

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1362

(03/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

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

Simple encryption procedure for Internet of things (IoT) environments

Recommendation ITU-T X.1362



International
Telecommunication
Union

Documents
Document Sharing Hub

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
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1379
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.1362

Simple encryption procedure for Internet of things (IoT) environments

Summary

It is considered that the Internet of things (IoT) is one of the most important areas for future standardization. From the ITU-T perspective, IoT is defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things.

In certain IoT environments, especially for IoT devices, there is a real-time processing requirement where tasks are processed within a certain period of time. To ensure data confidentiality and integrity protection, one of the most basic countermeasures is the application of data encryption/authentication algorithms. The problem with the standard applications of data encryption/authentication algorithms is that this requirement could not be met.

Recommendation ITU-T X.1362 specifies encryption with associated mask data (EAMD) for the Internet of things devices. It describes EAMD and how it provides a set of security services for traffic using EADM.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1362	2017-03-30	17	11.1002/1000/13196

Keywords

Application of data encryption/authentication algorithms, encryption with associated mask data EAMD, IoT devices, IoT environments, real-time processing requirement.

* 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/11.1002/1000/1830-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	2
6 Introduction of encryption with associated mask data (EAMD)	3
6.1 Specification of the EAMD procedure	3
6.2 Mask for extracting target data for encryption with associated mask data	5
7 Encrypt with associated mask data	5
7.1 Security association with mask (SAM)	6
7.2 Packet format of EAMD security payload (EAMDSP)	7
7.3 Packet processing	8
8 EAMD employing an authenticated encryption algorithm.....	9
8.1 Security association with mask (SAM)	9
8.2 Packet format of EAMD security payload (EAMDSP)	9
8.3 Packet processing	10
9 Guidance and limitation.....	12
9.1 Guidance on SAM establishment	12
9.2 Guidance of the proper usage of initialization vectors and nonces	13
9.3 Limitation of the use of EAMD.....	13
Annex A – Bindings to existing protocols	14
A.1 Binding to the IP security (IPSec) ESP protocol IETF RFC 4303.....	14
Bibliography.....	18

Introduction

It is considered that the Internet of things (IoT) is one of the most important areas for future standardization. From the ITU-T perspective, IoT is defined as 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 in [b-ITU-T Y.2060].

Ubiquitous sensor networks (USNs) appears to be one of the most relevant areas of IoT. USNs are networks of intelligent sensor nodes that could be deployed "anywhere, anytime, by anyone and anything". We consider that security techniques for ubiquitous sensor networks are effective in IoT because USN has many affinities with IoT in the sense that it deals with devices such as sensing and actuating devices. With respect to USN security, Recommendations such as security framework [b-ITU-T X.1311], middleware security guidelines [b-ITU-T X.1312], and security requirements for wireless sensor network routing [b-ITU-T X.1313] are already published. However, there has been no investigation of Recommendations on data confidentiality and integrity protection techniques that offer security for the device layer in USN. Therefore, the device layer security is a missing area in USN as well as in IoT; hence, this area should be studied and discussed for future standardization.

On the other hand, in certain IoT environments, especially for IoT devices such as sensing and actuating devices which can be used in industrial control systems (ICSs), there is a real-time processing requirement where tasks are processed within a certain period of time. To ensure data confidentiality and integrity protection, one of the most basic countermeasures is the application of data encryption/authentication algorithms. The problem with the standard applications of data encryption/authentication algorithms is that this requirement could not be met. The other problem is to integrate different security levels. More specifically, within a communication packet, data at different positions require different levels of important consequential security. Therefore, encryption of data at the position that indicates a low security level is considered as an unnecessary processing overhead.

As mentioned above, to achieve the security for IoT environments, especially for IoT devices, a new application is required for data encryption/authentication algorithms that meets the real-time processing requirement and that integrates different security levels.

Therefore, the encryption with associated mask data that only encrypts data, within a communication packet, whose security level is high is required. The associated mask data is used to indicate the security levels of data at each position within a packet.

Recommendation ITU-T X.1362

Simple encryption procedure for Internet of things (IoT) environments

1 Scope

This Recommendation provides an encryption procedure for the Internet of things device security. The procedure is intended to be applied to IoT environments, especially for IoT devices which have the mandatory capabilities for communication and the optional capabilities for sensing, actuation, data storage and data processing. This Recommendation specifies encryption with associated mask data (EAMD) for the IoT environments. It describes EAMD and how it provides a set of security services for traffic using EAMD. Application examples are also provided in Annex A.

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.

- | | |
|-----------------|---|
| [IETF RFC 4303] | IETF RFC 4303 (2005), <i>IP Encapsulating Security Payload (ESP)</i> . |
| [IETF RFC 7296] | IETF RFC 7296 (2014), <i>Internet Key Exchange Protocol Version 2 (IKEv2)</i> . |
| [IETF RFC 7321] | IETF RFC 7321 (2014), <i>Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)</i> . |
| [ISO/IEC 10116] | ISO/IEC 10116:2006, <i>Information technology – Security techniques – Modes of operation for an n-bit block cipher</i> . |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 actuator [b-ITU-T Y.4109]: A device performing physical actions caused by an input signal.

NOTE – As examples, an actuator might act on the flow of a gas or liquid, on electricity distribution, or through a mechanical operation. Dimmers and relays are examples of actuators. The decision to activate the actuator may come from an MOC application, a human or MOC devices and gateways.

3.1.2 encapsulating security payload (ESP) [IETF RFC 4303]: An IPsec protocol that is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of fractional sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.

3.1.3 security parameters index (SPI) [b-IETF RFC 4301]: An arbitrary 32-bit value that is used by a receiver to identify the SA to which an incoming packet should be bound.

3.1.4 sensed data [b-ITU-T F.4104]: Data sensed by a sensor that is attached to a specific sensor node.

3.1.5 sensor [b-ITU-T Y.4105]: An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.6 sequence number [IETF RFC 4303]: This unsigned 32-bit field contains a counter value that increases by one for each packet sent, i.e., a per-SA packet sequence number.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 programmable controller: An electronic device to control actuators based on sensed data from sensors.

3.2.2 security association with mask (SAM): This is a security-protocol-specific set of parameters. SAM defines the services and mechanisms necessary to protect traffic by applying encryption with associated mask data (EAMD). SAM is referred to by its associated protocol, depending on the protocol layers such as transport layer or Internet protocol (IP) layer. Algorithm identifiers, modes, layer identifiers at which EAMD is applied and cryptographic keys can be included in these parameters.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CMAC	Cipher-based Message Authentication Code
EAMD	Encryption with Associated Mask Data
EAMDSP	EAMD Security Payload
ESP	Encapsulating Security Payload
ICS	Industrial Control System
IP	Internet Protocol
IPSec	IP Security
IoT	Internet of Things
IV	Initialization Vector
MAC	Message Authentication Code
SA	Security Association
SAM	Security Association with Mask
SAMD	SAM Database
SPI	Security Parameters Index
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USN	Ubiquitous Sensor Networks
XOR	Exclusive OR

5 Conventions

None.