International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 12
(03/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1240 – Supplement on overall aspects of countering mobile messaging spam

ITU-T X-series Recommendations – Supplement 12

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
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

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

Supplement 12 to ITU-T X-series Recommendations

ITU-T X.1240 – Supplement on overall aspects of countering mobile messaging spam

Summary

Supplement 12 to ITU-T X-series Recommendations, in particular to Recommendation ITU-T X.1240, describes the basic concept and characteristics of mobile messaging spam. It also introduces and analyses current technologies on countering mobile messaging spam. In addition, this supplement proposes a general implementation framework for countering mobile messaging spam. The relative activities in different organizations are introduced in Appendix I.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 12	2012-03-02	17

Keywords

MMS, mobile messaging spam, SMS, spam.

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/.

© ITU 2012

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

Supplement 12 to ITU-T X-series Recommendations

ITU-T X.1240 – Supplement on overall aspects of countering mobile messaging spam

1 Scope

This supplement to Recommendation ITU-T X.1240 provides an overview of mobile messaging spam, including types, characteristics and delivery methods. Furthermore, this supplement analyses the current technologies on countering mobile messaging spam, and proposes an implementation framework for countering mobile messaging spam. The relevant activities in different standardization organizations and related organizations are introduced in Appendix I.

This supplement only focuses on mobile messaging spam, including SMS spam and MMS spam.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This supplement uses the following terms defined elsewhere:

3.1.1 mobile handset [b-ITU-T K.49]: Not fixed terminal equipment used for data or voice communication and connected to a fixed telecommunications network via radio interface.

3.1.2 multimedia messaging service (MMS) [b-ITU-T X.1231]: Multimedia messaging service refers to a kind of messaging service after short message service which can transfer various multimedia messages including text, graphics, audio, video and so on through mobile network, wireless network or fixed network.

3.1.3 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.

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

3.1.5 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.

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

3.2 Terms defined in this supplement

This supplement defines the following terms:

3.2.1 false positive: A result that is erroneously positive when a situation is negative.

3.2.2 MMS spam: Spam sent via MMS.

3.2.3 **mobile messaging spam**: Unsolicited electronic communications over mobile messaging services, typically consisting of SMS spam and MMS spam.

4 Abbreviations and acronyms

This supplement uses the following abbreviations and acronyms:

CBCS	Categorization-Based Content Screening
CDR	Call Detail Record
CI	Contextual Information
CSCS	Client Side Content Screening
FMD	Filtered Messages Database
GSM	Global System for Mobile communications
HMM	Hidden Markov Models
HPLMN	Home Public Land Mobile Network
ID	Identity
IMR	Identification, Marking and Reacting
IMS	IP Multimedia Subsystem
MAP	Mobile Application Part
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
MT-SMs	Mobile Terminated-Short Messages
NB	Naive Bayes Algorithm
OPH	Open Proxy Handshake
OSBF-Lua	Orthogonal Sparse Bigrams with confidence Factor
PLMN	Public Land Mobile Network
PS	Packet Switched
PUCI	Protection against Unsolicited Communication for IMS
SCIDM	Secure Content IDentification Mechanism
SCM	Service Control Module
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Centre
SPIT	SPam over Internet Telephony
SS	Supplementary Services
SSFM	SMS Spam Filtering Module
SVM	Support Vector Machine
TCAP	Transaction Capabilities Application Part
UC	Unsolicited Communication

UC-OPH	Unsolicited Communication - Open Proxy Handshake
UCS	supervised Classifier System
URD	User-specified Rules Database
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
USMM	User Service Management Module
VPLMN	Visited Public Land Mobile Network
WAP	Wireless Application Protocol

5 Conventions

None.

6 Overview of mobile messaging spam

6.1 Types

Mobile messaging spam is unsolicited electronic communications over mobile messaging services. Spam messages mainly include the following content:

– advertising information: advertisement of products or services, especially discount information, etc.

– fraud information: lottery winning fraud, bank card fraud, fake identity fraud, etc.

Based on the different carriers of unsolicited messages, mobile messaging spam could be classified into SMS spam and MMS spam.

SMS spam is spread widely throughout the world. Unsolicited spam included in short messages can seriously disturb people’s daily life by wasting their time and influencing their state of mind. With the low cost of bulk sending and the increasing number of SMS users, SMS spam has constituted the major mobile messaging spam. Service providers often cannot charge for SMS spam. In a postpaid environment, the users or customers may renege on payment. Furthermore, this bulk spam consumes an enormous amount of storage space and computing resources for mobile networks, which may affect the service quality of legitimate users. However, bulk transmission does not necessarily imply spam; for example, circulating an announcement within a company may also display similar features to those of SMS spam.

Because MMS is sent in the packet switched (PS) data channel of mobile networks, it is easier to be used for spreading malware. Therefore, it seems to be a more serious problem. The scale of MMS spam is not as large as SMS spam, due to the costly price and limitations of the delivery methods. Even if the price for the individual multimedia message is much higher than that for the short message service, bulk sending pricing will tremendously reduce the cost for spam distributors. Furthermore, the rate of spam return is higher for MMS than for SMS spam. Currently, there are more counter measures against SMS spam available to users and operators. Therefore, many spammers prefer to use MMS spam in some situations.

6.2 Characteristics

In order to counter mobile messaging spam effectively and efficiently, the characteristics of mobile messaging spam need to be analysed and summarized. Such an analysis could be taken into consideration in the development of the relative technologies and policy decisions in view of countering mobile messaging spam. Some of the most common characteristics are as follows:

- Spam messages can be as long as possible in order to transmit the maximum amount of information.
- Spam messages use some random characters dynamically inserted into the text of the message in order to avoid the identification of single bulk transmission, and to avoid spam keyword recognition filters.
- There is usually a phone number or a hyperlink for contact information. This phone number and hyperlink may not belong to the presumed advertiser.
- A spam message does not necessarily mean that there is no interest in receiving it. The decision should be made by the recipients.
- Spammers may send messages to a large proportion of a mobile phone number segment in a short time.
- Most spammers do not retry a failed message delivery.
- Spammers and recipients are usually unknown to each other, and there is no voice conversation between them. Besides, the responses to a spam message are not as frequent as to a normal message.
- Spammers seldom incur any other charges (such as voice call) other than the messaging charge.
- Spam messages with the same content may be originated from different mobile phone numbers.

6.3 Delivery methods

There are two common bulk delivery methods of mobile messaging that can be used for mobile messaging spam:

- Using spam tools to send bulk messages: spammers acquire subscriber identity cards (such as SIM, USIM, etc.), usually with a discount package for sending mobile messages, and they plug the cards into the spam tools that are controlled by computer software. Spammers can then send bulk messages by activating those spam tools. Generally, each computer has the ability to control more than one spam tool at the same time, and enable the bulk sending of spam messages. Bulk spam message sending is usually at a low price. With this method, the sending number will be shown in the recipient's mobile handset as a normal mobile phone number, and the recipients cannot recognize whether it is spam or not before they read it. Most mobile messaging spam is sent by this method, which is difficult to control.
- Using bulk message sending services: some service providers offer bulk message sending services. The customers are usually enterprises providing information services, such as stock information, newspaper, weather forecast, entertainment, etc., or bulk send notifications within a company. However, some of these customers may send these messages without the permission of the recipients. In this situation, the companies and the enterprises which order this service may be considered as spammers by the recipients. When a recipient receives a message through this method, the number of the sender will be shown as a service number allocated by a mobile operator and the number cannot be called back. In addition, there exists free-download messaging software that can be used to send messages from a computer to a mobile handset. This latter method could also be used by spammers for bulk sending messages.

7 Current technologies for countering mobile messaging spam

7.1 Blacklists/whitelists

Blacklists/whitelists of mobile phone numbers is a widely used technology to filter mobile messaging spam. The filtering system will accept messages if the sender's phone number is in the whitelist, and it will suspend messages if the sender's phone number is in the blacklist. The whitelist is usually established manually, while the blacklist may be established manually or generated automatically by the system. Both the blacklist and the whitelist should be updated frequently. In fact, filtering based on the blacklist inevitably contains inaccuracies, as it can lead to also blocking the legitimate messages; this is called false positive. False positive should be accounted for in the deployment of the blacklist.

Basically, the blacklist/whitelist is a simple and efficient technology with little system resource consumption, and could be easily deployed for filtering unwanted messages. However, with continuous updating, the recognition rate will be increased. This technology could be deployed on the network side and/or the user side. Mobile operators could block the well-known or recognized spammers, while the end users could define their unique blacklists/whitelists to block or accept any messages from particular sources. This technology is usually used together with other technologies.

7.2 Content-based filtering

Content-based filtering approaches have been confirmed as an effective solution for countering e-mail spam. They have also been used for countering mobile messaging spam. However, mobile messaging has some characteristics which are different form e-mail spam. That is, mobile messaging contains relatively shorter texts and less structured fields in comparison with e-mail, which makes it difficult for the content-based filtering method to have enough information to identify mobile messaging spam. Moreover, abbreviations, acronyms and regional words are more frequently used in short messages. The deployment of the content-based filtering for mobile messaging spam has to take those differences into account and make the necessary modifications to the content-based filtering methods used in e-mail spam.

The most common content-based filtering technology is keyword filtering based on user-specified rules, which is easy to implement. However, the keywords in the filtering database should be updated frequently because spammers usually misspell the characters, variant and homophonic words to counter filtering. Therefore, it is necessary to use more intelligent and sophisticated approaches such as text classification algorithms in content-based filtering. Many text classification algorithms can be used for countering mobile messaging spam, such as naive Bayes algorithm (NB), support vector machine (SVM), supervised classifier system (UCS), hidden Markov models (HMM), and orthogonal sparse bigrams with confidence factor (OSBF-Lua), etc. The differences between these algorithms should be considered in the deployment of the content-based filtering system. For example, NB is the most regular algorithm for countering spam due to its simplicity and speed, which could be implemented easily. SVM, on the other hand, needs more computation for classification and it is difficult to deploy at the mobile application level. If SVM is deployed on the user side, the storage space and computation capability of the mobile handset should be accounted for. However, SVM is a reliable algorithm to choose as it is highly efficient in spam message recognition.

In addition, content-based filtering for MMS spam should work in combination with the image recognition algorithm.

7.3 Spam reporting

Spam reporting can be done through the technology that is deployed with security software installed in a mobile handset, or integrated into a mobile network for blocking reported spam messages. A reporting mechanism could also be set up by governments or operators by establishing a reporting hotline; website, etc., to handle reported messages or mobile phone numbers, and periodically announce confirmed spam information. Moreover, because some messages are difficult to be identified as spam or not, a spam reporting mechanism enables recipients to define and report which messages or senders are unwanted.

7.4 Traffic statistics

This mechanism is to provide statistics on the sending message traffic of a user or a service provider. If the statistics exceed the specified threshold, the alarm system will be triggered and the message sender will be monitored and filtered. There are two methods for traffic statistics: one is to measure the amount of messages that a sender sends out within a unit of time; and the other method is to measure the interval between two message sending behaviours of a sender.

Traffic statistics are easy to implement, but it is difficult to set the threshold. If the threshold is too low, it is easier to cause false positive problems since legitimate messages are more likely to be blocked. However, if the threshold is too high, traffic statistics cannot achieve the expected results of recognition. In addition, the threshold can be tested easily, thus spammers can adjust the sending rate and the number based on the threshold to counter the mechanism.

7.5 Analysis of call detail records

This mechanism uses the call detail record (CDR) as a statistical resource. The filtering system continuously scans the charging server and downloads the latest CDRs to the local system. The statistics module will then scan the local working directory at specific intervals of time and analyse the CDRs based on the sequence of arrival. If the amount of messages that a sender originated successfully within a unit of time exceeds the threshold, the sender is considered suspicious and the information will be provided to the administrator so that he/she can determine whether the mobile phone number should be added to the blacklists.

7.6 Greylisting

Greylisting could be used in a situation where the spammer would not retry a failed delivery of messages. For each newly arrived message from an unknown source other than from a whitelist, a unit doublet in the format of a calling number, called number, etc., will be created. When a unit doublet first shows up, a temporary failure message will be sent to the sender, and message delivery will be refused. The first arrival time of the unit doublet will then be recorded. Otherwise, if the record for the unit doublet already exists, and the interval between the current time and first arrival time is larger than a preset threshold, then the message will be transferred. The deployment of greylisting has to make modifications on the network side. The disadvantage of greylisting is that it usually causes unacceptable delays for message sending of legitimate users.

7.7 Duplicate content recognition

This technology is based on the similarity of spam messages rather than on the content of an individual message. Due to the small size of short messages, spammers have limited ways to modify a message without changing the meaning of the message. Spam messages sent out in a unit of time are usually similar in structure. This similarity could be harnessed to cluster short messages, and to categorize larger clusters as being mobile messaging spam.

One solution in this area is based on the structural similarity of short messages sent during a time frame, and to cluster them into groups of messages. However, this solution has no way of determining by itself if such clusters correspond to spam or bulk sending legitimate messages.

Therefore, it needs to be complemented by a learning process where the system should be equipped to distinguish between spam and legitimate clusters.

This technology requires little involvement of the administrator and the maintenance cost is relatively low. The disadvantage is that it needs adequate training on the network side, and it may cause false positives for the legitimate distribution of mobile messages.

7.8 Indication information recognition

Some spam messages contain URLs or mobile phone numbers that recipients can access. Indication information recognition uses this information as a statistical resource. If the occurrence number of URLs or the mobile phone numbers exceed a threshold, the follow-up message that contains the same indication information is considered to be a spam message.

7.9 Analysis of messaging sending dispersion

Dispersion is the ratio of the number of sent messages related to a sender to the number of recipients. If the dispersion is approximately one-to-one, this would mean that each message is sent to a different recipient. In this case, the sender will be considered as a suspicious spammer. In reality, dispersion could be used in combination with other judgments to determine whether a sender is a spammer or not. For example, if the number of messages sent out from a sender within a day exceeds a preset threshold and the dispersion is less than 1:1, the sender should be considered as a high suspicious spammer. If the sender does not have a voice call charge within a month, or if the sender is a new user of the network, the sender should be considered a spammer.

7.10 Limitation on the total amount of sent messages

There is also a mechanism to reduce massive spam messages by limiting the total amount of sent messages, for example, a limit of 500 messages per day per mobile phone number. It is easy to deploy, but it is difficult to set the limit for sending messages. Moreover, it may disturb legitimate users, for example, when a company sends internal notifications that may exceed the threshold.

7.11 Security software

Security software is available for t users so that they could install it on their mobile handsets to recognize and filter spam messages. This will allow users to identify spammers or spam messages and block them themselves. However, it may not be a good solution in countries where users are charged for incoming messages. Even though the software prevents the messages from being displayed on the mobile handset, users may still be charged for the received messages.

8 Analysis for countering mobile messaging spam

8.1 Comparison

A comparison has been made of the various technologies, with six performance indicators. The results are shown in Table 1:

Table 1 – Performance comparison of technologies

No.	Technologies	Maintenance cost	Real-time performance	Recognition rate	False positive rate	Complexity	Training time
1.	Blacklists/ whitelists	High	Good	High	Medium	Easy	Medium
2.	Content-based filtering	High	Bad	High	Medium	Medium	Long
3.	Spam reporting	High	Medium	High	Low	Easy	Short
4.	Traffic statistics	Low	Medium	Medium	Medium	Medium	Medium
5.	Analysis of CDR	Low	Bad	Medium	Medium	Medium	Medium
6.	Greylisting	Low	Good	Medium	Medium	Medium	Short
7.	Duplicate content recognition	Low	Bad	Medium	Medium	Medium	Long
8.	Indication information recognition	Low	Bad	Medium	Medium	Medium	Medium
9.	Analysis of messaging sending dispersion	Low	Bad	High	Low	Medium	Medium
10.	Limitation on the total amount of sent messages	Low	Good	Medium	Medium	Easy	Low
11.	Security software	Medium	Good	High	Low	Medium	Medium

The maintenance cost indicator is the expenditure for maintaining effectiveness. Technologies that require continuous updating demand more maintenance efforts.

When choosing a solution, real-time performance is an important consideration, especially for those solutions deployed on the user side. Technologies which are deployed offline have a relatively low real-time performance, but they can be used in conjunction with other technologies.

The recognition rate indicator is the rate of accuracy in recognizing spam, and it is one of the most important indicators. Some technologies do not have a high recognition rate, but this rate could be increased if used in combination with other technologies.

The false positive rate indicator is the rate whereby a legitimate message/sender is identified as a spam/spammer. It is essential to protect the users from deleting useful messages such as credit card alert messages, payment messages and other important notification messages. This indicator could be considered together with the recognition rate to evaluate the efficiency of solutions.

Complexity is an indicator that shows the complexity of the deployment of a solution. Technologies that require complicated training processes or changing of the mobile network entities may need more effort to deploy.

The training time indicates the time required for the training process before a solution becomes effective. For example, filtering based on text classification algorithms needs a longer training time.

It can be concluded from the preceding analyses that there is no single solution to the problem of mobile messaging spam, but that a solution combining several technologies must be used. The objectives of the solutions to counter spam are to decrease the number of mobile messaging spam, reduce the false positive rate, avoid causing delays in message sending, and provide a better service quality to the users.

8.2 Deployment framework

There are two methods for the deployment of technologies: deployment in the operator network and deployment in the security applications of the mobile handset. Figure 1 illustrates the deployment framework of technologies in this supplement.

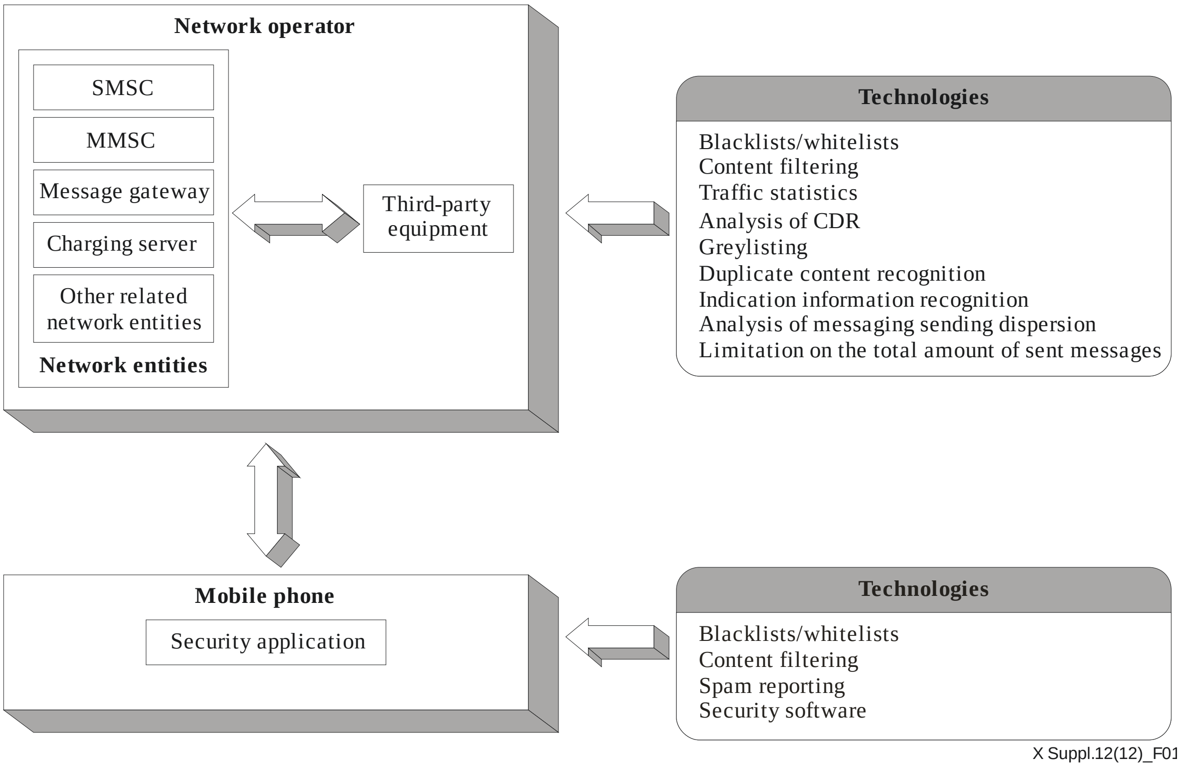

Figure 1 – Deployment framework of technologies

1) Deployment in the network operator:

Recognition of messaging spam and the labelling operation are carried out in the message service centre, the message gateway, the charging server and/or any network-related entities. This method could deploy relatively complex commercial solutions with a high performance rate. Moreover, multiple messaging service centres could be connected together to obtain an overall perspective in countering messaging spam.

- Blacklists/whitelists could be deployed in the network operators to block recognized or reported spammers.
- Technologies that need a high computation capability such as filtering based on text classification algorithms are appropriate for deployment in the network operators. These technologies could also be used together with the security applications of the mobile handset based on the client/server architecture.
- Technologies that need an analysis of information collected by the network operator have to be deployed on the network side: these include traffic statistics, analysis of CDR, duplicate content recognition, indication information recognition and analysis of messaging sending dispersion.
- Technologies that need the control of operators have to be deployed on the network side, such as greylisting and limitation on the total amount of sent messages.

2) Deployment in the security applications of the mobile handset:

Security applications installed in the mobile handset could be obtained by the users for countering messaging spam. The applications are usually developed by individual developers or commercial companies, and users could get the applications for free or obtain commercial products for acquiring better functionality. This method allows users to have more control for countering mobile spam. However, due to a limited processing ability, limited storage space and the multiple types of mobile handsets, this method cannot be used widely for all types of mobile handsets.

- Blacklists/whitelists could also be used in the mobile handset to block any unwanted message sender.
- Simple keyword-based filtering and content-based filtering technologies which use algorithms that do not need a high computation capability and large storage space could be deployed in the security applications of the mobile handset. The content-based filtering technology in the mobile handset could be used together with the network operator based on the client/server architecture.
- Spam reporting and security software could be used in the mobile handset.

Appendix I

Activities on countering mobile messaging spam

I.1 Development of technical specifications for countering mobile messaging spam

I.1.1 ITU-T

Recommendations with regard to countering mobile messaging spam in ITU-T are as follows:

– Technical strategies for countering spam

[b-ITU-T X.1231] describes technical strategies in general and does not identify technical strategies for any specific type of spam. In addition, it gives a hierarchical model for countering spam. The model includes the following five parts:

- equipment strategies
- network strategies
- service strategies
- filtering strategies
- feedback strategies.

The five parts above can be divided into three levels: infrastructure level, service level and application level. Figure I.1 shows the relationship between the different parts.

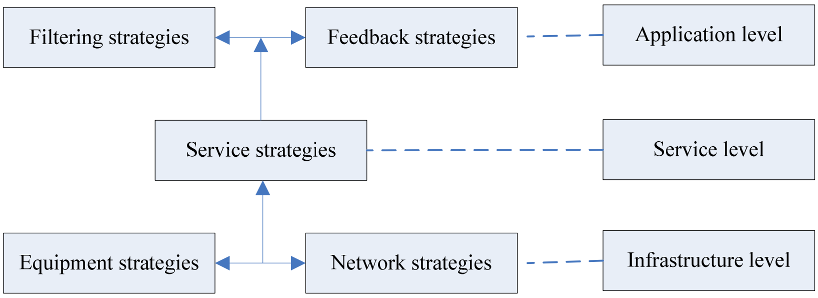

Figure I.1 – Relationship between the different parts

[b-ITU-T X.1231] also points out that the cost may be too high to satisfy all technical strategies. Therefore, it is very important to decide upon the technical strategies according to the different application scenarios.

– SMS spam filtering system based on user-specified rules

[b-ITU-T X. 1242] describes the realization of the SMS spam filtering system based on user-specified rules. The filtering rules can be based on the mobile phone number, time and content, etc., and they can be used either individually or in combination with other filtering rules. In addition, users can manage (query, delete and restore) the filtered short messages and filtering rules by SMS, or the web.

The SMS spam filtering system includes the following five logical modules: the service control module (SCM), the SMS spam filtering module (SSFM), the user service management module (USMM), the user-specified rules database (URD), and the filtered messages database (FMD). The structure of the SMS spam filtering system is shown in Figure I.2.

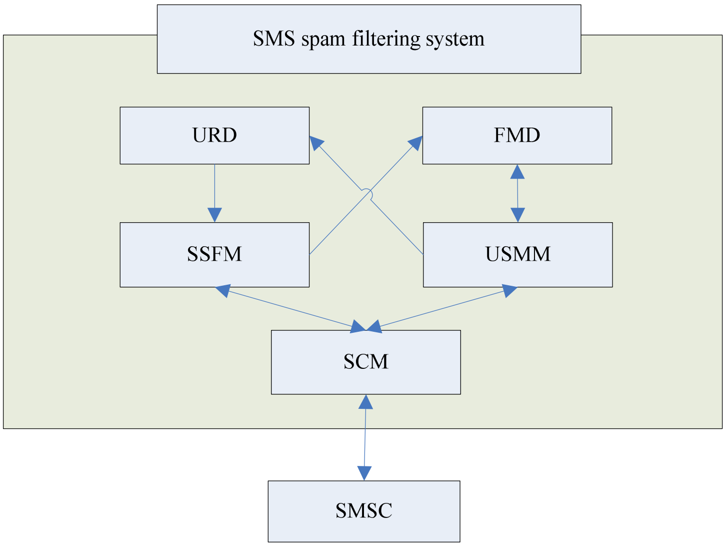

Figure I.2 – Structure of the SMS spam filtering system

The SCM is connected to the SMSC directly and is mainly responsible for the external entities accessing the filtering system. The SSFM implements SMS spam filtering, while the USMM implements the management of the filtering rules and the filtered short messages. The URD is used for storing the user-specified filtering rules. The FMD is used for storing short messages filtered out as spam by the SSFM.

I.1.2 3GPP (3rd Generation Partnership Project)

With respect to the anti-spam research in SMS and MMS, the following mechanisms have been proposed in 3GPP:

– Transaction capabilities application part (TCAP) user security

Accurate verification of the sender's identity is a precondition to the successful development of anti-spam technology. As the number of spam messages increases, operators are regularly confronted with difficulties in applying SMS spam protection rules because addresses for mobile-terminated SMS traffic are spoofed in the signalling connection control part or in the mobile application part (MAP). Furthermore, spoofed addresses may cause accounting differences between operators. [b-3GPP TS 33.204] defines TCAPsec mechanism for protecting all TCAP user messages. TCAPsec can be used together with TCAP handshake solutions. However, when using TCAPsec for MAP, SMS transfers between two public land mobile networks (PLMNs), running TCAP handshake in addition does not add more security. The benefit for an operator applying TCAPsec will gradually increase when more interconnected operators apply this same mechanism.

– Routing of MT-SMs (mobile terminated-short messages) via the HPLMN (home public land mobile network)

[b-3GPP TR 23.840] provides a study into the current core network architecture for inter-PLMN short message delivery. Since user equipment often lacks the capability for complex spam identification and processing, such functionality is provided by the HPLMN. However, as discussed in this report, if the receiving mobile station is roaming outside of the HPLMN, then short messages do not pass through the HPLMN and, consequently, cannot be intercepted by the HPLMN. As a result, the end user will receive such spam messages while roaming and, occasionally, incur a roaming charge for receiving them.

According to the analysis, it is proposed that all MT-SMs shall have the capability to be routed via a SMSC-like (for example, a SMS router) logical entity located in the HPLMN of the receiving mobile station. Before arriving at the visited public land mobile network (VPLMN) that the end user will visit, short messages will first pass through the receiving message's HPLMN which will apply the relevant anti-spam measures. The short messages will then be sent to the receiver.

– Protection against unsolicited communication for IMS (PUCI)

  [b-3GPP TR 33.937] describes several solutions that could be used to protect mobile users from receiving unsolicited communication (UC) over IMS. The following four solutions are described in the report:

  - SPIT (spam over Internet telephony)/UC protection with supplementary services (SS)
  - contextual information (CI) – an extension to SS
  - methods for authenticating the originating networks such as the open proxy handshake (OPH)
  - identification, marking and reacting (IMR).

  SS for SPIT/UC protection may be used to realize a form of user self-protection supported by the networks. While the network provides the supplementary services with resources such as blacklists or whitelists, the user may configure these resources according to his personal needs.

  CI provides means that can be used together with SSs to identify a potential UC when the communication is taking place for the first time between two parties.

  Unsolicited communication-open proxy handshake (UC-OPH) provides methods to secure communication between networks, especially IMS and non-IMS networks. Furthermore, UC-OPH is dependent on other solutions. Therefore, it should be used either with SS or IMR.

  IMR provisions for identifying, marking and reacting against UC are based on operator policies and user requirements.

  The four solutions presented in the report are complementary. SSs can be enhanced with CI. UC-OPH is the solution for inter-operator purposes, and IMR provides a framework that uses SSs as modules for identification and, where available, marking.

  [b-3GPP TR 33.838] focuses more on high-level solution possibilities for PUCI described in [b-3GPP TR 33.937].

I.1.3 OMA (Open Mobile Alliance)

The anti-spam work related to SMS and MMS has the following work items in OMA:

– Client side content screening (CSCS)

  With the growing amount of malicious content delivered to mobile terminals, CSCS defines the architecture for the content screening framework within the mobile terminal. The scope of this architecture is restricted to the client/terminal deployments only. The framework consists of three parts: a scan engine functional component, OMA and non-OMA enablers, and framework interfaces to OMA/non-OMA enablers for utilizing content scanning functionality to detect and screen malicious content. The logical model of the content screening framework in a mobile terminal is shown in Figure I.3.

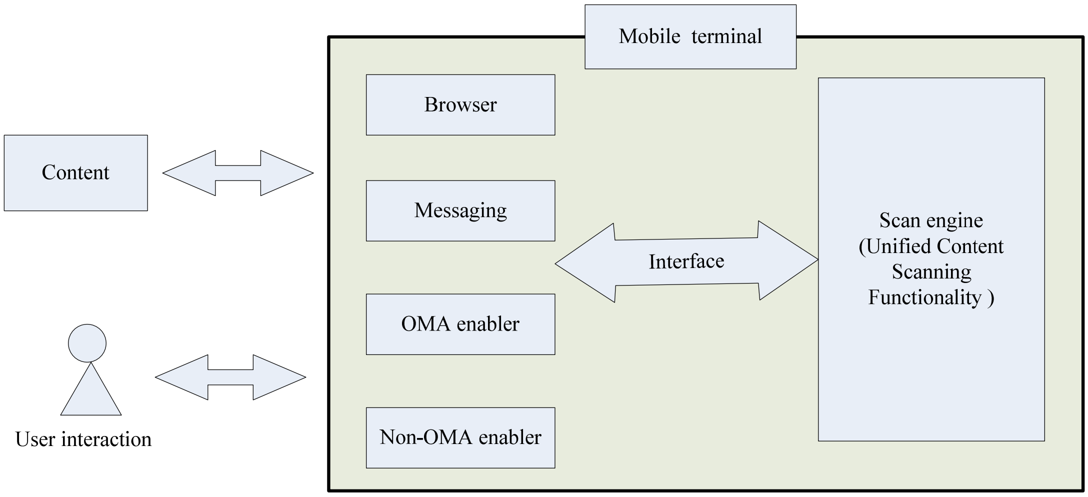

Figure I.3 – Client side content screening framework

The general process is as follows. An enabler would directly pass content to the scan engine for analysis before it is presented to the end user. The scan engine would analyse the content to verify if it is malicious or not, and then return the result of the analysis to the calling enabler. The calling enabler screens the content if the content is found to be malicious. It is recommended that the screening action be conveyed to the end user in the form of a warning message, notification, and so on. If the content is found to be non-malicious, then the enabler shall not screen the content but shall continue with its normal flow of operation.

– Categorization-based content screening (CBCS)

The objective of the CBCS enabler is to screen the content before delivering it to the user, based on content categories. The CBCS enabler can be applied to any content, regardless of the enabler or protocol that is used to deliver the content.

The CBCS enabler consists of two components: a content screening component that applies screening rules to determine whether the content should be categorized, modified in any way, and delivered; and a content categorization component that maps content and/or content references in the incoming request to a set of content categories.

– Mobile spam reporting (SpamRep)

The purpose of the spam reporting enabler is to provide a mechanism that allows users to designate received content as spam, and then to send a report to an external entity containing information about that content. The report may be used by the external entity to prevent further instances of unwanted content from reaching the users. The scope of the SpamRep enabler is intentionally narrow and includes only the SpamRep message format and the message transfer between the mobile handset and the network entity.

– Secure content identification mechanism (SCIDM)

The objective of SCIDM enabler is to leverage available identification mechanisms to identify all kinds of content, including both premier and user-generated content, for various applications. That is, this mechanism provides a basic service: a standardized trusted content ID that is a more trusted representation of the content than simply a content name. The mechanism could be used in content-based filtering, content tracing, automatic content monitoring, content management, etc. However, SCIDM only provides a unique ID based on the content of a message; it could not classify the message as unsolicited message. To counter mobile messaging spam, this method could be used in combination with the content categorization-based enablers such as CBCS.

I.2 International activities on countering mobile messaging spam

I.2.1 ITU

ITU implements a series of cooperative activities on countering spam which include mobile messaging spam to foster international cooperation, the creation of harmonized policy frameworks, the promotion of information exchange and best practices, as well as providing support to developing countries in the field of countering spam. The main activities of ITU on countering mobile messaging spam include:

– ITU World Summit on the Information Society (WSIS) thematic meeting on countering spam, which took place from 7-9 July 2004 in Geneva, recognized once more that spam has become a major concern, in particular considering developments such as phishing and other fraudulent activities, which are threatening public confidence in e-mails and in the Internet as a whole.

– ITU members approved Resolution 51 on Combating Spam and Resolution 52 on Countering spam by technical means during the ITU World Telecommunication Standardization Assembly (WTSA), held in Brazil in October 2004.

– ITU conducted a survey and created the "Spam Laws and Authorities" website to gather information on anti-spam legislations around the world, including details of the authorities responsible for anti-spam measures in each country. Some legislative/governmental actions are related to mobile messaging spam, such as "CAN-SPAM Act" of the USA, "Directive on Privacy and Electronic Communications" of European Union, "Law on Regulation of Transmission of Specified Electronic Mail" of Japan and "Spam Act 2003" of Australia, etc.

– ITU Global Symposium for Regulators held a breakout session on spam in December 2004, the meeting highlighted that cooperation between different authorities is necessary and should imply the exchange of information as well as joint action; cooperation should also involve the industry. International cooperation arrangements are essential in tackling the problem appropriately.

More ITU activities on countering spam could be referenced at http://www.itu.int/osg/spu/spam.

I.3 Industry alliances and initiatives for countering mobile messaging spam

I.3.1 Alliance of ISC (Internet Society of China)

The Internet Society of China established the Alliance of ISC (Internet Society of China) at a meeting held on 17 July 2008. The meeting was attended by leaders of the Ministry of Industry and Information Technology of China, along with the main Internet service providers, Internet content providers, and other stakeholders. A self-discipline convention statement was published during the meeting. All members promised to act together to counter messaging spam in their operating process.

12321 is an operational spam reporting centre in China, open to everybody who wishes to report spam information: on the web (www.12321.cn), by WAP (wap.12321.cn), by a telephone call (010-12321), by SMS (12321,) or by e-mail (abuse@12321.cn). On the website of 12321, the most recent spam information will be published. The 12321 spam message reporting centre forms part of the Alliance of ISC's efforts to counter mobile messaging spam.

I.3.2 Mobile Marketing Association (MMA)

The Mobile Marketing Association (MMA) is a global non-profit trade association established to foster growth of mobile marketing. MMA believes that strong consumer privacy standards are essential to the success of mobile marketing by protecting mobile users from unwanted communications on their mobile handset. Therefore, it has established a Code of Conduct that is supposed to limit the damage caused by mobile messaging spam. The code provides guidelines that all mobile makers should consider and build their mobile programs around The code describes the privacy principles that mobile marketers should adopt when they choose the user information to market their products and the services provided to those users via mobile handsets. For more information on the work of MMA, see http://mmaglobalcom.

I.3.3 GSM Association (GSMA)

The GSM Association (GSMA) is an association of mobile operators and related companies devoted to supporting the standardization, deployment and promotion of the GSM mobile telephone system. The GSMA has developed a Mobile Spam Code of Practice which has been devised to protect the secure and trusted environment of mobile services, and to ensure that customers receive a minimal amount of spam sent via SMS and MMS. To support this initiative, GSMA is encouraging member operators to sign up to the code and for governments and consumer associations to support the industry in its endeavours.

Bibliography

[b-ITU-T K.49] Recommendation ITU-T K.49 (2005), *Test requirements and performance criteria for voice terminal telephones subject to disturbance from digital mobile telecommunications systems*.

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

[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-3GPP TR 23.840] 3GPP TR 23.840 V7.1.0 (2007), *Technical Specification Group Core Network and Terminals; Study into routing of MT-SMs via the HPLMN*.

[b-3GPP TR 33.838] 3GPP TR 33.838 (2011), *Technical Specification Group Services and System Aspects; Study on protection against unsolicited communication for IP Multimedia Subsystem (IMS) (PUCI)*.

[b-3GPP TR 33.937] 3GPP TR 33.937 V10.0.0 (2011), *Technical Specification Group Services and System Aspects; Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI)*.

[b-3GPP TS 33.204] 3GPP TS 33.204 V10.0.0 (2011-03), *3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security*.

[b-OMA-RD-Client_Side_CS_FW] OMA-RD-Client_Side_CS_FW-V1_0-20070614-A (2007-06-14), *Client Side Content Screening Framework Requirements*.

[b-OMA-AD-Client_Side_CS_FW] OMA-AD-Client_Side_CS_FW-V1_0-20070614-A (2007-06-14), *Client Side Content Screening Framework Architecture*.

[b-OMA-RD-CBCS] OMA-RD-CBCS-V1_0-20111206-A (2011), *Categorization Based Content Screening Framework Requirements*.

[b-OMA-AD-CBCS] OMA-AD-CBCS-V1_0-20111206-A (2011), *Categorization Based Content Screening Framework Architecture*.

[b-OMA-RD-SpamRep] OMA-RD-SpamRep-V1_0-20101123-C (2010), *Mobile Spam Reporting Requirements*.

[b-OMA-AD-SpamRep] OMA-AD-SpamRep-V1_0-20101123-C (2010), *Mobile Spam Reporting Architecture*.

[b-OMA-RD-SCIDM] OMA-RD-SCIDM-V1_0-20081216-C (2008), *Secure Content Identification Mechanism Requirements*.

[b-OMA-AD-SCIDM] OMA-AD-SCIDM-V1_0-20090728-C (2009), *Secure Content Identification Mechanism Architecture*.

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	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
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012