

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

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/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
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

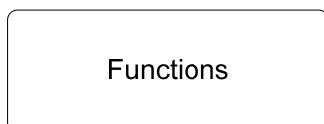
This Recommendation uses the following abbreviations and acronyms:

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

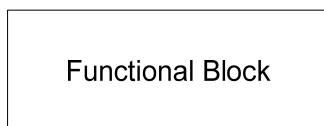
SASF	Sender-side Anti-Spam Functions
SPF	Sender Policy Framework
SR	Spam Recipient
SRF	Spam Recipient Functions
SSL	Secure Socket Layer
TCAC	Temporal Constraints Access Control
TTP	Trusted Third Party
TTS	Text To Speech
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

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.

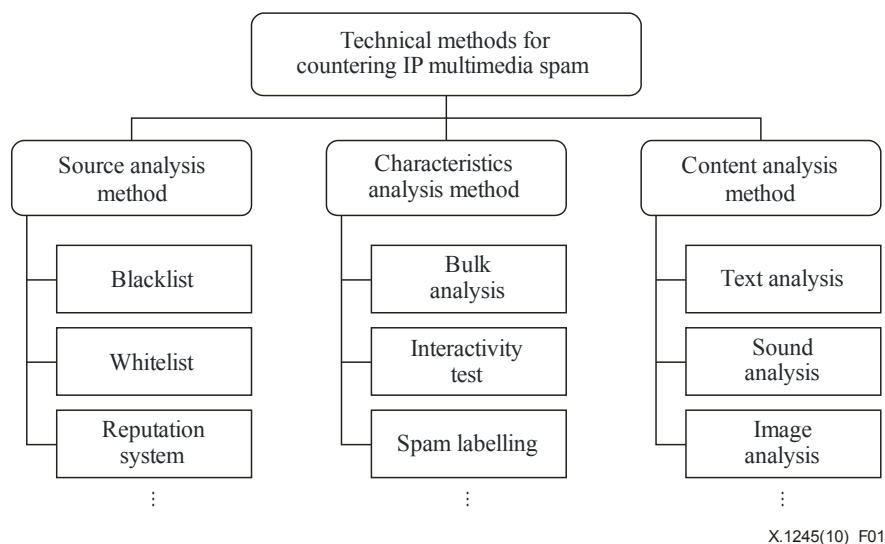


Figure 1 – Technical methods for countering IP multimedia spam

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.