International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 25

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1231 – Supplement on guidance to assist in countering spam for mobile phone developers

ITU-T X-series Recommendations – Supplement 25

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.

Supplement 25 to ITU-T X-series Recommendations

ITU-T X.1231 – Supplement on guidance to assist in countering spam for mobile phone developers

Summary

As mobile phones are widely used nowadays, malicious attackers tend to send spam intentionally to mobile application users, which causes financial problems and creates privacy issues. This Supplement to Recommendation ITU-T X.1231 provides guidance to assist in countering spam for mobile phone developers. In addition, this Supplement describes the following elements:

– Security threats of mobile phones with application level aspects;

– Guidance to assist in countering spam for mobile phone developers.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X Suppl. 25	2016-03-23	17	11.1002/1000/12854

Keywords

Countering spam, mobile phone developers, security threats.

[*] 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 publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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/.

Table of Contents

Supplement 25 to ITU-T X-series Recommendations

ITU-T X.1231 – Supplement on guidance to assist in countering spam for mobile phone developers

1 Scope

This Supplement defines guidance to assist in countering spam for mobile phone developers. It investigates various application level aspects of security threats on mobile phones and provides guidance to assist in countering spam for mobile phone developers.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 short message service (SMS) [b-ITU-T X.1231]: Short message service refers to a kind of message service, which allows mobile phones, telephones and other short message entities to transfer and receive text messages through a device-named service centre implementing functions such as saving and delivering.

3.1.2 spam [b-ITU-T X.1242]: The electronic information delivered from senders to recipients by terminals such as computers, mobile phones, telephones, etc., which is usually unsolicited, unwanted, and harmful for recipients.

3.1.3 smartphone [b-ITU-T X-Sup.19]: A mobile phone with powerful computing capability, heterogeneous connectivity and advanced operating system providing a platform for third-party applications.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 message operator: Message operator is an entity that receives a short message service from a sender and transfers the requested message to the corresponding receiver.

3.2.2 message sender: Message sender is an entity that sends a short message service to the corresponding receiver through the message operator.

3.2.3 message receiver: Message receiver is an entity that receives a short message service from the corresponding sender through the message operator.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

ID	Identity
SMS	Short Message Service

5 Conventions

None.

6 Introduction

A mobile phone (i.e., smartphone) is commonly widely utilized as a convenient way of sending messages (e.g., short message service (SMS)). However, vulnerabilities of mobile phones also become a problem (e.g., data disclosure of mobile phone, financial harm). An attack to the mobile phone can cause an unwanted modification of the authorization code (e.g., injection of malicious codes), especially when installed applications within the mobile phones are being upgraded. Security issues should not only be considered inside the mobile phones but also on the network sides.

In a message transfer scenario as illustrated in Figure 6-1, a message sender sends a message to a message receiver through a message operator which transfers the received message to the message receiver. The message operator has the ability to filter spam (e.g., by using security mechanisms) during this message transfer. Figure 6-1 briefly demonstrates the entities in this scenario of message transfer.

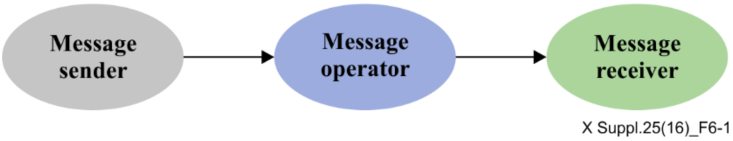


Figure 6-1 – Entities of message transfer in mobile phones

Nowadays, encryption is executed within the application based on encryption library that can protect personal information. It is possible for malicious attackers to use encryption manner that is intended for bypassing filtering manner.

The scope of this Supplement covers only a guidance to assist in countering spam for mobile phone developers. The term 'mobile phone developer' in this Supplement indicates an application developer who develops software applications for mobile phones. Therefore, this Supplement only considers the perspective of applications. An operating system of mobile phone is also important in security, but it is not the scope of this Supplement.

7 Security threats on countering spam in mobile phones

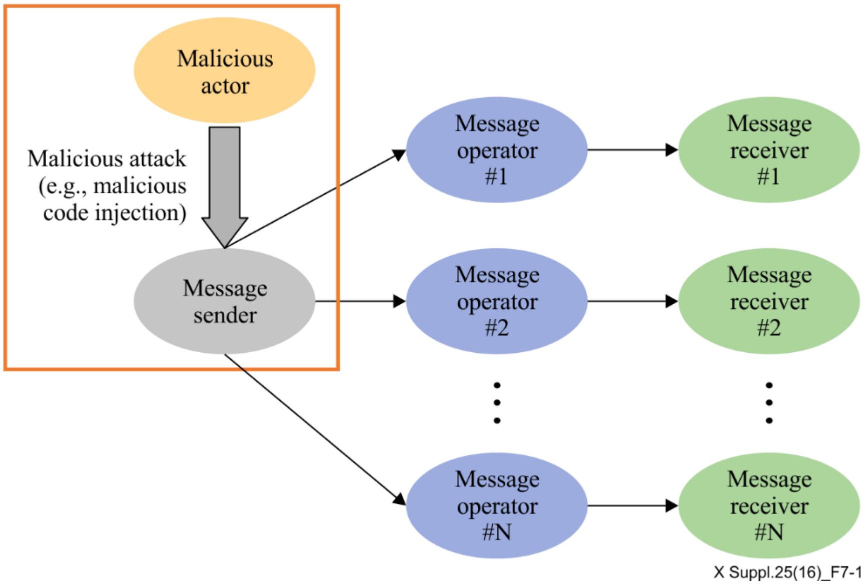


Figure 7-1 – Scenario for security threats of message transfer in mobile phones

Figure 7-1 illustrates a scenario for security threat of message transfer in mobile phones. It is assumed that there are several message operators and message receivers (i.e., *N* message operators and *N* message receivers). It is also assumed that there is only one message sender, and the message sender is connected to several message operators. Each message operator is connected with the corresponding message receivers. There is a malicious actor, who wants to attack the message sender that causes the security threat. In this case, malicious attack (e.g., injection of malicious code) can be executed by the malicious actor.

In mobile phone environments, users are vulnerable to the Persona security concept. Persona is not related to a person but rather to an identity (ID) or a credit card. The Persona perspective can be a breakaway from the existing 'user access control' concept and provide a different approach for authentication. However, mobile phones are also subject to other security threats faced at the application level, and at the network level; the latter issues are not addressed in this Supplement. From the perspective of applications, attacks can be produced by:

a) reverse engineering;

b) and repackaging.

Two security threats of the application perspective in mobile phones are as follows.

Disclosure of source code

Reverse engineering of a mobile app can yield decompiled source code; this causes the security threat where the source code becomes subject to disclosure. When the source code is disclosed, an application can be analysed. The disclosure of the source code yields the security risk whereby vulnerabilities (i.e., forgery, modification, disclosure of algorithms) become known and can be exploited. For instance, a disclosure of source code in financial applications can cause financial harm.

Repackaging

When the source code is disclosed, an identical application can be intentionally produced. This is called the repackaging problem. The repackaging problem causes a crack application, and it is one of the serious security threats in mobile phone environments. From [b-McAfee Report], other functions (e.g., calling, installing other mobile app, SMS sending without permission) can be added during the repackaging.

8 Guidance to assist in countering spam for mobile phone developers

In [b-ITU-T X.1231] it is mentioned that there is no single solution for countering spam. One of the feasible methods for countering spam is to mitigate hosts of spam. In [b-McAfee Report], it is mentioned that 80% of the identical Flappy Bird application is malware. The identical application can send SMS or electric mail without user permission, and it causes the host of spam. This Supplement provides the following guidance to assist in countering spam for mobile phone developers.

8.1 Countering spam in mobile phones by binary obfuscation

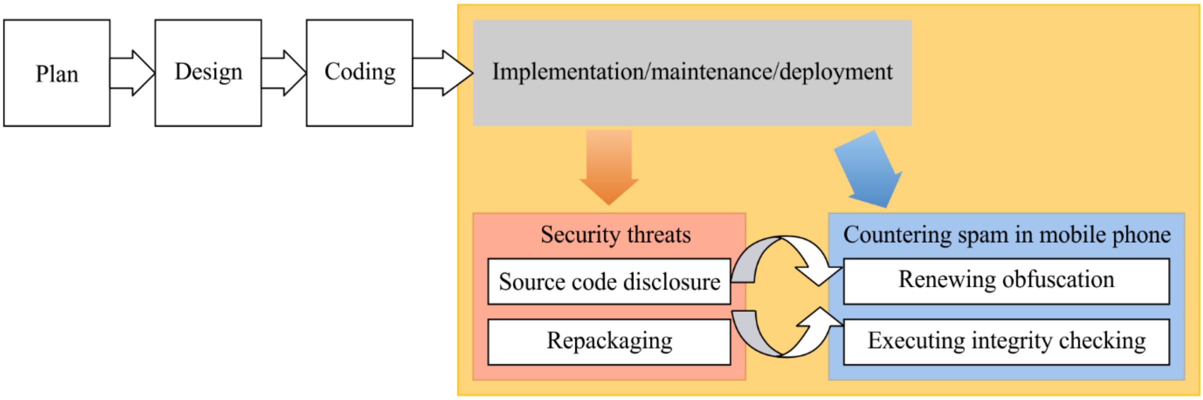
A binary obfuscation of the source code is a recommended method for mitigating the disclosure of the source code. The binary obfuscation of the source code renders the unauthorized and dedicated modification of applications more difficult.

8.2 Countering spam in mobile phones by integrity checking

A popular method for the prevention of repackaging is the usage of modification detection through an integrity check. In order to mitigate the repackaging problem, integrity checking of application is recommended to determine whether applications are modified. It is to construct an integrity checking system to identify whether the mobile app is forged. The use of hashing is one of the integrity protection methods.

8.3 Guidance to assist in countering spam for mobile phone developers

Countering spam can be provided by mapping of security threats and countering spam. Figure 8-1 illustrates the guidance to assist in countering spam for mobile phone developers, in terms of life cycle for mobile phone development.


Plan
Design
Coding
Implementation/maintenance/deployment
Security threats
Source code disclosure
Repackaging
Countering spam in mobile phone
Renewing obfuscation
Executing integrity checking

X Suppl.25(16)_F8-1

Figure 8-1 – Guidance to assist in countering spam in the life cycle for mobile phone development

The life cycle for mobile phone development is composed of four phases (i.e., plan, design, coding, and implementation/maintenance/deployment). Among the four phases, the guidance to assist in countering spam for mobile phones is only related to implementation/maintenance/deployment phase.

Plan

The first phase of the life cycle for mobile phone development is a plan phase. In the plan phase of the life cycle for mobile phone development, mobile phone developers plan for designing mobile phone applications in the plan phase.

Design

In the design phase, mobile phone developers design the mobile phone applications that are based on the result of the plan phase.

Coding

In coding phase, mobile phone developers do the coding for the mobile phone applications that are based on the result of the design phase.

Implementation / maintenance / deployment

The coded mobile phone applications, which are based on the coding phase, are moved to the next phase (i.e., implementation/maintenance/deployment phase). Two of the security threats (mentioned in clause 7) are source code disclosure and repackaging. Then, two methods for countering spam in a mobile phone (mentioned in clause 8.1 and 8.2) are renewing obfuscation and executing integrity checking. Renewing obfuscation can prevent source code disclosure, and countering spam in a mobile phone can prevent the repackaging.

Bibliography

[b-ITU-T X-Sup.19] ITU-T X-series Recommendations – Supplement 19 (2013), *ITU-T X.1120-X.1139 series – Supplement on security aspects of smartphones*.

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam.*

[b-ITU-T X.1242] Recommendation ITU-T X.1242 (2009), Short message service (SMS) spam filtering system based on user-specified rules.

[b-McAfee Report] McAfee Labs Threats Report: June 2014
<http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf>

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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016