International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1245

(12/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Framework for countering spam in IP-based multimedia applications

Recommendation ITU-T X.1245

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
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.

Recommendation ITU-T X.1245

Framework for countering spam in IP-based multimedia applications

Summary

Recommendation ITU-T X.1245 provides the general framework for countering spam in IP-based multimedia applications such as IP telephony, instant messaging, multimedia conference, etc. The framework consists of four anti-spam functions, i.e., core anti-spam functions (CASF), recipient-side anti-spam functions (RASF), sender-side anti-spam functions (SASF), and spam recipient functions (SRF). This Recommendation describes the functionalities and the interfaces of each function for countering IP multimedia spam.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1245	2010-12-17	17

Keywords

Anti-spam functions, IP multimedia spam, 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 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

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation	1
4	Abbreviations and acronyms	2
5	Conventions	3
6	Technical methods for countering IP multimedia spam	3
6.1	Source analysis method	4
6.2	Characteristics analysis method	5
6.3	Content analysis method	6
7	Framework for countering IP multimedia spam	7
7.1	Spammer	7
7.2	SAS functions	7
7.3	RAS functions	11
7.4	CAS functions	13
7.5	SR functions	17
7.6	Reference points in the framework	19
Appendix I – Countering spam by imposing spamming difficulties		20
Appendix II – Security and practical considerations in using the framework		21
II.1	Security considerations	21
II.2	Practical considerations	22
Bibliography		24

Recommendation ITU-T X.1245

Framework for countering spam in IP-based multimedia applications

1 Scope

This Recommendation provides the general framework for countering IP multimedia spam. The framework can be applied to IP-based multimedia applications such as IP telephony, instant messaging, multimedia conference, etc. The framework includes four anti-spam functions, i.e., core anti-spam functions (CASF), recipient-side anti-spam functions (RASF), sender-side anti-spam functions (SASF), and spam recipient functions (SRF). It describes the functionalities and the interfaces of each function for countering IP multimedia spam. Technical means for the implementation of the framework are outside the scope of this Recommendation.

Compliance with all relevant laws and regulations should be considered before adopting the anti-spam methods described in this Recommendation.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 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.

3.1.2 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 function (ASF): A logical function for countering spam in IP-based multimedia applications. ASF can be located in network elements such as proxy server, application server, etc.

3.2.2 blacklist: An identification list of persons or sources in communication services, where the identifications of the list are denied to access particular communication resources.

3.2.3 core ASF (CASF): An instance of ASF which identifies and blocks IP multimedia spam. It also has the capabilities to manage anti-spam policies and to control RASF and SASF.

3.2.4 IP multimedia spam: Unsolicited messages or calls through IP-based multimedia applications which usually have special characteristics of spam such as bulkiness. Distinguished from traditional e-mail spam, IP multimedia spam indicates spam on communication methods over IP, such as instant messaging or voice over IP services.

3.2.5 recipient-side ASF (RASF): An instance of ASF which identifies and blocks IP multimedia spam being delivered to spam recipients through the boundary of internal network. RASF can be located in the network elements where inbound communication requests to spam recipients are sent as the last hop.

3.2.6 sender-side ASF (SASF): An instance of ASF which identifies and blocks IP multimedia spam being delivered from spammers to the boundary of external network. SASF can be located in the network elements where outbound communication requests from spammers are sent as the first hop.

3.2.7 spam recipient: An entity or a person that receives spam.

3.2.8 spam recipient function (SRF): An ASF whose role is to identify and block IP multimedia spam arrived to spam recipients. SRF can be located in the home-network or terminals of spam recipients.

3.2.9 whitelist: An identification list of persons or sources in communication services, where the identifications of the list are known, trusted, or explicitly permitted.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ARS Automated Response System

ASF Anti-Spam Functions

CA Certification Authority

CAS Core Anti-Spam

CASF Core Anti-Spam Functions

CRL Certificate Revocation List

DAC Discretionary Access Control

HBAC History-based Access Control

IM Instant Messaging

IP Internet Protocol

IPSec Internet Protocol Security

L2TP Layer 2 Tunneling Protocol

MAC Mandatory Access Control

MTA Mail Transfer Agent

NDAC Non-Discretionary Access Control

OTP One Time Password

PBAC Purpose-based Access Control

PKI Public Key Infrastructure

RAS Recipient-side Anti-Spam

RASF Recipient-side Anti-Spam Functions

RBAC Role-based Access Control

RuBAC Rule-based Access Control

SAS Sender-side Anti-Spam

SASF Sender-side Anti-Spam Functions

SPF Sender Policy Framework

SR Spam Recipient

SRF Spam Recipient Functions

SSL Secure Socket Layer

TCAC Temporal Constraints Access Control

TTP Trusted Third Party

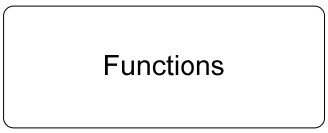
TTS Text To Speech

VoIP Voice over Internet Protocol

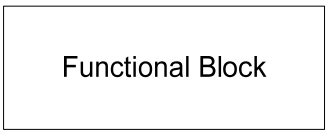
VPN Virtual Private Network

5 Conventions

Functions: In the context of the framework for countering IP multimedia spam, "functions" are defined as a collection of functionalities. It is represented by the following symbol:



Functional block: In the context of the framework for countering IP multimedia spam, a "functional block" is defined as a group of functionalities that has not been further subdivided at the level of detail described in this Recommendation. It is represented by the following symbol:



6 Technical methods for countering IP multimedia spam

IP multimedia spam can be defined as unsolicited messages or calls through IP-based multimedia applications. To distinguish IP multimedia spam from traditional e-mail spam, IP multimedia spam denotes spam on communication methods over IP, such as voice over IP, instant messaging, etc. IP multimedia spam usually has special characteristics which can be distinguished from normal IP-based multimedia applications. These characteristics can be used for anti-spam functions to identify and to filter spam by implementing the functions on the appropriate IP network elements. Technical methods for countering IP multimedia spam can be classified into the following three categories:

– countering IP multimedia spam by source analysis of IP-based multimedia applications,

– countering IP multimedia spam by characteristics analysis of IP-based multimedia applications,

– countering IP multimedia spam by content analysis of IP-based multimedia applications.

Figure 1 presents the three technical methods for countering IP multimedia spam and examples of anti-spam techniques.

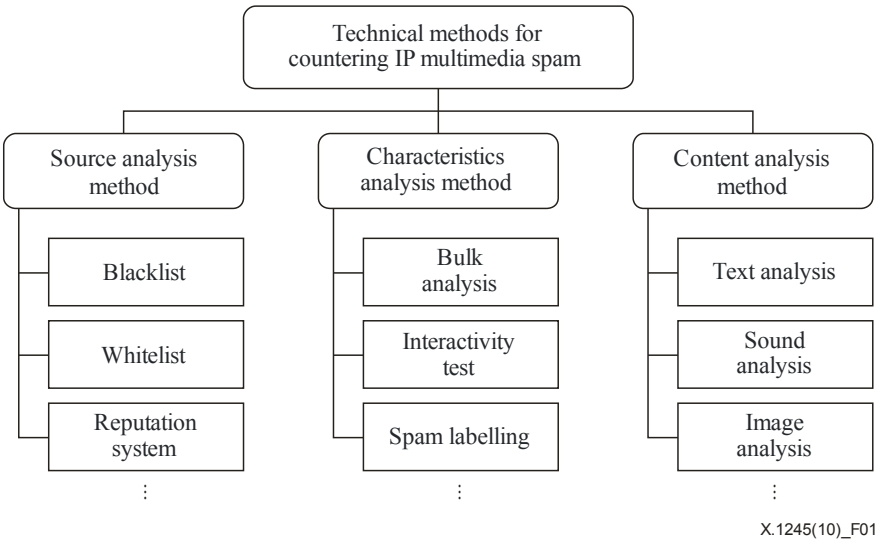


Figure 1 – Technical methods for countering IP multimedia spam

Many anti-spam techniques in Figure 1 have been applied for countering e-mail spam, and they are also applicable to IP multimedia spam. Anti-spam techniques for countering IP multimedia spam are not limited to these examples.

Anti-spam functions on IP network need to interact with each other to make use of these anti-spam techniques. Functions and interfaces of the anti-spam entities needed for implementing the anti-spam methods are described in the following clauses. Using only one anti-spam technique may not be effective enough for countering IP multimedia spam. In that case, more than one anti-spam technique may need to be deployed simultaneously on the IP network for more effective spam filtering.

6.1 Source analysis method

An IP-based multimedia application from a certain source can be identified whether it is spam or not by analyzing the source information of the IP-based multimedia application such as the reputation information or the spamming history of the source. IP address, domain name, phone number, and user identifier can be used as source identifiers.

Examples of source based anti-spam techniques are whitelist, blacklist, reputation system, etc. They have been widely used for countering e-mail spam and can also be applied for countering IP multimedia spam. The applicability of these techniques to IP multimedia spam is described in [b-ITU-T X.1244]. However, the source analysis methods may have some weaknesses which reduce the effectiveness of anti-spam techniques, e.g., spammers may try sender spoofing or be able to make many service accounts. Therefore, the following measures are expected to help the source based anti-spam techniques for countering IP multimedia spam become more effective:

– strong authentication of the sources of IP-based multimedia applications,

– effective management of spam identification policy and related information.

First of all, a high reliability of source information of IP-based multimedia applications is needed for effective spam filtering, since spammers can try to make a detour to avoid these anti-spam techniques by creating a great number of service accounts, or by attempting sender spoofing to cover that the sender is a spammer. Therefore, strong authentication of the sources of IP-based multimedia application can be helpful to provide a high reliability of source information.

As described above, spam filtering information (e.g., whitelist, blacklist, etc.) as well as sources of IP-based multimedia applications are used to identify spam. Therefore, spam filtering information and spam identification criteria need to be managed effectively.

This technique has an advantage since spam can be blocked before it is delivered to the recipient. Moreover, on the assumption that the considerations above are satisfied, effective spam countering is possible with a relatively small effort in comparison with the other anti-spam techniques such as content analysis, characteristics analysis, etc.

6.2 Characteristics analysis method

6.2.1 Anti-spam methods based on characteristics analysis

IP multimedia spam has many special characteristics which can be distinguished from normal IP-based multimedia applications. For example, IP multimedia spam is sometimes delivered in bulk and has limited interactivity compared with normal IP-based multimedia applications. An IP-based multimedia application can be considered as spam and filtered out when it has one or more of the characteristics. The following are some characteristics, but are not limited to, of IP multimedia spam:

– Bulk

IP multimedia spam is sometimes delivered in bulk, since spammers usually try to send spam to a large number of spam recipients at one time to minimize the spamming cost. When a great quantity of IP-based multimedia applications is delivered from a source to many destinations in a short time, it can be considered as potential spam.

– Limited interactivity

IP multimedia spam, in many cases, provides only limited interactivity since spammers tend to send spam using machines instead of persons to reduce the spamming cost. For example, in instant messaging spam or in chat spam, spam senders may not reply since the spam message is sent by spamming machines. VoIP spam, a form of telemarketing, may also provide limited interactivity when it is sent using ARS. It is possible, therefore, to identify spam by testing whether the sender of the IP-based multimedia application provides interactivity or not. The most common anti-spam techniques based on this method in an e-mail system are the Turing test and greylisting, which test the interactivity of the sender and the MTA, respectively.

6.2.2 Usage of protocol information for countering spam

It is more efficient to make use of the protocol information than of the content information for identifying spam using the characteristics analysis method. The protocol part of the IP-based multimedia application can be used for the identification of spam by analyzing the source of the IP-based multimedia application. Identifying spam, using the protocol information before the content of the IP-based multimedia applications is delivered to the recipient, takes less effort and is more effective in comparison with other anti-spam techniques which use content information. The following results render this conclusion more viable:

– Application provision information

The protocol part of the IP-based multimedia applications carries information related to the provision of IP-based multimedia applications, e.g., source, destination, time of delivery, delivery protocol used, etc. Some of these protocol parts can be used to identify spam.

– Timing of analysis

Protocol information for service initiation is delivered before the content of the IP-based multimedia applications is delivered. For example, in VoIP service, the signalling process during which the protocol information is used is executed before the call session is initiated. Therefore, it can be possible to identify spam before spam is delivered to the recipient by analyzing the protocol information.

– Encryption

Protocol messages are usually delivered without encryption, although the content of the IP-based multimedia applications may be delivered with encryption. Encryption of IP packets makes the packet analysis very difficult or impossible to decrypt. Therefore, the protocol part can be easier analyzed than the content part of the IP-based multimedia applications.

– Type of media

The protocol part of the IP-based multimedia applications uses only one kind of media; whereas, the content part is sometimes in the form of multimedia, which is difficult to analyze.

– Delivery path

Protocol messages for session or service initiation transit through a network equipment, e.g., an application server for instant messaging and proxy servers for VoIP communication, which can obtain provisioning information of IP-based multimedia applications from the protocol messages. On the other side, content messages may be delivered directly from the sender to the recipient without transiting through the network equipment. In this case, the content of IP-based multimedia applications can be difficult to analyze.

6.3 Content analysis method

In the content analysis method, the content analysis result of the IP-based multimedia applications is used to identify spam. This method has been used widely for countering e-mail spam. Content analysis of the IP-based multimedia applications can be much more difficult than the case of e-mails, since IP-based multimedia applications can be real time and/or use multimedia, while e-mails are usually text-based and not real time. The following are considerations for the effective countering of IP multimedia spam in the content analysis method:

– Time duration of content analysis

The content needs to be analyzed within a reasonable amount of time, to enable IP-based multimedia application users to identify spam. In real-time IP-based multimedia applications, it may be impossible to execute content analysis before the application is initiated.

– Accuracy of content analysis

The accuracy of the content analysis of IP-based multimedia applications needs to meet a certain level of quality for effective spam identification. Highly advanced sound and image recognition technologies will be helpful, since the content analysis of multimedia is very difficult compared to text analysis.

– Encryption of content

The content analysis of IP-based multimedia applications may be very difficult or impossible to decrypt when the IP packets are encrypted.

– Delivery path of content

The IP-based multimedia application content is analyzed when it transits through certain network equipment such as an application server or a media server, which has a content analysis function.

In many cases, IP-based multimedia applications may not satisfy the required criteria. In the case of real-time IP-based multimedia applications such as VoIP, it seems to be impossible to detect and filter spam within a reasonable amount of time for the service users of the content analysis, since it is possible to analyze the content only after the communication session has been established between the caller and the called. On the other hand, there might be sufficient time to analyze the content in the case of non real-time IP-based multimedia applications such as recorded voice messages. Nonetheless, content analysis may have difficulties in obtaining sufficient information to identify spam because of immature technologies for speech and image recognition or an insufficient quantity of content. When the content of text-based IP-based multimedia applications, such as IM

services and text message services, is analyzed, spam identification can also be difficult when the content is encrypted or delivered directly between the service users without transiting through a proper network equipment for content analysis.

7 Framework for countering IP multimedia spam

IP network entities with anti-spam functions need to interact with each other for countering IP multimedia spam. Functions and interactions of the anti-spam entities needed for implementing the anti-spam methods are described in this clause. Application of only one anti-spam technique may not be effective enough for countering IP multimedia spam. Therefore, more than one anti-spam technique may need to be implemented simultaneously in the IP network for more effective spam filtering.

This clause describes the framework for countering IP multimedia spam. It is designed in such a way that it can be easily extended to various technical means for countering spam in various applications and networks. The framework is designed to protect users and networks from IP multimedia spam. Spam can appear anywhere; therefore, detection and filtering mechanisms for various spam need to be provided throughout the network.

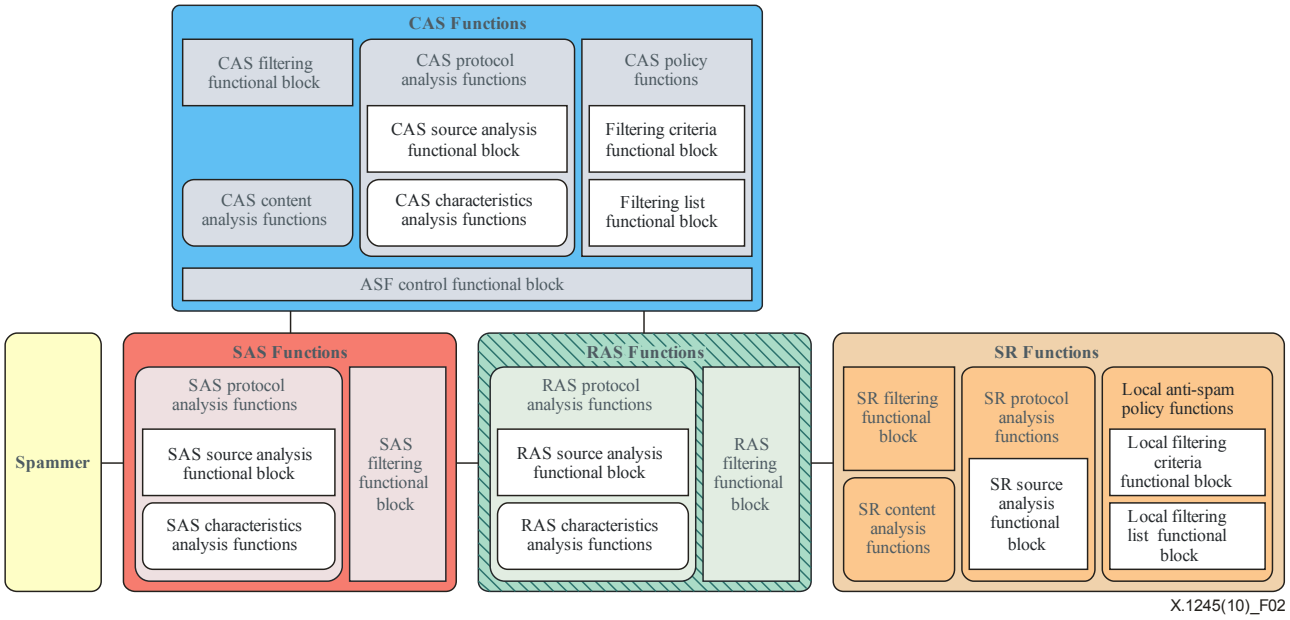


Figure 2 – Framework for countering IP multimedia spam

The framework for countering IP multimedia spam consists of five elements as shown in Figure 2. The following clauses describe the functions and interfaces of each element.

7.1 Spammer

The spammer creates and spreads spam throughout the network. It is the originator of spam. Anti-spam functions are not implemented in the spammer.

7.2 SAS functions

The SASF (sender-side anti-spam functions) is a group of anti-spam functions the role of which is to identify and block IP multimedia spam which is initiated from spammers. The SASF can be implemented on network elements such as a proxy server, where outbound communication requests from spammers are sent as the last hop. The SASF interacts with the CASF (core anti-spam functions) for the execution of anti-spam functions in the SASF. It is more efficient to block spam

at the source-side before it spreads through the network, although the SASF may play a less active role than other components in the real communication environment.

The SASF is composed of SAS protocol analysis functions and SAS filtering functional block for the control of spam filtering. The following clauses describe various techniques that can be adopted by the SASF to counter IP multimedia spam.

7.2.1 SAS filtering functional block

The SAS filtering functional block determines whether the analyzed IP-based multimedia application is spam or not, based on the analysis result of the SAS protocol analysis functions and anti-spam policy. Therefore, it interacts with the CASF and other anti-spam functions or functional blocks in the SASF.

7.2.2 SAS protocol analysis functions

The SAS protocol analysis functions analyze the protocol information of the received IP-based multimedia applications. It is composed of the SAS source analysis functional block and the SAS characteristics analysis functions which analyze the source information and the characteristics of the received IP-based multimedia applications, respectively.

i) SAS source analysis functional block

The SASF can distinguish IP multimedia spam from non-spam IP-based multimedia applications, based on the source information of the IP-based multimedia applications. The SASF has two aspects related to the source of IP-based multimedia applications. One aspect is source filtering with the anti-spam policy provided by the CASF, and the other aspect is sender authentication.

– Anti-spam policy

The SASF can identify and filter spam using the source address of the IP multimedia data packet. The filtering is not only done with the source address but also with other protocol information that are available to the SASF. Figure 3 represents anti-spam functions and the interactions among the functions for countering IP multimedia spam by the source analysis in the SASF.

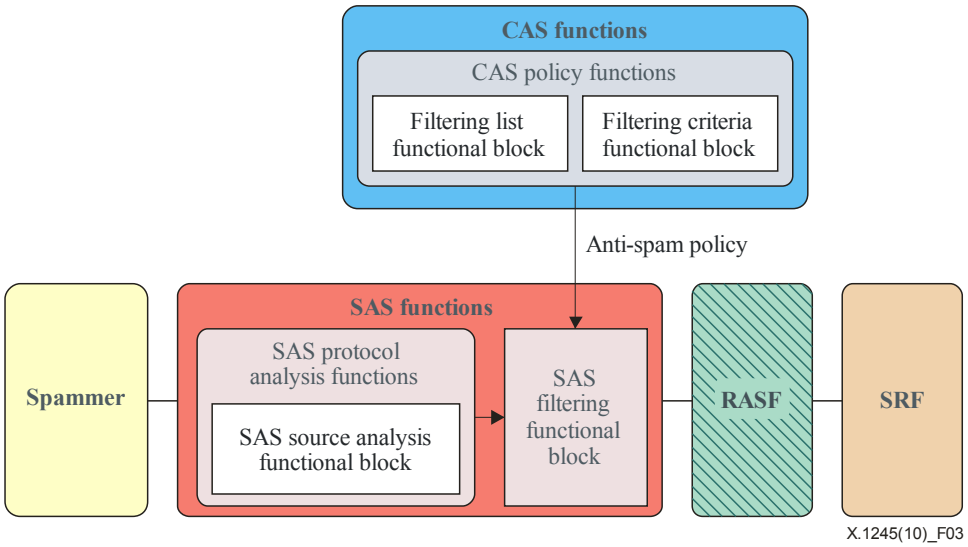


Figure 3 – Countering IP multimedia spam by the source analysis in SASF

The SAS filtering functional block can obtain the anti-spam policy from the CAS policy functions. The SAS filtering functional block filters the IP packet sent by the spammer when the IP packet is identified as spam, based on the analysis result.

– Sender authentication

The SASF has the authentication information of the senders and the SASF can provide user authentication for the originated traffic. The SASF may prevent unauthorized entities from using the IP-based multimedia applications, when required.

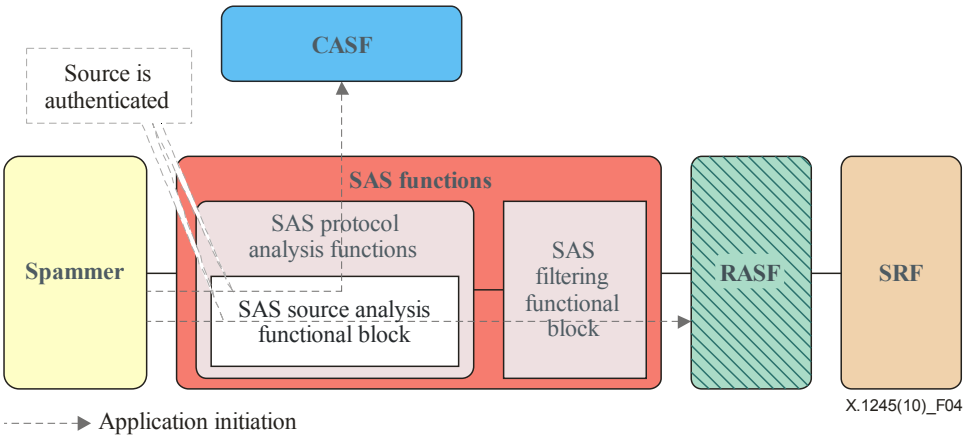


Figure 4 – Source authentication of SASF

Figure 4 shows the schema for the source authentication by the SASF. The source analysis capability of the SASF has an authentication functionality that can authenticate spammer traffic before being sent to the CASF or the RASF (recipient-side anti-spam functions). The SASF may discard traffic that has failed the authentication, if it is needed, and only the authenticated traffic may be sent to other ASFs. Discarding unauthorized traffic can be helpful to prevent the spammers who try spoofing.

– Filtering procedure

The procedure in which the SASF filters IP multimedia spam by the source analysis is as follows:

1) Delivery of anti-spam policy: The SASF receives the anti-spam policy from the CASF. The anti-spam policy can be delivered to the SASF as a notification or as a request/reply manner.

2) Reception of IP-based multimedia applications: The SASF receives an initiation of IP-based multimedia applications.

3) Source authentication: The SASF authenticates the source of the applications. If the authentication process fails, the SASF declines the initiation request from the spammer.

4) Spam identification and filtering: The SASF makes a decision on the received IP-based multimedia application, based on the received anti-spam policy from the CASF and the source of the request. The SASF can decline or ignore the traffic that is determined as IP multimedia spam.

ii) SAS characteristics analysis functions

The SASF can distinguish spam by using the characteristics of applications such as service bulk. The SASF can utilize a threshold that can be used to check for bulk. The SAS characteristics analysis functions can include several specific characteristics analysis functional blocks. The functionality and interface of each functional block is a specific technical means for countering IP multimedia spam, and they are outside the scope of this Recommendation. The following lists are some examples of the characteristics that can be distinguished by the SASF to apply the anti-spam method.

– Bulk

The SAS characteristics analysis functions may have the capability to analyze the amount of service request from a single source and analyze the rate of the service request. The SAS filtering functional block identifies IP multimedia spam, based on the analysis result of the SAS characteristics analysis functions and the anti-spam policy received from the CAS filtering criteria functional block.

– Limited interactivity

The SASF may have the capability to test for service interactivity on the spammer, although an interactivity test for the source of the IP-based multimedia applications may usually be done by the CASF. Spammers tend to use machines which cost relatively less than human resources to initiate IP-based multimedia applications. Therefore, testing interactivity is one method to check for IP multimedia spam.

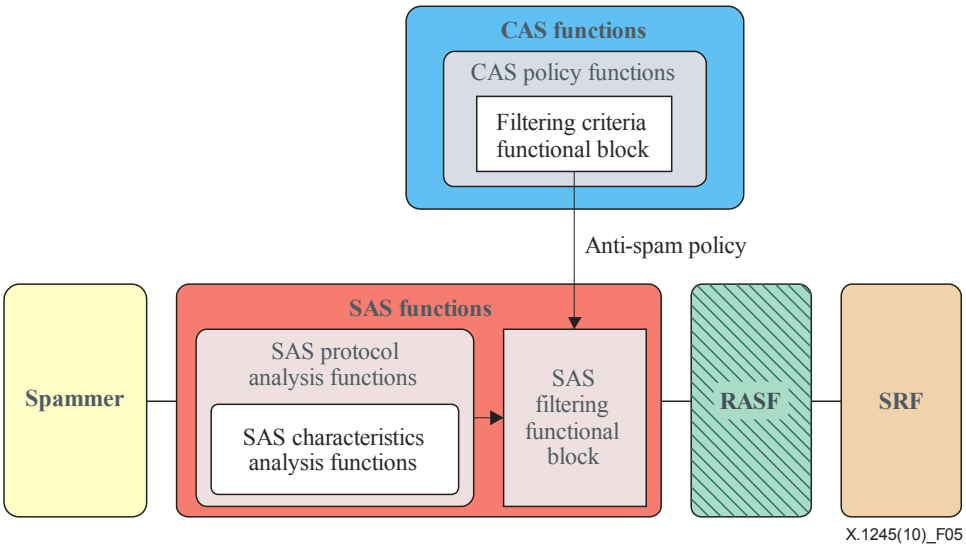


Figure 5 – Countering IP multimedia spam by the characteristics analysis in SASF

The procedure in which the SASF filters IP multimedia spam by the characteristics analysis is as follows:

1) Delivery of anti-spam policy: The SAS filtering functional block receives the anti-spam policy on the characteristics analysis from the CASF. The anti-spam policy can be delivered to the SASF as a notification or as a request/reply manner.
2) Reception of IP-based multimedia applications: The SASF receives an initiation of IP-based multimedia applications.
3) Characteristics analysis: The SAS characteristics analysis functions extract the spam-related characteristics of the received IP-based multimedia applications.
4) Result processing: The results of the characteristics analysis are sent from the SAS characteristics analysis functions to the SAS filtering functional block.
5) Spam filtering: The SAS filtering functional block processes spam according to the anti-spam policy. If the outcome of the analysis results is spam, the SASF can decline or ignore the traffic that is determined as IP multimedia spam.

Spam management policy for IP multimedia spam depends on the service providers, the service users, the IP-based multimedia applications, the national regulations, etc. Thus, the SASF and the RASF need to interact with the CASF to get information about the anti-spam policy to counter spam, based on the characteristics of an IP-based multimedia application.

7.3 RAS functions

The RASF is a group of functions the role of which is to identify and block IP multimedia spam which is delivered to the spam recipient. The RASF can be implemented on network elements such as a proxy server where inbound communication requests to spam recipients are sent as the last hop. The RASF interacts with the CASF for the execution of anti-spam functions in the RASF.

The CASF and the RASF can be implemented in the same network equipment which covers spammers and spam recipients at the same time. However, the anti-spam functions which operate in the equipment are different according to the traffic flow. In other words, the anti-spam functions of the equipment operate as the SASF when the traffic is from IP-based multimedia application users which the equipment covers, and they operate as the RASF when the traffic is forwarded to IP-based multimedia application users which the equipment covers.

The RASF is composed of the RAS protocol analysis functions and the RAS filtering functional block for the control of spam filtering.

Although it is technically possible for the SASF or the RASF to analyze the content of the delivered traffic for countering spam, they are not covered by the content analysis functions in this Recommendation, as this will require additional processing constraints on them. When an IP-based multimedia application does not pass through the CASF as a default, the RASF may deliver the IP-based multimedia application to the CASF and request the CASF to analyze the content of the IP-based multimedia application for the identification of spam.

The following clauses describe the various techniques that can be adopted by the RASF to counter IP multimedia spam.

7.3.1 RAS filtering functional block

The RAS filtering functional block determines whether the analyzed IP-based multimedia application is spam or not, based on the analysis result and the anti-spam policy. Therefore, it interacts with the CASF and other anti-spam functions or functional blocks in the RASF.

7.3.2 RAS protocol analysis functions

The RAS protocol analysis functions analyze the protocol information of the received IP-based multimedia applications. It is composed of the RAS source analysis functional block and the RAS characteristics analysis functions, which analyze the source information and the characteristics of the received IP-based multimedia applications, respectively.

i) RAS source analysis functional block

The RASF can distinguish IP multimedia spam from non-spam IP-based multimedia applications, based on the source information of the IP-based multimedia applications. For the identification of spam, the RASF characterizes the anti-spam policy regarding the source provided by the CASF such as blacklist, whitelist, reputation score, etc. Figure 6 represents the anti-spam functions and interactions of the functions for countering IP multimedia spam by the source analysis.

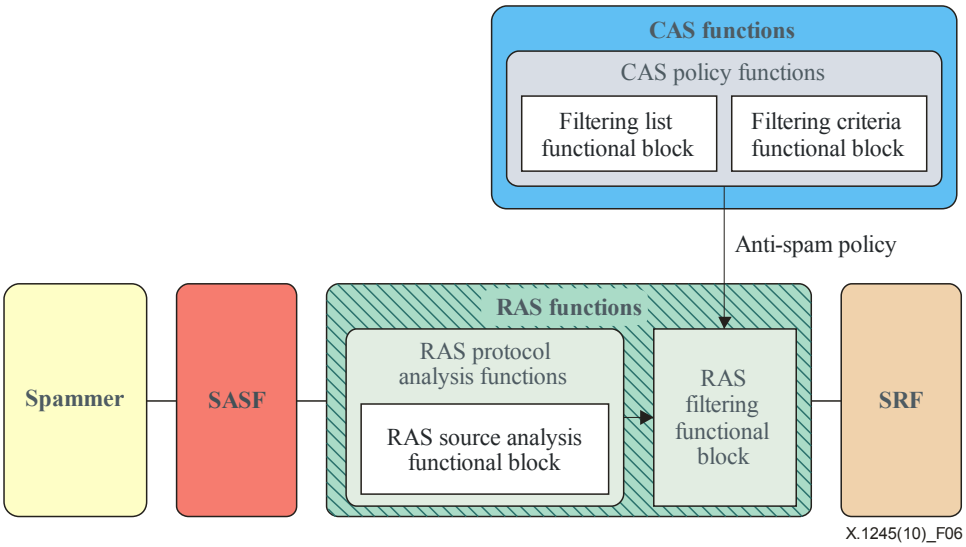


Figure 6 – Countering IP multimedia spam based on the source analysis

The RASF determines whether an IP-based multimedia application is spam or not, based on the source information of the IP-based multimedia application, and handles it according to the result. Since a high reliability of the source information is required for the effectiveness of the source-based anti-spam technique, it is assumed that the IP-based multimedia application which the RASF receives from the SASF is trustworthy, i.e., authenticated. The RASF identifies the IP multimedia spam according to the spam filtering criteria or to the spam filtering list provided by the CASF. The CASF maintains the filtering list and the filtering criteria to support the RASF, the SASF, or the CASF itself to identify spam. The following are processes of spam identification and filtering of the RASF using the source analysis method:

1) Delivery of anti-spam policy from the CASF: The RASF receives the anti-spam policy from the CASF. The anti-spam policy can be delivered to the RASF as a notification or as a request/reply manner.

2) Reception of IP-based multimedia applications: The RASF receives an IP-based multimedia application and checks the source of the IP-based multimedia application.

3) Spam identification and filtering: The RASF makes a decision on the received IP-based multimedia application, based on the source information and the anti-spam management policy received at the previous stage. The RASF can decline or ignore the traffic that is determined as IP multimedia spam, according to the anti-spam policy of the service provider or of the service users.

When the RASF identifies spam based on the blacklist or whitelist, the filtering list from the CASF can be used. When the RASF identifies spam based on the reputation score, the filtering criteria, such as the threshold reputation score at which an IP-based multimedia application is determined as spam, can be used.

ii) RAS characteristics analysis functions

The RASF can identify spam by using the IP-based multimedia application to check whether spam has the characteristics of IP multimedia spam or not. The RAS characteristics analysis functions can include several specific characteristics analysis functional blocks. Technical means for countering IP multimedia spam are outside the scope of this Recommendation.

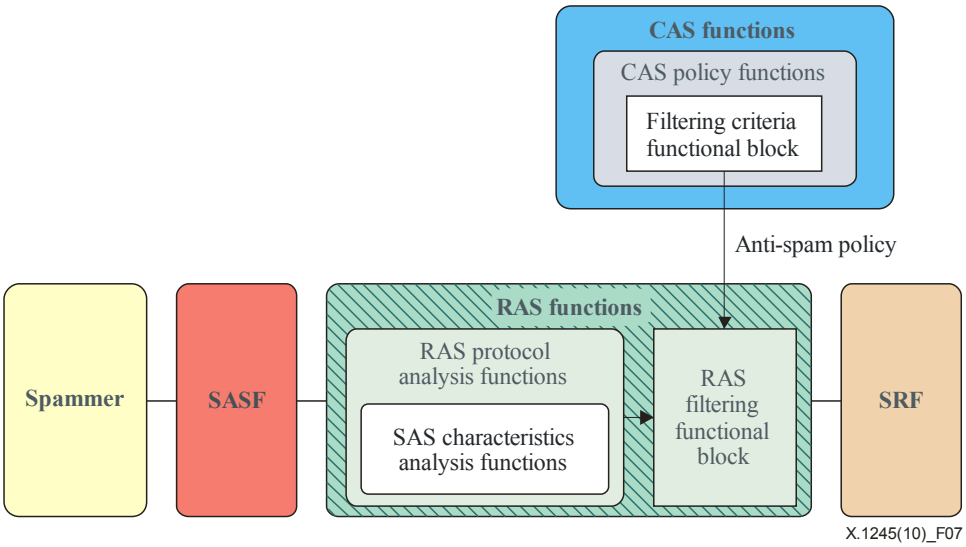


Figure 7 – Countering IP multimedia spam based on the characteristics analysis

Figure 7 represents the anti-spam functions and interactions among the functions for countering IP multimedia spam by the characteristics analysis in the RASF. The procedure in which the RASF identifies IP multimedia spam by the characteristics analysis is as follows:

1) Delivery of anti-spam policy: The RAS filtering functional block receives the anti-spam policy on the characteristics analysis from the CASF. The anti-spam policy can be delivered to the RASF as a notification or as a request/reply manner.

2) Reception of IP-based multimedia applications: The RASF receives an initiation of IP-based multimedia applications.

3) Characteristics analysis: The RAS characteristics analysis functions extract the spam-related characteristics of the received IP-based multimedia application.

4) Result processing: The RAS characteristics analysis functions provide the analysis result to the RAS filtering functional block.

5) Spam filtering: The RAS filtering functional block processes spam according to the anti-spam policy. If the outcome of the analysis results is spam, the RASF can decline or ignore the traffic that is determined as IP multimedia spam.

7.4 CAS functions

The CASF has the capabilities to manage anti-spam policies and to control the RASF and the SASF. It also has the capabilities to analyze the source or the characteristics of the IP-based multimedia applications to identify and filter spam when there is a path of IP packets between spammers and spam recipients in providing the IP-based multimedia applications, according to the type of IP-based multimedia applications. The CASF has the CAS protocol analysis functions, the CAS content analysis functions, the CAS filtering functional block, the CAS anti-spam policy functions, and the ASF control functional block. This clause describes the functionalities and interactions of each entity in the CASF to counter IP multimedia spam.

7.4.1 CAS filtering functional block

The CAS filtering functional block determines whether the analyzed IP-based multimedia application is spam or not, based on the analysis result and the anti-spam policy. Therefore, it interacts with other anti-spam functions or functional blocks in the CASF.

7.4.2 CAS protocol analysis functions

The CAS protocol analysis functions analyze the protocol information of the received IP-based multimedia applications. It is composed of the CAS source analysis functional block and the CAS characteristics analysis functions, which analyze the source information and the characteristics of the received IP-based multimedia applications, respectively.

i) CAS source analysis functional block

When an IP-based multimedia application is provided under the control of the network component where the CASF resides, e.g., a user's logon in an instant messaging service or in a VoIP service under the control of application servers, the CASF can be a possible functional entity to identify spam by the source analysis. Figure 8 represents the anti-spam functions and interactions among the functions for countering IP multimedia spam by the source analysis in the CASF.

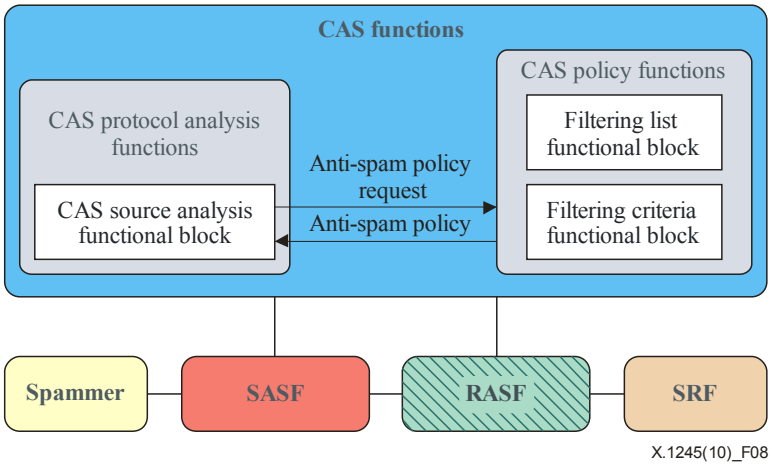


Figure 8 – Countering IP multimedia spam based on the source analysis

The following describes a possible procedure of countering IP multimedia spam, based on the source information of an IP-based multimedia application at the CASF:

1) Authentication: A user wants to use an IP-based multimedia application (e.g., instant messaging service), and the user is authenticated by a network component such as an application server which has the CASF.
2) Reception of IP-based multimedia applications: The user sends a request of an IP message delivery to the CASF, and the CAS source analysis functional block checks the source of the user.
3) Obtaining the anti-spam policy: The CAS source analysis functional block requests the anti-spam policy and receives it from the CAS policy functions.
4) Spam identification and filtering: The CASF makes a decision on the received IP-based multimedia application, based on the source information and the anti-spam policy received at the previous stages. The CASF can decline or ignore the traffic that is determined as IP multimedia spam, and it is then handled according to the anti-spam policy of the service provider or the service user when it is identified as spam.

ii) CAS characteristics analysis functions

The CASF can be a characteristics analysis point for countering spam when an IP-based multimedia application is provided under the control of a network entity of the CASF. The CASF analyzes an IP-based multimedia application as to whether it has the characteristics of spam, and it utilizes the filtering criteria in the anti-spam policy to determine whether it is spam or not. Figure 9 shows the

overall architecture and interfaces in the characteristics analysis method for countering IP multimedia spam at the CASF.

The CASF policy functions have the filtering criteria functional block which contains the spam filtering criteria required to identify IP multimedia spam and provides the criteria to the SASF or the RASF to support them in identifying spam. For example, when the CAS characteristics analysis functions attempt to identify spam when an IP-based multimedia application is in bulk, the CASF filtering criteria functional block can provide the quantity criteria which identifies the quantity level of an IP-based multimedia application as IP multimedia spam.

Figure 9 represents the anti-spam functions and interactions among the functions for countering IP multimedia spam by the characteristics analysis in the CASF.

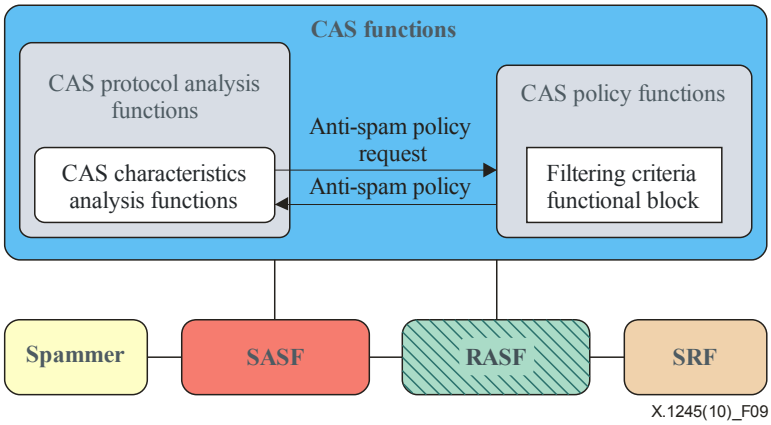


Figure 9 – Countering IP multimedia spam based on the characteristics analysis

The following are the procedures of the characteristics analysis for countering IP multimedia spam at the CASF:

1) Spam characteristics analysis: When an IP-based multimedia application attempts to be connected under the control of a network entity to which the CASF belongs, the CASF analyzes whether it has the characteristics of spam, e.g., bulkiness, limited interactivity, etc.

2) Obtaining the anti-spam policy: The characteristics analysis functions request the CAS policy functions for the anti-spam policy related to the characteristics analysis for filtering spam. The anti-spam policy block sends the requested information to the CAS characteristics analysis functions.

3) Spam identification and filtering: The CAS characteristics analysis functions determine whether the IP-based multimedia application is spam or not, based on the analysis result of the characteristics analysis functions and the received anti-spam policy.

7.4.3 CAS content analysis functions

The CASF has the CAS content analysis functions. These functions analyze the content of an IP-based multimedia application for the identification of spam when the IP-based multimedia application is delivered to the recipient via the network equipment, where the CASF resides such as an application server or a media server.

Identifying spam by using the protocol information of the IP-based multimedia applications, e.g., the source information or the characteristics of spam, any of the CASFs, the SASFs, or the RASFs can be the analyzer. On the other hand, identifying spam by using the content analysis, the CASF, where the IP-based multimedia applications content is transited, is a reasonable functional entity point for content analysis where content-based anti-spam techniques are used for countering IP multimedia spam.

Figure 10 represents the anti-spam functions and interactions among the functions for countering IP multimedia spam by the content analysis in the CASF.

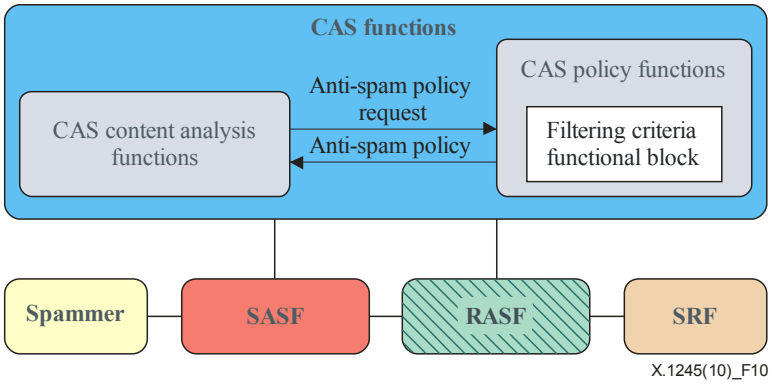


Figure 10 – Countering IP multimedia spam based on the content analysis

The following are the procedures of the content analysis for countering IP multimedia spam at the CASF:

1) Reception of IP-based multimedia applications: The content of IP-based multimedia application arrives at the CASF.

2) Content analysis: The CAS analysis functions analyze the content of the IP application.

3) Obtaining the anti-spam policy: The CASF requests the CAS policy functions for the anti-spam policy and receives the policy from the filtering criteria functional block.

4) Spam identification and filtering: The CASF decides whether the IP-based multimedia application is spam or not, based on the analysis result and the anti-spam policy.

As described in clause 6, the applicability of the content analysis method may be limited according to the characteristics of an IP-based multimedia application, e.g., whether the IP-based multimedia application is real time or not, whether it is multimedia or not, or whether the content of IP-based multimedia applications is encrypted or not.

7.4.4 CAS policy functions

The CAS policy functions maintain the anti-spam policies for countering IP multimedia spam and are composed of the filtering criteria functional block and the filtering list functional block.

i) Filtering criteria functional block

The filtering criteria functional block maintains the anti-spam filtering criteria for the identification of IP multimedia spam. There can be various kinds of filtering criteria, according to the deployed anti-spam techniques. For example, in bulk analysis, the threshold amount of IP-based multimedia applications, which is sent at a time from one source, can be a filtering criterion. Creation and management mechanisms of the filtering criteria are outside the scope of this Recommendation.

ii) Filtering list functional block

The filtering list functional block manages the filtering list for the identification of IP multimedia spam, based on the source analysis. There can be various kinds of spam filtering lists, according to the deployed anti-spam techniques. For example, blacklist, whitelist, and reputation score can be used as filtering lists. The filtering list can either be a public list for many identical service users, a personal list managed personally, or a combination of both. The creation and management mechanisms of the filtering list are outside the scope of this Recommendation.

7.4.5 ASF control functional block

The ASF control functional block interacts with the SASF and the RASF to support them in the identification and filtering of spam. It delivers the anti-spam policies from the CAS policy functions to the RASF and the SASF.

7.5 SR functions

The spam recipient is the endpoint for IP multimedia spam. Users can be affected and damaged by the IP multimedia spam, if there is no spam-countering mechanism.

The spam recipient has SR (spam recipient) functions to protect itself from IP multimedia spam. The users can set the anti-spam policy or receive it from the service providers to filter IP multimedia spam. The SR functions are composed of the SR protocol analysis functions, the SR content analysis functions, the SR filtering functional block, and the local anti-spam policy functions. This clause describes the functionalities and interactions of each anti-spam function that can be adopted by the spam recipient for countering spam.

7.5.1 SR protocol analysis functions

The SR protocol analysis functions have the SR source analysis functional block which can identify spam, based on the sender information. Although it is possible to filter spam on the CASF, the SASF, and the RASF, in case of directly connected IP-based multimedia applications, the anti-spam functions and the anti-spam policy of the SRF can be used for countering IP multimedia spam.

The spam recipient can define a local filtering list and local filtering criteria, or it can receive the list from other anti-spam functions such as the CASF. The specific mechanisms for defining the anti-spam policy are outside the scope of this Recommendation. Figure 11 represents anti-spam functions and interactions among the functions for countering IP multimedia spam by the source analysis in the SRF.

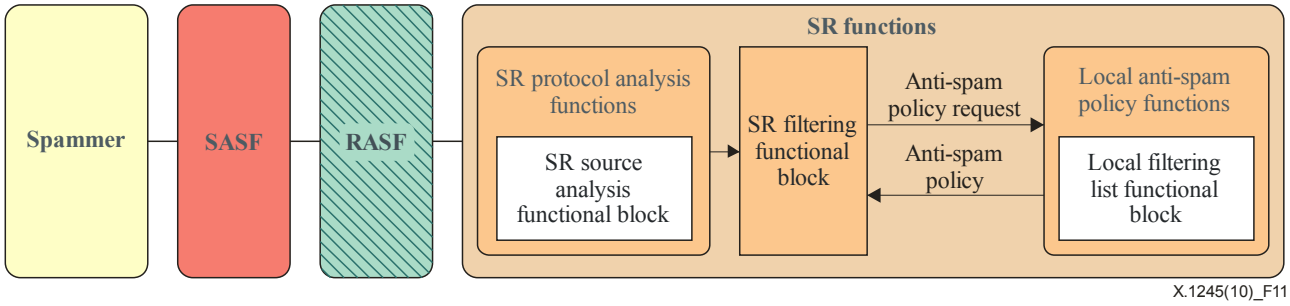


Figure 11 – Countering IP multimedia spam by the source analysis in the spam recipient

The following describes a possible procedure for countering IP multimedia spam, based on the source information of an IP-based multimedia application at a spam recipient.

1) Reception of IP-based multimedia applications: The SRF receives an initiation of IP-based multimedia applications and checks the source of the IP application.

2) Obtaining the anti-spam policy: The SR protocol analysis functions request the anti-spam policy and receive it from the local anti-spam policy functions.

3) Spam identification and filtering: The SR filtering functional block makes a decision on the received IP-based multimedia application, based on the anti-spam policy and the source analysis result. The spam recipient can decline or ignore the traffic that is determined as IP multimedia spam.

The spam recipient functions may technically identify spam by using the characteristics analysis. However, the SR protocol analysis functions do not have the characteristics analysis functional block, since it is risky to depend on the spam recipient to perform sophisticated spam countering functions, as in the characteristics analysis method, because the SR protocol analysis functions are under the control of a highly variable group of users.

7.5.2 SR content analysis functions

It is possible for the spam recipient to counter spam, based on the content analysis. The spam recipient can maintain its own content analysis mechanism, which is user specific, or receive the mechanism from the service providers. The anti-spam policy of the content analysis is placed in the local anti-spam policy functions as part of the local filtering criteria functional block. Figure 12 represents the anti-spam functions and interactions among the functions for countering IP multimedia spam by the content analysis in the SRF.

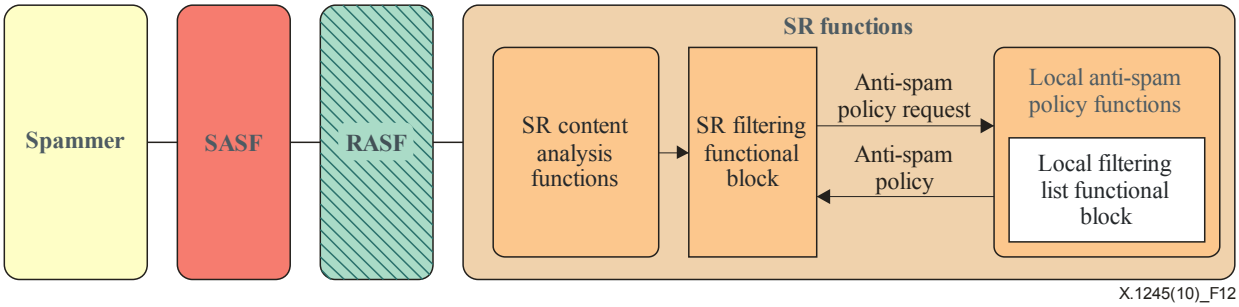


Figure 12 – Countering IP multimedia spam by the content analysis in the spam recipient

The procedure in which the spam recipient filters IP multimedia spam by the content analysis is as follows:

1) Reception of IP-based multimedia applications: The SRF receives an initiation of IP-based multimedia applications. The SR content analysis functions execute the content analysis for the identification of spam.

2) Obtaining the anti-spam policy: The result of the content analysis is sent to the SR filtering functional block. The SR filtering functional block requests and receives the anti-spam policy from the local anti-spam policy functions.

3) Spam identification and filtering: The SR filtering functional block makes a decision on the received IP application, based on the anti-spam policy and the content analysis result. The spam recipient can decline or ignore the traffic that is determined as IP multimedia spam.

7.5.3 SR filtering functional block

The SR filtering functional block determines whether the analyzed IP-based multimedia application is spam or not, based on the analysis result and the anti-spam policy. Therefore, it interacts with other anti-spam functions or functional blocks in the SRF.

7.5.4 Local anti-spam policy functions

The local anti-spam policy functions maintain user-specific anti-spam policies for countering IP multimedia spam. The functions are composed of the local filtering criteria functional block and the local filtering list functional block.

i) Local filtering criteria functional block

The local filtering criteria functional block maintains user-specific anti-spam filtering criteria for the identification of IP multimedia spam. The types of the filtering criteria depend on the anti-spam functions that the SRF supports.

ii) Local filtering list functional block

The local filtering list functional block manages the user-specific filtering list for the identification of IP multimedia spam, based on the source analysis. The types of lists depend on the source analysis functionalities that the SRF supports.

7.6 Reference points in the framework

This clause defines the reference points between various elements in the framework. Figure 13 identifies the reference points in the framework.

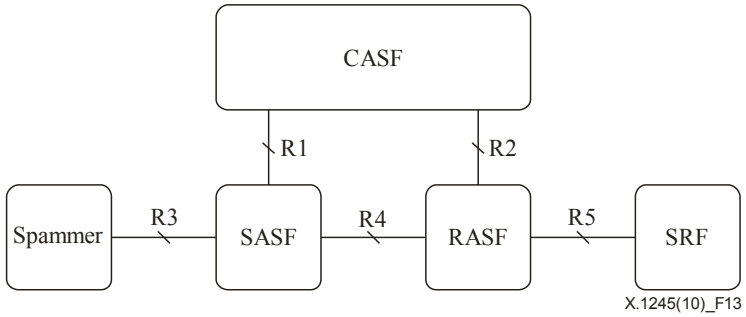


Figure 13 – Reference points in the anti-spam framework

7.6.1 Reference point R1

The R1 is located between the CASF and the SASF, and is used to obtain the filtering policy from the CASF to the SASF. The CASF controls the SASF through R1.

7.6.2 Reference point R2

The R2 is located between the CASF and the RASF, and is used to obtain the filtering policy from the CASF to the RASF. The CASF controls the RASF through R2.

7.6.3 Reference point R3

The R3 is located between spammers and the SASF, and is used in the IP-based multimedia application protocol and/or transmitting data traffic.

7.6.4 Reference point R4

The R4 is located between the SASF and the RASF, and is used in the IP-based multimedia application protocol and/or transmitting data traffic.

7.6.5 Reference point R5

The R5 is located between the RASF and the spam recipients, and is used in the IP-based multimedia application protocol and/or transmitting data traffic.

Appendix I

Countering spam by imposing spamming difficulties

(This appendix does not form an integral part of this Recommendation.)

Imposing spamming difficulties can be one of the technical methods for countering IP multimedia spam. However, this method is somewhat different from the other methods which identify and filter spam directly. Imposing spamming difficulties help reduce the amount of spam indirectly, but this method requires effort, time, and is costly. One way to decrease the quantity of IP multimedia spam could be achieved by increasing the spamming difficulties for spammers, through raising the cost and effort required to create and deliver spam. The spamming charges for spammers are composed of a regulation fee, including an expected penalty fee for illegal spam, an IP-based multimedia application usage fee paid to the service provider or the network provider, and a spam delivery fee, i.e., an interactivity test, etc. The following methods can be used to increase the spamming difficulties:

– Rendering access to the IP addresses difficult: Increase the amount of effort required to gather information about spamming targets, such as IP addresses and IP-based multimedia application service accounts, and make it more difficult for spammers to send IP multimedia spam.
– Payment system: Charging for IP multimedia spam may be helpful to reduce the amount of spam. Adoption of a payment system for potential spam, e.g., bulk IP messages, however, is not a technical issue.
– Bulk prevention: Considering that spam is sent in bulk in many cases, bulk prevention may help decrease the amount of spam.
– Interactivity test: Interactivity tests for the spammers can increase their spamming charges. However, this can have a side effect as it can also bother normal IP-based multimedia application users.

The methods for countering spam by imposing spamming difficulties are not limited to the examples above.

In the interactivity test, the CASF can play the role of the tester. In the bulk prevention method, the CASF, the SASF, or the RASF can identify bulkiness, i.e., a determined level of quantity, and a block of IP-based multimedia applications which have bulkiness. Charging bulk communications or messages under the control of the CASF is also a possible method to increasing the spamming difficulties.

The SASF or the RASF can sometimes analyze the protocol information, but it usually does not take additional actions to increase spamming difficulties such as bulk prevention control, payment management, or interactivity test. In short, it is expected that the SASF or the RASF take some actions to support the CASF to handle spam, and for the CASF to play a main role in increasing spamming difficulties.

Appendix II

Security and practical considerations in using the framework

(This appendix does not form an integral part of this Recommendation.)

II.1 Security considerations

The following are security considerations for countering IP multimedia spam:

– Authentication

Authentication is a process where an entity, either the spam recipient or the CASF, confirms its, his, or her identity by presenting credentials that are difficult for anyone but the actual user to produce.

It is necessary to carry out user authentication to identify the sender of the IP-based multimedia application messages, which helps in blocking out many spoofing attack types of spam. Failure to provide user authentication properly will not be able to trace spammers because they could counterfeit their IP address by a spoofing attack.

Authentication can be accomplished in many ways. Some authentication methods, such as a plain password authentication, are easily implemented but are in general weak and primitive. Other methods of authentication such as secure socket layer (SSL), IPSec, secure shell, Kerberos, which may be more complex and require more time to implement and maintain, provide strong and reliable authentication.

Other emerging technologies, such as cryptographic signature methods, may still prove to be a better solution. However, the most widely adopted and currently available method of sender authentication continues to be the classic sender policy framework (SPF), domain keys.

– Access control

Access control is a means of implementing and enforcing authorization policies. Access control grants a user permission to perform, or prohibit the user from performing an action on the spam recipient and the ASFs, as dictated by a security policy.

Access controls usually apply after authentication has been established. Access control is generally classified as discretionary access control (DAC) and non-discretionary access control (NDAC). In DAC, the object owner specifies who has access to the object or specifies the policies. All access control policies, other than DAC, are categorized as NDAC. In NDAC, policies are rules that are not specified at the discretion of the user. Mandatory access control (MAC), role-based access control (RBAC), purpose-based access control (PBAC), history-based access control (HBAC), temporal constraints access control (TCAC) and rule-based access control (RuBAC) are some examples of NDAC.

– Confidentiality

Confidentiality refers to mechanisms which ensure that only authorized users may access secure communications. There are two main mechanisms to provide confidentiality for electronically transmitted information: encryption or transmission over a secure infrastructure, for example, via a virtual private network (VPN) or other encrypted link.

The IPSec is the protocol used in most VPNs to establish a secure connection over the Internet. IPSec is a widely accepted standard for secure transmission and is flexible and less expensive than some other encryption methods. IPSec provides strong encryption, integrity, and authentication and is particularly useful for organizations needing to transfer data securely through the Internet.

The layer 2 tunneling protocol (L2TP) is a tunneling protocol used to support VPNs. It encapsulates a given network layer protocol inside the point-to-point protocol (PPP) to cryptographically protect the PPP frames and to encapsulate the data inside a tunneling protocol.

– Data integrity

Integrity means that information is unchanged as it moves between the spam recipient and the spammer. Without proper protection, spammers may be able to alter or scramble the content of IP-based multimedia messages.

By using message digests generated by a cryptographic hash function, a system administrator can detect unauthorized changes in messages. Hash functions can also be combined with other standard cryptographic methods to verify the source of data. When hashing algorithms are combined with encryption, they produce special message digests that identify the source of the data.

When digital signatures are used to support data integrity, a public key infrastructure (PKI) may be required to manage encryption keys. The PKI keeps track of the assignment and revocation of public encryption keys to users and organizations.

As an alternative to digital signature and PKI, secret cryptography can be used to provide data integrity. A secret key application is simpler in that only one key is used and must be in the possession of both the sender and the recipient for the encryption and decryption to function. Secret key systems are widely used but suffer from the difficulties that come with the task of distributing the secret keys in a secure manner.

– Non-repudiation

Non-repudiation means a method whereby a sender of a message or originator of a transaction cannot later deny that the transaction took place.

Non-repudiation is achieved through the legal document binding, and the binding of the following security mechanisms and trusted processes for server management: SSL, a challenge-response OTP token, secure hashing, and audit logs.

A common practice for implementing non-repudiation is to take advantage of digital signatures, which could be considered as one of the best alternatives for replacing traditional signatures in electronic data processing. To enable digital signatures, a trusted third party (TTP) or PKI should be available. The TTP or PKI may support at least a certification authority (CA) for issuing digital certificates and certificate revocation lists (CRLs) for checking against revoked certificates.

II.2 Practical considerations

One of the principal goals of the framework is to ensure that the negative impact on business is kept to a minimum. It should be made clear that compliance with anti-spam measures can result in positive outcomes for individuals and businesses, by complying with the requirements of the company.

The following practical considerations are based on the processing operations. They are intended as guidance to implement an anti-spam system and to provide potential suppliers with a high level of information:

– Provide high accuracy and good performance
– Be deployable at the Internet perimeter
– Integrate with popular IP-based multimedia application systems
– Run on the customer's server platform of choice: UNIX, Windows, etc.
– Filter both incoming and outgoing IP multimedia spam
– Provide flexibility to match organization policies and preferences
– Provide the ability for the user to establish individual or specific filters
– Allow end users to manage their own IP-based multimedia application spam folders and set simple preferences

– Provide the ability to manage whitelist and blacklist functionality
– Provide the ability to have content filtering, including the ability to add a server side content filtering with tiers of administration of the toll down to the user level.

Bibliography

[b-ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam.*

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications.*

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, 2011