International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1247

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Technical framework for countering mobile messaging spam

Recommendation ITU-T X.1247

ITU-T

International
Telecommunication
Union

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.

Recommendation ITU-T X.1247

Technical framework for countering mobile messaging spam

Summary

Mobile messaging spam is proliferating dramatically along with the fast development of mobile messaging services. Unfortunately, no single measure has proved to be the silver bullet against mobile messaging spam. Therefore, it is necessary to establish a practical framework for countering mobile messaging spam. Recommendation ITU-T X.1247 gives an overview of mobile messaging anti-spam processes, and proposes a technical framework for countering mobile messaging spam. Entity functions and processing procedures are specified in this framework. In addition, this Recommendation provides information sharing mechanisms against mobile messaging spam within the anti-spam domain and among anti-spam domains.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1247	2016-03-23	17	11.1002/1000/12600

Keywords

Anti-spam, mobile messaging spam, technical framework.

* 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/.

Table of Contents

Introduction

Mobile messaging, including short message service and multimedia message service, is developing very fast due to its low price, high flexibility and ease of use. However, mobile messaging spam is causing disturbances to customers' daily lives and has many negative effects.

It is difficult to mitigate mobile messaging spam effectively using only one solution. When a number of anti-spam technologies are applied to mobile messaging in cooperation, the harm caused by mobile messaging spam could be significantly reduced. Besides, considering that mobile messaging spam is widely spread all over the world, the cooperation among multiple anti-spam domains may lead to a much lower cost and to higher efficiency. Therefore, it is necessary to establish an open framework which accommodates various solutions and supports collaboration mechanisms. The framework is compatible with most anti-spam technologies and it is not limited to particular technical details. The procedures involved in this framework shall require consent to be explicitly granted by the end user of the mobile device and shall conform to national regulations and laws.

Recommendation ITU-T X.1247

Technical framework for countering mobile messaging spam

1 Scope

This Recommendation provides a technical framework for countering mobile messaging spam. In this framework, entity functions and processing procedures are specified. The procedures involved in this framework shall require consent to be explicitly granted by the end user of the mobile device and must conform to national regulations and laws. In addition, this Recommendation provides information sharing mechanisms against mobile messaging spam within an anti-spam domain and among anti-spam domains.

This Recommendation is applicable for short message service (SMS) and multimedia message service (MMS).

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 SMS spam [b-ITU-T X.1242]: Spam sent via SMS.

3.1.2 spam [b-ITU-T X.1240]: The meaning of the word "spam" depends on each national perception of privacy and what constitutes spam from the national technological, economic, social and practical perspectives. In particular, its meaning evolves and broadens as technologies develop, providing novel opportunities for misuse of electronic communications. Although there is no globally agreed definition for spam, this term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging for the purpose of marketing commercial products or services.

3.1.3 spammer [b-ITU-T X.1240]: An entity or a person creating and sending spam.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 anti-spam domain: An independent system which includes an anti-spam management function, an anti-spam monitoring function, an anti-spam processing function and a mobile messaging client.

NOTE – Functions in the anti-spam domain are subject to the operator's unified management.

3.2.2 anti-spam filtering entity: Equipment or system which applies anti-spam measures to filter mobile messages according to filtering rules. It can block the spam, mark messages as suspicious or send messages to the recipient.

3.2.3 anti-spam management functions: A group of functions which are applied to administer and supervise the anti-spam domain, including communicating with other anti-spam domains to share information on spam, generating new filtering rules from spam analysis and delivering them to anti-spam processing functions.

3.2.4 anti-spam monitoring functions: A group of functions which are applied to monitor and analyse the filtering result of anti-spam processing domain, including validating the suspicious spam captured by honeypot, analysing spam data, generating spam statistics and spam analysis results.

3.2.5 anti-spam processing functions: A group of functions which are applied to process mobile messages with filtering rules and policies. It processes messages by blocking spam, sending with special mark or sending messages to the recipient.

3.2.6 false negative: A mobile message spam was erroneously processed as non-spam by filtering system.

3.2.7 false positive: A message was erroneously identified as spam by filtering system.

3.2.8 filtering rules: A set of rules of countering algorithms which are deployed by the anti-spam filtering entity, such as blacklists/whitelists, similarity threshold and statistical threshold. The filtering rules may also include user-specified filtering rules.

3.2.9 mobile messaging client: The mobile message service subscriber.

3.2.10 mobile messaging spam: Unsolicited electronic communications over mobile messaging services, typically consisting of short message service (SMS) spam and multimedia message service (MMS) spam.

3.2.11 multimedia message spam (MMS) spam: Spam sent via MMS.

3.2.12 reporting service: A service which provides to collecting and aggregating subscriber's spam report under user permission, regulations and national laws.

3.2.13 spam analysis report: The analysed result represents the performance of filtering system. It should include false negative/positive rate of filtering, characteristic of message spam, trends of spam and other analysis.

3.2.14 spam statistics: The aggregated spam data represents the extent of spam under certain constraint conditions, such as a time interval in an anti-spam domain. It should include the amount of message spam within, entering or leaving domains, proportion of different types of spam, spammer list and other statistical data of spam.

3.2.15 suspicious spam: The undetermined mobile message which is suspected of spam.

3.2.16 user report: A complaint from a subscriber receiving spam mobile message. In general, the report may include the receiving time of spam, the mobile subscriber international integrated services digital network/public switched telephone network (ISDN/PSTN) number (MSISDN) of sender and recipient, etc. This report includes information about message incorrectly marked as mobile spam or not marked when it should have been i.e., false positive, false negative.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AO	Application Originated
AMgmt	Anti-spam Mobile messaging management function
Amon	Anti-spam mobile messaging monitoring function
APr	Anti-spam mobile messaging Processing function
GGSN	Gateway GPRS Supporting Node
GPRS	General Packet Radio Service
HPLMN	Home Public Land Mobile Network
HTTP	HyperText Transfer Protocol

ISDN	Integrated Services Digital Network
MAP	Mobile Application Part
MMS	Multimedia Message Service
MMSC	Multimedia Message Service Centre
MNO	Mobile Network Operator
MO	Mobile Oriented
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber International ISDN/PSTN Number
MT	Mobile Terminated
PSTN	Public Switched Telephone Network
SMPP	Short Message Peer-to-Peer
SMS	Short Message Service
SMSC	Short Message Service Centre
UICC	Universal Integrated Circuit Card
VPLMN	Visited Public Land Mobile Network
WAP	Wireless Application Protocol

5 Conventions

None.

6 Overview of anti-spam mobile messaging

As shown in Figure 6-1, short message service (SMS) spam can be created mostly in two ways. One way is that the spammers use spam tools to send bulk messages through sending normal point-to-point short messages with many acquired or duplicated universal integrated circuit cards (UICC). The other way is that the spammers make use of bulk message sending services offered by service providers by using the operator's short message gateway interfaces. Since operators have no effective technical and managerial supervision mechanism on the short message gateway interface, it can be easily utilized by spammers.

According to messaging forwarding direction, there are two procedures for the spammers to create SMS spam, named mobile oriented (MO)/application originated (AO) procedure and mobile terminated (MT) procedure. In the MO procedure, the spam generated by spam tools is sent to the short message service centre (SMSC) through related entities of the sender's network. In the AO procedure, the short message injected into spam from the operator's short message gateway is forwarded to SMSC. Afterwards, SMSC queries the recipients' serving mobile switching centre (MSC) and then forwards the message to it. Eventually, the short message is forwarded to the recipient through the visiting network of MSC, which is called the MT procedure.

With the permission of subscriber and administrative regulations, the mobile network operators (MNO) are empowered to mitigate messaging spam by filtering entities. Anti-spam process shall follow applicable law clauses carefully in order to avoid violating subscriber's privacy.

It is widely accepted anti-spam filtering entities are deployed in the MO/AO procedure, the MT procedure or both. For spam filtering in the MO procedure, anti-spam filtering entities collect short messages from SMSC. In order for spam filtering to be effective in the recipients' network, communication between MSC and the anti-spam filtering entity is also needed.

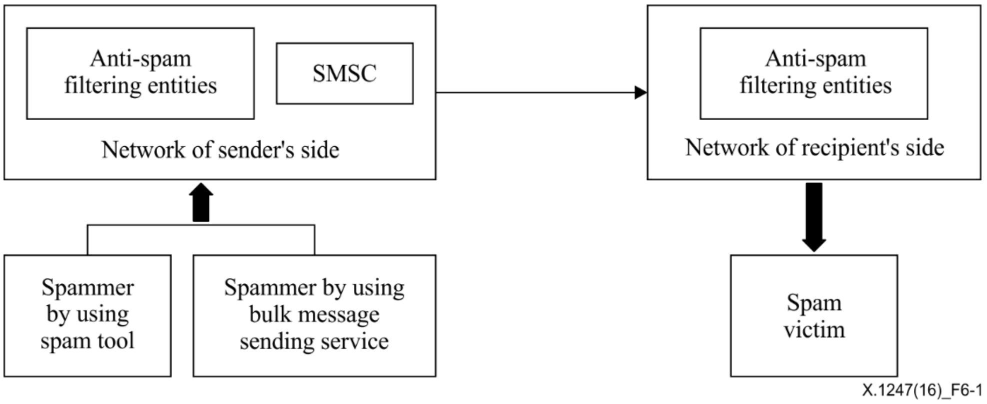
Anti-spam filtering entities
SMSC
Network of sender's side
Anti-spam filtering entities
Network of recipient's side
Spammer by using spam tool
Spammer by using bulk message sending service
Spam victim
X.1247(16)_F6-1

Figure 6-1 – SMS spam in mobile network

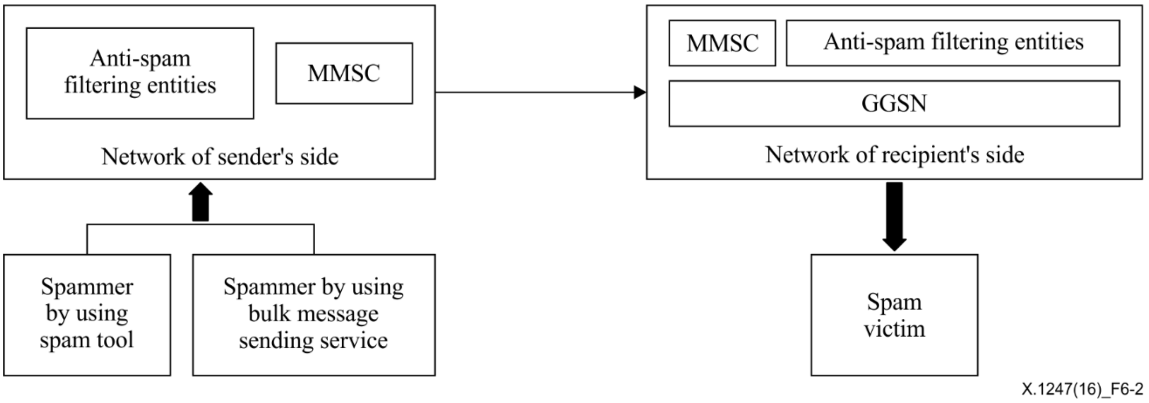
Anti-spam filtering entities
MMSC
Network of sender's side
MMSC
Anti-spam filtering entities
GGSN
Network of recipient's side
Spammer by using spam tool
Spammer by using bulk message sending service
Spam victim
X.1247(16)_F6-2

Figure 6-2 – MMS spam in mobile network

As shown in Figure 6-2, the multimedia message service (MMS) messaging procedure is similar to the procedure in SMS except that MSC is replaced by the gateway GPRS supporting node (GGSN) and SMSC is replaced by the multimedia message service centre (MMSC). The MMS message will be forwarded to MMSC of the recipient's network after which SMSC will send SMS message to the recipient. The recipient will then download the MMS message from MMSC. For that reason, MMS anti-spam filtering entities can be deployed adjacent to MMSC which means that if the filtering entities are deployed on sender's side or recipient's side it does not make a difference.

7 Structure of anti-spam mobile messaging functions

The structure of anti-spam mobile messaging functions includes anti-spam mobile messaging management function (AMgmt), anti-spam mobile messaging monitoring function (AMon), anti-spam mobile messaging processing function (APr) and mobile messaging clients. These functions define the anti-spam mobile messaging domain.

Different anti-spam mobile messaging domains are recommended to be associated; they can coordinate with each other according to rules or policies defined by relevant agreements.

These functions can communicate with each other through existing messaging protocols and their characteristics are described as follows.

7.1 General structure

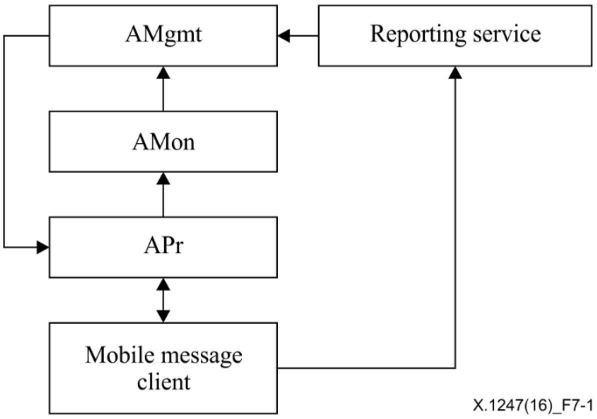

Figure 7-1 – General structure

AMgmt receives spam statistics from AMon and updates the filtering rules in its domain. AMgmt also shares information on spam with the reporting service and other AMgmts.

AMon receives suspicious mobile messaging spam from APr, which is captured by honeypot or similar platforms, and verifies whether they are spam. AMon also reports the spam analysis and spam statistics to AMgmt after aggregating and analysing spam data.

APr applies the rules to mobile messages, then chooses to send, to send with mark as spam or to block them according to different polices and filtering results under user permission. APr receives filtering rules from AMgmt and user feedbacks from mobile messaging clients. It is recommended to deploy some platforms such as honeypot on APr to accumulate the suspicious spam.

The mobile messaging client contributes to the anti-spam mobile messaging process by user’s sending feedback that the received mobile message marked as spam is incorrect to APr and spam report to reporting service.

Reporting service is provided to collect and aggregate subscriber's spam report under user permission, regulations and national laws. It helps to share user report data between anti-spam domains. Reporting service could be operated by regulatory bureaucracy, security corporation or MNO, etc. Inter-domain agreements enable anti-spam mobile messaging domains to share customized information on spam.

7.2 Reference model

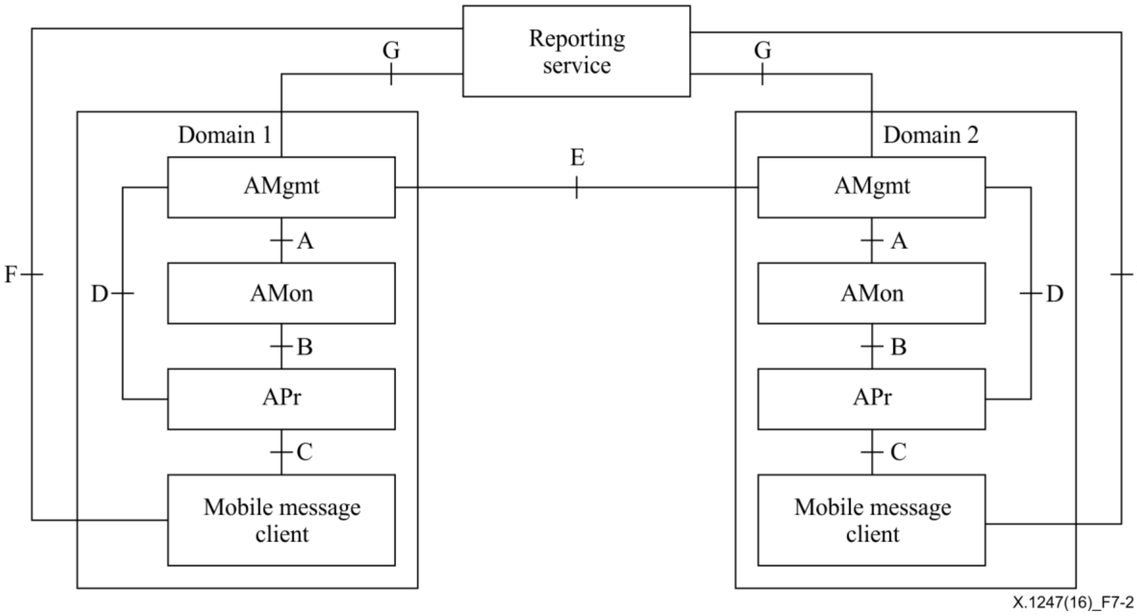

Figure 7-2 – Reference model

Interface A is a logical interface between AMgmt and AMon. Interface A is used to transmit the spam analysis reports and spam statistics.

Interface B is a logical interface between AMon and APr. Interface B is used to transmit the suspicious spam caught by honeypot and the user's feedback that the received mobile message marked as spam is incorrect from mobile messaging client.

Interface C is a logical interface between APr and the mobile messaging client. Interface C is used by the mobile messaging client to inform APr of receiving a message was wrongly marked as spam by MNO. Besides, interface C is also used to send messages from APr to mobile messaging client. According to different types of mobile messaging clients, various protocols should be supported at interface C, such as mobile application part and wireless application protocol (MAP/WAP), hypertext transfer protocol (HTTP) and short message peer-to-peer (SMPP).

Interface D is a logical interface between AMgmt and APr. Interface D is used to transmit filtering rules.

Interface E is a logical interface between AMgmts with other domains. Interface E is used to exchange spam data between different anti-spam mobile messaging domains.

Interface F is a logical interface between mobile messaging client and reporting service. Interface F is used by the mobile messaging client to send a user report to reporting service with explicit user consent. Various protocols should be supported at interface F, such as mobile application part and wireless application protocol (MAP/WAP), hypertext transfer protocol (HTTP) and short message peer-to-peer (SMPP).

Interface G is a logical interface between AMgmt and reporting service. Interface G is to transmit spam report information from reporting service to AMgmt.

In this reference model, interfaces A to D are intra-domain interfaces, interface E to G are inter-domain interface.

7.3 Functions of components

7.3.1 Mobile messaging clients

The functions of the mobile messaging client include:

- Providing mechanisms to help users send user reports to reporting service.
- Providing mechanisms to help users to inform APr of receiving messages which are wrongly marked as spam.
- Filtering messages by specific filtering rules using security Apps.

7.3.2 APr

The functions of APr include:

- Applying countering spam rules from AMgmt and choosing to send, to send with mark as suspicious or to block them according to different polices and filtering result.
- Receiving user's feedback from mobile message client claiming that the received mobile message, which is marked as spam, is actually not.
- Collecting the suspicious spam by honeypot or other similar platforms.
- Delivering user's feedback as well as the suspicious spam captured by honeypot to AMon.

7.3.3 AMon

The functions of AMon include:

- Aggregating the suspicious spam which was collected by honeypot from APr and the user report information from reporting service.
- Validating the suspicious spam from APr.
- Analysing the aggregated spam data to mine the characteristics of new spam.
- Reporting spam statistics and spam analysis to AMgmt.

7.3.4 AMgmt

The functions of AMgmt include:

- Receiving spam statistics and analysis report from AMon.
- Analysing the reported data from AMon to generate filtering rules.
- Sending filtering rules to APr, the filtering rules will be applied to mobile messaging clients.
- Communicating with the other AMgmts to exchange and share spam data, such as the amount of spam, resource and characteristic of spam, new spammer list, etc.
- Receiving user report information from reporting service, including top abuser, spam statistics and trends. The user report information may be customized and includes some processed data from user report according to agreement with reporting service within the sphere permitted by regulations and national laws.
- Providing the ability of setting user-specific filtering rules to the subscriber, and sending the rules to APr after verifying their validity.

7.3.5 Reporting service

The functions of reporting service include:

- Collecting user's reports and verifying if they are spam.
- Storing and analysing spam to generate characteristic of spam, using fingerprints instead of content to avoid violation of privacy.

- Providing user report data to enable MNO the ability of understanding the extent of spam within, entering and leaving their networks from other operators, which asked MNOs to use this visibility to target enforcement action against messaging spam only, without impacting users and content.

8 Technologies of anti-spam mobile messaging

Technologies introduced in this clause apply to the anti-spam structure above and provide an example. All these measures shall be used carefully to conform to the applicable regulations, national laws and with the permission of the user. This is intended to avoid the violation of subscriber privacy.

8.1 User feedback mechanisms

User feedback mechanisms enable subscribers to inform the filtering system of their opinions about the spam filtering result. A reporting service and user's feedback are recommended to be implemented to improve the result of filtering of the MNO.

A reporting service is a system to collect users' reports of receiving spam messaging, which may be set up by governments, operators, etc. The reporting service can be a hotline, a website or a short message spam reporting centre; thus the MNO can collect short message spam and adjust the filtering rules. In general, the record of the reported short message spam complaint should include the hash of the spam message, the receiving time, as well as the senders' MSISDN, etc. According to different policies and only if the user has granted their consent, the MNO may not only block the spam but also offer the recipients access to a quarantine, which means these messages could be sent with a mark or recorded in specific website. This allows recipients to view these "potential spam", which have been marked as suspicious spam, and gives them an opportunity to offer feedback if they consider a decision on a specific message to be incorrect or a "false positive". Not all user's feedback is reliable on its own. Recipients may make mistakes or have alternative reasons for reporting messaging as spam. Spam recognition information needs to be verified manually before it is used to generate fingerprints or filtering rules. The development of a reporter trust rating system can be introduced to automatically determine valid feedback versus erroneous or malicious feedback.

8.2 Honeypot

A phone number honeypot is an account that is created as a "trap" for the purpose of detecting, deflecting or counteracting unauthorized use of the mobile messages. It usually involves an account that is used or created to be discovered by spammers, including inactive or non-existent phone numbers. In this way, any message that differs from what is expected can be treated as suspicious spam and may be appropriate to analyse the content. The phone numbers are subject to rapid reassignment and phone numbers are often mistyped, so that the phone number honeypots will receive many accidental and non-spam messages. Verification of this suspicious spam is necessary to filter out these unwanted data before analysing the suspicious spam to abstract characteristics.

User feedback suffers from delays, as minutes to days may elapse before an unwanted message is reported by recipients. In contrast, honeypots traps may detect unwanted messages as soon as they are delivered.

8.3 Identification method by MNO

Except user feedback and honeypot, MNO can take some other measures to identify the spam before sending them to recipients. With different policies, these messages will be blocked or sent with special mark as suspicious. These identification methods may depend on characteristics of spam or pattern of sending.

- Blacklist/whitelist of sender's mobile subscriber international integrated services digital network/public switched telephone network (ISDN/PSTN) number (MSISDN):

MSISDN is the most basic information to distinguish a message from a subscriber or a spammer. Blacklists/whitelists use the sender's MSISDN to suspend/accept messages. Mobile operators could block the well-known or recognized spammers, while the subscribers could define their own blacklists/whitelists to block or accept messages from particular senders.

- Fuzzy recognition:

  In order to evade the spam filtering, some confusion works are used by spammers. For example, some specific characters, such as "*","^", etc., are arbitrarily inserted into the text of the messages. Letters are replaced by similar characters, for example, "porn" may be changed to "p0rn". Images may be enlarged or rotated. Fuzzy recognition is in charge of recognizing this circumvention and filtering it, where permitted.

- Sending frequency:

  To quickly spread spam, spammers may send messages to a large proportion of recipients in a short time. The spammers send their messages in a much greater speed than that of a normal sender so that the time interval between two messages is shorter. When a user's sending frequency exceeds the pre-set threshold, the user will be identified as a highly suspicious spammer.

- Successful rate of messaging sending:

  Messaging spam is sent to unknown recipients, for that reason the spammer chooses the recipients randomly. It is therefore common that there are some non-existent called numbers. The successful messaging sending rate of spam is remarkably lower than that of the normal mobile messaging.

- Sender's call record:

  The user's call record can help the operator to analyse the sending pattern. The record should include at least the sender's phone number, the recipient's phone number, and the sending time. If the message is sent to many subscribers and has a very low rate of responding or reply, the sender may be suspected as a spammer. Spammers seldom use other services (such as voice calls) provided by the operator other than the message service.

8.4 Additional enhancement

- User-specific rules configuration:

  A user-specific rules configuration mechanism enables recipients to define and inform the filtering system what type of messages that recipient is unwilling to receive. Filtering messages according to user-specific rules can be accomplished by the MNO or by using software installed by the recipients.

- Routing back to the recipient's home public land mobile network (HPLMN):

  Operators may apply different anti-spam processes for the clients who are roaming outside of HPLMN. The process of routing messages back to HPLMN is optional, so it may incur that roaming recipients receive a message without spam filtering. Thus the messages sent to the roaming clients have to route back to anti-spam filtering entities in HPLMN instead of relying on the visiting network. Before arriving at the visited public land mobile network (VPLMN), the recipient's HPLMN needs to receive and filter the messages with relevant anti-spam measures.

9 Relationship between anti-spam domains

The performance of anti-spam measures in a single anti-spam domain is limited both technically and economically. Interconnections and interworking are required between MNOs; collaboration mechanisms between their anti-spam domains are also essential. Collaboration mechanisms can help to improve the efficiency and enhance the performance of their anti-spam systems.

There are two types of relationships between anti-spam domains, namely a trust relationship and a non-trust relationship (Figure 9-1). The default relationship between anti-spam domains should be a non-trust relationship, in which case all messages from untrusted peers will be filtered. Under co-operative agreements, the trust relationship may be built between peer anti-spam domains; for this relationship, operators may choose not to filter messages from trusted peers based on their policies and filtering rules.

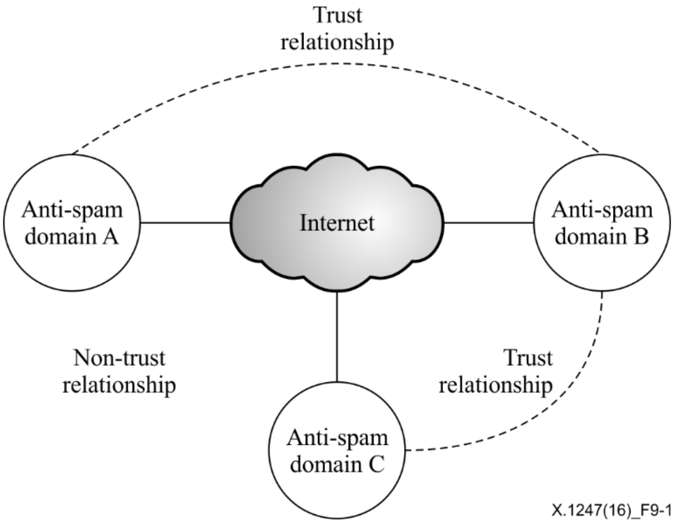

Figure 9-1 – Trust relationship and non-trust relationship

The trust relationship is non-transitive. For example, if domain A trusts domain B, and domain B trusts domain C, then domain A may not trust domain C unless they have directly negotiated and established the trust relationship. The trust relationship is bidirectional which means that the trusted peers treat each other equally.

After a trust relationship is established, the following coordination mechanisms are recommended.

- Spam data sharing:

  Certain spam data is shared through the AMgmt connection. The shared information may include blacklists, keywords, complaint reports, and new spam characteristics. The intent of this information will be consulted during the trust relationship establishment process. The spam data sharing shall require consent to be explicitly granted by the end user of the mobile device and must conform to national regulations and laws.

- Message source authentication:

  The message from a trusted peer will be considered authentic only if the message source is authenticated.

- Dispense with filtering:

  The messages from a trusted domain can be sent directly to the recipient so that duplication of message-processing is avoided.

- User complaint report and the suspicious spam feedback:

  If spam reports and suspicious spam are received on messages from trusted peers, they should be sent to the trusted peers for improving their filtering rules under applicable regulations and national laws.

In order to satisfy different coordination mechanisms, APr and AMon should carry out different procedures when dealing with mobile messages. APr will decide whether it filters the message or not.

According to the agreement, AMon will forward/block the message, or send a feedback to trusted peers. Figures 9-2 and 9-3 describe the operation flows of APr and AMon.

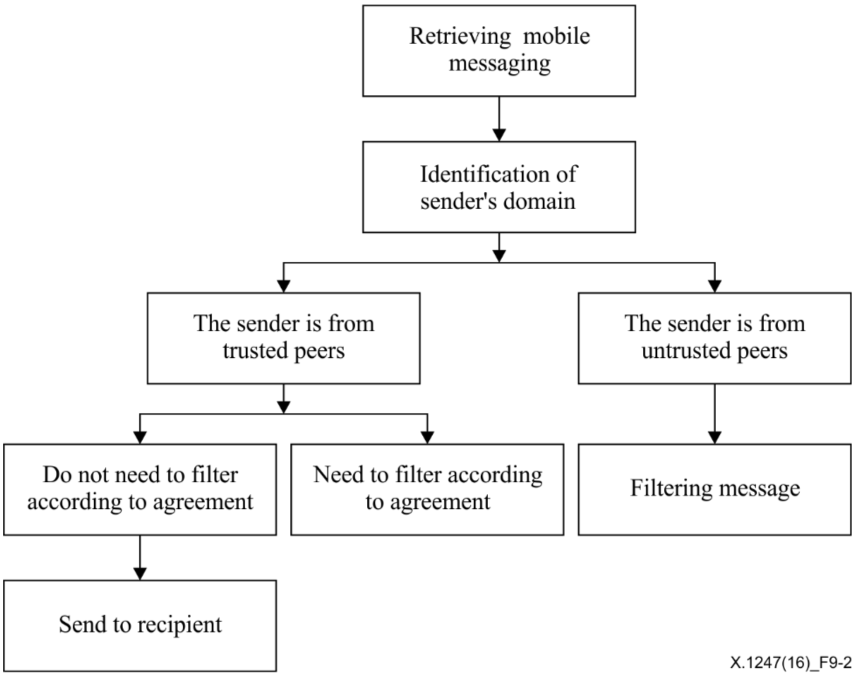
Retrieving mobile messaging
Identification of sender's domain
The sender is from trusted peers
The sender is from untrusted peers
Do not need to filter according to agreement
Need to filter according to agreement
Filtering message
Send to recipient
X.1247(16)_F9-2

Figure 9-2 – Flows of dealing with mobile messaging in APr

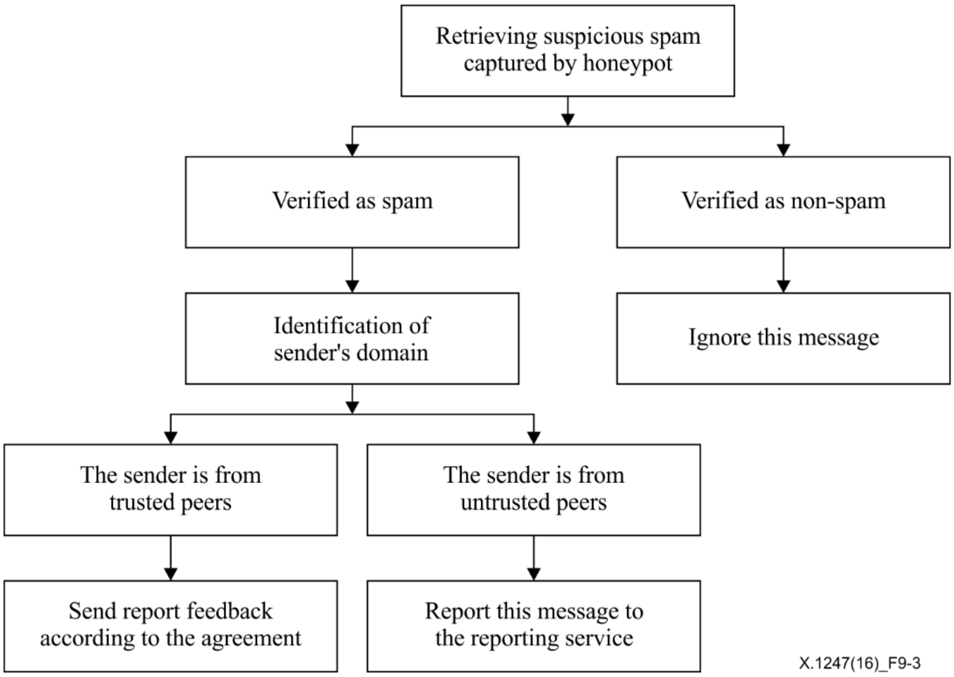
Retrieving suspicious spam captured by honeypot
Verified as spam
Verified as non-spam
Identification of sender's domain
Ignore this message
The sender is from trusted peers
The sender is from untrusted peers
Send report feedback according to the agreement
Report this message to the reporting service
X.1247(16)_F9-3

Figure 9-3 – Flows of dealing with mobile messaging in AMon

10 Mobile message anti-spam processing

In the mobile messaging anti-spam process, an adaptive mechanism should be introduced to accommodate the constantly emerging new spam and their new variations. In general, it can be considered that the anti-spam process consists of eight procedures as shown in Figure 10-1. These procedures constitute an adaptive system which contributes to the optimization of system performance.

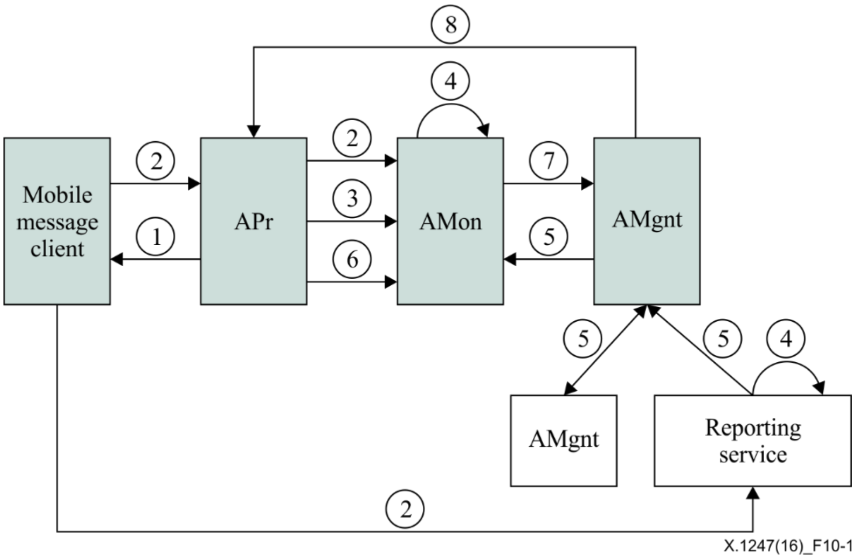

Figure 10-1 – Anti-spam processing procedures

Procedure 1: Message filtering

Based on policies and filtering rules, APr specially marks or filters spam messages before sending messages to the recipient. These filtering rules can be set by operators or user customization.

Procedure 2: User sending feedback

The mobile messaging client sends the user's complaints to reporting service to report the unfiltered spam as well as user's feedbacks to AMon to express receiving messages with erroneous mark as spam. This will help operators to improve their filtering rules.

Procedure 3: Suspicious spam forwarding

APr will send the suspicious spam accumulated by honeypot to AMon for verification.

Procedure 4: Spam verification

AMon tackles suspicious spam by verifying as well as reporting services dealing with user spam report. This procedure is complex and based on manual intervention, conforming to the applicable regulations and national laws. Verification should use fingerprint or hashed data of spam instead of using messaging content. Some information can be supplement to this judgement, e.g., the spammer's and reporter's reputation which means it gives trust rating to user's reporting.

Procedure 5: Information sharing

AMgmt exchanges spam data with trusted peers, as well as AMgmt receives customized spam analysis from reporting service. Complying with the consensus of the negotiation, the data may include user report statistics, spammer list, complaint feedback and new characteristics of spam. This spam data shall be carefully processed to make sure there is no user content included.

Procedure 6: System performance monitoring

AMon is also responsible for monitoring the performance of the spam filtering system. AMon collects data from APr to generate performance reports and analyse them. The performance report may include figures on the real-time performance the ratio of spam and the false negative rate, etc.

Procedure 7: Spam analysis

The confirmed spam data from reporting service, trusted peers and Amon will be aggregated and stored, taking into account regulations and national laws. Periodically, AMon may analyse these data and mine for new spam patterns and characteristics. This will help to improve the filtering rules and the performance of the system. Finally it will use to generate spam statistics and spam analysis report which will be transmitted to AMgmt.

Procedure 8: Adjustment of countering measures

According to spam statistics and analysis report from AMon, AMgmt evaluates the anti-spam performance of the spam filtering system for possible improvements. Based on the evaluation result, measures and policies may be adjusted and collaboration mechanisms with other domains may be changed. Relevant measures will be carried out, such as the establishment or disestablishment of trusted relationship and the distribution of new filtering rules and policies to APrs.

Bibliography

[b-ITU-T X.1240]	Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail 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-M3AAWG report]	M3AAWG, *Mobile Messaging Best Practices for Service Providers*, Updated August 2015. https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.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