

Recommendation

ITU-T X.1237 (09/2024)

SERIES X: Data networks, open system communications
and security

Cyberspace security – Countering spam

Technical security framework for personally identifiable information protection while countering mobile messaging spam

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
Cybersecurity	X.1200-X.1229
Countering spam	X.1230-X.1249
Identity management (IdM) and Authentication	X.1250-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1237

Technical security framework for personally identifiable information protection while countering mobile messaging spam

Summary

Driven by commercial interests (advertising), nowadays spam content is infiltrating every media to reach us. Operators, national organizations and software developers provide various sorts of technologies, platforms, services and apps to counter spam. However, the functionality and effectiveness of these approaches might be impaired if personally identifiable information (PII) protection is not considered in their design and implementations.

Recommendation ITU-T X.1237 takes PII protection into account in the design and implementation of mobile messaging anti-spam solutions. It provides an overview of mobile messaging anti-spam processes and proposes a technical security framework for PII protection while countering mobile messaging spam. Entity functions and processing procedures are also introduced.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1237	2024-09-06	17	11.1002/1000/15896

Keywords

Mobile messaging spam, personally identifiable information (PII), security framework.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

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
4 Abbreviations and acronyms	2
5 Conventions	2
6 Overview	2
7 Lifecycle of data in the process of countering mobile messaging spam	3
8 Structure for data protection while countering mobile messaging spam.....	4
8.1 Reference structure	4
8.2 Security capabilities for mobile message client	5
8.3 Security capabilities for reporting service	5
8.4 Security capabilities for AMgmt	6
8.5 Security capabilities for AMon	7
8.6 Security capabilities for APr	7
8.7 Security capabilities for interfaces	7
Bibliography.....	9

Introduction

Along with the development of telecommunication technologies, information technologies (IT) and smart terminal technologies, spam is also reaching us through all sorts of (new) media including short message service (SMS), multimedia message service (MMS), spam over instant messaging (SPIM), telemarketing calls and internet protocol (IP) based in-application advertising spam. In order to counter spam, new technologies are being developed, new regulations have been introduced and new apps have been developed. Still, we often find that the intended functionalities and effectiveness of these measures have failed to be fully realized. In rare circumstances, users even complain that spam gets worse with the application of these new measures.

This Recommendation takes personally identifiable information (PII) protection into account in the design and implementation of mobile messaging anti-spam solutions. It provides an overview of mobile messaging anti-spam processes and proposes a technical security framework for PII protection while countering mobile messaging spam. Entity functions and processing procedures are also introduced.