International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1311

Corrigendum 1

(11/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Ubiquitous sensor network security

---

Information technology – Security framework for ubiquitous sensor networks

Technical Corrigendum 1

Recommendation ITU-T X.1311 (2011) – Technical Corrigendum 1

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.

INTERNATIONAL STANDARD ISO/IEC 29180
RECOMMENDATION ITU-T X.1311

Information technology – Security framework for ubiquitous sensor networks

Technical Corrigendum 1

Summary

This Technical Corrigendum 1 to Rec. ITU-T X.1311 (2011) | ISO/IEC 29180:2012 corrects references to withdrawn standards.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1311	2011-02-13	17	11.1002/1000/11058
1.1	ITU-T X.1311 (2011) Cor. 1	2014-11-29	17	11.1002/1000/12344

* 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 2015

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	Clause 2.2	1
2	Clause 2.3	1
3	Clause 6	1
4	Clause 7.1.1	1
5	Clause 7.1.2	1
6	Clause 7.2	2
7	Clause 8	2
8	Clause 9.1.1	2
9	Clause 9.2	2
10	Clause 10.7	2

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Security framework for ubiquitous sensor networks

Technical Corrigendum 1

Conventions used in this corrigendum: Original, unchanged, text is in normal font. Deleted text is struck-through, thus: ~~deleted text~~. Inserted text is underlined, thus: inserted text.

1 Clause 2.2

Modify clause 2.2 as follows:

2.2 Paired Recommendations | International Standards equivalent in technical content

– Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

ISO/IEC 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

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

~~– ISO/IEC 18028-2:2006, *Information technology – Security techniques – IT network security – Part 2: Network security architecture.*~~

2 Clause 2.3

Add the following reference to clause 2.3:

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

3 Clause 6

Modify the 10th paragraph as follows:

There are three components in the SN: the application server communicating with the sink node; the sink node called the base station, which interfaces the sensor network and the application server, and the collection of sensor nodes using wireless communication to communicate with each other. The sink may communicate with the application server via the Internet or a satellite. Security architecture in the IP-based network is very similar to that in Rec. ITU-T X.805~~ | ISO/IEC 18028-2~~. Therefore, this Recommendation | International Standard focuses on the security of the wireless sensor network (SN) consisting of a set of sensor nodes using wireless transmission.

4 Clause 7.1.1

Modify the first sentence of the first paragraph as follows:

Rec. ITU-T X.800 | ISO/IEC 7498-2 and Rec. ITU-T X.805 ~~| ISO/IEC 18028-2~~cite the following security threats to the networks (note that these are also security threats applicable to the SN):

5 Clause 7.1.2

Modify the first sentence of the first paragraph as follows:

Rec. ITU-T X.800 | ISO/IEC 7498-2 and Rec. ITU-T X.805 ~~| ISO/IEC 18028-2~~ identify five threats that are applicable to routing-related message exchange in the SN. In addition to these, seven threats are identified in (see Karlrof *et al.* in the Bibliography) with regard to the routing messages exchanged between sensor nodes.

6 Clause 7.2

Modify the first sentence of the first paragraph as follows:

The threat models developed in Rec. ITU-T X.805~~+ISO/IEC 18028-2~~ can be applied to the IP network. Therefore, refer to Rec. ITU-T X.805~~+ISO/IEC 18028-2~~ for the details of those threats.

7 Clause 8

Modify the second paragraph as follows:

To counter the aforesaid threats in both the SN and the IP networks, the following security dimensions in Rec. ITU-T X.805~~+ISO/IEC 18028-2~~ are applicable:

8 Clause 9.1.1

Modify the first paragraph as follows:

Table 1 lists the security requirements and describes the relationship between the security dimensions and the security threats identified in Rec. ITU-T X.805~~+ISO/IEC 18028-2~~. The letter "Y" in a cell formed by the intersection of the table's columns and rows suggests that a particular security threat is opposed by the corresponding security dimension.

9 Clause 9.2

Modify the first paragraph as follows:

The security threats and security dimensions developed in Rec. ITU-T X.805 ~~+ISO/IEC 18028-2~~ can directly be applied to a secure message exchange through the IP network. Therefore, refer to Rec. ITU-T X.805 ~~+ISO/IEC 18028-2~~ for related details.

10 Clause 10.7

Modify the first paragraph as follows:

The IP network security technologies in Rec. ITU-T X.805 ~~+ISO/IEC 18028-2~~ can directly be applied to secure message exchange through the IP network. Therefore, related details can be omitted.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015