months).

7.2 Authentication

The authentication serves to confirm the identities of communicating entities. There are three types of authentication factors:

- knowledge factor ("something only a user knows"), such as passwords;
- possession factor ("something only a user has"), such as automatic teller machine (ATM) cards; and