International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1244

(09/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Overall aspects of countering spam in IP-based multimedia applications

Recommendation ITU-T X.1244

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.1244

Overall aspects of countering spam in IP-based multimedia applications

Summary

Recommendation ITU-T X.1244 specifies the basic concepts, characteristics, and technical issues related to countering spam in IP multimedia applications such as IP telephony, instant messaging, etc. The various types of IP multimedia application spam are categorized, and each categorized group is described according to its characteristics. This Recommendation describes various spam security threats that can cause IP multimedia application spam. There are various techniques developed to control the e-mail spam which has become a social problem. Some of those techniques can be used in countering IP multimedia application spam. This Recommendation analyses the conventional spam countering mechanisms and discusses their applicability to countering IP multimedia application spam. This Recommendation concludes by mentioning various aspects that should be considered in countering IP multimedia application spam.

Source

Recommendation ITU-T X.1244 was approved on 19 September 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 procedure.

Keywords

Instant messaging spam, IP multimedia application spam, spam, voice over IP spam.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

Page

Introduction

Spam has been a social problem in the network e-mail system. Various solutions have been developed and deployed to resolve this problem, but none of them have actually solved the spam problem. The IP multimedia application consists of various types of services, such as IP telephony, instant messaging, etc. These IP multimedia services are becoming a new target for the sender of spam, since it is technically a simpler and economically cheaper approach for spamming. IP multimedia application spam must be dealt with before it becomes a public problem.

This Recommendation describes the concept and characteristics of various types of spam that can occur in IP multimedia applications. It discusses some issues on technical and security viewpoints for countering IP multimedia application spam, thus provides some consideration aspects by several participating members in providing IP multimedia service such as service providers, service users, etc. in countering IP multimedia application spam.

Recommendation ITU-T X.1244

Overall aspects of countering spam in IP-based multimedia applications

1 Scope

This Recommendation provides an overview of IP multimedia spam, with a focus on the following issues:

- Concept and characteristics of IP multimedia spam
- Technical issues related to IP multimedia spam
- Security threats related to spam
- Spam countering methods and their applicability to counter IP multimedia spam
- Various aspects that should be considered for countering spam in IP-based multimedia applications

NOTE – The use of the term "identity" in this Recommendation does not indicate its absolute meaning. In particular, it does not constitute any positive validation.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control list (ACL) [b-ITU-T X.741]: The access control list attribute is used to contain identities of initiators that are either specifically granted access to management information or specifically denied access to management information.

3.1.2 certification authority (CA) [b-ITU-T X.509]: An authority trusted by one or more users to create and assign public-key certificates. Optionally, the certification authority may create the users' keys.

3.1.3 conference [b-ITU-T T.124]: A number of nodes that are joined together and that are capable of exchanging audiographic and audiovisual information across various telecommunication networks.

3.1.4 DomainKeys identified mail (DKIM) [b-IETF RFC 4871]: A mechanism by which e-mail messages can be cryptographically signed, permitting a signing domain to claim responsibility for the introduction of a message into the mail stream. Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key, and thereby confirm that the message was attested to by a party in possession of the private key for the signing domain.

3.1.5 instant messaging (IM) [b-IETF RFC 3428]: An exchange of content between a set of participants in near real time. Generally, the content is short text messages, although that need not be the case.

3.1.6 peer-to-peer (P2P) relationship [b-ITU-T T.180]: In a peer-to-peer relationship, the users may negotiate the characteristics of their interaction and, afterwards, communicate obeying the rules they have negotiated; both users (an entity and its peer entity) have potentially equal rights. [b-IETF RFC 4981] indicates that P2P networks are those that exhibit three characteristics: self-organization, symmetric communication, and distributed control.

3.1.7 pretty good privacy (PGP) [b-IETF RFC 1991]: PGP uses a combination of public key and conventional encryption to provide security services for electronic mail messages and data files. These services include confidentiality and digital signature. PGP was created by Philip Zimmermann and first released, in Version 1.0, in 1991. Subsequent versions, e.g., open PGP that is described in [b-IETF RFC 4880], have been designed and implemented by an all-volunteer collaborative effort under the design guidance of Philip Zimmermann. *PGP and Pretty Good Privacy are trademarks of Philip Zimmermann*.

3.1.8 public key infrastructure (PKI) [b-ITU-T X.509]: The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

3.1.9 transport layer security (TLS) [b-ITU-T Q.814]: The TLS protocol optionally provides communications privacy. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and intrusion. The TLS protocol also provides strong peer authentication and data flow integrity.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 bait spam: Its name derived playfully from the analogy to fishing (and phishing (see clause 3.2.10)), bait spam is a variety of spam which includes an element, e.g., an e-mail subject or embedded link, to lure users. The lured user is attacked by the bait spam.

3.2.2 blog: A contraction of "web log"; a blog is an online, possibly multimedia, list of its owner's personal interests that is available for general public to view and, sometimes, to enhance.

3.2.3 bot: Bot is a contraction of "robot", which is a program that operates as an agent for a user or another program to simulate a human activity.

3.2.4 DNS cache poisoning: DNS cache poisoning is a technique that tricks a domain name system server (DNS server) into believing the DNS address of a certain server has been changed when, in reality, it has not. Once the DNS server has been poisoned, this information is generally cached for a certain period of time, spreading the effect of the attack to the users of the server.

3.2.5 IP multimedia message: IP multimedia message is a text, voice, or video message that is delivered and stored in an IP multimedia terminal or server for the recipient to check afterward. It is similar to voice mail in telephony service, but serviced in IP multimedia service.

3.2.6 IP multimedia spam: Unsolicited messages or calls through IP multimedia applications. To distinguish this from traditional e-mail spam, IP multimedia spam denotes spam on newly emerging telecommunication methods over IP, such as instant messaging (IM), presence, or voice over IP (VoIP) services.

3.2.7 modality: In general usage, this term refers to the forms, protocols, or conditions that surround formal communications. In the context of this Recommendation, it refers to the information encoding(s) containing information perceptible for a human being. Examples of modality include textual, graphical, audio, video or haptical data used in human-computer interfaces. Multimodal information can originate from, or be targeted to, multimodal-devices. Examples of human-computer interfaces include microphones for voice (sound) input, pens for haptic input, keyboards for textual input, mice for motion input, speakers for synthesized voice output, screens for graphic/text output, vibrating devices for haptic feedback, and Braille-writing devices for people with visual disabilities.

3.2.8 multimodal message: This is a multimedia message that contains differently encoded information for interaction via multiple modalities. For example, a MMS (multimedia messaging service) message may convey text, graphic and audio modalities. A web-page may also contain multimedia modal content such as text and video. Similarly, an e-mail may contain a graphic attachment together with text. Multimodality enables the user to select a preferred modality due to environment, convenience or content.

3.2.9 online game: Real-time game that is played over the networks.

3.2.10 phishing: An attempt to acquire criminally and fraudulently sensitive information, such as usernames, passwords and financial account details, by masquerading as a trustworthy entity in an electronic communication.

3.2.11 session hijacking: A mechanism of stealing a valid user session to gain unauthorized access to information or services.

3.2.12 spam over instant messaging (SPIM): A spam targeting users of instant messaging service.

3.2.13 spam over Internet telephony (SPIT): Spam targeting users of Internet telephony service

3.2.14 spammer: Sender of spam.

3.2.15 spamming: A chain of activities carried out by spammers to send spam, such as collection of target lists, creation of spam, delivery of spam, etc.

3.2.16 spimmer: Sender of SPIM.

3.2.17 spitter: Sender of SPIT.

3.2.18 user created content (UCC): UCC is any form of content such as video, blog, images, audio, etc. that was created by end-users (average public) to be available for general public.

3.2.19 user generated content (UGC): UGC is equivalent to UCC.

3.2.20 vishing: An illegal act of gaining access to private personal and financial information through the voice over IP (VoIP) service. The term vishing is a contraction of "voice phishing".

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
APEC	Asia-Pacific Economic Cooperation
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
DB	Database
DKIM	DomainKeys Identified Mail
HTTP	HyperText Transfer Protocol
IM	Instant Messaging
IP	Internet Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRC	Internet Relay Chat
ISP	Internet Service Provider

ITSP	Internet Telephony Service Provider
IVR	Interactive Voice Response
MAC	Media Access Control
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
NDP	Neighbour Discovery Protocol
OS	Operating System
P2P	Peer-to-Peer
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
RTP	Real-time Transport Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoD	Video on Demand
VoIP	Voice over IP

5 Conventions

None.

6 Concept and typical types of IP multimedia spam

Although there is no globally agreed definition of spam, this term is commonly used to describe unsolicited electronic bulk telecommunications over e-mail or mobile messaging for the purpose of marketing commercial products or services. Currently, spam is not limited to e-mail or mobile messaging. It is spreading to IP multimedia applications such as VoIP and instant messaging. IP multimedia spam can be defined as unsolicited electronic bulk telecommunications over IP multimedia applications for the purpose of marketing commercial products or services. IP multimedia application spam can emerge over various kinds of IP multimedia applications, such as VoIP and instant messaging.

This clause lists some of the typical types of IP multimedia spam that can occur in IP multimedia applications. A description of its characteristics is given for each spam type.

6.1 VoIP spam

VoIP spam is a spam emerging over VoIP services. VoIP spam is a real-time voice spam, such as telemarketing, which includes communications with a telemarketer and interaction with IVR (interactive voice response) systems. Because telemarketing services using VoIP service are rapidly increasing by the fast deployment of VoIP services worldwide, the threat of VoIP spam is also increasing. Especially, making bulk calls is not difficult. It is possible to use cheaper labour from other countries as telemarketers than typically available in the target country, since the price of international calls has decreased dramatically through the use of VoIP service. It is much easier for spammers to collect information of target IP multimedia applications users. With these strengths, VoIP spam can emerge as a threat to VoIP service providers and users.

6.2 IP multimedia message spam

IP multimedia message is a text, voice, or video message that is delivered and stored in IP multimedia terminals or servers for the recipient to check afterward. It is similar to voice mail in telephony service, but is serviced in IP multimedia service. IP multimedia message spam is spam that uses the IP multimedia message service. The spam recipient checks the message and deletes the spam as with e-mail spam or mobile messaging spam. Many terminals of IP multimedia applications, such as VoIP phones, support multimedia messaging functions, making them target applications for spammer to send IP multimedia message spam.

Multimedia message spam can be categorized as text message spam and voice/video message spam. Text message spam is a short message which includes commercial or invited text. It has similar characteristics to e-mail spam or mobile SMS spam, since it is in the form of text. However, the spamming cost of text message spam is expected to be much lower than mobile SMS spam. Voice/video message spam is a message in the form of voice/video which includes commercial or invited contents. This type of spam is expected to spread widely along with the usage of IP multimedia applications. Voice/video messages are anticipated to occupy a great part of the voice/video mailbox of IP applications users, or the storage of IP service providers, since the size of multimedia messages is much greater compared to text message. Multimedia message spam can also be used by malicious spammers to deliver malicious software such as worms, computer viruses, spyware, Trojan horses, etc.

6.3 Instant messaging spam

Spam over instant messaging, namely SPIM, is another kind of threatening IP multimedia application spam, which is targeting instant messaging service users. Many users use IM service for convenient communications with other users in the networks. Most IM spam is text-based short messages and has many features in common with e-mail spam, but IM spam is a real-time message and can be more annoying. Multimedia message spam can also emerge over IM, since IM service supports many functions in addition to real-time text message delivery.

Sending IM spam may not be easy without illegal technical manipulation, since most IM services adopt consent-based buddy lists, with only the users in a buddy list being allowed to send messages. However, a weak security system for IM services may allow spammers to steal a buddy list or white list of a spam target to send spam messages, disguised as a member of the buddy list.

While message delivery is only possible between users in buddy lists, requesting consent to be added to the buddy list can be made by anyone. In many IM services, buddy request messages can contain a few sentences introducing the requester to help the IM service user to know who is requesting and to determine whether to permit the requester to be added to the buddy list. A spammer who is not in the buddy list can send spam messages using this function of IM service.

6.4 Chat spam

Chat spam can occur in various kinds of IP multimedia applications which provide chatting functions among service users. The chatting function and messaging function are provided in many IP multimedia applications such as online chatting services, online game services, etc. Chat spam is usually in a short text message format, with the same message being sent repeatedly to all chatting participants. Thus, some online chatting services and online game services limit the number of reiterations of the same message being delivered, to counter repetition of spam messages. However, the effect of this method is limited and more countermeasures for countering various types of chat spam are required.

Chat service has the same characteristics as the IM service, but the types of spam that can occur to these services are different. A user of IM services usually communicates with the correspondents in a buddy list, who are authorized by the IM service user to communicate. Thus, a spammer must penetrate the buddy list in order to send spam. Chat service occurs in online services, where the participants of the communications are usually unknown. Anyone can participate in the chat service, thus a spammer can join the chat service to send spam. The type of spam that can be found in chat services involves sending the same message repeatedly. Thus, it is much simpler to spam in chat service compared to IM service.

6.5 Multimodal spam

The "spamming" security problem extends to the situation of multimodal interactions where a single multimedia "spam" message may yield multiple targets on a user interface varying with the modality. 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 content or even with a different content. As such, multimodalities increase the exposure to multimedia "spam", and hence, the multimodal "spam" problem is expected to increase once multimodal interactions become more widespread.

6.6 Spam over P2P based file sharing service

IP multimedia application spam also can emerge over P2P based IP multimedia applications targeting users of P2P based services, such as P2P file sharing service. People connected to IP-based networks using P2P software helps users to use peer-to-peer communication to share various kinds of computer files with each other. In such services, spammers can lure other users to download spam files by naming the spam file with a name of popular movie, popular song, etc. Spammers do not need to find spam targets. They only need to share spam files to make other P2P service users access them. Many downloaded spam files are expected to be executed, since the spam recipient downloads them voluntarily. So, the damage of spam over P2P service can be great when the spam contains malicious software, such as worms and viruses instead of commercial contents.

6.7 Website spam

Spammers can post articles or files with commercial contents on many websites operated with various kinds of purposes. The spam that is posted on a bulletin board can be seen by many visitors of the website. For example, replies with commercial contents for many articles of web portals and commercial articles on blogs can be website spam. In addition to the text-based articles, spammers can also upload commercial audio and video files on audio/video sharing sites, such as UCC and UGC or bulletin boards to make other service users watch the commercial video files. Website spam can be read or viewed by a great number of website service users. Spammers do not need to gather spam targets to send bulk spam to targets in this type of spam.

7 Classification of IP multimedia spam

IP multimedia application spam is classified into two groups, according to its features. IP multimedia application spam can be classified according to various criteria such as the type of IP multimedia applications where the spam emerges, media type used in spamming, protocol used for service provision, type of protocol message, etc. In this clause, IP multimedia spam is classified according to the following characteristics of IP multimedia applications, considering that anti-spam techniques can be applied according to those characteristics.

– Real-time or non real-time IP multimedia spam: IP multimedia application services can be classified by the criterion of being real-time.

– Media type of IP multimedia spam: An IP multimedia application service can support text, voice, video, or a combination of such. Video includes both still image and animation.

In real-time IP multimedia application services, the communication is established, a message is delivered, and recipient checks the message in real-time. Typical examples of real-time IP multimedia applications are VoIP service and IM service. In non real-time IP multimedia application services, the recipient can check messages when he or she wants. Examples of non real-time IP multimedia applications are web services, P2P service, online game services, etc. Classification of IP multimedia application spam and the representative examples are presented in Table 7-1.

Table 7-1 – Classification of IP multimedia application spam

	Text	Voice	Video
Real-time	• Instant messaging spam • Chat spam	• VoIP spam • Instant messaging spam	• Instant messaging spam
Non Real-time	• Text/multimedia message spam • Text spam over P2P file sharing service • Website text spam	• Voice/multimedia message spam • Voice spam over P2P file sharing service • Website voice spam	• Video/multimedia message spam • Video spam over P2P file sharing service • Website video spam

7.1 Real-time voice spam

Real-time voice spam can be defined as unsolicited real-time voice communications with the purpose of advertising commercial product or service. A representative example of real-time voice spam is VoIP spam. Real-time voice spam may be less frequent than e-mail spam, but the damage of a spam to a service user is considered to be much greater. Real-time voice spam is very annoying to spam recipients. In e-mail service, service users can check e-mail when they want, can identify e-mail spam within a short period of time, and can delete spam with relatively small effort. But real-time voice spam is more intrusive, since it requires the immediate response of the spam recipient. Moreover, it takes more time to recognize that the received message is a voice spam. Real-time voice spam is more effective compared to e-mail spam and mobile SMS spam. Generally, spammers try to persuade the spam recipient to buy a specific product or service. In real-time voice spam, telemarketers try to persuade the spam recipient through interactive communication, which is more invasive when compared to e-mail and SMS spam, which can only deliver short text or video-based on non-interactive format. As the persuasion rate of spam grows, the damage of spam generally grows as well. So damage from real-time voice spam can be relatively great considering the quantity of spam.

Real-time voice spam may try to improve the efficiency of the spam by using various IP supplementary services, in addition to the basic voice communications. Real-time voice spam is generally delivered to spam recipients through terminals which support VoIP service. Many of this kind of terminal can support many additional functions, such as multimedia messaging, video phone, and display sharing, with voice communications as the default function. Spammers can try to enhance the effect of spam by combining real-time voice spam with additional video or text type services.

Real-time voice spam can be an illegal or fraudulent spam, which has a malicious intention as also is encountered in the traditional wireline and mobile telephone services. Moreover, the cheap price of VoIP can make these illegal VoIP spam more active than the traditional telephone services. For example, malicious spammers may try to find financial information by delivering VoIP phishing, namely vishing, to obtain information of service users illegally. Malicious spammers can send bait spam to make a spam recipient use a very expensive service without the recipient's intention. For example, spammers can use an 'automated one time-ringing machine.' This machine makes a connection with the spam recipient and terminates the call after one or two rings, or makes a quick disconnection after just saying a small word like, "Hello." Many recipients would tend to call back using the caller ID information. The spam recipient then is connected to an automatic advertisement system, or some very expensive service. This kind of spam is more attractive to a spammer, since the spamming cost is very low. Bait spam can be delivered by malicious spammers who abuse security vulnerabilities of VoIP systems. For example, spammers can spoof themselves by hijacking VoIP call session. Spammers can make a VoIP service user connect to the spammer by spoofing when the user wants to communicate with other service users. Similarly, various kinds of bait spam luring spam recipients can emerge over IP multimedia applications.

7.2 Real-time text spam

Real-time text spam can be defined as unsolicited bulk real-time text message, for example with the purpose of advertising a commercial product or service. Real-time text spam may emerge over many IP multimedia applications, which provide real-time text message delivery between service users. The characteristics of real-time text spam are similar to those of e-mail spam since the spam is text-based. However, real-time text spam is more annoying than e-mail spam since at the moment the spam is delivered, the spam recipient gets interrupted. Examples of real-time text spam are IM spam and chat spam.

In many IP multimedia application services, including IM service, online chatting service, and online game, message delivery function is provided for service users for free or at a very low price. So spammers can send text message spam at a very low cost. Spammers can often get general or specific information of service users by various methods. This information can increase expected profit from spam for spammers compared to e-mail spam which is targeting unspecified people.

7.3 Real-time video spam

Real-time video spam can be defined as unsolicited real-time video communication with the purpose of advertising a commercial product or service. Video includes both still image and animation. Real-time video spam can emerge over IP multimedia application services which provide real-time video telecommunication function between service users.

In the early stage of IP multimedia application spam, text or voice type message spam which can be made without considerable difficulty, can be delivered with low cost, and does not pose a burden to the IP network. Real-time voice spam in the form of telemarketing can be a large part of IP multimedia application spam. However, as media sharing and delivery technologies among IP multimedia application services users develops and as network capability increases, real-time video spam can also spread widely.

7.4 Non real-time voice spam

Non real-time voice spam can be defined as unsolicited bulk non real-time voice messages with the purpose of advertising a commercial product or service. The representative example of non real-time voice spam is recorded voice message spam.

In many cases, VoIP service can support multimedia messaging service such as sending and receiving of text, audio, and video messages, in addition to real-time voice call connection function. Spammers can send voice message spam which is already recorded in the terminal of the spam recipient using this function of VoIP service. This kind of voice message spam does cause great damage to VoIP service users and VoIP service providers by occupying voice mailbox or storage, since the size of voice message spam is large.

7.5 Non real-time text spam

Non real-time text spam can be defined as unsolicited bulk non real-time text message, for example with the purpose of advertising a commercial product or service. Characteristics of non real-time text spam are similar to those of e-mail spam. Non real-time text spam can emerge over various IP multimedia applications, since it is not difficult to create and deliver text message and spamming cost is usually low.

Non real-time text spam can be delivered to IP terminals, which can receive long text messages like e-mail, or to VoIP telephones, which can receive short text message like mobile SMS. It can be delivered over many IP multimedia application services including IM and various online services. In addition to those types of text spam, which is delivered to spam recipients regardless of the intention of the spam recipient, there are other kinds of text spam to which IP service users are exposed, such as advertisement posting on websites. Characteristics of non real-time text spam are similar to those of e-mail spam and many of the same techniques for countering e-mail spam are expected to be applied to this kind of spam. The applicability of these techniques may decrease when the length of text spam is short.

7.6 Non real-time video spam

Non real-time video spam can be defined as unsolicited bulk non real-time video message, for example with the purpose of advertising a commercial product or service. This kind of spam may be one of the following two types: IP service users get or download video spam file, or IP service users' get access to video spam in the form of VoD from IP multimedia application services. Delivery methods of non real-time video spam can be divided into two kinds. First, spam recipients may get unintentionally video advertisement files sent by the spammer. The other case is that IP multimedia application service users download spam files through file sharing services, not thinking that the file is a spam.

When the spam recipient downloads a video spam file, the effort and time of downloading the spam file can be wasted. When video message spam is delivered, regardless of the intention of spam recipient, the spam harms service users and service providers by occupying the mailbox or storage, since the size of a video message is generally large.

8 Technical issue for countering IP multimedia spam

Similar to e-mail or mobile SMS spam, the following is a series of procedures related to creating, sending, and preventing spam over IP multimedia application services:

- Creation and delivery of spam.
- Detection and filtering of spam by the service user and/or the service provider of IP multimedia applications.
- Countermeasure against received spam.

Prior to the establishment of a technical framework for countering IP multimedia application spam, it is required to investigate the weakness of prevention of IP multimedia application spam for the respective procedures described above. Mindful of the vulnerabilities, the type of technical issues should be considered at each step for countering IP multimedia application spam. Analyses of the influences these issues can have on the IP multimedia spam creation and delivery process are provided below. When studying the technical framework and technical means for countering IP multimedia spam, the issue analysis provided in this clause can be helpful in determining an effective way to counter IP multimedia application spam.

8.1 Creation and delivery of spam

The fundamental assumption for the spread of IP multimedia spam is that spamming cost should be low compared to the profit that the spammer expects from IP multimedia spam. The spamming cost includes not only monetary cost, but also various kinds of resources such as time, effort, and the technical difficulty required for the creation and delivery of IP multimedia spam. The factors that affect the spamming cost are as follows:

- Cost of collection of target addresses or target phone numbers: required cost for the collection of addresses and phone number of the spam targets.
- Cost of creation and delivery of spam: required cost for the creation and delivery of spam for spammer.

8.1.1 Collection of target list

Before sending spam, first of all, collection of spam target lists is required. Spammers can obtain e-mail spam target lists by dictionary attacks, e-mail address collection programs, and illegal access to collected target lists without much difficulty. In the case of mobile SMS spam, simple combinations of numbers can make spam target lists, since the source of mobile phone numbers is limited.

The type of specific subject identifier used for communication and message exchange between IP multimedia application service users may vary according to the type of IP multimedia applications, protocol, national regulations, etc. Subject identifiers which can be used for VoIP service may be in the form of telephone numbers, similar to the PSTN service; of IP addresses; IP service accounts, such as e-mail accounts, etc. For IM service, an e-mail address is generally used for the subject identifier, and other kinds of information such as a mobile phone number can be also used.

When these kinds of subject identifiers are used for VoIP and IM, the subject identifiers and service accounts for those services can be collected by spammers using existing target list collection methods used for e-mail spam. User addresses for VoIP and IM are expected to be collected without great difficulty through a dictionary attack, identifier collection program through a network search, etc.

In addition to VoIP and IM, there can be various types of IP multimedia application spam that can emerge such as chatting services, online game services, P2P based services, etc. It also seems that making spam target lists for these IP multimedia applications does not require much effort. Many of those IP multimedia applications, such as online services, use widely used type of accounts such as e-mail addresses and phone numbers as subject identifiers. It is usually not difficult to get into the user's list of IP multimedia application services, which allows only accepted users to deliver files or messages. Considering these points, without a specific measure to make it difficult to gather user identifiers of IP multimedia application services, it is not difficult for spammers to make subject identifiers of IP services technically or economically.

8.1.2 Creation and delivery of spam

The cost required for the creation and delivery of IP multimedia application spam is expected to be the biggest part of the spamming cost of IP multimedia spam. VoIP service or voice communications over various kinds of IP multimedia applications usually costs less than circuit-based wireline telephone service or mobile telephone service. For traditional spammers, who have been using telemarketing over traditional wireline or wireless telephone services for active marketing, VoIP or voice communications over IP multimedia applications is an attractive target service for spam delivery. Moreover, long distance calls and international calls are much cheaper compared to the traditional telephone services. So telemarketing spam can be spread to other countries which use the same language, and telemarketing spam can be made from other countries where telemarketer cost and spam delivery costs are very low.

In addition to VoIP service, many IP multimedia applications such as IM, P2P based service, and online chatting services are provided for free, or with very low cost. Spam creation and delivery on these applications is not expected to take much effort or cost, since they usually do not take much money, time, or technical difficulty.

8.2 Detection and filtering of spam

Detection and filtering of IP multimedia application spam is the most important technical point to counter spam effectively. It is practicable to filter out e-mail spam at the server of the ISP, or intranet or terminal of e-mail recipient, before spam recipient checks the spam, since e-mail service adopts a store-and-forward communications mechanism. An amount of e-mail spam can be filtered out by application using various kinds of filtering techniques, such as contents analysis, because most e-mail has text-based contents. Unlike e-mail spam, it is considered to be difficult to filter IP multimedia spam for the following features of IP multimedia application:

– Real-time communications.

– Difficulty of contents analysis of voice and video.

– Difficulty of spammer authentication.

Some IP multimedia applications such as VoIP and IM provide real-time communications between service users. Spam over those applications is delivered in real-time to the spam recipient without being stored at a server. In some cases, contents of VoIP and IM do not traverse the servers of the service provider. Instead, they are delivered to the service user directly. Therefore, it is difficult to acquire sufficient information about the communication and to analyse communication contents to identify spam before the call is established or the message is delivered. For example, when a message from a sender and a spam recipient has been established and the spam recipient recognizes that the message is a spam, it is too late to filter the spam, since the connection is already completed. In the case of IM spam, it may be possible to analyse the contents of the IM message during a very short time, since IM messages are usually text-based. However, the shortness of IM messages may reduce the effectiveness of traditional filtering techniques developed for countering e-mail spam. Terminals of service users get the responsibility of filtering spam when the contents of IP multimedia applications do not pass through the ISP server. But adding spam filtering to the terminals of service users and management of the spam filtering function by users are not that simple. Consequently, detecting and filtering of real-time IP multimedia application spam, such as VoIP spam and IM spam by contents-analysis filtering may not work.

Store-and-forward communications mechanisms may be adopted with some IP multimedia applications that are not positively necessary to be real-time, such as multimedia messaging. File delivery over P2P can be a technique to counter spam through contents analysis when it is required by service providers or service users. However, detection and filtering spam through the analysis of contents is still difficult, since the voice and video recognition technology is immature and applications of such technology can place a great load to the network.

It is also possible to identify spam based on the information of the sender, not the information of the telecommunications itself. It is possible to identify whether the sender is a spammer, or not, through various techniques, such as blacklists, whitelists, reputation systems, etc. Applications of these techniques to IP multimedia application spam have several weak points. First, making service accounts or subject identifiers for IP multimedia applications is not difficult and a great quantity of them can be made. Spammers can make a new identifier with ease when their old identifier is classified as spammer. It is also possible to pretend that they are normal service users abusing security weaknesses of IP multimedia applications. Considering these points, it is required to combine anti-spam techniques, which identify spam based on sender information, with effective authentication mechanisms.

8.3 Action for the received spam

Spam recipients can take several actions after they receive spam. They can add spammer's identifier to a blacklist to prohibit the spammer from sending more spam to themselves or other users. They also can give a bad score to the spammer to be reflected in reputation systems. It is also possible to report illegal spam to punish spammers. However, as mentioned earlier, identification of spammers over many IP multimedia applications is not easy and creating a new identifier is not difficult. At this point, an effective authentication mechanism is also required to be adopted to increase the effectiveness of actions for the received spam.

9 Security threats related to spam

This clause discusses security-related issues on IP multimedia spam. Some of the security threats are defined and categorized along with their countermeasures.

9.1 Security threats related to spam

This clause discusses some security threats that can occur to IP multimedia applications. Security threats are defined from the viewpoint of sending spam to the network. Spammers can send spam using the following technical attacks in IP multimedia environments.

9.1.1 Identifier collection

In order to send spam, a spammer collects identifiers to find targets for spamming. Thus, identifier collection is the most common spam threat and essential preliminary process. A spammer tries to collect as many identifiers as possible, because the number of identifiers means the number of targets to attack from the spammer's perspective. Identifiers can be gathered in various ways. They may be collected through search engines, open boards, etc. Identifiers can be generated with general words and names. Sometimes, they can be collected from illegal transactions with companies and schools, which can have many clients along with personal information.

Unique identifiers such as e-mail addresses and URI have been used to distinguish users in many IP multimedia applications. Unlike the phone service, services in IP multimedia applications have several advantages such as multichannel telecommunications, low price, etc. Spammers have an affinity for sending spam especially in IP multimedia environments. Therefore, users should be cautious in protecting their identification and not let it be exposed to spammers.

9.1.2 Spam sender spoofing

Spoofing is one kind of hacking techniques. A malicious network invader makes a website and lures people to visit their website to acquire the user's authority using an organizational defect of TCP/IP to steal their personal information. Moreover, if a spammer sends spam disguised as a famous company, a recipient may think that it is from a trustworthy sender. That spam has a high probability of being accepted. This is also called 'Spoofing'.

Sending spam via sender spoofing is a threat through which a spammer disguises himself as someone else by forging a message header field or sender's identifier used in IP multimedia applications. This threat can disrupt the white list and black list that are well-known spam solutions. For example, if spammers change their identifier into a valid user who is registered in the receiver's buddy list or white list, the spammer can bypass the white list-based policy. Moreover, due to the nature of the multimedia communication, it is difficult to determine whether the message is spam or not before the connection is established. Therefore, in this case, there is nothing that the receiver can do but get spammed.

9.1.3 Registration information sniffing

Sniffing is the behaviour in which a spammer eavesdrops on the ongoing connections between other users. The tool that is used for sniffing is called a sniffer.

In the IP multimedia environment, a spammer can send spam by using a sniffer, unlawfully. First, a spammer eavesdrops on the valid user's registration information for specific applications using a sniffer and generates fake registration information using the acquired information. Next, the spammer inserts an attacker's IP address instead of the valid user's IP address in the registration message. Then the spammer can send the spam using the fake registration.

9.1.4 Session hijacking

Session hijacking is a technique in which a person hijacks a communication session between other users. It can be used for sending spam in IP multimedia environments. Spammers can force a disconnection between the two users in the middle of the session. In that case, users tend to re-establish the previous ongoing sessions. Spammers can then hijack the session and can insert a RTP media transmission containing spam in the middle of the re-established session.

9.1.5 SQL injection

SQL injection is a hacking technique that brings an abnormal result by inserting query syntax that the requester did not intend. In an IP multimedia applications environment, SQL injection can be used when an HTTP Digest mechanism is applied for authentication. The spammer modifies the authentication header and inserts a forged SQL query. Then the spammer forges an authentication header of the message in the proxy server that the HTTP Digest mechanism uses for authentication, and inserts a forged SQL query. If this attack is finished successfully, the spammer can disguise himself as an authenticated user and send spam with valid authorization by faking a valid user's registration information.

9.1.6 Spam bot

A spam bot is a malicious bot that is in the form of a program, or code, which can be controlled and operated from a remote location but cannot be activated by itself. Generally, it is controlled via a connection using an IRC protocol. A network consisting of bots is called a botnet. It is possible for a spammer to control many infected systems using just one command, because botnet can be linked together. Therefore, a spammer can send a large quantity of spam easily using this technique in IP multimedia applications.

9.1.7 Cache poisoning

Cache poisoning is an attack that replaces domain addresses with other faulty addresses. Cache poisoning can be used for ARP and NDP in IP multimedia applications. ARP is used to match IP and MAC addresses in IPv4 networks, and NDP is used to discover neighbours in IPv6 networks. ARP and NDP packets are forwarded to all devices that are connected on a single link. Spammers can use the cache poisoning method to modify contents in the ARP cache or NDP cache by packet interception.

For example, a spammer can disguise himself as a gateway by using ARP cache poisoning to intercept all packets on the same link. Thus, if the user starts a connection, the spammer can insert a prepared RTP spam in the ongoing session. Spammers can change the target's identifier. If a user's identifier is changed, the user may try to establish another connection with another party who has the identifier addressed by the spammer, but is not the original party. Through this attack, spammers can send spam to the user who requests the connection.

9.1.8 Routing control

Assuming that communication for IP multimedia applications is ongoing between the routers and users, a spammer can play a routing role in the communication within a network via hacking. If a user tries to establish connections with other users belonging to a specific network, the spammer responds to the request by disguising himself as a valid user and sends spam to the user who requested the connection.

9.1.9 Vulnerable management system

There can be other threats which use the vulnerabilities of the service management system. In case of this threat, spammers can modify valid user's registration information and send spam with valid user's qualification.

9.2 Classification of spam security threats

The above-mentioned spam security threats can be classified by attack technique. The classified spam security threats are shown in Table 9-1.

Table 9-1 – Spam security threats classified by attack technique

Attack techniques	Spam security threats
Malicious code/remote control	Spam Bot
Session hijacking	Session hijacking
SQL injection	SQL injection
Sniffing	Registration information sniffing
Spoofing	Sender spoofing, cache poisoning, routing control
Others	Identifier collection, vulnerable management system

Malicious code/remote control is a technique that enables a large quantity of spam to be forwarded easily. Spammers can spread malicious codes through various ways and control the infected devices to send spam. Spam bots are one example.

Session hijacking is a hacking technique that steals someone's session. Generally, it can be done by merely guessing the session ID and by using the session ID cookie. Spammers can eavesdrop on the connection between a server and a user without authentication procedures or with server authority.

SQL injection is a hacking skill that exploits a vulnerability of databases. This can change the normal SQL query and can pass the authentication process, unlawfully. Usually, this method is used in website hacking to steal user information.

Sniffing is a technique in which a hacker eavesdrops on the packets exchanged between two or more users.

Spoofing is a technique in which a person disguises as another person. This can trick the other party's machine into believing that the spammer is another trustworthy person.

9.3 Countermeasures

There are three countermeasures to solve the above-mentioned spam problem: authentication, authorization, and security management. Security management means the countermeasure that can be applied to suitable security configuration by installing a security patch in systems built to maintain, repair, and enhance user awareness about security. There are various countermeasures such as flow control, encryption, etc., that can be dealt with. This clause looks at the three main countermeasures.

Relationships between countermeasures and spam security threats are summarized as in Table 9-2.

Table 9-2 – Relationship between countermeasure and multimedia communication spam security threats

Countermeasures Threats	Authentication	Authorization	Security management
Identifier collection			X
Sender spoofing	X		
Registration information sniffing	X		
Session hijacking	X		
SQL injection		X	X
Spam Bot			X
Cache poisoning	X		
Routing control	X		
Vulnerable management system		X	X

Authentication can solve many spam security threats by resolving spoofing problems. Spoofing is used in various threats such as sender spoofing, registration information sniffing, session hijacking, cache poisoning, and routing control. For sender spoofing, each sender is authenticated through authentication after the message is received. For registration information sniffing attacks, an unauthenticated user is prohibited from modifying registration information through authentication. For session hijacking and cache poisoning attacks, authenticated users can join in the connections. For routing control, only the authenticated user can control the router.

However, the spam security threats to SQL injection cannot be solved by authentication. Accordingly, it is required to establish authorization policy in such cases. Vulnerable management systems can also belong to this case. A system manager should give different access authorities to users according to user accounts.

Finally, some of the spam security threats require careful security management. Identifier collection, SQL injection, spam bot and vulnerable management systems belong to this case. Spammers can collect a user's identifier through many channels and send spam. Hence, careful identifier management is required. System developers should take this into account during development of systems, because SQL injection threats are sometimes caused by faulty code. Spam bot is caused by malicious bot infection. Therefore, computer users should be careful in downloading files or accessing websites, and protecting their OS. In the vulnerable management system, system managers should be careful of managing their systems.

10 Applicability of well-known countering spam mechanisms for IP multimedia applications

There have been many studies on various mechanisms to counter conventional e-mail spam. Some of the solutions for e-mail spam can also be used for countering IP multimedia spam. Before dealing with the solution space for IP multimedia spam, it is necessary to analyse the conventional spam countering mechanisms and discuss their applicability to countering IP multimedia spam. Hence, this clause will discuss some of the well-known spam countering mechanisms with respect to their applicability in countering IP multimedia spam.

10.1 Identification filtering

10.1.1 Black list

A black list denotes a list of identification (for example, e-mail address for e-mail) that is suspicious or identified as spammers. The mechanism of a black list is to filter messages or calls originated from senders in the list. Identification can be lists of IP addresses, domain names, caller identification or address, content of headers or body, or some combination of these different types, which might be used to help identify spam.

Using only a black list for countering spam may not be effective in IP-based applications. The spammer can use the identification of other innocent people and spoof the receiver. This problem can be resolved with authentication mechanisms based on the source address. Another problem of this method is that the user can create new identifications very easily. Various IP multimedia applications made for telecommunication use e-mail addresses. The e-mail address can easily be created through various well-known portal sites. An average non-spamming subscriber mostly uses these addresses made from the well-known portal sites; thus, the domain name of the portal sites cannot be black listed. In order to solve this problem, portal service providers must add some complexity in creating new addresses. If considerable time and effort are required in creating the new address, the spammer will eventually use some other method to create new addresses for spamming. These new addresses will be more likely filtered through domain black listing. Therefore, the black listing method becomes effective when used with other methods.

The black list method is applied only once at the start of the communication when an identification of the source is encountered for the first time. Thus, it is possible to use the black list method for any type of IP multimedia application that uses identification, such as source address. This method can be used for website applications, since it is possible to apply the black list method by granting posting rights only to non-spammers, i.e., a user not in the black list. Thus, the black list method can be used to block out any types of IP multimedia spam that uses any type of identification for real-time and non real-time application.

10.1.2 White list

A white list is the opposite of a black list. This list contains trusted user information. E-mails originated from senders in the white list will be always accepted. Unlike a black list, massive creation of e-mail addresses to change one's identity would not help to get through the white list, but it is still exposed to address spoofing. Spam with address spoofing can be easily filtered by using strong authentication methods.

Although the white list method can filter almost all of the spam, a normal person would need to communicate with other people not in the white list. If a sender who is not in the white list needs to communicate with the user, some type of authorization method is needed in order to get into the user's white list. Users would have to validate the sender through identification or some introductory comments from the sender. The user can accept or deny the communication request. An accepted sender can get into the user's white list. If the users have to accept or deny every new request, it would be very annoying since most new requests are spam. Another problem with this approach is that the user has to configure the white list when the environment of the user changes which would be a waste of time and energy.

The concept of white lists is already included in the IM system which is known as the buddy list. The many IM systems allow only the users in the buddy list to communicate with a consent style capability for the new user to be accepted to join in the buddy list. Thus, with strong authentication mechanisms, it can be a useful method to counter IM spam. However, VoIP has a different feature from IM systems. Like e-mail systems, white lists can be helpful as a supplementary method with the use of other methods, as users have a tendency to still accept calls from unknown callers.

The white list method is used only at the start of the communication, thus it is appropriate for real-time or non real-time application. This method can be used for website applications, since it is possible to apply the white list method by granting posting rights only to users in the white list.

10.1.3 Reputation system

A reputation system is used in conjunction with a white or black list. If a sender who is not in the receiver's black list or white list wishes to communicate with the receiver, the reputation score is shown in the receiver's terminal. The reputation score helps the receiver in deciding whether he should accept or reject the call. If the user accepts the communication request and discovers that the sender is a spammer, he or she can report spamming to the reputation system and the sender identification is not added to the user's white list. The reports are accumulated in the reputation server and form a reputation score.

The problem of this method is that the spammer with a negative reputation score can change his identification and start spamming with a new identification. The new identification would not have a negative score and it will take some time for that user to be regarded as a spammer through accumulation of a negative score. Another problem with this approach is that some group of bad people can bully an innocent victim by threatening to give a negative reputation score. The innocent victim with negative reputation score will have difficulty in continuing his business through the IP-based networks.

Another type of reputation system is positive reputation system. The receiver gives a positive score for non-spammers. It would not be easy to spam with a new identification based on this method, since new identification would have a fairly low score. The problem with this method is that several spammers can get together and give positive scores to each another. However, spammers would need to form some sort of consortium in order to accomplish this, which would be very expensive. Therefore, a positive reputation system is more efficient than the negative reputation system.

In order to make the reputation system work, it needs a centralized and monolithic controlling telecommunication system. This method can work well with IM types of applications which are normally operated by one service provider. However, VoIP applications assume communication between various service providers. The reputation score may differ from various service providers, since there is no standardized definition. Therefore, this method is not appropriate for applications such as VoIP with no standardized description system.

The reputation system can also be used in applications that use some sort of identification of senders, since the reputation score can be given to the identification. If the sender has passed the reputation system, the sender will be added to the receiver's white list. Thus, this method can be used in any real-time or non real-time application.

This method can be used also for web-based applications by granting posting rights only to users who have exceeded a certain level of reputation score. The website can keep a reputation score for each member by keeping a score for the previous activities.

10.1.4 Circles of trust

In the circles of trust method, groups of trusted people or trusted domains get together and share their white lists. The methodology in this approach is that a person would trust a friend of a trusted friend. The group would form a trusted relationship, and they would also agree to enforce some type of penalty if one of the members is caught spamming.

A variant of circles of trust is a distributed black list approach in which a group of trusted people or group share their black lists. This approach is very effective in filtering out abusive spam. There are many servers that collect the black lists based on this approach and open the collected black list to the public for use.

This type of method works well with a small group or small sets of providers where sharing and enforcing such a policy is feasible. If the size of the trusted circles increases, it would be impossible to come up with feasible consensus on reaching an appropriate level of penalty for spamming.

10.2 Address masking

Various IP multimedia applications need addresses to use their services. Therefore, it is important not to expose one's address to the public. But, when using web-based services, addresses should be exposed for the new customer to easily make contact with the owner. Spammers make use of this weakness for collecting spam target addresses. Spammers scan various web pages and collect addresses with "@" and "." structure. The collected address is used for spamming, and the collected addresses are also propagated to other spammers, since spammers tend to share target addresses.

Address masking is a method to hide one's address so that the spammer cannot automatically collect one's address. Most simple method is to change "@" to AT and "." to DOT. In this way, the address would look like a normal text, thus it could pass the automatic address screening system that is used by spammers.

Address masking is not a spam countering method, but a spam prevention method. This method prevents exposure of one's address from automated address collecting program that is used by spammers to collect addresses. Thus, this method is appropriate in preventing spam in the IP multimedia applications that use the same address with the web-based service.

This clause describes some other techniques that can be used in address masking.

10.2.1 Java script

In the JavaScript environment, it is easy to add "abc@xyz.com" type of address using Java functions. The web page would show an "abc@xyz.com" form, but when used with the document.write() function in JavaScript, it is very easy to hide the e-mail address. One example is shown below.

```
<SCRIPT TYPE="text/javascript">

  document.write('abc@' + 'xyz.com')

</SCRIPT>
```

It is possible to use other functions or methods in JavaScript to hide the e-mail address. The point here, however, is to describe that it is possible to hide addresses in the JavaScript environment. Thus, using JavaScript to hide addresses, a spammer would have difficulty in collecting an e-mail address with automatic methods, even though the webpage clearly shows a normal e-mail address.

This method can only be used in JavaScript environments. But, if the user wants to express his messenger ID or VoIP contact address in a web-page using JavaScript, this method can help to avoid becoming a target for spammers.

10.2.2 ASCII code

The ASCII code method is to hide important information in the form of ASCII code which is "&#number". The important information can be an e-mail address or a telephone number, which is a target of the spammer. The webpage would not be shown in a normal text, but in an image. Thus, when the webpage is downloaded, it would only show an ASCII code. If the spammer has ASCII code conversion function in its webpage search tool, the ASCII code can easily be decoded.

10.3 Human interactive proof

Each communicator gets a puzzle or challenge which is designed so that only a human can recognize it, but machines cannot. The puzzle or challenge is an image or sound of word or number in which only a person can understand, not a machine. It can be an image hidden behind various colours or a sound hidden behind various noises, which would be difficult for a machine to understand. Nowadays, it is more difficult to make puzzles that are not comprehensible by machines, due to the advancement in the areas of automatic image or sound processing and artificial intelligence.

Human interactive proof method is normally used in the web-based applications during a subscription stage of network services, thus it is very appropriate for countering web-based spam. This method can also be used in filtering call spam with authorization method using sounds. When a caller not in the black or white list starts a voice call, the receiver automatically activates the interactive voice response (IVR) system requesting the caller to enter a certain number in the phone keypad. If the caller enters the number correctly, the telephone number of the caller is automatically added to the user's white list. A chat user may go through the interactive proof method in order to join in the conversation.

10.4 Content filtering

Content filtering on the subject line is the most common and widely used method for countering spam in e-mail. It scans the subject line for suspicious words which are often used for spam.

IM involves communicating with short text messages, so this mechanism can easily apply for countering IM spam. The body contents of each IM could be scanned by the same technology as scanning the subject line of the e-mail.

However, this is not applicable to VoIP or other IP multimedia telecommunications which include audio and/or video at this moment. The media will be sent after the call set-up, so pre-filtering of the content does not give any benefits. On the other hand, although a spam has been delivered as a voice or video mail form which would be stored in a server, the current technology to scan certain words is not good enough to be used for countering spam.

10.5 Authentication by key exchange

Authentication has an ability to securely identify the sender of IP multimedia messages which helps in blocking out many spoofing attack types of spam.

10.5.1 PKI and PGP

It is possible to authenticate senders to block connection requests from spammers disguising as someone else, especially a person in the white list. Public key infrastructure (PKI) and pretty good privacy (PGP) are well-known authentication methods that use public key mechanisms. PKI uses a public key mechanism in which the sender can be authenticated through the public key that is certified by the certificate authority (CA). PGP uses a computer program that provides a signing function for authentication. In e-mail systems, these mechanisms are used for the encryption of the message and adding digital signatures. They are strong mechanisms to prevent spam.

Key exchange mechanisms are useful for almost every IP multimedia telecommunication system. They should be carefully applied on IP conference services, since the group key of a conference has a high risk of being stolen.

PKI and PGP methods can be used for almost any type of IP multimedia application, such as VoIP and IM. This method can also be used in web-based applications, which permits uploading of files or messages only by certified persons.

10.5.2 DKIM [b-IETF RFC 4871]

DomainKeys identified mail (DKIM) is a method that is developed by the IETF (Internet Engineering Task Force) that can be used in e-mail authentication. The e-mail server attaches a cryptographic signature to the mail to validate that the server has actually sent the pertinent e-mail. DKIM allows an organization to take responsibility for a message to be validated by the receiver. DKIM defines a domain-level digital signature authentication framework for e-mail through the use of public-key cryptography and key server technology. E-mail fraud can cause damage not only to the receiver, but also to the reputation of the major enterprise or organization. The use of the DKIM method can protect the enterprise or organization from such damages.

The use of DKIM can prevent fraudulent communications through VoIP or IM. The receiver can check with the server of the sender if the received message or call is actually from the claimed sender. The authentication process can be made at the beginning of the communications; thus, it would not affect even a critical real-time application.

10.5.3 HTTP authentication and TLS connection

The use of HTTP digest authentication [b-IETF RFC 5090] along with TLS (transport layer security) connection with the server is very effective for IP multimedia applications with a client-server structure. The server of the domain validates its users through HTTP digest authentication. The HTTP digest authentication is used to authenticate the user of the IP multimedia applications, usually through username and password. The client, which is the user, maintains a persistent TLS connection to the server. The client verifies the server identity by maintaining the TLS connection with the server. The server authenticates the client using digest exchange over the TLS connection. When an authenticated user sends a message to another domain, the sending domain certifies the user by inserting a signature to validate the message. The sending and receiving domains should form a mutual authentication to trust each other's users.

This method can be used to authenticate users communicating through IM or VoIP. The authentication process can be made at the beginning of the communications; thus, it would not affect even a critical real-time application.

10.6 Network-based spam filtering

The spam filtering mechanisms discussed above have been designed to work on the server side and the client side of the telecommunications. However, it is important to build secure networks to prevent spam. This clause briefly discusses some network-based spam filtering methods.

10.6.1 Packet rejection at the network entity

It is possible for some policy such as ACL (access control list) in a router or any network entity to discard packets suspected to be spam from a particular IP address source or IP prefix source. The source of a spammer can be inside the ISP network or outside the ISP network. The ISP who wants to protect its network from spam will need to solve both problems with different approaches.

If the source of spam is inside the ISP network, the ISP can set the network entity of the source to cut off the IP connectivity of the spam source. The spammer will realize that the network connectivity is lost and will be forced to admit his or her wrong doing. However, some criterion should be made in order to prevent misuse. A person can falsely accuse an innocent person of being a spammer by cutting him or her off of network connectivity. A deceitful person can use the IP address of an innocent person to send his spam, thereby cutting off the network connectivity of an innocent person and also carrying out spamming for a certain amount of time.

Let us assume that the ISP A network is connected to ISP B network, and spammer uses the ISP B network. If the source of a spam is outside the ISP A network, the ISP A must check if ISP B is willing to control the spam in its network. If ISP B does not have any policy in controlling the spam, the ISP A must set a policy for spam in the gateway of ISP B to prevent spam flooding into ISP A network. In this approach, ISP A cannot block the spammer from network connectivity, but it can protect its network from spam. This method can protect and save network resources. The downfall of this approach is that it can block an innocent user from ISP B from connecting to its network.

Another problem with this approach is that the spammer can change its IP address frequently. Thus, the ISP of the spammer side must control and authenticate the IP address used by the spammer to make this method work.

Packet rejection at the network entity method can be used in any application, since this approach is unrelated to IP multimedia applications.

10.6.2 Distributed black list

A distributed black list is a black list that resides in the network to be shared by the network community. Distributed black lists are usually implemented in the DNS. Users can add an address that was caught spamming to the distributed black list. Many sites will reject messages from an IP address after it appears in a distributed black list. The applicability of this method to IP multimedia applications is equivalent to the black list method.

10.6.3 Spam firewall

Corporate networks or ISP networks use spam firewalls to protect their networks from spam. A spam firewall uses many methodologies mentioned previously to block spam before it enters its network. The user in a protected network does not suffer much from spam. This method is a merging of the black list and content filtering methods, since it maintains the black list and filters content as the packets pass through the corporate network.

The spam firewall is currently used for e-mail and IM. This method may not be effective for VoIP services, since nothing can be captured at the start of the VoIP calls. This method can be used to filter web-based spam, since it is possible to filter by examining the content.

10.7 Online stamp

In the online stamp method, a sender not in the white list of the receiver would have to buy an on-line stamp to send a message. If a non-listed sender sends a message without an online stamp, it will be dumped by the server of the service provider. Only the non-listed message with an online stamp can appear in the receiver's terminal. If the receiver accepts the message, he will return the online stamp to the sender. The address of the sender is automatically added to receiver's white list. If the receiver decides that the sender is a spam, he can keep the money from the online stamp. The spammer would have to send a large volume of messages, thus increasing spamming expenses.

This method can equally be used in e-mail, VoIP, or IM services. Since the sender would need to buy an online stamp only once, this method is neither a cumbersome nor an expensive method. Therefore, it is efficient for countering spam when used with an appropriate sender identity authentication.

10.8 Authorization-based spam filtering

One important building block in filtering spam is to provide a mechanism to instruct some entities in the network to "filter" incoming connection requests according to the user or network policies. Various entities, such as users or system administrators, might create and modify authorization policies. A network policy is needed to define communication flows between domains.

Authorization policies can be applied at the end host and/or by network elements. The rule maker might be an end user that owns the device, a VoIP service provider, a person with a relationship to the end user (e.g., the parents of a child using a mobile phone). This clause is based on various authorization-based spam filtering mechanisms.

10.8.1 Consent-based communications

The consent-based communications is based on the direct authorization of the message by the receiver. It is used in conjunction with a white or black list. If a sender not in the black or white list attempts to communicate with the user, he sends his identification and/or any short text to the user to identify himself. The sender is initially rejected. The user is then informed that the caller is attempting to communicate. The user may accept or reject the sender by examining the identification and/or the short text sent by the sender.

This type of filtering approach is currently used in various IM services. It has been very effective in managing the white list. This approach is feasible in dealing with the call spam by acquiring consent at the outset, but not appropriate for web-based spam, which is a unidirectional service. It may not be appropriate for services involving multiple users, since it would be inefficient to acquire consent from all of the participants in the ongoing services.

The problem with this approach is that the user can be bothered by too many consent requests. Thus, some of the consent requests should be filtered by another filtering system.

10.8.2 User-policy based authorization

In user-policy based authorization, an IP multimedia user defines an acceptance policy to filter a request from an unknown sender. Policy is set to the user terminal or the application server in order to accept or deny a request automatically. The policy can be applied to the spam source address, identification, and/or short text sent by the sender as in the consent-based communication method. Policy may also be applied to the received content of image, sound, or text to automatically filter the policy-violating communication request. The information of the rejected requests should be logged in a repository, so that the user can go back and check for requests that should not have been declined. The user can modify the policy to fulfil one's needs.

The problem of the consent-based method is that the user would have to respond to all communication requests. In the policy-based authorization method, however, most spam is automatically filtered so that the user would not be bothered by the problem of too many consent requests. The creation of policy would depend on the characteristics of the IP multimedia applications used. The user-policy based filtering method should be defined for all spam-vulnerable applications.

This approach has been very effective in managing white lists. This method is a user-based approach; thus, it can be used in any type of bidirectional service, such as VoIP and IM service.

10.8.3 Network-policy based authorization

The network operator should use network-policy based authorization on filtering spam to protect the network. The network policy can be used in a single network or between the neighbouring networks. This method is equivalent to packet rejection at the network entity method.

In order to provide scalable spam filtering, network operator may outsource part of the administration rights to skilful end users and enable them to configure network policy on their links to the provider network. Necessary authentication may be implemented in the service router to validate a user's identity and administration rights. Only valid users are authorized to provision corresponding network policies as they are granted.

10.9 Legal action and regulations

To prevent spam, it is important to set related regulations and law to prohibit spam, although there is a debate about the efficiency of this part. Many countries have set laws for the victim to take legal action against annoying spam. In most cases, the advertiser must insert a special set of contents in which the receivers can recognize spam as advertisements, and get penalized when the rule is violated.

The problem with this method is that there are some difficulties in enforcing local anti-spam laws to spam originating from foreign countries. Some international agreement must be created across many countries to truly make this method effective. International organizations including ITU-T, OECD, APEC, etc., are making efforts to define effective anti-spam legislation, international cooperation and enforcements.

This method is not a technical method and is unrelated to the characteristics of IP multimedia applications.

11 Considerations in countering IP multimedia application spam

Using IP-based networks for advertisement is not only economical, but very effective. Spam is a problem that occurs with the misuse of advertisement. Serious social problems can occur due to spam. Such problems include the volume of advertisement, fraud, enticement that causes harassment and damage to the network users.

Various IP multimedia application spam countering methods have been introduced in this Recommendation. IP multimedia applications have various characteristics; thus, their pertinent spam can also have various features. Using only one or two methods would not counter all types of IP multimedia spam. Detailed research on various types of spam relevant to the various multimedia application entities should be conducted to actually solve, or at least alleviate, the spam problem. Therefore, spam countering methods should be analysed in accordance with the characteristics of the IP multimedia applications. This clause attempts to show some points to be considered in countering IP multimedia application spam.

In order to effectively counter IP multimedia application spam, different approaches in various aspects of the service participating groups should be considered. These are service user (and/or service subscriber), service providers, network operator, public organization, and advertisers. Thus, this clause describes some points to be considered to counter IP multimedia application spam with regard to each aspect.

11.1 Service user (service subscriber)

The service user and/or the service subscribers are the actual victims of spam and should feel the importance of blocking spam to protect one's rights. These are some of the points that a service user should consider in countering spam, although application of these suggestions may vary based on the medium.

- Users should acquire spam filtering engines and keep the spam filtering engines up to date to block unwanted spam. New spam can always appear, so the filtering engine should be updated to control new spam.
- Users should subscribe to various spam filters, such as black list, white list, etc., and continuously make updates to the filter lists.
- When encountering spam, users should make an immediate elimination, and inform the public of this problem to prevent an identical victim.
- Users should participate in spam prevention training to learn of new spam and new countering techniques. New types of spam can occur in conventional services along with the new services. Although, it is not necessary to use every countering technique, one should try to find an adequate solution in order to control spam.
- Users should be cautious in protecting one's personal information from being exposed to spammers. Users should not use easy to remember or easy to guess types of identification or numbers.
- Users should use prevention techniques to block communication requests from spammers and configure one's system to make it difficult for the spammer to communicate.

11.2 Service provider

Service providers can have a high profit by providing quality service. Spam can cause serious damage to the service, with spammers misusing and abusing the service. The service providers should be aware of the problem of spam in order to protect their network and to provide better services. These are some of the points that service providers may consider in countering spam.

- Before launching a new IP multimedia service, service provider could perform an analysis on the possibilities of new IP multimedia services or applications being a target for potential spam. Every IP multimedia service is not a target for spammers. Carrying out spam analysis and finding solutions to make spamming difficult can increase the possibilities of success to new services. If a spam susceptible service is deployed without this process, it would be very difficult to control spam and the users would neglect the new services after being victimized by spam.
- Service providers could check all the entities such as user, network, service components, etc., that constitute the IP multimedia service or application and analyse various spamming methods in each entity, in order to find more simple and effective solutions to counter spam. It is possible to use spam countering techniques only within the IP multimedia service, but better solutions can exist when the network entities are perceived altogether.
- Service providers could perform persistent research on the emergence of new spam in conventional applications. New types of spam can occur even in the oldest services. Service providers might want to observe this phenomenon and try to find solutions to handle new types of spam, even to old services.
- Service providers could make use of various filters, such as black lists and white lists to control users from accessing the services. The best is to prevent the spammer from using the service, since the spammer would only abuse the service.
- If the service contains a subscription process, service providers could make the subscription difficult enough to keep spammers from joining the service. Many spammers use automated methods or hire cheap employees to make many subscriptions which is very effective for spamming. The subscription process could contain strong authentication methods to verify the subscriber and have some scheme for preventing multiple subscriptions by one user and for preventing spammers from joining the service.
- If the service maintains a list of service users, the service provider could have a method to evaluate the credibility of a service user to ensure that the user does not abuse the service or other service users. The service provider should have a protection technique to prevent the exposure of the subscriber's personal information by internal and external users.
- If the service maintains a repository, the service provider may want to monitor that the content in the website should be monitored to remove web spam. Content analysis can be made even to video and audio data to find inappropriate contents.
- Service providers might choose to have a method for the service user to control spam. It can be a filtering engine, filter list, policy configuration tools, spam countering manuals or anything that the user can use for countering spam.

11.3 Network operator

Spam can cause waste to network resources, especially if spam contains multimedia content. Network operators should attempt to block spam to protect the network and to provide efficient network services. These are some of the points that network operators should consider in countering spam.

- Network operators could monitor the network traffic to find abnormal traffic which can be considered as spam. The network operator should be able to analyse the abnormal traffic and perform an appropriate action. It would not be easy to capture spam by analysing the network traffic. Nevertheless, various malicious spam or programs tend to show abnormal traffic patterns.
- Network operators could limit spammer traffic or perform any other task to stop spamming.

- Network operators can cooperate with the service provider by sharing information related to spam. The network operator can actually stop spamming traffic, which can make spamming useless.
- Network operators could make use of the various spam firewalls that protect the network.
- Networks could be configured only with trusted networks, so that only the users who are authenticated and authorized by the trusted network could communicate. If the networks have such trusted relationships, it is possible for the network to control the traffic and users. Eventually, the entire network can be secure from spam and other malicious traffic when all subnetworks trust traffic from their peer subnetworks.

11.4 Public organization

A public organization can be a governmental organization or a private organization consisting of interest groups that work in controlling spam. The private organization can be a for-profit or a non-profit organization which has an effective solution in controlling spam. These are some of the points that public organizations may want to consider in countering spam.

- Public organizations could have a system for the victim to submit a report on damage due to spam. The organization may warn or penalize the spammer. This organization may be a governmental organization or any strong private organization that has the power to effectively warn the spammer.
- Public organizations might choose to have a program to train or provide some guidelines to IP multimedia service users, IP multimedia service providers, and IP network operators in countering spam. Spam countering skills requires extensive experience in which the new IP multimedia service provider or network operator may not be prepared.
- Public organizations may provide black lists or filters that can be shared by the public. The public can participate in constructing the black lists or filters.
- An advertisement approval system that is a non-forgeable and authenticated that the advertisement agency can use without being misconceived as a spammer would help advertising agencies.

11.5 Other considerations

Other considerations which are unrelated to those mentioned above are as follows.

- The problem of spam would probably not disappear, regardless of the various efforts being researched to counter spam. New spam will always appear, and new studies should be made to counter these problems. But if research on spam countering method is made beforehand, better application environments can be made for better application services.
- Various spam countering methods should be used together. There is no a super solution yet that can solve the spam problem. Various methods should be used together to counter various types of spam that can occur in various locations with various techniques.
- The optimal solution could be to make spamming difficult and expensive. The ultimate objective of a spammer is to use a cheap and easy method for advertisement. The spammer would stop spamming eventually, if spamming is difficult and expensive, or if the penalty for spamming is too strong.

Bibliography

[b-ITU-T Q.814] Recommendation ITU-T Q.814 (2000), *Specification of an electronic data interchange interactive agent*.

[b-ITU-T T.124] Recommendation ITU-T T.124 (1998), *Generic Conference Control*.

[b-ITU-T T.180] Recommendation ITU-T T.180 (1998), *Homogeneous access mechanism to communication services*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.741] Recommendation ITU-T X.741 (1995) | ISO/IEC 10164-9:1995, *Information technology – Open Systems Interconnection – Systems management: Objects and attributes for access control*.

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats*. <http://www.ietf.org/rfc/rfc1991.txt?number=1991>

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*. <http://www.ietf.org/rfc/rfc3428.txt?number=3428>

[b-IETF RFC 4871] IETF RFC 4871 (2007), *DomainKeys Identified Mail (DKIM) Signatures*. <http://www.ietf.org/rfc/rfc4871.txt?number=4871>

[b-IETF RFC 4880] IETF RFC 4880 (2007), *OpenPGP Message Format*. <http://www.ietf.org/rfc/rfc4880.txt?number=4880>

[b-IETF RFC 4981] IETF RFC 4981 (2007), *Survey of Research towards Robust Peer-to-Peer Networks: Search Methods*. <http://www.ietf.org/rfc/rfc4981.txt?number=4981>

[b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam*. <http://www.ietf.org/rfc/rfc5039.txt?number=5039>

[b-IETF RFC 5090] IETF RFC 5090 (2008), *RADIUS Extension for Digest Authentication*. <http://www.ietf.org/rfc/rfc5090.txt?number=5090>

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