

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1361

(09/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Internet of things
(IoT) security

Security framework for the Internet of things based on the gateway model

Recommendation ITU-T X.1361

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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.1361

Security framework for the Internet of things based on the gateway model

Summary

Recommendation ITU-T X.1361 describes a security framework for the Internet of things (IoT) using security gateways. The IoT is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

This Recommendation analyses security threats and challenges in an IoT environment, and describes capabilities that could address and mitigate these threats and challenges. A framework methodology is provided for determining which security capabilities are required for mitigating and addressing these threats and challenges for the IoT.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1361	2018-09-07	17	11.1002/1000/13607

Keywords

Internet of things, security framework, security requirements.

* 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 2019

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	Terms and Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	4
5	Conventions	4
6	Overview.....	4
7	Functional architecture and framework	4
8	Security threats to the Internet of things.....	6
	8.1 Security threats to IoT sensors/devices	6
	8.2 Security threats to IoT gateways	6
	8.3 Security threats to the network	7
	8.4 Security threats to platform/services	7
9	Requirements for Internet of things	8
10	Security capabilities for the Internet of things.....	8
	10.1 Overview	8
	10.2 Security capabilities for sensors/devices	9
	10.3 Security capabilities for gateways	10
	10.4 Security capabilities for the network.....	11
	10.5 Security capabilities for platforms/services.....	11
	Annex A – Security and privacy requirements described in ITU-T Y.4100/Y.2066	12
	A.1 Communication security.....	12
	A.2 Data management security	12
	A.3 Service provision security	12
	A.4 Integration of security policies and techniques	12
	A.5 Mutual authentication and authorization	12
	A.6 Security audit.....	12
	Appendix I – Security and privacy capabilities described in ITU-T Y.4401/Y.2068	13
	I.1 Communication security capability	13
	I.2 Data management security capability.....	13
	I.3 Service provision security capability.....	13
	I.4 Security integration capability.....	13
	I.5 Mutual authentication and authorization capability	13
	I.6 Security audit capability	13
	Appendix II – Implementation view of the IoT functional framework building over the next generation network functional architecture in ITU-T Y.4401/Y.2068.....	14

	Page
Bibliography.....	15

Recommendation ITU-T X.1361

Security framework for the Internet of things based on the gateway model

1 Scope

This Recommendation describes a security framework for the Internet of Things (IoT) using security gateways.

This Recommendation analyses security threats and challenges in the IoT environment and describes capabilities that address and mitigate these security threats and challenges. A framework methodology is provided for determining which security capabilities are required for mitigating and addressing security threats and challenges for the IoT.

The focus of this Recommendation is on IoT security capabilities using security gateways and considers the reference model described in [b-ITU-T Y.4401] with a focus on technical, not management aspects.

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 Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

3 Terms and Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 attack [b-ISO13491-1]: Attempt by an adversary on the device to obtain or modify sensitive information or a service they are not authorized to obtain or modify.

3.1.2 authentication [b-NIST SP 800-53]: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.3 capability [b-ISO 19440]: Construct that represents the collection of capability characteristics (expressed as capability attributes) of either a Resource (its provided Capability) or an Enterprise Activity (its required Capability).

NOTE – Capabilities can be aggregated.

3.1.4 context [b-ITU-T X.1252]: An environment with defined boundary conditions in which entities exist and interact.

3.1.5 cryptographic algorithm [b-ISO/IEC 19790]: Well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output.

3.1.6 cryptographic-quality random-number [b-ITU-T X.667]: A random number or pseudo-random number generated by a mechanism, which ensures sufficient spread of repeatedly-generated values to be acceptable for use in cryptographic work (and is used in such work).

3.1.7 cryptography [b-ITU-T X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

NOTE – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

3.1.8 cryptosystem [b-ISO 11568-1]: Set of cryptographic primitives used to provide information security services.

3.1.9 device [b-ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.10 identity management [b-ITU-T X.1250]: A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- assurance of identity information (e.g., identifiers, credentials, attributes);
- assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects); and
- supporting business and security applications.

3.1.11 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.12 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.

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

3.1.14 intrusion prevention [b-ISO/IEC 27033-1]: Formal process of actively responding to prevent intrusions.

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

3.1.16 key management [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.17 lightweight cryptography [b-ISO/IEC 29192-1]: cryptography tailored for implementation in constrained environments.

3.1.18 malware [b-ISO/IEC 27033-1]: Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.

NOTE – Viruses and Trojan horses are examples of malware.

3.1.19 network monitoring [b-ISO/IEC 27033-1]: Process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis.