International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1241

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Technical framework for countering email spam

Recommendation ITU-T X.1241

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

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

Recommendation ITU-T X.1241

Technical framework for countering email spam

Summary

Recommendation ITU-T X.1241 provides a technical framework for countering email spam. The framework describes one recommended structure of an anti-spam processing domain and defined function of major modules in it. The key point of the framework is that it establishes a mechanism to share information about email spam between different email servers. Systems following the framework would improve efficiency through interconnection.

Source

Recommendation ITU-T X.1241 was approved on 18 April 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

Keywords

Anti-spam, email, interconnection, spam, technical framework.

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 2009

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

CONTENTS

Introduction

With the development of the IP-based telecommunication network, a great number of emails are exchanged between users. At the same time, more and more spam messages are sent to users through the IP-based telecommunication network and cause serious problems.

Email spam has become a plague that degrades the capability of service on the IP-based telecommunication network. Service providers have to spend a lot of money to counteract problems caused by spam. Users have to take a lot of time to delete email spam.

Some detection techniques have been proposed to detect and delete email spam. However, spammers are highly creative in avoiding detection. For example, spammers can falsify normal email and randomize the content to avoid the detection of spam filters. Therefore, it is urgent to develop an effective technical framework to deal with the global problem of email spam.

Different anti-spam solutions may use different techniques for countering email spam; these anti-spam technologies are evolving continuously. It is very difficult to find a changeless description that can cover all details of anti-spam technologies in the long term.

Therefore, it is necessary to establish an open framework containing these various solutions. The framework should be compatible with all anti-spam technologies, and not be limited to a particular technical detail. Requirements of the framework are as follows:

- Can systematically estimate whether or not an email is a spam.
- Can enable various email service systems to share anti-spam information with each other.
- Can improve veracity of email service systems' anti-spam tools.
- Ensure that entities within different administrative domains share counter-spam information.

Recommendation ITU-T X.1241

Technical framework for countering email spam

1 Scope

This Recommendation provides a technical framework for countering email spam. The framework describes one recommended structure of an anti-spam processing domain and defined function of major modules in it. The key point of the framework is that it establishes a mechanism to share information about email spam between different email servers. Systems following the framework would improve efficiency through interconnection.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 header fields [b-IETF RFC 2822]: Header fields have the same general syntactic structure: A field name, followed by a colon, followed by the field body.

3.1.2 mail objects [b-IETF RFC 2821]: SMTP transports a mail object. A mail object contains an envelope and content.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 anti-spam processing domain: It is an independent system, which contains an anti-spam processing entity, anti-spam processing sub-entities, email servers and email clients.

3.2.2 anti-spam processing entity: Anti-spam processing entity is the core in the anti-spam processing domain. It collects information of email spam from entities at lower levels, and then builds a uniform and integrated rule system. Finally, the rule system should be submitted to all of the entities at lower levels.

3.2.3 anti-spam processing sub-entity: Anti-spam processing sub-entity is connected to one or more email service providers. It receives email spam information from email servers or anti-spam equipment, and reports information to the high-level entities after analysing it periodically. It also receives updating rules from high-level entities periodically and distributes these to sub-entities.

3.2.4 compound rule: A compound rule is composed of two or more simple rules.

3.2.5 email: This term is mainly used to indicate the electronic mail transmitted over a telecommunication network.

3.2.6 email spam: This term is used to describe unsolicited electronic communications over email, which is usually sent for specific purposes.

3.2.7 rule: The rule is a set of conditions and basic actions. Rules include many forms, such as behaviours, filters, and so on.

3.2.8 sample email: This term is used to describe an email that is received from email servers according to certain rules.

3.2.9 **spammer**: This term is used to describe the entity or the person creating and sending email spam.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DNS	Domain Name System
Email	Electronic Mail
ESMTP	Extended Simple Mail Transfer Protocol
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IMAP4	Internet Message Access Protocol version 4
IP	Internet Protocol
POP3	Post Office Protocol version 3
RBL	Real-time Blacklist
SASL	Simple Authentication and Security Layer
SMTP	Simple Mail Transfer Protocol
URL	Uniform Resource Locator

5 Conventions

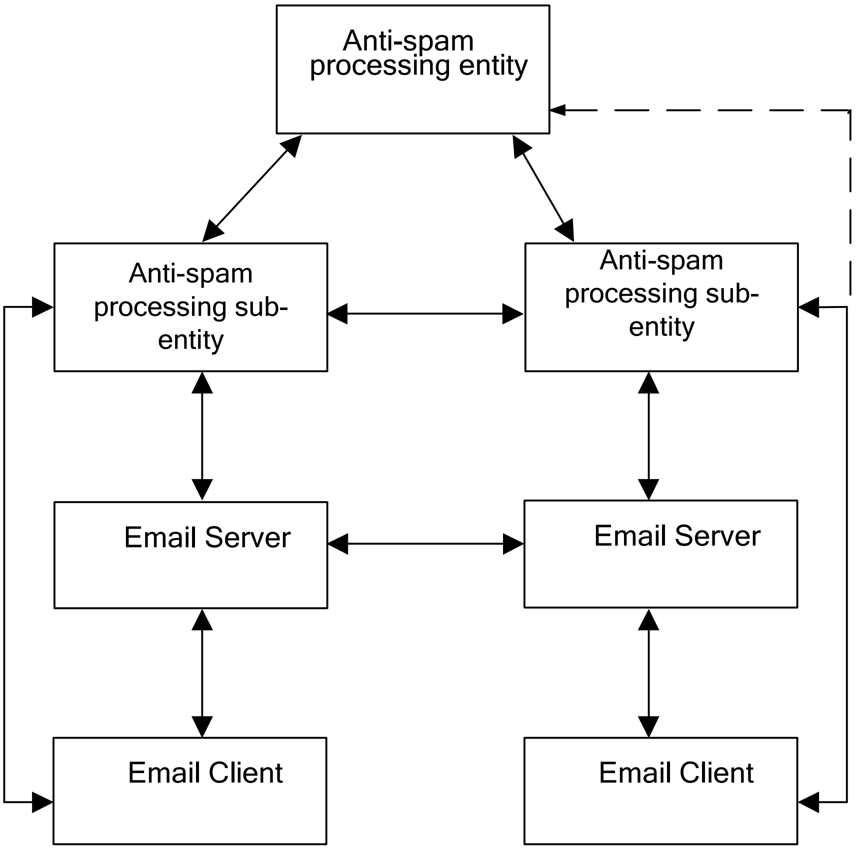
None.

6 General structure of anti-spam processing domain

6.1 General structure

This Recommendation describes components of the framework. It includes the anti-spam processing entity, anti-spam processing sub-entities, email servers and email clients.

These components can communicate with each other by popular message protocols. The characteristics of these components are described in this clause.


Anti-spam processing entity
Anti-spam processing sub-entity
Anti-spam processing sub-entity
Email Server
Email Server
Email Client
Email Client

NOTE – The solid lines represent the path of information that is exchanged between components of the anti-spam processing domain.

Figure 1 – General structure

In Figure 1, the anti-spam processing entity receives reports from anti-spam processing sub-entities and delivers new rules to them.

Anti-spam processing sub-entities must check the validity of the rules that come from the anti-spam processing entity, and refine them.

The email client is the entity that customers deal with directly. The email server performs the delivery of emails in the IP-based telecommunication network.

The email client sends complaints to the anti-spam processing sub-entity. In specific situations, an email client can send complaints directly by the top anti-spam processing entity.

6.2 Reference model

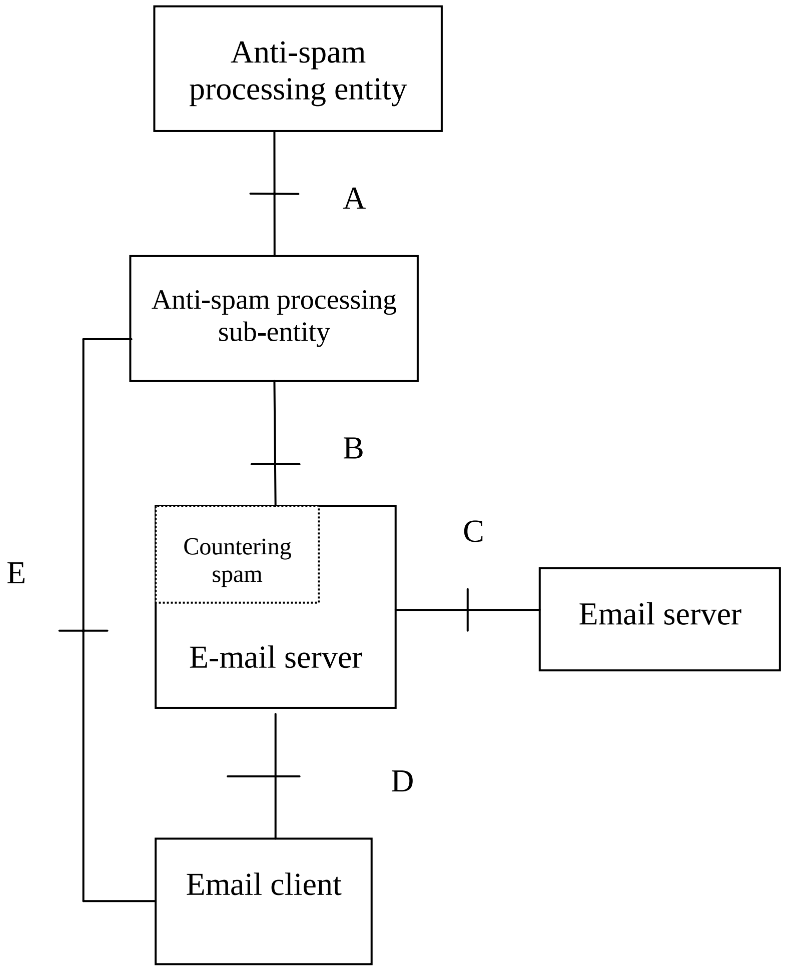


Figure 2 – Reference Model

Interface A is between the anti-spam processing entity and the sub-entity. Complaint reports and rules on countering spam are transmitted through interface A. The rules can be compound rules such as "the source IP + URL". Interface A should support FTP and HTTP.

Interface B is between the anti-spam processing sub-entity and email server. It is used to transmit the complaint reports and the rules. Similarly, the rules can be compound rules such as "the source IP + URL". Interface B should support FTP and HTTP. In specific situations, the email server can communicate directly with the top anti-spam processing entity.

Interface C is between the email servers, through which messages are transmitted with SMTP.

Interface D is between the email server and the email client. Various protocols can be used to transmit emails, such as POP3, IMAP4.

Interface E is between the email client and the anti-spam processing sub-entity. The email client can send complaints to the anti-spam processing sub-entity. In specific situations, the email client can send complaints directly to the top anti-spam processing entity. Web online, phone, email and client software can be used at this interface.

7 Functions of the anti-spam processing domain

7.1 Functions of the email client

The functions of the email client include:

- In addition to performing the general functions of email transmission, the email client provides a mechanism to help users send a spam complaint information to the anti-spam processing entity. Email recipients only need judge whether an email is spam according to contents, title or address. For example, if recipients do not want advertisements, electronic publications or propaganda materials they can send the complaint of such emails to the anti-spam processing entity by the mechanism of the email client.
- The email client can download spam filtering rules automatically from the anti-spam processing entity. The filtering rules are established according to the complaint reports from email clients. They include the size limit of a single email, the number of emails that are sent out in a period of time, keywords in main body of emails, etc. The filtering rules are periodically updated according to the complaint reports. They are indexed by user name of mailbox, output IP address and domain name.
- The email client can forward email spam to the anti-spam processing entity for further processing or withdrawing some filtering rules that cause false positives. The anti-spam processing entity can update the filtering rules immediately according to the requirements or the complaint from the email client.
- The email client can filter email spam directly. Normally, recipients should know the filtering results in order to avoid the false positive problem.

7.2 Functions of the email server

The functions of the email server include:

- Realizing the general functions of email transmission, the email server completes its normal actions of exchanging email with other email server, or sending and receiving email between email clients; at the same time, the email server should forbid the function of open relay to prevent spammers imposing on it to transmit spam email to other email servers.
- Any customer must pass verification before sending email through an email server. Different email systems may use different verification mechanisms. The verification is deployed between the email server and email client.
- Any email service provider may keep a blacklist about spammers, the blacklist covers some information (such as host name, domain name or email address) about spammers, and the email server refuses to receive emails coming from these spammers.
- The email server may send back a verify command to the source, which is indicated in the email sender's information (as DNS, host name or others); if the verify command does not confirm the authenticity of the source, the email server will reject this email.
- Some commands of SMTP may be used by spammers to guess the real account of the email server. The email server forbids these commands as EXPN and VRFY.
- Some advertisement and propagandist email is being sent without any information about the sender. The email server should automatically add an HTTP link in the email body. Customers can submit complaint reports conveniently.
- Email servers detect spam email by anti-spam technology and report the spam to the anti-spam processing sub-entity, and download filtering rules from it.
- When spam email is detected, the email server should back up the original spam that at least includes the header of the source email, and submit it to filter.

- The email server should provide the system log and statistics information for the email server that is backed up periodically and submit them to the anti-spam processing sub-entity.
- The email server returns a different state number according to different rules.
- The email server can restrict the amount of traffic sent by a specific email customer.

7.3 Functions of the anti-spam processing entity

The functions of the anti-spam processing entity include:

- Exchange the filtering rules with other anti-spam processing entities, various protocols can be used to transmit information, such as FTP and HTTP.
- Store the original information of spam emails from customers and the anti-spam processing sub-entity.
- Broadcast filtering rules to anti-spam processing sub-entities, and warn them of dangerous emails.
- The anti-spam processing entity should administer and maintain filtering rules, these rules can be obtained through a website for:
  - Receiving reports from customers and anti-spam processing sub-entities.
  - Broadcasting authoritative information, including supervision and management information.

7.4 Functions of the anti-spam processing sub-entity

The functions of the anti-spam processing sub-entity include:

- Receive complaint reports from customers and filtering rules from the anti-spam processing entity.
- Store the original information of spam from customers (at least the header of the spam) and other entities.
- Broadcast filtering rules to email servers or email clients, and warn of dangerous emails to users as needed.
- Trace the spread of spam and collect correlative information.
- Report the status of the spread of spam and correlative information to entities at higher levels.
- Create new filtering rules from the backup of doubtful emails, check and modify the existing filtering rules. These rules can be obtained through a website for:
  - Creating reports of spam from customers and email servers.
  - Creating new filtering rules.

8 Identification of email spam

This clause describes familiar characteristics and criteria for email spam.

8.1 Familiar characteristics of email spam

These familiar characteristics of email spam are listed as follows:

- Hiding or falsifying the true address of the sender

  The content in "from" or "sender" of the originator field is blank or invalid.
- Hiding or falsifying the real source of the email

  The "message-id" in the identification field is blank or invalid.

- Sender is a known spammer

  A spammer's address from a blacklist is included in "from" or "sender" of the originator field.

- False receivers' information

  The content that has been included in the receiver field ("to") or the carbon copy receiver field ("cc") is false or concerned with spammers.

- Inclusion of common words used by spammers

  Common words used by spammers are included in the subject field ("subject") or email content.

- False relaying information

  The content that is included in the "resent-from" or "resent-sender" of the resent field is false.

- False tracing information

  Spurious content is included in the trace field.

- Size is improper

  The size of the whole email, header field or the email content is similar to the size of header fields and email content in spam emails.

- Too many receivers

  There are too many receivers in a certain field.

- Too many retransmission hops

  There are too many traces in the trace field.

- The sender's IP address is contained in certain fields

  Information concerning spammers is included in "from" or "sender" of the originator field.

- The email server's IP address is contained in certain fields

  Information concerning spammers is included in "received" of the trace field, "resent-from" or "resent-sender" of the resent field.

- New spam

  The anti-spam processing entity can summarize characteristics from the new spam sample and create the corresponding filtering rules.

8.2 Common rules to fight email spam

Individual rules can be integrated into a compound rule with different priority.

The email server can apply individual and/or compound rule to deal with email spam.

8.2.1 Common fundamental rules

The email server can set the criteria according to the following factors:

- The originator field ("from" or "sender") is blank or has invalid content.
- The identification field ("message-id") is blank or has invalid content.
- The originator field ("from" or "sender") includes keywords that are listed in a blacklist.
- Keywords given by a blacklist are included in the receiver field ("to") or the carbon copy receiver field ("cc").
- The subject ("subject") or email content includes given keywords.
- The true original source cannot be found in the "resent-from" and "resent-sender" of the resent field, or the content of the trace field.

- The size of the whole email, header field or the email content is (approximately) equal to a given value.
- The total number of addresses defined in "to", "cc" and "bcc" of the originator field exceeds the limit given by the email server; or the number of times that one email is to be delivered exceeds the limit given by the email server.
- The number of traces in the trace field exceeds the limit given by the email service provider or administrator of this domain.
- The result of DNS reverse following "from" or "sender" information in the originator field is included in the specific blacklist.
- The result of DNS reverse that should follow "received" in the trace field, "resent-from" or "resent-sender" in the resent field is included in a specific blacklist.
- If email spam cannot be identified with a single rule, a compound rule is requested to be used.

8.2.2 Priority of criteria

Confirm the priorities of criteria. If one email conforms to several rules (called a rule conflict), it will be disposed of according to the rule with the highest priority. If the priorities of rules are equal, the final rule used by the conflict priority principle is used. Conflict should be avoided as far as possible.

8.2.3 Conflict detection of criteria

A function is used to detect conflicts between different assigned criteria. The familiar conflicting conditions are described as follows:

- Both "rule's conditions" include the same kind of "simple rules" (fundamental rules) of keyword-search class (such as "the subject includes XXX", "what decoded from the front 10 lines includes XXX", and so on), and the keywords in both "simple rules" are the same, and one keyword includes another.
- Both "rule's conditions" include the same kind of "simple rules" of IP-restricted class (such as "the IP of client is XXX", and so on), and both IP spaces given in the "simple rules" are the same or have an intersection set.
- Both "rule's condition" includes the same kind of "simple rules" of size-restricted class and the size-restricted conditions agree with the form of "the size of XXX is the setting value" (It cannot be "more than" or "less than"), and the values are the same. For instance, the two rules include the same simple rule: "the size of email text is 5343 bytes".

9 Methods of countering email spam

The major methods of countering email spam include turning off the open-relay function of the email server, mastering the email-delivery authorization, and filtering techniques. The countering email spam system should support, or optionally support, the following methods.

9.1 Turning off the open-relay function

Open-relay means that the email server relays all the coming email, no matter whether the email senders or receivers are the setting customers. Generally, if the email server turns on the unlimited relay function, it is considered to be open-relay.

9.2 Mastering email-delivery authorization

To prevent unauthorized customers from using the email server,

- The senders must be the legal customers of the server.

- The server should certify the senders' IP addresses.
- Number of email hops is restricted to avoid exponential spread of spam.
- The email server can check the source of the email to make sure of the reality.

9.3 Filtering technique

Filtering technology can be divided into two classes: IP address filtering and text-scanning filtering.

9.3.1 IP address filtering

IP address filtering can restrict the connection to the SMTP of the email system. Its essential attributes are IP range and restriction modes.

IP range includes:

- The real-time IP range from the anti-spam processing entity.
- The real-time IP range from the filtering rules of other organizations.
- The real-time IP range added by itself.

The restriction modes include:

- Connection refusal.
- Unconditional connection permission.
- Repeated connections from one client's IP to email server should be limited to a certain period of time.

If one client's IP belongs to the given IP range, the restriction modes will be adopted.

9.3.2 Text-scanning filtering

The filtering rules could be set by the email server and downloaded from the anti-spam processing entity. The filtering rules could be modified by administrators in certain conditions.

If an email matches a certain rule, the email will be sorted based on related behaviour. The behaviours of the text-scanning rules include:

- Rejection: Return the rejection message to the sender after extracting the characteristics.
- Discard: Normal response for each command without any behaviour.
- Delivery: Normal delivery. Ignoring the drop after choosing delivery.
- Tag: Add the specific tag in the header.
- Report: Report the characteristics extracted from the email to the report centre.
- Buffer: Keep the email intact as far as possible, and report the copy to the anti-spam processing entity.

9.4 Examination of traceability

At times, it is difficult to detect whether the sender is a valid customer. Because it is impossible for the email-receive server to get all of the information about the email-send server, the email-receive server cannot certify all the information for legal customers.

Email can be divided into two sorts: the traceable and the un-traceable. The traceable junk mail will be put into filtering rules if warnings do not take effort. It is difficult to dispose of the un-traceable junk mail because it usually uses a fake email source. Most un-traceable mail is junk mail, so examination of traceability is the base of countering email spam. The following three steps are suggested:

First step: requirement:

- Most email-receive (the "MX" in the domain name) servers are email-send servers.

- Most separating email-receive servers and email-send servers have neighbouring IPs with each other.
- Other computers allowed to deliver email may have neighbouring IPs with the "MX" email servers.
- Some email servers can be looked up by the DNS reverse, and the result is the same as the customer claims.

Second step: traceability notice mechanism:

Support certification on the telecommunication network:

- Confirm that the email field of the sender is permitted.
- Confirm that the sender is the legal customer of the email field.

Third step: backtrack mechanism:

- Traceable service and the traceable examination constitute a backtrack chain.
- The backtrack chain cannot be faked.
- It is easy to distinguish the fake part and the genuine part.

The trace system can investigate automatically by the backtrack chain.

10 Interconnection between anti-spam processing domains

When anti-spam processing domains interconnect with one another, there are three modes to choose from: interconnection between top processing entities, interconnection between processing entities and sub-entities, interconnection between processing sub-entities and email servers. Each choice can meet certain scenarios or requirements.

10.1 Interconnection between top processing entities

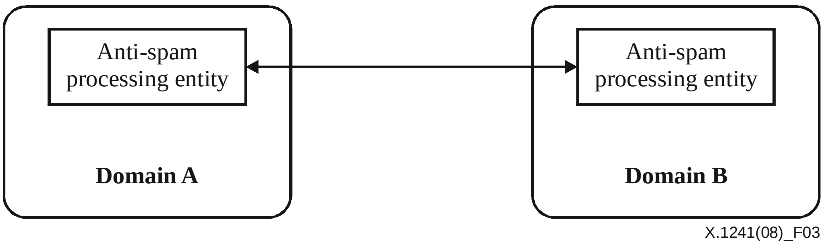


Figure 3 – Interconnection between top processing entities

The mode of interconnection is a bidirectional connection between top processing entities. There are only rules exchanged between the two entities. If one entity receives information from the other, it will implement certain mechanisms and procedures to select useful rules from the receiving information.

10.2 Interconnection between processing entity and sub-entity

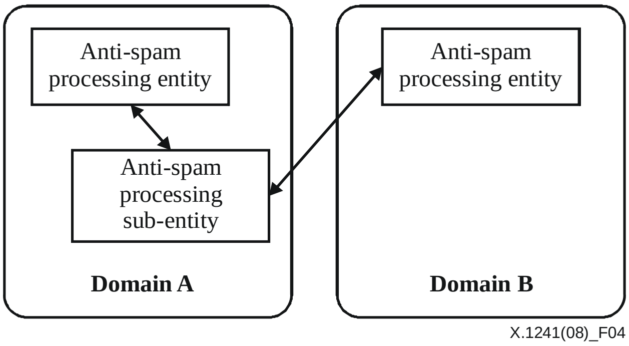

Anti-spam processing entity
Anti-spam processing sub-entity
Domain A
Anti-spam processing entity
Domain B
X.1241(08)_F04

Figure 4 – Interconnection between processing entity and sub-entity

The mode of interconnection is a bidirectional connection between a processing entity and a sub-entity. The sub-entity should download two tables of filtering rules from the two processing entities. The sub-entity creates rules according to the doubtful mail from the attached servers. It should report the rules to the two entities.

This mode has some security, but it refers to a complex administrative relationship between the sub-entity and the two entities. This mode may have problems about scalability. It is not a comprehensive interconnection among domains.

10.3 Interconnection between processing sub-entity and email server

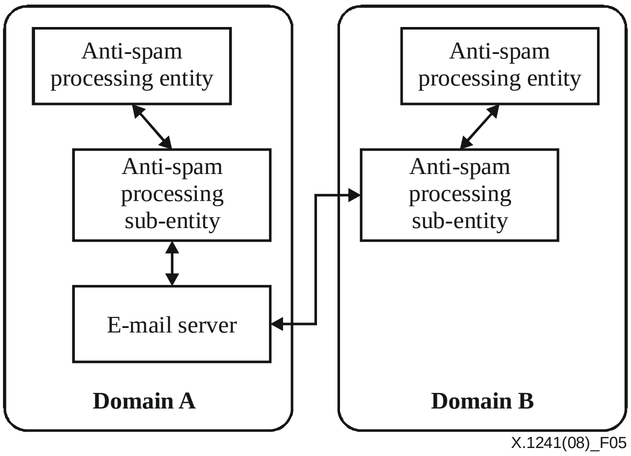

Anti-spam processing entity
Anti-spam processing sub-entity
E-mail server
Domain A
Anti-spam processing entity
Anti-spam processing sub-entity
Domain B
X.1241(08)_F05

Figure 5 – Interconnection between processing sub-entity and email server

The mode of interconnection is a bidirectional connection between a processing sub-entity and an email server. The email server will download the filtering rules of spam from the sub-entity and report junk mail to the sub-entity of the other domain. The sub-entity will receive reports of junk mail from the email server and publish its own rules to the server of the other domain.

This mode is simple to realize between domains, but the extra-domain servers may attack the anti-spam processing domain, so this mode may have security problems. It also has problems about scalability. Thus, it is not a comprehensive interconnection among domains. The mode defined in clause 10.1 is secure and the recommended interconnection mode.

Bibliography

[b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions.* <http://www.ietf.org/rfc/rfc1869.txt>

[b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3.* <http://www.ietf.org/rfc/rfc1939.txt>

[b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1.* <http://www.ietf.org/rfc/rfc2060.txt>

[b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL).* <http://www.ietf.org/rfc/rfc2222.txt>

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs.* <http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication.* <http://www.ietf.org/rfc/rfc2554.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol.* <http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format.* <http://www.ietf.org/rfc/rfc2822.txt>

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	Telephone transmission quality, telephone installations, local line networks
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, 2009