International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1231

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Technical strategies for countering spam

Recommendation ITU-T X.1231

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.1231

Technical strategies for countering spam

Summary

Recommendation ITU-T X.1231 emphasizes technical strategies for countering spam and also includes general characteristics of spam and main objectives for countering spam. Furthermore, recognizing that there is no single solution to resolve the spam problem, this Recommendation also provides a checklist to evaluate promising tools for countering spam.

Source

Recommendation ITU-T X.1231 was approved on 18 April 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

Keywords

Countering spam, spam, technical strategies.

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/.

CONTENTS

Introduction

Along with the development of the information industry, spam is becoming a widespread problem causing benefit loss to telecommunication operators, service providers and business users, as well as bad influences on common users in general. Spam has grown from a mere nuisance into a global plague.

Therefore, it is necessary to find effective and efficient ways to counter spam. There are a lot of aspects for countering spam: legislation, training, international cooperation and so on. This Recommendation mainly focuses on technical means.

Recommendation ITU-T X.1231

Technical strategies for countering spam

1 Scope

This Recommendation emphasizes technical strategies for countering spam and also includes general characteristics of spam and main objectives for countering spam. Furthermore, recognizing that there is no single solution to resolve the spam problem, this Recommendation also provides a checklist to evaluate promising tools for countering spam.

This Recommendation describes technical strategies in general and does not identify technical strategies for any specific types of spam. In addition, this Recommendation gives a hierarchical model of general categories that can be targeted to establish an efficient and effective infrastructure for countering spam. The model includes the following parts:

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

In practice, this Recommendation provides technical strategies for countering various types of spam that an administration considers to be inappropriate, in alignment with national laws and policies.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.

3.1.2 IP phone [b-ITU-T Q-Sup.49]: IP phone refers to a terminal (e.g., dedicated voice terminal or multipurpose personal computer) that is connected directly (e.g., through an Ethernet interface or an xDSL line) to an IP network.

3.1.3 short message entity (SME) [b-ITU-T Q.1742.3]: Entity that composes and decomposes short messages. A SME may or may not be located within, and be indistinguishable from, an HLR, MC, VLR, MS, or MSC.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 instant messaging (IM): Instant messaging refers to the transfer of messages between users in near real-time. These messages are usually, but not required to be, short. IM is often used in a conversational mode, that is, the transfer of messages back and forth is fast enough for participants to maintain an interactive conversation.

3.2.2 IP multimedia spam: IP multimedia spam refers to unsolicited messages or calls over real-time IP multimedia applications. Different from traditional e-mail spam, IP multimedia spam denotes spam on newly emerging communication methods over IP, such as instant messaging, presence service, voice over IP (VoIP) and so on. Spam over internet telephony (SPIT), voice spam or VoIP spam (VAM) and spam over instant messaging (SPIM) are current names for specific IP multimedia spam.

3.2.3 modality: Modality refers to information encoding, containing information perceptible for human beings. Examples: modality information includes text, graphics, audio, video or haptical data used in a human-computer interface. The multimodal information can originate from or be targeted to multimodal devices such as a microphone for voice/sound input, pen for haptical input, keyboard for textual input, mouse for motion input, speaker for synthesized voice output, screen for graphic/text output, vibrating device for haptical feedback, or a Braille-writing device for people with visual disabilities.

3.2.4 multimodal message: Multimodal message refers to a kind of multimedia message containing different encoded information for interaction via multiple modalities.

3.2.5 multimedia messaging service (MMS): Multimedia messaging service refers to a kind of messaging service after short message service which can transfer various multimedia messages including text, graphics, audio, video and so on through mobile network, wireless network or fixed network.

3.2.6 short message service (SMS): Short message service refers to a kind of message service, which allows mobile phones, telephones and other short message entities to transfer and receive text messages through a device-named service centre implementing functions such as saving and delivering.

3.2.7 spammer: Spammer refers to the entity or the person creating and sending spam.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDoS	Distributed Denial of Service
DoS	Denial of Service
E-mail	Electronic Mail
HLR	Home Location Register
IM	Instant Messaging
IP	Internet Protocol
MC	Message Centre
MMS	Multimedia Messaging Service
MS	Mobile Station
MSC	Mobile Switching Centre
PSTN	Public Switched Telephone Network
SME	Short Message Entity
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPIM	Spam over Instant Messaging

SPIT	Spam over Internet Telephony
VAM	Voice Spam or VoIP Spam
VLR	Visitor Location Register
VoIP	Voice over IP

5 Conventions

None.

6 General aspects

Spam is electronic information delivered from senders to receivers by terminals such as computers, mobile phones, telephones, etc., which is usually unsolicited, unwanted and harmful for receivers. Spam may be carried in e-mail, mobile messaging service, IP multimedia and other electronic forms. As a matter of fact, the meaning of "spam" depends on certain perceptions of nations, organizations or individuals. In particular, its meaning is evolving and broadening with the development of information communication technologies which provide novel opportunities to make spam. Generally, spam has the following common characteristics:

Electronic: Spam is electronic information that is usually transmitted in an open telecommunication network, especially the Internet, which is very different from traditional methods of postal mail, paper advertisements or direct marketing. Spam is cheap, convenient and easy to disguise.

Unsolicited: Spam usually contains advertisements, fraudulent information, or viruses, etc.

Furthermore, spam typically has the following characteristics entirely or partly:

Bulk and repetitive: Message spam and e-mail spam are typically sent in bulk indiscriminately, while real-time communication spam is always initiated repetitively. However, spammers usually do not know anything except the receiver's communication address (e.g., e-mail addresses, receiver's phone number).

Utilization of addresses without the owner's consent: Spammers often utilize communication addresses collected without the owners' explicit consent to send spam. Actually, some software programs can gather communication addresses from the web or create communication addresses automatically.

Hidden or false message origins: Spam is often sent in a manner that disguises the originator by using a false message header or simply hides the originator. Spammers typically use unauthorized servers of third parties which do not validate the originator information.

Difficulty to block: It is very difficult to detect spam because of the large volume of messages. Attempts to block spam may be difficult and, at times, will result in false positives or false negatives.

The strategies should be technology-neutral, yet worthwhile to evaluate a number of factors: which particular communication media is misused or causes problems within the jurisdiction, which communication media has a strong potential to be misused in the future, and which is unlikely to be misused. The common options are:

E-mail

Currently, e-mail spam is the most significant threat among various types of spam due to vulnerabilities of e-mail protocol and insecurities of basic infrastructure, i.e., Internet, by which e-mails are transmitted. Simple mail transfer protocol (SMTP) is the most popular protocol to relay e-mails. SMTP defines an envelope and a header for an e-mail. The envelope contains the address of the receiver and cannot be seen by the receiver. It is used as the destination address to transfer

messages from the sender to the receiver. Normally, during transmission, the destination address in the envelope is copied to the e-mail header that the receiver can see. Spammers exploit two types of vulnerability in the SMTP authentication process:

- No authentication required, therefore users can hide or forge their addresses.
- Most records can be forged in the envelope and the header of e-mails.

In addition, the cost to send e-mail spam is very small while its negative influences are always very large.

Mobile messaging service

The remarkable advantages of mobile communications are convenience, efficiency, low price and easy usage. But nowadays, users are facing mobile messaging spam while enjoying the benefits of mobile communication. Mobile messaging spam is a term typically used for unsolicited messages sent via SMS or MMS. Currently, the main types of short message spam are as follows:

- service-subscription deceit;
- advertisement information;
- illegal cheat;
- pornographic information.

These kinds of messages are typically deceptive or fraudulent, and are also known as scam messages.

It is important to note that it is now common to receive e-mails on mobile devices with the advent of mobile e-mail services, which is easier to be utilized by spammers.

IP multimedia

With the development of IP multimedia, the concept of spam has started to be broadly used for IP multimedia such as instant messaging spam, Internet telephony spam, presence spam, blog spam, usenet newsgroup spam, online game messaging spam, etc. In some instances, there are different terminologies for spam delivered on certain types of media, such as SPIM (spam over instant messaging), SPIT (spam over internet telephony), etc. Furthermore, multimodal interactions, as new types of multimedia, are also affected by spam where a single multimedia "spam" may have multiple appearances on user interfaces. For example, a "spam" network message may result in playing a "spam" audio clip, in displaying a "spam" video clip and in showing a "spam" text message on the screen; all either with the same or different content. However, multimodalities increase the exposure to multimedia "spam" and, hence, the multimodal "spam" problem is expected to increase once multimodal interactions become more widespread.

SPIM: Instant messaging is a kind of convenient, real-time and cheap communication method in the Internet with rapid development. It is mainly used for private communications. Meanwhile, instant messaging applications are used increasingly in enterprises. But unfortunately, more and more illegal information, such as viruses, malicious codes, etc., are distributed by instant messaging, which is commonly referred to as SPIM. Although SPIM is a small percentage of all spam, it is growing quickly.

SPIT: Some spam problems which have been identified up to now include those usually associated with IP networks, plus other more sophisticated threat, such as misrepresentation, eavesdropping, VoIP-specific denial of service attacks, packet injections and unwanted messages (spam over VoIP, or SPIT). The latter is mainly due to the possibility offered by VoIP of sending voice messages at a very low cost, which may lead to a situation similar to the one already experienced with e-mail spam: large numbers of unwanted voicemail messages can be sent through the world in a few seconds.

Evolution of spam

Spam is not limited to the above options. With the introduction of more and more information communication technologies and applications, spam will evolve ubiquitously. Furthermore, any communication technologies and applications can be the media of spam if proposed solutions for countering spam are ineffective.

7 Generic objectives

The purpose of this clause is to describe the ultimate goals for countering spam. The focuses are what should be achieved rather than identifying practical implementation steps.

The objectives for countering spam:

- Validation of entities, whether they have privileges to send messages or initiate communications after authentication and/or with authorization.
- Protection of the address and/or other important information of messages or communications sent by legitimate entities from being hidden or being disguised.
- Protection of privacy during information transmission.
- Responsibility of all entities for their own behaviours on information transmission or relay.
- Protection of the telecommunication networks from unauthorized access or operation in order to ensure effective and efficient accessibility.
- Provision of necessary information of originator for future traceability.
- Protection of service equipments from viruses and unauthorized access in order to ensure availability.
- Spam filtering and, if necessary, spam storage on specific equipment for traceability and forensic analysis.
- Provision of a feedback platform, which not only encourages the accurate and effective reporting of information, but also supports international cooperation, legislation, etc.
- Application of well-known international protocols for appropriate information sharing and dissemination on countering spam.

In addition, the realization of the above objectives should be based on the specific environment.

8 Technical strategies

A multi-faceted approach that includes the following aspects is necessary to counter spam: industry-driven technology; industrial self-discipline; international cooperation, legislation, feedback and training. Among these aspects, technology is essential to guarantee the implementation of the other aspects. This Recommendation mainly focuses on general technical strategies for countering spam.

In order to analyse easily, it is better to first classify services. According to transmission methods, services can be classified as store-and-forward class and real-time communication class. Store-and-forward class includes e-mail services, mobile messaging services, multimedia messaging services, etc. Real-time communication class includes IP telephony, IP fax, instant messaging, etc. The methods to counter spam in different services are different; therefore, detailed analysis is needed for a particular service based on the general technical strategies.

To effectively counter spam, it is recommended to implement a hierarchical model with different parts. Furthermore, the more parts that are put in place, the more effective it is. Figure 1 shows the hierarchical model for countering spam, which is described as follows.

Filtering strategies	Feedback strategies
Service strategies	
Equipment strategies	Network strategies

Figure 1 – Hierarchical model for countering spam

In this hierarchical model, the five parts are divided into three levels: infrastructure level, service level and application level. Equipment strategies and network strategies, which belong to the infrastructure level, are the foundation of the hierarchy model. The realization of them can be a secure and reliable footstone for technical strategies in the upper layers. By the way, equipment strategies and network strategies influence each other. Secure networks need secure equipment, while secure equipment need reasonable networks. Service strategies, belonging to the service level, is the most important among the five parts because the layer is directly responsible of the provision of service. Finally, filtering requirements and feedback requirements belong to the application level, which are closer to users for countering spam; however, they interact with each other. Figure 2 shows the relationship between different parts:

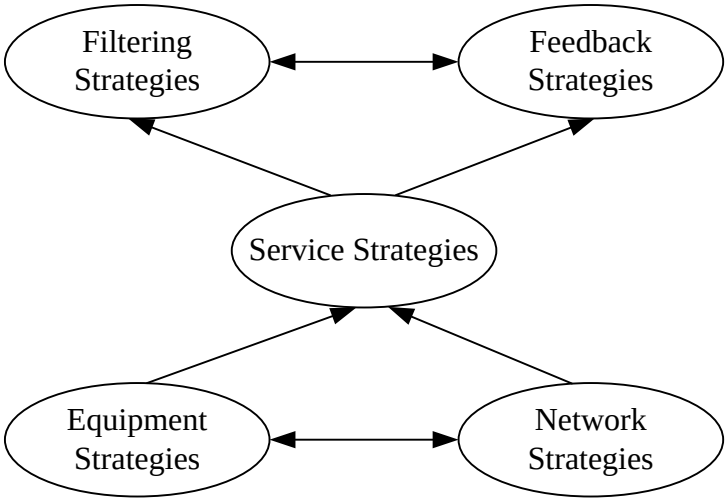

Figure 2 – Relationship between different parts

In addition, well-known international protocols are recommended to meet these technical strategies. But if all the technical strategies are satisfied, the cost may be too high compared with the value of the services being protected. Therefore, it is very important to customize the technical strategies according to application scenarios. In addition, the methods to counter spam should be provided in a way that permits customization. Due to the large number of possible combinations of technical strategies, it is desirable to have profiles that cover a broad range of services. Standardization via industry and research-led organizations will facilitate the reuse of solutions and products. At the same time, technical solutions for countering spam can be deployed faster and at a lower cost.

8.1 Equipment strategies

Equipment is the footstone of infrastructure for countering spam; therefore, the protection of equipment is essential to counter spam.

8.1.1 Improving the software security of the relevant equipment

Spammers can distribute spam by using computer resources and network resources that belong to third parties once these resources have evident vulnerabilities. The resources become victims and are named botnets or zombie computers. Spammers can remotely control the victims to send spam. It is effective to install a secure operating system and application software, and update antivirus software in time to protect the relevant equipment from viruses.

8.1.2 Providing different management roles

Due to the importance of service systems, different management roles should be provided. They should at least include user management role, system management role and audit management role. The user management role is used to manage configuration of the managers, operators and auditors. The system management role is used to maintain and operate the equipment. The audit management role is used to audit the operating logs and system logs. In addition, some particular management roles may be needed for specific services.

8.1.3 Providing operation log and system log

The system is required to provide operation logs and system logs to guarantee regular operation of the system and maintain the normal running state of the system.

Operation logs are used to provide the operation history. All the login and operation events should be recorded. At least, operation logs should include the following fields: operator's name, operation time, operation command and operation result.

System logs can provide history of the system running state. It mainly includes performance information, failure information, etc. The records of system logs may be different for different systems or different services.

However, operation logs and system logs cannot only serve the maintenance of the system, but can also assist managers to ensure operational procedures without destructive activities.

8.1.4 Improving security and flexibility of terminals

Terminals are the most important end-user equipment, which are always direct victims of spam. Because functions are always different among various types of terminal, only general strategies can be figured out. They are listed, but not limited to, the following:

- supporting authentication and authorization, especially for intelligent terminals;
- supporting blacklist and whitelist;
- providing anti-virus software, especially for intelligent terminals.

8.2 Network strategies

Similar to equipment requirements, network security is also the basis for countering spam. Spam can be remarkably reduced by proper design of network topology and deployment of various security equipment, such as firewalls, secure routers, secure gateways, etc.

8.2.1 Protecting service network from the Internet

Various network services are facing threats from the Internet because most of these services are based on IP technologies with open standards.

The following functions are required:

- Protect service networks from Internet attacks, such as DoS and DDoS attacks. The service networks are very important and are usually controlled remotely by administrators. Because the Internet is open to everyone, service networks should be able to withstand exploitation of Internet vulnerabilities. Usually, firewalls and other secure equipment are used to protect the service networks from these vulnerabilities.

- Protect protocol signals in control plane to block illegal intrusions. It is especially important for VoIP. PSTN is always secure and reliable while the Internet is insecure and unreliable. Therefore, VoIP gateways should be able to block illegal protocol signals in order to achieve the same security level as that on PSTN.

8.2.2 Providing redundant and backup mechanism to keep stability of service network

Service equipment and networks are so important that redundant equipment and backup routes should be provided. In addition, the redundant and backup mechanism should be practical, effective and cost-reasonable.

8.3 Service strategies

Service strategies is the most important part of the hierarchical model because services directly satisfy users' requirements. But there are so many kinds of services with different functions and various vulnerabilities. So service strategies for countering spam in different services differ from each other. However, different services have the same general service strategies on countering spam, which are listed as follows.

8.3.1 Supporting authentication

When entities (user or equipment) access services, strict authentication should be supported by service systems. On the one hand, strict authentication can prevent an invalid entity from accessing services. On the other hand, accurate authentication records can be used for traceability.

Nowadays, some countries have achieved a lot on mobile networks due to the implementation of authentication and real name mechanisms.

8.3.2 Supporting configurable relay address

Open relay should be shut down and limited relay should be adopted in service equipment. The service equipment should support configurable relay address lists. They only relay messages from the permissible addresses. On the contrary, the messages from other addresses will be blocked.

8.3.3 Supporting strict message format

For particular messages, especially commercial messages, the message format should be defined strictly. Thus, service systems can get enough information to deal with the messages.

8.3.4 Compatible with international standards

In order to strengthen the capability of interconnection and interoperability, communication protocols of services are requested to be compatible with international standards.

8.3.5 Improving traceability of spam

On the one hand, service systems should identify and authenticate entities (users or equipments) while they are accessing the service systems, and get accurate origination information of the entities, then record the appropriate information into databases. On the other hand, service systems should provide audit functions for traceability based on the records in databases.

8.3.6 Supporting flow control

System managers can limit the bandwidth of communication or the number of messages transmitted in every specific time slot.

8.3.7 Providing statistics functions

The statistics information highlights to system managers the current status of the system, such as traffic volume and visitors' information.

8.4 Filtering strategies

Filtering is the most common anti-spam technology. The main advantage of filtering is simplicity and flexibility of implementation.

8.4.1 Supporting spam filtering

Generally, there are two types of filtering: address-based filtering and content-based filtering (including keyword-based filtering).

Address-based filtering can be used in both store-and-forward services and real-time services. For store-and-forward services, address-based filtering is used to filter messages and e-mails according to their originators' addresses. It is effective to prevent service systems from sending or relaying spam messages and e-mails. For real-time services, address-based filtering is used to block calls according to callers' phone numbers or addresses. Generally speaking, address-based filtering is effective and convenient to countering spam.

Content-based filtering can also be used in both store-and-forward services and real-time services. For store-and-forward services, content-based filtering is used to filter messages and e-mails based on contents or keywords. For real-time services, content-based filtering is used to cut off the communications based on their content. Theoretically, content-based filtering is more reasonable compared to address-based filtering. However, content-based filtering always consumes a lot of resources, and accuracy of content-based filtering is tightly related to analysis algorithms.

Neither filtering method can filter all spam. Therefore, it is better to use both methods simultaneously. In addition, the service equipment should support filtering viruses.

8.4.2 Providing backup/recording mechanism for spam filtering

Regarding store-and-forward services, service equipment should backup spam automatically. Regarding real-time services, service equipment should record profiles of spam automatically. They are both stored for possible query in the future.

8.4.3 Performance requirements of spam filtering

Performance is very important for spam filtering. The false positive rate and false negative rate are the most important factors to evaluate performance of spam filtering. The term false positive refers to negative instances being detected when there are no negative instances, while the term false negative refers to no negative instances being detected when there are negative instances. Therefore, the false positive rate is the proportion of negative instances that are erroneously reported as positive instances. The false negative rate is the proportion of positive instances that are erroneously reported as negative instances. Table 1 is the result of spam filtering.

Table 1 – The result of spam filtering

		Actual condition	
		Positive instances	**Negative instances**
Test result	Positive instances detected	A	B
	Negative instances detected	C	D
NOTE – Positive instance is spam, negative instance is not spam.			

The total number of test instances is T.

T = A + B + C + D

The number of false positives is B.

The number of false negatives is C.

False positive rate = B / (B + D).

False negative rate = C / (A + C).

The false positive rate and false negative rate are tightly correlative. Usually, the bigger false positive rate is, the smaller the false negative rate. However, which rate is more important depends on the practical environment. In commercial practice, it is better to increase the false negative rate rather than the false positive rate.

8.4.4 Providing easy and flexible filtering configuration

In the face of numerous and varied spam, an easy and flexible filtering configuration should be provided, such as friendly interfaces, selectable configuration methods and so on. In addition, general filtering rules can be classified into different filtering categories, which will be put into databases or repositories. If necessary, such filtering categories can be selected and used easily.

8.4.5 Decreasing filtering cost as much as possible

It is better to filter spam as early as possible, not after spam has occupied a lot of resources. Therefore, spam should be filtered at the beginning of transmission and should not be left for the later service equipment.

8.4.6 Supporting blacklists and whitelists

There are two types of address-based filtering: whitelists of acceptable senders and blacklists of suspected spammers.

Blacklists are based on the listing of spam originators. This list can include the names of machines, IP addresses, MAC addresses or other kinds of electronic addresses. Filtering system can filter messages or block communications according to the blacklists.

Whitelists are based on the listing of acceptable originators. The working mechanism is similar to that of blacklists except that the whitelists are lists of acceptable addresses.

Actually, the whitelists/blacklists approach is usually too crude to be acceptable for most users. However, such approaches are very simple and do not need significant resources. In order to increase filtering efficiency, filters should support whitelists and blacklists, especially blacklists for countering spam.

8.4.7 Supporting filtering of multimodal messages

For multimodal messages, it is required to:

- Support the capability to entirely block certain multimodal messages.
- Support the capability to remove certain multimodal message attachments or partial multimodal content within a multimedia message.
- Support the capability to filter incoming (received) and/or outgoing (sent) multimodal messages.

8.5 Feedback strategies

End-users are the final receivers of spam, the possible victims of viruses and scams. The participation of end-users will be helpful for countering spam effectively and efficiently. Therefore, feedback of end-users should be taken into account when developing solutions for countering spam. However, the participation of the end-user at the feedback mechanism shall be on a voluntary basis.

8.5.1 Providing platform for feedback of spam

Recourse should be provided to individuals who are affected by harmful spam. The rights of natural persons, as the receivers of spam, need to be protected by legislation. Therefore, avenues for recourse need to be made available to them. Mechanisms need to be established to support this aim, including avenues for the reporting of spam violations to an appropriate authority. Such feedback-handling procedures need to be transparent, efficient and effective. A feedback platform can play such a role.

8.5.2 Providing standard formats for feedback sharing

It is necessary for a feedback platform to record feedback adopting standard recording format. Therefore, different operators and entities can share feedback. From the shared feedbacks, the main addresses of spammers can be obtained, which can be used in blacklists.

9 System evaluation

In order to evaluate efficiency and effectiveness of technologies and systems on countering spam, the following aspects should be taken into consideration:

- False positive rate.
- False negative rate.
- Cost: The methods of countering spam should be flexible to provide customized solutions. Due to the large number of possible combinations of strategies, it is desirable to have profiles that cover a broad range of services.
- Interoperability of current systems: The precondition of countering spam is guaranteeing the normal operations of current systems. In other words, we could not disrupt current systems by implementing the solutions on countering spam.
- Conformance to international standards: Technical solutions should preferably be based upon international standards in order to achieve global interconnection and expansion. In addition, standardization will facilitate reuse of solutions and components. This will help new counter-spam solutions and techniques to be introduced rapidly and at low cost.

The above aspects are general criteria to evaluate the measures on countering spam. In practical service networks, other specific aspects need to be considered.

Bibliography

[b-ITU-T Q.1742.3] Recommendation ITU-T Q.1742.3 (2004), *IMT-2000 references (approved as of 30 June 2003) to ANSI-41 evolved core network with cdma2000 access network*.

[b-ITU-T Q-Sup.49] Recommendation ITU-T Q-series Recommendations – Supplement 49 (2004), *Technical Report TRQ.2840: Signalling requirements to support IP telephony*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[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 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*. <http://www.ietf.org/rfc/rfc2635.txt>

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

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*. <http://www.ietf.org/rfc/rfc3685.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