

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1243

(12/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Interactive gateway system for countering spam

Recommendation ITU-T X.1243



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.1243

Interactive gateway system for countering spam

Summary

Recommendation ITU-T X.1243 specifies the interactive gateway system for countering spam as a technical means for countering inter-domain spam. The gateway system enables spam notification among different domains, and it prevents spam traffic from passing from one domain to another.

In addition, this Recommendation specifies the architecture for the gateway system, describes basic entities, protocols and functions of the gateway system, and provides mechanisms for spam detection, information sharing and specific actions in the gateway system for countering spam.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1243	2010-12-17	17

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 Architecture	3
6.1 Spam-countering entities and functions	3
6.2 Spam identification.....	4
6.3 Spam-countering action.....	4
6.4 Spam discovery	4
6.5 Spam notification through spam-countering peering protocol.....	4
7 Spam-countering filtering techniques.....	5
7.2 Supported spam-countering techniques.....	5
8 Process of spam-countering peering protocol.....	9
8.1 Peer discovery	9
8.2 Peer set-up	9
8.3 Spam-countering message exchange.....	9
8.4 Peer release.....	9
9 Implementation model of gateway systems for countering spam	10
9.1 Integrated model.....	10
9.2 Domain-based model.....	10
9.3 Bypass deployment model.....	11
Appendix I – Example of SCPP message definition.....	12
Bibliography.....	14

Recommendation ITU-T X.1243

Interactive gateway system for countering spam

1 Scope

The interactive gateway system for countering spam is a general interactive mechanism for countering various inter-domain spam messages, including e-mail spam, SMS spam, etc., to enable information sharing for countering spam among different domains, and to prevent spam from being sent as well as from being received. This Recommendation supports the diversity of spam-countering filtering techniques, and offers flexibility for upcoming techniques.

Compliance with all relevant national laws and regulations should be considered before adopting this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.509] Recommendation ITU-T X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

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 interactive gateway system for countering spam (IGCS): The interactive gateway system for countering spam is an entity which is responsible for detecting and blocking spam. It has a pair of functions: sender gateway function (SGF) and receiver gateway function (RGF). An IGCS should work with other peers to implement full functions for countering spam.

3.2.2 local spam-countering database: This term specifies a database which is used for storing spam information, blacklist, spam-countering rules for local receiver gateway functions and sender gateway functions.

3.2.3 modality: Modality refers to information encoding(s) containing information perceptible for a human being.

3.2.4 multimodal message: A multimodal message refers to the multimedia message containing differently encoded information for interaction via multiple modalities.

3.2.5 receiver agent: A receiver agent is a server which receives messages for message receivers. In e-mail applications, a POP server acts as a receiver agent.

3.2.6 receiver gateway function: The receiver gateway function is a function of receiver party for countering spam, which detects and blocks spam during the receiving process.

3.2.7 sender agent: A sender agent is a server which sends messages for message senders. In e-mail applications, a SMTP server acts as a sender agent.

3.2.8 sender gateway function: A sender gateway function is a function of sender party for countering spam, which detects and blocks spam during the message sending process.

3.2.9 spam-countering peer: During the process for countering spam, two IGCSs work together to identify and block spam, thus, one IGCS is a spam-countering peer to another.

3.2.10 spam-countering peering protocol: The protocol is defined to exchange spam alert messages and blacklists between spam-countering gateways.

3.2.11 user spam report protocol: The protocol is defined for message receivers to report the spam to the gateway.

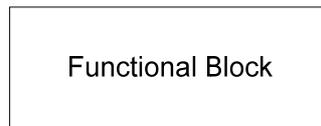
4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

E-mail	Electronic Mail
FE	Functional Entity
IGCS	Interactive Gateway system for Countering Spam
IM	Instant Message
IRC	Internet Relay Chat
LscDB	Local Spam-Countering Database
POP	Post Office Protocol
RA	Receiver Agent
RBL	Real-time Blackhole List
RGF	Receiver Gateway Function
SA	Sender Agent
SCPP	Spam-Countering Peering Protocol
SGF	Sender Gateway Function
SMTP	Simple Mail Transfer Protocol
WPF	Weighted Parameter Filter

5 Conventions

Functional block: In the context of interactive gateway system for countering spam, "functional block" is defined as a collection of functionalities. It is represented by the following symbol:



6 Architecture

6.1 Spam-countering entities and functions

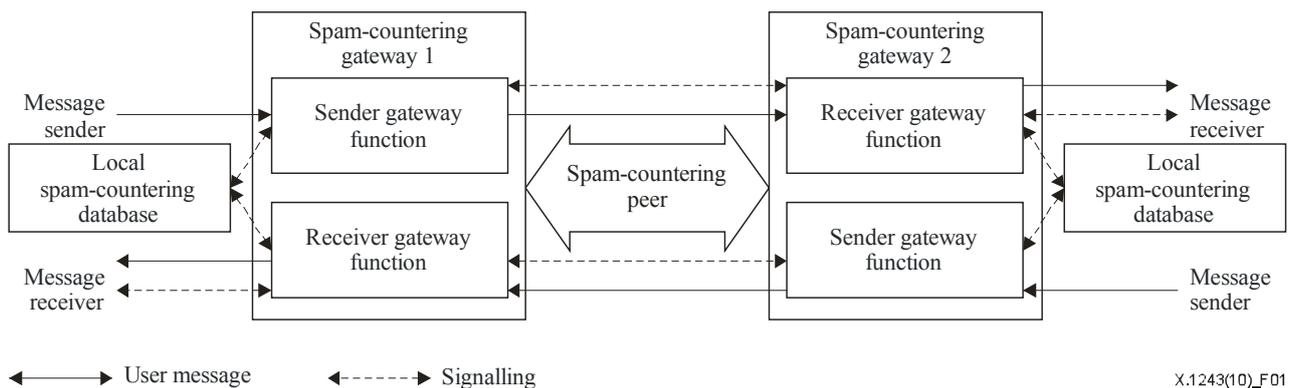


Figure 1 – Architecture of interactive gateway system for spam-countering

Interactive gateway system for spam-countering (IGCS)

An IGCS system is composed of a spam-countering gateway and a local spam-countering database. The spam-countering gateway has two sub-function entities: SGF and RGF. These two function entities act both as policy decision points and policy enforcement points. SGF is used to process outgoing spam and RGF is used to process incoming spam. The local spam-countering database (lscDB) provides spam-countering rules for spam identification and spam-countering actions. The local spam-countering gateway is also responsible for updating spam-countering rules to lscDB.

The responsibilities of RGF and SGF are defined as follows:

A RGF basically has three responsibilities:

- to take spam-countering actions (blocking, isolating or warning, etc.) on known incoming spam;
- to detect new spam through receiver's spam reports and update local spam-countering rules to lscDB;
- to notify spam sender's SGF by sending a notification when a spam is detected.

An SGF has two responsibilities:

- to take spam-countering actions (blocking, isolating or warning, etc.) on known outgoing spam;
- to process spam notifications issued by receiver's RGF and update local spam-countering rules to lscDB.

Local spam-countering database (lscDB)

An lscDB is used for storing spam-countering information. This information can be further categorized into the following three types:

- Spam identification information: such as source address of spam and key words in spam subject field.
- Spam-countering rules: such as blacklist and whitelist.
- Suspect spam record: suspicious spam samples that are reported by RGF and SGF.

6.2 Spam identification

The RGF or SGF identifies known spam, based on spam identification information stored in lscDB. Spam will be classified into several levels and treated as corresponding actions.

6.3 Spam-countering action

Once spam is identified, the corresponding RGF or SGF will take actions based on the level of the identified spam. The spam-countering actions may include but are not limited to:

- spam warning: RGF/SGF sends a warning to the message receiver/sender;
- spam isolation: RGF/SGF isolates the spam message and periodically sends an isolation summary to the message receiver/sender;
- spam blocking: RGF/SGF blocks the spam message.

6.4 Spam discovery

6.4.1 RGF spam discovery

The receiver may report the anti-spam rules to its on-duty RGF. Anti-spam rules include, but are not limited to, the source/destination address blacklist, and key words in the e-mail subject field. The RGF updates spam identification and the rules in the lscDB. When a suspicious message comes in, the RGF starts an evaluation process to judge whether the message is a spam, according to the spam-countering rules stored in lscDB. If the message is judged as spam, the RGF will take the corresponding action.

6.4.2 SGF spam discovery

The spam discovery process for the SGF is similar to that for the RGF. The SGF also receives spam notifications from the receiver's RGF. The SGF evaluates the RGF notifications and updates the verified spam rules in the lscDB.

6.5 Spam notification through spam-countering peering protocol

6.5.1 Peer discovery

When an SA is trying to send a message to an RA, the peer discovery procedure is initiated to discover an active peer IGCS in the message delivery path. The discovery procedure can be initiated by one of the IGCSs. A peer relationship will be established after a handshake process of peer authentication.

6.5.2 Spam notification between peers

After a peer relationship has been established, the IGCS can exchange spam notification with its peer through the spam-countering peering protocol. Because spam is basically identified by the receiver, the receiver's RGF is responsible for identifying spam and providing spam information to the sender's SGF. Once an RGF detects a spam message, it will notify the sender's SGF through the spam notification process. After receiving the spam notification, the SGF should decide whether to accept it or not, according to the local spam-countering policy.

6.5.3 Security aspect

A certification mechanism, as specified in [ITU-T X.509], is recommended to be included in the spam notification process for peer authentication. A notification message is recommended to be digitally signed by the RGF. It is recommended to only accept a notification message from a trusted source RGF.

7 Spam-countering filtering techniques

7.1 Technique-independent consideration

IGCS should support the diversity of techniques for countering spam and provide flexibility to integrate existing and upcoming spam-countering filtering techniques. Each filtering technique could be implemented optionally. In order to efficiently detect spam messages, an IGCS may support several filtering techniques and integrate them into one physical network device. The specific implementation of filtering techniques is out of scope of this Recommendation. This Recommendation only defines interfaces, data formats for each filtering technique to ensure the interoperability in exchanging spam-countering information between IGCS peers.

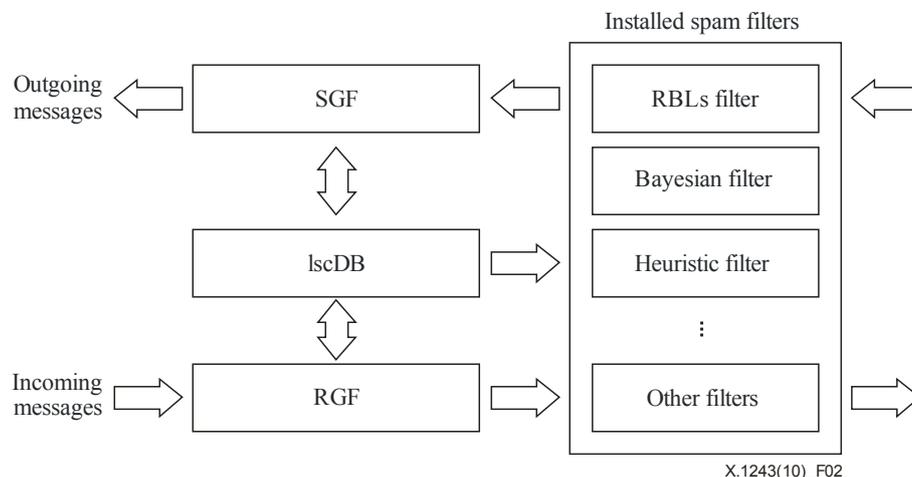


Figure 2 – An IGCS with multiple spam filters

7.2 Supported spam-countering techniques

7.2.1 Address list

Real-time blackhole list (RBL): RBLs are provided by various organizations that study spam and develop its source address lists. A system for spam-countering can subscribe to the list, and can determine whether it is a spam or not by checking the list.

Blacklists: Blacklists are a basic access control mechanism that allows everyone access, except for the members of the blacklists. In addition, like RBLs, the lists can be constantly updated, and the scheme also suffers from the fact that many spam messages do not contain source addresses. Some systems also allow users to maintain whitelists of allowed senders, but which may restrict users from getting desirable messages from previously unknown sources.

7.2.2 Heuristic filtering

These filters are based on the principle of testing for the presence in the message of certain typical features of spam, such as the exclusive use of HTML or the type of customer to whom the message is sent. The test is weighted through a learning process based on a set of known messages and a set of e-mails known to be legitimate.

These filters carry the risk that a message using spamming techniques – spectacular messages in HTML, for example – will be classified as spam.

This filter can detect a large proportion of messages, and it does not need to be taught or configured. However, since it uses a large number of tests, it is better to change the configuration of which tests are run and the scores used to classify messages as spam.

7.2.3 Bayesian filtering

The principle of Bayesian filtering is that its spam-countering engine is trained by a set of known spam and a set of messages known to be legitimate. After the training process, the vocabulary characteristics used by the spam message is collected. Bayesian filtering will use Bayesian probabilities to calculate whether a new message is spam or not. In the case of a group filtering, the learning is usually conducted by the system administrator.

Based on the algorithm of Bayesian probabilities, Bayesian filtering has a heavy calculation overhead and it may introduce scalability problems in a large spam-countering system. In a small-scale and highly uniform environment (for example, an enterprise or a university network), this may be acceptable. However, this would undoubtedly not be the case for a major service provider and particularly a public provider.

Although Bayesian filtering has been used for spam-countering, it has some constraints when spammers forge their information.

7.2.4 Multimodal filtering

If an IGCS system is to process multimodal filtering, SGF and RGF implement multimodal filtering, respectively, by a couple of functional entities: the modality detection FE, the filtering FE and other necessary functional entities like multimodal message processing FE. In order to support information storage and exchange, countering multimodal spam information data sets need to be defined. The lscDB will store the countering multimodal spam information which holds suitable multimodal message categories (and themes) and the filtering criteria (which have been entered by users or operators, or have been learned from IGCS peers).

If the description of multimodal metadata is available and the description of metadata is considered to be trustworthy, multimodal applications may filter multimodal information based on the metadata description of the multimodal content. Otherwise, filtering should preferably consider the entire multimodal information where the following functional entities shall accomplish the tasks below:

- a database or repository holds suitable multimodal message categories and the filtering criteria. The database or repository may be hosted in the same premises/domain as the DB interface agent FE, the modality detection FE, the multimodal processing FE and the multimodal user agent. In another case, the database or repository may be hosted in different premises or domains than the filtering FE;
- a modality detection functional element inspects a sent or received multimodal message to identify the contained modalities;
- a DB interface agent functional entity fetches the filtering criteria from the DB in the given modalities and message categories;
- a filtering functional entity filters the multimodal message against the filtering criteria. The filtering FE may entirely block or partially block the selected multimodal parts of a processed multimodal message.

Figure 3 describes the general architecture for filtering multimodal messages and the necessary functional entities. The filtering architecture encompasses the modality detection FE, the filtering FE, the DB interface agent FE and the multimodal DB. However, Figure 3 shows other functional entities that typically do not perform any multimodal filtering tasks such as the multimodal message processing FE and the multimodal user agent.

The multimodal message processing FE processes multimodal (filtered) messages; synchronizes multimodal messages received from the multimodal user agents, and multiplexes or dispatches filtered multimodal messages towards the multimodal user agents. Each of the various multimodal user agents handles the specific modalities such as modal (device-specific) input and/or output.

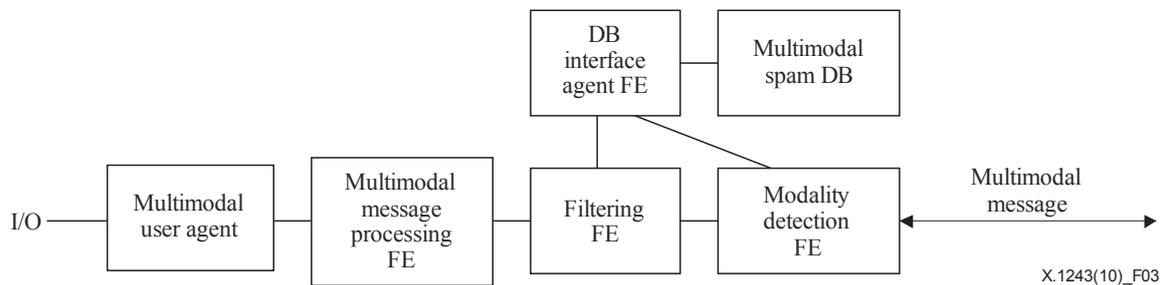


Figure 3 – Multimodal filtering architecture

Figure 4 details the generic multimodal filtering architecture by mapping the functional entities to the receiver gateway function (RGF). The following steps describe the procedures when the FEs receive a multimodal message:

- 1) The RGF receives a multimodal message.
- 2) The modality detection FE identifies the conveyed modalities and the message type(s) conveyed in the received multimodal message.
- 3) The filtering FE may have been configured statically with the filtering rules for all potential multimodal messages (i.e., independent of a particular received multimodal message) or may be configured dynamically with a message and/or modal-dependent rule for each received multimodal message individually.
 - a) The modality detection FE may either submit the identified modalities and message type parameters to a DB interface agent, or the modality detection FE may attach the parameters to the received multimodal message.
 - b) The modality detection FE forwards the multimodal message, possibly annotated with extracted modality and message type parameters, to the filtering FE.
- 4) In case the filtering FE has not yet been configured with rules, the filtering FE passes on the modalities and message type parameters to the DB interface agent, unless the DB interface agent has obtained those parameters directly from the modality detection FE.
- 5) The DB interface agent FE queries the multimodal DB to obtain the corresponding modalities and message criteria. The DB interface agent FE compiles those values into specific rules and provides those rules to the filtering FE.
- 6) The filtering FE applies the available rules and performs the filtering upon the received multimodal message. Depending on the rules and policy settings, the multimodal message is allowed to pass, or is blocked entirely or is blocked partially where only certain modalities within the multimodal message are blocked.
- 7) The filtering FE passes on the filtered multimodal message to the multimodal message processing FE, possibly annotated with some filtering results (i.e., information for logging or security warnings).
- 8) The multimodal message processing FE processes the received (filtered) multimodal message. The FE synchronizes input(s) received from the various input multimodal user agents, dispatches the multimodal message into their modality components and forwards those modality-specific parts to the output multimodal user agents.

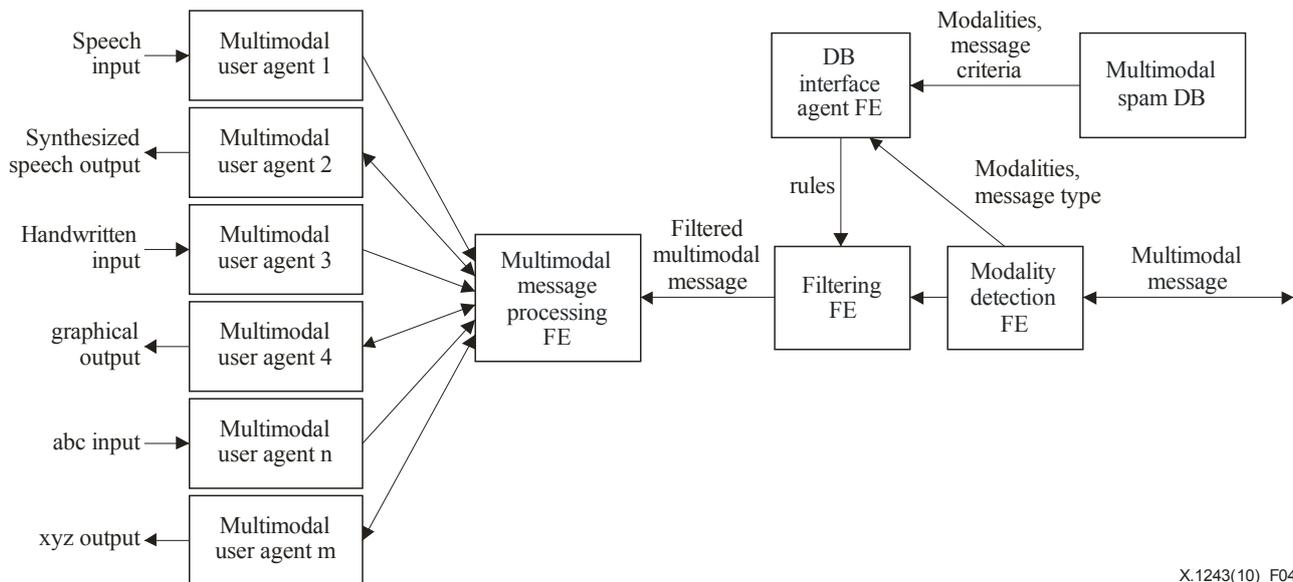


Figure 4 – Multimodal filtering in receiver gateway function (RGF)

NOTE – Figure 4 describes various multimodal user agents. The RGF may not require all shown multimodal user agents to be present.

7.2.5 Damp spam filter

Damp spam filter is used to control message receiving rate. An important input parameter to damp spam filter is spam damp coefficient. This parameter is a measurement to suspicious messages and it controls message receiving rates. When highly suspicious messages are received, the coefficient increases accordingly and damp spam filter will lower the receiving rate of suspicious e-mails. This parameter is usually generated from external spam-countering systems such as experience or reputation database. Damp spam filter may also affect e-mail response delay, transport window size and damp cycle time, etc.

7.2.6 E-mail header filter

E-mail header filter (EHF) monitors SMTP conversation and ensures its compliance to relevant protocols. It can be used to identify protocol inconsistency and forged e-mail header. In order to reconstruct SMTP sessions and trace protocol states, EHF may require packet de-fragment, TCP stream assembling, etc. EHF focuses on protocol level analysis and it provides additional information to improve overall spam identification accuracy. EHF is commonly integrated in many commercial anti-spam systems as well as some open source anti-spam systems.

7.2.7 Weighted parameter filter (WPF)

The weighted parameter filter (WPF) is used to detect spam by analysing multi-parameters. The parameters are based on statistical information including the number of e-mail sessions, the number of destination servers, the number of e-mail trials, the period of sending e-mails, the rate of sending e-mails, the rate of trial e-mails and successful e-mails, and so on. Each parameter has a configured threshold and a configured weight value. Besides, the whole set of weighted value, which may be justified by several times of experiments in advance, is also needed. For each e-mail, all parameters in the rules will be checked. The only parameters that pass the configured threshold will be weight added. If the sums of parameters are beyond the predefined threshold, the WPF could distinguish spam e-mails from the normal ones.

8 Process of spam-countering peering protocol

8.1 Peer discovery

A peer discovery process establishes peer relationship for two IGCSs. This process is initialized when an IGCS is trying to discover a valid IGCS along the message delivery path. When a RGF detects a suspicious spam message, the peer discovery process starts.

The peer discovery message is recommended to include the following information:

- Address list of RGF/SGF of initial IGCS: source address (e.g., source IP address and port pair). To protect against single point failures, an IGCS may integrate multiple RGFs and SGFs for redundancy. The address list may contain all RGF/SGF's addresses of the initial IGCS
- Address of counter party's IGCS: IGCS@{address of the proxy of counter party}
- Spam originator: spam sender's address
- Type of the suspected spam: WELL_KNOWN, USER_REPORTED or OTHER
- Attached suspected spam: The suspected spam attached.

When a peer discovery message is sent, the initial IGCS will start a timer. If no responding message is received after a configured expiration period, the initial IGCS fails to discover a peer IGCS. A peer discovery reply message may contain the following information:

- Address list of RGF/SGF of the replying IGCS.
- Confirmation of the suspected spam: to confirm if the suspected spam has been considered as a spam by the replying IGCS.

8.2 Peer set-up

Before time expires, if the initial IGCS receives the peer discovery reply message, it may start to establish a peer relationship. The process will have two major actions:

- IGCS updates peer list: Add address list of the counter party's IGCS into the peer list.
- Name list of supported spam filter: Supported spam filters in each IGCS.

8.3 Spam-countering message exchange

After the peer set-up process, the IGCS starts the spam-countering message exchange. In this process, two peering IGCSs exchange the information of common supported spam filters. Each IGCS updates its lscDB with the exchanged message accordingly.

8.4 Peer release

If no spam has been detected through a period of time, one IGCS may terminate the peer relationship by sending a peer release message. After receiving the peer release message, the IGCS will remove or reuse the related peer information according to the policy.

9 Implementation model of gateway systems for countering spam

9.1 Integrated model

9.1.1 Model description

In the integrated model, the IGCS is integrated with a message system which consists of an RA and an SA. Each system has a gateway (an RGF and an SGF) and an lscDB. In the e-mail system, for instance, an RA can be a POP3 server and an SA can be an SMTP server. An RGF/SGF could be implemented as an integrated server providing both POP3 and SMTP services. An lscDB is also required for an e-mail system to provide spam-countering rules. An integrated model is shown in Figure 5.

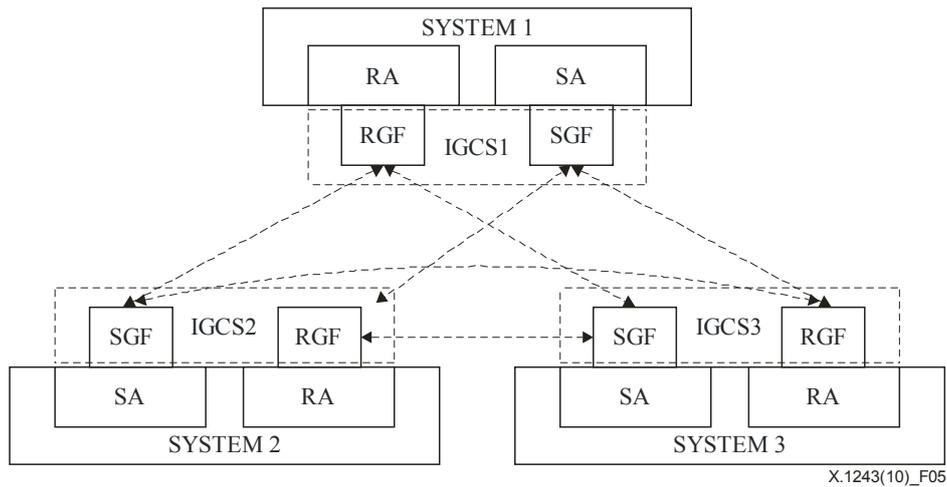


Figure 5 – Integrated model of IGCS

9.1.2 Use cases

An integrated model is suitable for the client/server model, where a server is responsible for sending/receiving many clients' messages. In this case, the server acts as a decision point and policy enforcement point for anti-spam activities.

9.2 Domain-based model

9.2.1 Model description

In the domain-based model, the IGCS acts as a message delivery proxy in a domain which may have multiple SAs and RAs for load balance requirements. The SGF/RGF may have several instances distributed in a domain. Each SGF/RGF instance is in charge of several SAs/RAs in a domain and is responsible for countering both local domain and inter-domain spam messages.

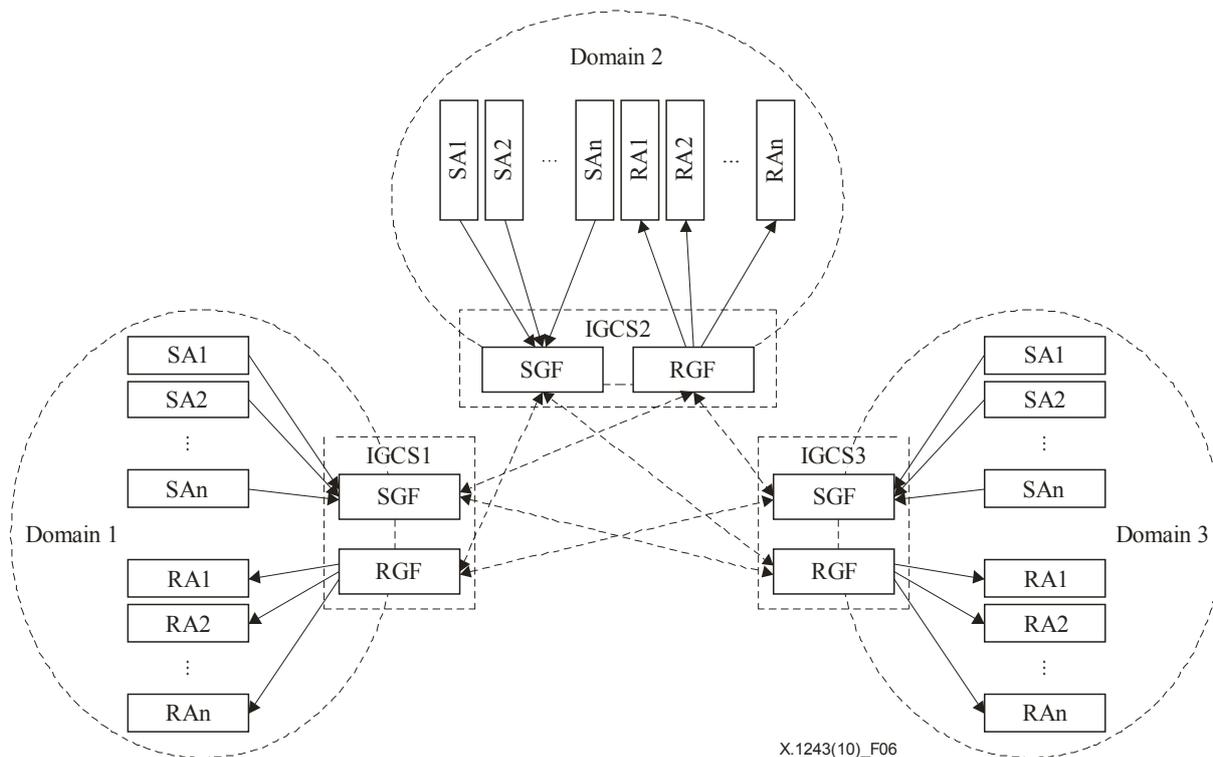


Figure 6 – Domain-based model

9.2.2 Use cases

The domain-based model could be used for domain-based spam-countering purposes. It is especially suitable for peer-to-peer communication systems, such as many popular IM applications: IRC, etc. For a peer-to-peer model, a user-side system itself acts as a RA and SA at the same time. It will be very difficult to manage a large number of user-side RAs and SAs with an integrated IGCS model. However, a domain-based model is able to address the problem through a distributed manner.

9.3 Bypass deployment model

9.3.1 Model description

In a wireless network, the IGCS can be also deployed with a wireless access point. Wireless access points bypass all messages to the IGCS. The IGCS judges the incoming messages based on the rules stored in lscDB and injects normal messages into the wireless network.

9.3.2 Use cases

The bypass deployment model could be used in the wireless network. Spam can be filtered before it enters the wireless network so that the unnecessary cost of delivering spam traffic to end users can be reduced.

Appendix I

Example of SCPP message definition

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

An example of SCPP messages defined in ASN.1 language is listed as follows and has been checked by the ASN.1 compiler:

```
SCPP-MESSAGES {itu-t(0) recommendation(0) x(24) igscs(1243)
asn1-module(0) scpp-messages(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- SCPP Message body definition
SCPP-PDU ::= SEQUENCE {
    sourceAddress      IGCS-Address,
    destAddress        IGCS-Address,
    igcs-message-body  CHOICE {
        peerDiscovery  PeerDiscoveryDEF,
        peerSetup      PeerSetupDEF,
        dataExchange   DataExchangeDEF,
        peerKeepAlive  PeerKeepAliveDEF,
        peerRelease    PeerReleaseDEF},
    nonStandardData   OCTET STRING OPTIONAL,
    ...
}

-- PeerDiscovery Message definition
PeerDiscoveryDEF ::= SEQUENCE {
    setupRequest      BOOLEAN,
    igcsSignature     IGCS-Signature
}

-- PeerSetup Message definition
PeerSetupDEF ::= SEQUENCE {
    setupResponse     BOOLEAN,
    sgfList           SEQUENCE OF IGCS-Address,
    rgfList           SEQUENCE OF IGCS-Address,
    supportedFilters  SupportedSpamFilters,
    igcsSignature     IGCS-Signature
}

-- Countering Spam Data Exchange Message definition
DataExchangeDEF ::= SEQUENCE {
    csData            SET OF SpamFilterData,
    ...
}

-- Peer Keep Alive Message definition
PeerKeepAliveDEF ::= SEQUENCE {
    sgfUpdates        GF-Updates,
    rgfUpdates        GF-Updates,
    filtersUpdates    SupportedSpamFilters
}

-- Peer Release Message definition
PeerReleaseDEF ::= SEQUENCE {
    peerRelease       ENUMERATED{request(0), confirm(1)},
    nonStandardData   OCTET STRING OPTIONAL,
    ...
}
```

```

-- IGCS supported addresses, include IGCS,SGF,RGF address definition
-- Support IP address, Email ID and other types of address
IGCS-Address::=CHOICE{
    ipAddress
    SEQUENCE { ip OCTET STRING(SIZE(4)),
                port INTEGER(0..65535) },
    ip6Address
    SEQUENCE { ip OCTET STRING(SIZE(16)),
                port INTEGER(0..65535) },

    emailAddress      IA5String(SIZE(1..512)),
    nonStandardAddress OCTET STRING,
    ...
}

-- Signature data for authentication
IGCS-Signature::=SEQUENCE {
    igcsID      INTEGER(0..65535),
    signatureData OCTET STRING,
    ...
}

-- RGF/SGF status update information
GF-Updates::=SEQUENCE {
    gateType      ENUMERATED {sgf(0),rgf(1)},
    gateAdd       IGCS-Address,
    gateRemove    IGCS-Address
}

-- IGCS Supported Spam filters and related data

SupportedSpamFilters::= SEQUENCE {
    supportedFilter SEQUENCE OF SpamFilters
}

SpamFilters::=SEQUENCE{
    filterID      INTEGER(0..128),
    filterName    IA5String(SIZE(1..512))
}

SpamFilterData::=SEQUENCE {
    filterID      INTEGER(0..128),
    filterData    OCTET STRING,
    ...
}

END

```

Bibliography

- [b-ITU-T X.680] Recommendation ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*
- [b-ITU-T X.681] Recommendation ITU-T X.681 (2008) | ISO/IEC 8824-2:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*
- [b-ITU-T X.682] Recommendation ITU-T X.682 (2008) | ISO/IEC 8824-3:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*
- [b-ITU-T X.683] Recommendation ITU-T X.683 (2008) | ISO/IEC 8824-4:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*
- [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.1241] Recommendation ITU-T X.1241 (2008), *Technical framework for countering e-mail spam.*
- [b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions.*
- [b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3.*
- [b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1.*
- [b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs.*
- [b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*).*
- [b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol.*
- [b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format.*
- [b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions.*

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