

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

X.1244

(09/2008)

X系列：数据网、开放系统通信和安全性
电信安全

打击IP多媒体应用中垃圾信息的概述

ITU-T X.1244建议书

ITU-T X 系列建议书
数据网、开放系统通信和安全性

公用数据网	
业务和设施	X.1-X.19
接口	X.20-X.49
传输、信令和交换	X.50-X.89
网络概貌	X.90-X.149
维护	X.150-X.179
管理安排	X.180-X.199
开放系统互连	
模型和记法	X.200-X.209
服务限定	X.210-X.219
连接式协议规范	X.220-X.229
无连接式协议规范	X.230-X.239
PICS书写形式	X.240-X.259
协议标识	X.260-X.269
安全协议	X.270-X.279
层管理对象	X.280-X.289
一致性测试	X.290-X.299
网间互通	
概述	X.300-X.349
卫星数据传输系统	X.350-X.369
以IP为基础的网络	X.370-X.379
报文处理系统	X.400-X.499
号码簿	X.500-X.599
OSI 组网和系统概貌	
组网	X.600-X.629
效率	X.630-X.639
业务质量	X.640-X.649
命名、寻址和登记	X.650-X.679
抽象句法记法1(ASN.1)	X.680-X.699
OSI 管理	
系统管理协议子集和结构	X.700-X.709
管理通信服务和协议	X.710-X.719
管理信息的结构	X.720-X.729
管理功能	X.730-X.799
安全	X.800-X.849
OSI 应用	
托付、并发和恢复	X.850-X.859
事务处理	X.860-X.879
远程操作	X.880-X.889
ASN.1的一般应用	X.890-X.899
开放分布式处理	X.900-X.999
电信安全	X.1000-

欲了解更详细信息，请查阅 *ITU-T* 建议书目录。

ITU-T X.1244建议书

IP多媒体应用垃圾信息的概述

摘要

ITU-T X.1244规定了有关打击IP电话、即时消息等IP多媒体应用中垃圾信息的基本概念、特性和技术问题。本文对各种IP多媒体应用进行了分类并按特性对每类进行描述。本建议书阐述了可造成IP多媒体应用中垃圾信息的各种安全隐患。控制已成为社会问题垃圾电子邮件的技术五花八门。一些技术可用来打击IP多媒体应用垃圾信息。本建议书分析了传统的打击垃圾信息机制并探讨了这些机制对于打击多媒体应用垃圾信息的适用性。本文最后提出了打击IP多媒体应用垃圾信息应考虑的各种问题。

来源

ITU-T第17研究组（2005-2008年）按照世界电信标准化全会（WTSA）第1号决议规定的程序，于2008年9月19日批准了ITU-T X.1244建议书。

关键词

即时消息垃圾信息、IP多媒体应用垃圾信息、垃圾信息、IP话音垃圾信息。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准ITU-T建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2009

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

1	范围	1
2	参考文献	1
3	定义	1
3.1	在其他文献中规定的术语	1
3.2	在本建议书中规定的术语	2
4	缩写词和首字母缩略语	3
5	惯例	4
6	多媒体垃圾信息的概念和典型类型	4
6.1	VoIP垃圾信息.....	4
6.2	IP 多媒体消息垃圾信息.....	5
6.3	即时消息垃圾信息	5
6.4	聊天垃圾信息	5
6.5	多模垃圾信息	6
6.6	基于P2P的文件共享业务的垃圾信息.....	6
6.7	网站垃圾信息	6
7	IP多媒体垃圾信息的分类.....	6
7.1	实时语音垃圾信息	7
7.2	实时文本垃圾信息	8
7.3	实时视频垃圾信息	8
7.4	非实时语音垃圾信息	8
7.5	非实时文本垃圾信息	9
7.6	非实时视频垃圾信息	9
8	关于阻止IP多媒体垃圾信息的技术问题.....	9
8.1	垃圾信息的创建和发送	10
8.2	垃圾信息的检测和过滤	11
8.3	对所接收的垃圾信息采取的行动	12
9	与垃圾信息相关的安全威胁	12
9.1	与垃圾信息相关的安全威胁	12
9.2	垃圾信息安全威胁的分类	14
9.3	对策	14
10	共知的阻止垃圾信息机制对于IP 多媒体应用的适用性.....	15
10.1	识别过滤	15
10.2	地址掩蔽	18
10.3	人工交互验证	18
10.4	内容过滤	19
10.5	通过密钥交换的认证	19
10.6	基于网络的垃圾信息过滤	20

10.7	在线邮票	21
10.8	基于授权的垃圾信息过滤	21
10.9	法律法案和规则	22
11	关于阻止IP多媒体应用垃圾信息的考虑	23
11.1	业务用户（业务订户）	23
11.2	服务提供商	23
11.3	网络运营商	24
11.4	公众组织	25
11.5	其他需要考虑的事项	25
	参考资料	26

引言

对于网络电子邮件系统，垃圾信息已经成为了一个社会问题。已经在开发各种解决方案试图解决此问题，但至今仍未真正解决垃圾信息问题。IP 多媒体应用包括各种业务类型，如 IP 电话、即时消息等等。这些 IP 多媒体业务正在成为垃圾信息的制造者的新的攻击目标，因为这是一种操作简单、成本低廉的传播垃圾信息的手段。IP 多媒体应用的垃圾信息在其成为公共社会问题之前一定要解决。

本建议书描述了可能出现在 IP 多媒体应用中的不同类型垃圾信息的基本概念、特性。讨论了关于阻止 IP 多媒体应用垃圾信息方面在技术上和安全角度的各种观点，因而，通过提供 IP 多媒体业务的各方，如服务提供商、业务用户等等在阻止 IP 多媒体应用垃圾信息的问题上提出各方的考虑。

打击IP多媒体应用中垃圾信息的概述

1 范围

本建议书提供了 IP 多媒体垃圾信息的概述，关注于以下几方面的问题：

- 定义IP多媒体垃圾信息的概念和特性
- 确定关于IP多媒体垃圾信息的技术问题
- 垃圾信息的安全威胁
- 打击垃圾信息的方法及其对打击IP多媒体垃圾信息的适用性
- 打击IP多媒体应用垃圾信息应考虑各个方面

注 - 本建议书中“身份”一词不具备其绝对含义，在实际应用中它不能形成任何肯定确认。

2 参考文献

无。

3 定义

3.1 在其他文献中规定的术语

本建议书使用以下在其它文献中规定的术语：

3.1.1 Access Control List (ACL) [b-ITU-T X.741] 访问控制表：访问控制表属性用以包含启动者身份，即为或者明确被允许访问的管理信息，或者明确被拒绝访问的管理信息。

3.1.2 Certification Authority (CA) [b-ITU-T X.509] 认证机构：由一个或多个用户信任的创建并指配公开密钥的机构。认证机构可任意创建用户的密钥。

3.1.3 Conference [b-ITU-T T.124] 会议：许多结合在一起并能够通过不同的电信网络交换声波图和视听信息的节点。

3.1.4 Domain Keys Identified Mail (DKIM) [b-IETF RFC 4871] 域密钥识别邮件：一种机制，据此电子邮件消息可以按密码加符号，允许一个有符号的域申明负责将消息引入邮件流中。消息接收方验证符号的方法是，直接通过询问符号的域找回适用的公开密钥，因此通过拥有加符号域的专用密钥的一方确认消息无误。

3.1.5 Instant Messaging (IM) [b-IETF RFC 3428] 即时消息发送：在一组参与者之间近实时地交换内容。通常该内容为文本短消息，虽然不是必需如此。

3.1.6 Peer-to-peer (P2P) relationship [b-ITU-T T.180] 对等关系：在对等关系中，用户可以对其互通的特性进行协商并按照协商达成的规则通信：用户双方（一个实体和其对等实体）潜在地具有同等的权限。[b-IETF RFC 4981] 指示，P2P 网络显示出 3 个特性：自组织、对称通信和分布式控制。

3.1.7 Pretty Good Privacy (PGP) [b-IETF RFC 1991] 最优保密: PGP 采用公开密钥与常规加密相结合的方式为电子邮件消息和数据文件提供安全服务。这些服务包括机密性和数字签名。PGP 由 Philip Zimmermann 创立，并在 1991 年首先发行第 1.0 版。随后的各版本例如，在 [b-IETF RFC 4880] 中表述的开放 PGP 根据 Philip Zimmermann 的设计导则，已经通过所有志愿人员的努力被设计并执行。PGP 和 Pretty 最优保密为 Philip Zimmermann 的商标。

3.1.8 Public Key Infrastructure (PKI) [b-ITU-T X.509] 公共密钥基础设施: 能够支持公共密钥管理的基础设施可以支持认证、加密、完整性或非否认业务。

3.1.9 Transport Layer Security (TLS) [b-ITU-T Q.814] 传送层安全: TLS 协议任选地提供通信保密。该协议允许客户/服务器应用以防止窃听、削减和侵扰的设计方式进行通信。TLS 协议也提供很强的对等认证和数据流完整性。

3.2 在本建议书中规定的术语

本建议书规定以下术语：

3.2.1 Bait Spam 诱饵垃圾信息: 该名称由钓鱼术语类推得出（phishing 见第 3.2.10 段）。诱饵垃圾信息多种多样，其中包括引诱用户的内容，如电子邮件主题或嵌入式链路。受到诱惑的用户遭受诱饵垃圾信息的攻击。

3.2.2 Blog 博客: “网络日志”的收缩版。博客可能是一种在线多媒体列举了所有者个人兴趣，可被普通公众阅读、观赏甚至改进。

3.2.3 Bot 机器人: Bot 是机器人的缩写，它是用户代理运行的程序或另一种模拟人类行为的程序。

3.2.4 DNS Cache Poisoning DNS 高速缓冲存储器中毒: DNS 高速缓冲存储器中毒是一种技术，欺骗一个域名服务器（DNS 服务器）相信某服务器的 DNS 地址已经改变，而实际上其并未变化。DNS 服务器一旦中毒，此信息通常隐蔽一段时间，扩散对服务器用户攻击的影响。

3.2.5 IP Multimedia message IP 多媒体消息: IP 多媒体终端服务器中存储并传送的一种文本、音频或视频消息，接收方再行检查。这类类似于电话业务中的语音邮件不同在于在 IP 多媒体业务中提供服务。

3.2.6 IP Multimedia spam IP 多媒体垃圾信息: 在 IP 多媒体应用中未经请求就提供的消息或呼叫。为与传统的邮件垃圾信息区别开来，IP 多媒体垃圾信息表示在新出现的 IP 通信方式上的垃圾信息，如即时消息（IM）、临场、或通过 IP 的视频（VoIP）。

3.2.7 Modality 形式: 一般情况下，该术语指有关正规通信的形式、协议或条件。它指信息编码，包含为人类可感知的信息。例如，形式信息包括人机接口中使用的文本的、图形的、音频的、视频的或触觉的数据。多模信息可以来源于或目标是多模设备，例如人机接口（用于声音输入的麦克风、触觉输入的笔、文本输入的键盘、运动输入的鼠标、合成声音输出的扬声器、图形/文本输出的屏幕、用于触觉反馈的振动设备或用于视觉残疾人的盲文书写设备）。

3.2.8 Multimodal message 多模消息: 即为一种多媒体消息，包含通过多种形式交互作用而不同编码的信息。例如，MMS（多媒体消息传送业务）消息可传输文本、图形和音频形式。互联网网页也可包括多媒体形式内容如文本和视频。同样一个邮件可以包括连同文本的图形附件。多种模式可使用户根据环境、方便程序或内容选择一种最佳形式。

3.2.9 Online game 在线游戏：通过网络玩的实时游戏。

3.2.10 Phishing 网络钓鱼：在电子通信中，通过伪装成可信实体，违法并欺诈性地企图获得敏感信息，如用户名、密码和财务账号详细资料的行为。

3.2.11 Session hijacking 会话入侵：一种偷窃有效用户会话以获得未经授权就访问信息或服务的装置。

3.2.12 Spam over Instant Messaging 即时消息上的垃圾信息（SPIM）：目标是即时消息业务用户的垃圾信息。

3.2.13 Spam over Internet Telephony 互联网电话上的垃圾信息（SPIT）：目标是互联网电话业务用户的垃圾信息。

3.2.14 Spammer 垃圾信息散播者：垃圾信息的散播者。

3.2.15 Spamming 垃圾信息散播：发送垃圾信息的动作链，如收集目标名单、创建垃圾信息、传播垃圾信息等等。

3.2.16 Spammer：SPIM 的散播者。

3.2.17 Spitter：SPIT 的散播者。

3.2.18 User Created Contents (UCC) 用户创建的内容：可以是任何形式的内容，如视频、博客、图像、音频等等，由终端用户创建（通常公开）可被普通公众获得。

3.2.19 User Generated Contents 用户产生的内容（UGC）：等于 UCC。

3.2.20 Vishing：通过 IP 语音（VoIP）业务非法访问个人保密及财务信息的行为。Vishing 为“音频（Voice）”和“网络钓鱼（Phishing）”的组合。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

ACL	访问控制表
APEC	亚太经济合作组织
ARP	地址解决方案协议
ASCII	美国信息互换标准码
CA	证书机构
DB	数据库
DKIM	域密钥识别邮件
HTTP	超文本发送协议
IM	即时消息
IP	网际协议
IPTV	网际协议电视
IPv4	网际协议版本 4
IPv6	网际协议版本 6
IRC	互联网转接聊天
ISP	互联网服务提供商

ITSP	互联网电话服务提供商
IVR	交互式语音响应
MAC	媒体访问控制
MIPv4	移动 IPv4
MIPv6	移动 IPv6
NDP	邻近发现协议
OS	操作系统
P2P	对等
PGP	最优保密
PKI	公开密钥基础设施
PSTN	公共电话交换网
RTP	实时传送协议
SMS	短消息业务
SMTP	简单邮件发送协议
SQL	构成询问语言
TCP	传输控制协议
TLS	传送层安全
URI	统一来源标识符
URL	统一来源定位器
VoD	视频点播
VoIP	IP 上的视频

5 惯例

无。

6 多媒体垃圾信息的概念和典型类型

虽然对垃圾信息没有全球公认的定义，但该术语通常用于描述：以销售商业产品或服务为目的，通过发送电子邮件或移动消息的方式未经请求提供的大批电子信息。当前，垃圾信息已不限于电子邮件或移动消息。它也扩散到了IP 多媒体应用中，如VoIP 和即时消息。IP 多媒体垃圾信息可定义为：以销售商业产品或服务为目的，通过IP 多媒体应用方式未经请求提供的大批电子信息。IP 多媒体应用垃圾信息可能出现在各类IP 多媒体应用中，如VoIP和即时消息。

本节列举了几种典型的出现在 IP 多媒体应用中的 IP 多媒体垃圾信息。对每种类型的垃圾信息就其特性进行了描述。

6.1 VoIP垃圾信息

VoIP垃圾信息为出现在VoIP业务上的垃圾信息。VoIP垃圾信息是实时语音垃圾信息，如电话推销，包括与电话推销商的通信以及与IVR（交互式语音响应）系统的互动。由于

VoIP业务在全球的迅速部署，使用VoIP业务的电话推销服务日益增加，VoIP垃圾信息的威胁也随之加大，特别是大量群发也不困难。使用其他国家的比目标国家更廉价的劳动力作为电话推销商也是可能的，因为采用VoIP业务的国际电话的价格显著下降。垃圾信息发布者收集目标IP多媒体应用用户的信息也非常容易。综上所述，VoIP垃圾信息可能对VoIP服务提供商和用户造成严重的威胁。

6.2 IP多媒体消息垃圾信息

IP多媒体消息是文本、语音或视频消息，在IP多媒体终端或服务器中存储并传送，接收方再进行检查。这类似于电话业务中的语音邮件，不同在于在IP多媒体业务中提供服务。IP多媒体消息垃圾信息是采用IP多媒体消息业务的垃圾信息。垃圾信息接收方检查消息并删除垃圾信息，与电子邮件垃圾信息或移动消息垃圾信息一样。IP多媒体应用的许多终端，如VoIP电话支持多媒体消息发送功能，因此成为发送IP多媒体消息垃圾信息的目标应用。

多媒体消息垃圾信息分为文本消息垃圾信息和语音/视频消息垃圾信息。文本消息垃圾信息是一种短消息，包括商业或其诱惑性案文。由于其具有的文本格式，其特性也类似于电子邮件垃圾信息或移动SMS垃圾信息。然而，预计文本消息垃圾信息的成本应远远低于移动SMS垃圾信息。语音/视频消息垃圾信息是语音/视频形式的消息，包括商业或诱惑性内容。预计随着IP多媒体的应用此类垃圾信息会广泛传播。语音/视频消息将占用IP应用用户的语音/视频邮箱或IP服务提供商存储量的很大容量。因为多媒体消息比文本消息垃圾信息大很多。恶意多媒体消息垃圾信息发布者还可能用它传送有害软件，如蠕虫、计算机病毒、间谍软件、木马等。

6.3 即时消息垃圾信息

即时消息上的垃圾信息，即SPIM是另一种危险的IP多媒体应用垃圾信息，它的目标是即时消息业务用户。许多用户与其他网络用户通信时采用IM业务。大部分的IM垃圾信息是基于文本的短消息，许多性能与电子邮件垃圾信息是相同的，但IM垃圾信息是实时消息并更加令人讨厌。多媒体消息垃圾信息也可能出现在IM上，因为IM业务支持除实时文本消息传递以外的许多功能。

不通过违法的技术操作发送IM垃圾信息是很困难的。因为大部分IM业务采用“基于同意的伙伴名单”，只允许向伙伴名单中的用户发送消息。然而，IM业务脆弱的安全系统也可能允许垃圾信息散播者窃取伙伴名单或垃圾信息目标的白名单，伪装成伙伴名单中的伙伴成员来发送垃圾信息。

然而，只可能在伙伴名单中的用户间传递消息，但是，任何人都可以申请加入到伙伴名单中。在许多IM业务中，伙伴请求消息可以包括对请求者的介绍以帮助IM业务用户了解请求者并决定是否允许其加入到伙伴名单中。不在伙伴名单中的垃圾信息消息散播者可以采用IM业务的此项功能发送垃圾信息消息。

6.4 聊天垃圾信息

在各类提供业务用户间的聊天功能的IP多媒体应用中都会出现聊天垃圾信息。许多IP多媒体应用提供聊天功能和消息发送功能，如在线聊天业务、在线游戏业务等等。聊天垃圾信息通常为短文本消息格式，重复地向所有聊天参与者发送相同的消息。因此，某些在线

聊天业务和在线游戏业务限制相同消息重复发送的次数，以阻止垃圾信息消息的重复发送。然而，本方法的作用有限且需要更多的对策来阻止各种类型的聊天垃圾信息。

聊天业务与IM业务的性能相同。但是，可能出现在这些业务中的垃圾信息类型不同。IM业务的用户通常与伙伴名单中的伙伴通信，他已经通过IM业务用户的通信授权。因而，垃圾信息散播者进入伙伴名单以发送垃圾信息。聊天业务也出现在通信参与者通常互不相识的在线业务中。每个人都可以参与聊天业务，因此垃圾信息散播者可加入聊天业务中散播垃圾信息。在聊天业务中发现的垃圾信息的类型是重复地发送消息。因此与IM业务相比，在聊天业务中散播垃圾信息更简单一些。

6.5 多模垃圾信息

“垃圾信息散播”安全问题扩展到多模交互作用的情形，其中单个多媒体“垃圾信息”消息可能在随形式变化的用户接口上产生出多个目标。例如，一个“垃圾信息”网络消息可导致播放“垃圾信息”音频片断，播放“垃圾信息”视频片断和在屏幕上显示“垃圾信息”文本消息；这些可以是相同内容的或不同内容的。同样的，多模形式增加了多媒体“垃圾信息”的出现。因此，多模“垃圾信息”问题随着多模交互作用变得更加广泛会更加突出。

6.6 基于P2P的文件共享业务的垃圾信息

IP多媒体应用垃圾信息也可能出现在基于P2P的IP多媒体应用的目标用户中，如，P2P文件共享业务。采用P2P软件连接到IP网络的人们帮助用户使用对等通信，以彼此间共享各类计算机文件。在这些业务中，垃圾信息散播者通过采用流行电影或流行歌曲命名的垃圾信息，引诱用户下载垃圾信息文件。垃圾信息散播者不需要寻找垃圾信息目标。他们只需要共享垃圾信息文件以诱导其他P2P业务用户访问这些文件。许多下载的垃圾信息文件有可能被执行，因为垃圾信息接收者自愿地下载了这些文件。因此，当垃圾信息包含病毒软件，如非商业内容的蠕虫和病毒时，P2P业务上的垃圾信息的损害就可能很大。

6.7 网站垃圾信息

垃圾信息散播者可以在以各种目的运营的网站上发布商业内容的文章或文件。发布在公告栏上的垃圾信息可以被网站的众多访问者看到。例如，网站垃圾信息可以用许多商业内容回复门户网站的许多文章、以及博客上的商业文章也可以是网站垃圾信息。另外，在音频/视频共享网站上，垃圾信息散播者也可以在基于文本的文章中上载商业音频及视频文件，如UCC和UGC或公告栏以使其他业务用户看到商业视频文件。网站垃圾信息可以被大量网站业务用户阅读或观看。垃圾信息散播者也不需要针对垃圾信息的类型收集大量垃圾信息目标以发送该垃圾信息。

7 IP多媒体垃圾信息的分类

IP多媒体应用垃圾信息根据其特性被分为两组。IP多媒体应用垃圾信息可根据不同标准进行分类，如承载垃圾信息的IP多媒体应用的类型，垃圾信息散播中采用的媒体类型，业务提供所采用的协议，协议消息的类型等等。在本节中，IP多媒体垃圾信息按照下列IP多媒体应用特征进行分类，按照下列特征可以实施抵制垃圾信息技术。

- IP多媒体垃圾信息的实时或非实时性：IP多媒体应用可以以是否实时作为标准进行分类。
- IP多媒体垃圾信息的媒体类型：IP多媒体应用业务可以支持文本、语音、视频或综合体，视频包括静止图像及动漫。

在实时 IP 多媒体应用业务中，连接通信、传递消息，接收方实时地检查消息。实时 IP 多媒体应用的典型实例是 VoIP 业务和 IM 业务。在非实时 IP 多媒体应用业务中，接收方可以根据意愿检查消息。非实时 IP 多媒体应用的例子是万维网业务、P2P 业务、在线游戏业务等等。IP 多媒体应用垃圾信息的分类和典型示例介绍见表 7-1。

表 7-1 – IP 多媒体应用垃圾信息的分类

	文本	语音	视频
实时	<ul style="list-style-type: none"> • 即时消息垃圾信息 • 聊天垃圾信息 	<ul style="list-style-type: none"> • VoIP垃圾信息 • 即时消息垃圾信息 	<ul style="list-style-type: none"> • 即时消息垃圾信息
非实时	<ul style="list-style-type: none"> • 文本/多媒体消息垃圾信息 • P2P文件共享业务上的文本垃圾信息 • 互联网站上的文本垃圾信息 	<ul style="list-style-type: none"> • 语音/多媒体消息垃圾信息 • P2P文件共享业务上的语音垃圾信息 • 互联网站语音垃圾信息 	<ul style="list-style-type: none"> • 视频/多媒体消息垃圾信息 • P2P文件共享业务上的视频垃圾信息 • 互联网站视频垃圾信息

7.1 实时语音垃圾信息

实时语音垃圾信息定义为：以提供商业产品和服务的广告为目的，未经请求而主动进行的实时语音通信。实时语音垃圾信息的典型实例是 VoIP 垃圾信息。实时语音垃圾信息的发生频率低于电子邮件垃圾信息，但该垃圾信息对业务用户的损害更大。实时语音垃圾信息非常令垃圾信息接收方厌恶。在电子邮件业务中，业务用户可以按需要检查电子邮件，并在短时间内识别电子邮件垃圾信息，并相对轻松地删除垃圾信息。但是，实时语音垃圾信息更扰民，因为它要求垃圾信息接收方立即应答。而且，需要更多的时间来确认收到的消息为语音垃圾信息。相比较电子邮件垃圾信息和移动 SMS 垃圾信息，实时语音垃圾信息更为有效。通常，垃圾信息散播者追踪并说服垃圾信息接收方购买其产品或服务。在实时语音垃圾信息中，电话推销商以相比较电子邮件和 SMS 垃圾信息更具入侵性的互动通信方式说服垃圾信息接收方，后者只能发送基于非互动格式的短文本或视频的垃圾信息。随着垃圾信息说服力的提高，垃圾信息的危害也不断增加。因此，源自实时语音垃圾信息的损害随着大量的垃圾信息而日益严重。

采用除基本语音通信之外的 IP 增补业务的实时语音垃圾信息更增强了垃圾信息的功效。实时语音垃圾信息通常经由支持 VoIP 业务的终端传送至垃圾信息接收方。许多这种类型的终端支持许多附加功能，如多媒体消息、视频电话和与语音通信的显示共享（作为默认功能）。垃圾信息散播者可能将实时语音垃圾信息与附加视频或文本类型业务相结合来提高垃圾信息的效果。

实时语音垃圾信息可能是违法或欺诈性的垃圾信息，它怀有恶意并也可能威胁到传统的有线和移动电话业务。而且，VoIP 低廉的价格可以使这些违法 VoIP 垃圾信息比传统的电话

业务垃圾信息更活跃。例如，恶意垃圾信息散播者可以通过发送 VoIP 网络钓鱼（Phishing）来窃取金融信息，即 vishing，以非法获得业务用户信息。恶意垃圾信息散播者可能发送诱饵垃圾信息使垃圾信息接收方不情愿地使用非常昂贵的业务。例如，垃圾信息散播者可使用“自动响一声机器”，这种机器与垃圾信息接收方连接，并在振铃一声或两声后终止，或在只应答一词如“Hello”后很快切断，许多接收方会根据呼叫者的 ID 信息回拨过去。垃圾信息接收方就被自动接入到自动广告系统或某些非常昂贵的业务。此类垃圾信息对垃圾信息散播者非常有吸引力，因为垃圾信息散播的成本非常低。恶意垃圾信息散播者通过利用 VoIP 系统的安全弱点来发送诱饵垃圾信息。例如，垃圾信息散播者可以通过入侵 VoIP 呼叫会议进行诈骗。当用户需要与其他业务用户通信时，垃圾信息散播者可以通过诈骗使 VoIP 业务用户连接到垃圾信息散播者。类似地，各种诱惑垃圾信息接收方的诱饵垃圾信息可能出现在 IP 多媒体应用中。

7.2 实时文本垃圾信息

实时文本垃圾信息可定义为：以提供商业产品和服务的广告为目的，未经请求便主动提供的大量实时文本消息。实时文本垃圾信息可出现在许多在业务用户之间提供实时文本传送功能的 IP 多媒体应用上。实时文本垃圾信息的特征类似于电子邮件垃圾信息，因为垃圾信息是基于文本的。然而，实时文本垃圾信息比电子邮件垃圾信息更加令人厌烦，因为在垃圾信息传送的瞬间，垃圾信息接收方会被中断。实时文本垃圾信息的实例为 IM 垃圾信息和聊天垃圾信息。

在许多 IP 多媒体应用业务，包括 IM 业务、在线聊天业务和在线游戏中，为业务用户提供的消息传送功能是免费的或很便宜的。因此，垃圾信息散播者可以以很低廉的成本发送文本消息垃圾信息。垃圾信息散播者通常可以通过各种方法获得业务用户的普通或特定信息。对于垃圾信息散播者，这种垃圾信息相比较针对未指明人群的电子邮件垃圾信息的利润有望增加。

7.3 实时视频垃圾信息

实时视频垃圾信息可定义为：以提供商业产品和服务的广告为目的，未经请求便主动提供的实时视频通信。视频包括静止图像和动漫两种。实时视频垃圾信息可出现在业务用户之间提供实时视频通信的 IP 多媒体应用业务中。

在 IP 多媒体应用垃圾信息的初期，文本或语音类型消息垃圾信息可以不很困难地制造，并可以很低成本地发送，并不会对 IP 网络产生很大的负担。电话推销形式中的实时语音垃圾信息可占 IP 多媒体应用垃圾信息中的很大一部分。然而，随着媒体共享和 IP 多媒体应用业务用户间传输技术的发展，以及网络能力的扩大，实时视频垃圾信息也会广泛传播。

7.4 非实时语音垃圾信息

非实时语音垃圾信息可定义为：以提供商业产品和服务的广告为目的，未经请求便主动提供的大量非实时语音消息。非实时语音垃圾信息的典型实例称为语音消息垃圾信息。

在许多情况下，VoIP 业务可支持多媒体消息发送业务，如发送和接收文本、音频和视频消息，以及实时语音呼叫连接功能。垃圾信息散播者可发送语音消息垃圾信息，其已经被记录在采用 VoIP 业务功能的垃圾信息接收方终端中。在占用语音邮箱或存储器容量方面，此类语音消息垃圾信息会对 VoIP 业务用户和 VoIP 服务提供商造成很大的危害，因为语音消息垃圾信息的量很大。

7.5 非实时文本垃圾信息

非实时文本垃圾信息可定义为：以提供商业产品和服务的广告为目的，未经请求便主动提供的大量非实时文本消息。非实时文本垃圾信息特征类似于垃圾邮件。非实时文本垃圾信息可出现在各种 IP 多媒体应用中，因为制造和传送文本消息以及散播垃圾信息并不困难并且成本通常很低。

非实时文本垃圾信息可传送到可接收长的文本消息如电子邮件的 IP 终端，或如可接收短文本消息如移动 SMS 的 VoIP 电话的 IP 终端。它可以通过许多 IP 多媒体应用业务传送，包括 IM 和各种在线业务。除了这些类型的无视垃圾信息接收方意愿就传送给垃圾信息接收方的文本垃圾信息，还有其他类型的被 IP 业务用户访问的文本垃圾信息，如网站上的广告。非实时文本垃圾信息的特性类似于垃圾邮件，许多阻止电子邮件垃圾信息的技术有望应用于这类垃圾信息上。当文本垃圾信息长度很短时，这些技术的适用性会降低。

7.6 非实时视频垃圾信息

非实时视频垃圾信息可定义为：以提供商业产品和服务的广告为目的，未经请求便主动提供的大量非实时视频消息。此类垃圾信息可能是下列 2 种类型中的一种：IP 业务用户获得或下载视频垃圾信息文件，或在 IP 多媒体应用业务中，IP 业务用户访问 VoD 形式的视频垃圾信息。非实时视频垃圾信息的传输方法可以分为两类。首先，垃圾信息接收方可能偶然收到垃圾信息散播者发送的违背垃圾信息接收方意愿的视频广告文件。另一种情况是，IP 多媒体应用业务用户通过文件共享业务下载垃圾信息，而没有意识到该文件是垃圾信息。

当垃圾信息接收方下载视频垃圾信息文件时，下载垃圾信息文件对垃圾信息接收方来说可能造成精力的浪费。当视频消息垃圾信息违背垃圾信息接收方意愿发送时，垃圾信息损害了业务用户和服务提供商的利益，因为视频消息通常非常大地占据邮箱或存储空间。

8 阻止IP多媒体垃圾信息的技术问题

类似于电子邮件或移动 SMS 垃圾信息，以下是有关在 IP 多媒体应用业务上创建、发送和防止垃圾信息的系列程序：

- 垃圾信息的创建和发送
- 通过IP多媒体应用的业务用户和/或服务提供商删除和过滤垃圾信息
- 接收垃圾信息的对策

在建立阻止 IP 多媒体应用垃圾信息的技术框架之前，需要就防止 IP 多媒体应用垃圾信息问题研究上述各程序所存在的弱点。考虑到这些弱点，对每类技术问题的描述应在阻止 IP 多媒体应用垃圾信息的每个步骤加以考虑，并且在 IP 多媒体垃圾信息创建和传送过程中分析这些问题的影响。当研究阻止 IP 多媒体垃圾信息的技术框架和技术手段时，本节中提出的问题分析可能有助于确定阻止 IP 多媒体应用垃圾信息的有效方法。

8.1 垃圾信息的创建和传送

IP 多媒体垃圾信息得以广泛传播的基本假设是，垃圾信息散播的成本低于垃圾信息散播者期望从 IP 多媒体垃圾信息中获得的收益。垃圾信息散播成本不只包括金钱成本还包括各种开销，如创建和传送 IP 多媒体垃圾信息所需要的时间、精力、技术难点。影响垃圾信息散播成本的因素有下列几项：

- 收集目标地址或目标电话号码的成本：收集到垃圾信息发送对象的地址或电话号码所需要的成本。
- 垃圾信息创建和传送的成本：垃圾信息散播者创建和发送垃圾信息的所需要的成本。

8.1.1 收集目标名单

在发送垃圾信息前，首先需要收集垃圾信息目标名单。垃圾信息散播者通过地址库攻击、电子邮件地址收集程序获得电子邮件垃圾信息目标名单，并违法访问收集到的目标名单。在移动 SMS 垃圾信息的情况下，通过对号码的简单组成可以构成垃圾信息目标名单，因为移动电话号码的资源是有限的。

用于 IP 多媒体应用业务用户之间通信和消息交换的特定主题标识符的类型，可以根据 IP 多媒体应用、协议、国内规则等不断变化。可用于 VoIP 业务的主题标识符的形式可以是电话号码，类似于 PSTN 业务、IP 地址、IP 业务账户，如电子邮件账户等等。对于 IM 业务，电子邮件地址通常用于主题标识符和其他信息类型，如移动电话号码也可以使用。

当这些类型的主题标识符用于 VoIP 和 IM 时，通过使用现有的用于电子邮件垃圾信息的目标名单收集方法，这些业务的主题标识符和业务账户可以被垃圾信息散播者收集到。通过地址库攻击、经由网络搜索的标识符收集程序等等，收集到 VoIP 和 IM 的用户地址没有很大困难。

除了 VoIP 和 IM 外，还可能出现各种类型的 IP 多媒体应用垃圾信息，如聊天业务、在线游戏业务、基于 P2P 的业务等等。似乎为这些 IP 多媒体应用制造垃圾信息目标名单不需要做太多的努力。许多这样的 IP 多媒体应用，如在线业务使用广泛采用的账户类型，如电子邮件地址和电话号码作为主题标识符。对于只允许被认可用户发送文件或消息的 IP 多媒体应用业务，获得其用户名单也并不困难。考虑到这些诸多方面，没有一个特定的方法能使得收集 IP 多媒体应用业务的用户标识符变得困难，从技术和经济两个角度，垃圾信息散播者制造 IP 业务的主题标识符也是不困难的。

8.1.2 垃圾信息的创建和传送

IP 多媒体应用垃圾信息的创建和传送所需要的成本有望成为 IP 多媒体垃圾信息的垃圾信息散播成本中最大的部分。在 IP 多媒体应用中的 VoIP 业务或语音通信成本通常低于基于电路的有线电话业务或移动电话业务。对于传统的采用传统有线或无线电话业务进行电话推销的垃圾信息散播者，在 IP 多媒体应用中的 VoIP 或语音通信是发送垃圾信息的一种有吸引力的目标业务。而且，长途电话和国际电话比起传统的电话业务还便宜很多。因此，电话推销垃圾信息可以延伸到使用相同语言的其他国家，并且电话推销垃圾信息也可以在电话推销商成本和垃圾信息发送成本更低的其他国家制造。

除了 VoIP 业务外，许多 IP 多媒体应用，如 IM、基于 P2P 的业务和在线聊天业务的提供也是免费的或非常便宜的。在这些应用中的垃圾信息的创建和传送不需要太大的努力或成本，因为他们没有支付高价、时间或技术难题方面的问题。

8.2 垃圾信息的检测和过滤

在有效地阻止垃圾信息的技术层面上，检测和过滤 IP 多媒体应用垃圾信息是最为重要的部分。切实可行的办法是：在垃圾信息接收方检查垃圾信息之前，在 ISP 的服务器、企业内部互联网或电子邮件接收方的终端过滤出电子邮件垃圾信息，因为电子邮件业务采用的是存储转发通信原理。采用各种过滤技术可以过滤出大量的电子邮件垃圾信息，如内容分析等等，因为大部分电子邮件具有基于文本的内容。不同于电子邮件垃圾信息，对于下列性能的 IP 多媒体应用，过滤 IP 多媒体垃圾信息是很困难的：

- 实时通信
- 难以进行的语音和视频的内容分析
- 难以进行的垃圾信息散播者认证

某些 IP 多媒体应用，如 VoIP 和 IM 提供业务用户间的实时通信。通过这些应用传送的垃圾信息实时发送至垃圾信息接收方而不存储在服务器中。在某些情况下，VoIP 和 IM 的内容不通过服务提供商的服务器，相反，他们被直接发送给业务用户，因此，在呼叫建立或消息递送之前，获得通信的足够信息并分析通信内容以识别垃圾信息相当困难。例如，当发送方向垃圾信息接收方发送一条消息，为垃圾信息接收方认定该呼叫为垃圾信息时，过滤此垃圾信息就太晚了，因为呼叫连接已经完成。在 IM 垃圾信息的情况下，在很短的时间内分析 IM 消息的内容是可能的，因为 IM 消息通常是基于文本的。然而，短 IM 消息可能降低为阻止电子邮件垃圾信息而开发的传统过滤技术的有效性。当 IP 多媒体应用内容未被 ISP 服务器旁路掉时，业务用户终端就承担了过滤垃圾信息的责任。但是，将垃圾信息过滤功能增加到业务用户终端并由用户控制垃圾信息过滤功能并非一项简单工作。因此，通过内容分析过滤来检测和过滤实时 IP 多媒体应用垃圾信息，如 VoIP 垃圾信息和 IM 垃圾信息效果可能不大。

当某些 IP 多媒体应用不必一定是实时的时候，可以采用存储转发通信原理，如多媒体消息，根据服务提供商或业务用户要求，通过 P2P 技术发送文件，采用内容分析来阻止垃圾信息。然而，通过内容分析检测和过滤垃圾信息仍然非常困难，因为语音和视频识别技术还未成熟并且该技术的使用会给网络造成很大的负担。

根据发送方的信息而非通信本身的信息确认垃圾信息也是可行的。可以采用各种技术确认一个发送方是否垃圾信息散播者，如黑名单、白名单、信誉系统等等。这些技术应用于 IP 多媒体应用垃圾信息有几个弱点。首先，为 IP 多媒体应用制造业务账户或主题标识符并不困难并可大量制造。当其旧的标识符被归类为垃圾信息散播者时，垃圾信息散播者可轻易地再制造一个新的标识符。他们还可能利用 IP 多媒体应用的安全弱点假装成普通业务用户。鉴于这些问题，就要求将基于发送方信息识别垃圾信息的反垃圾信息技术与有效的认证机制结合起来。

8.3 对所接收的垃圾信息采取的行动

在收到垃圾信息后，垃圾信息接收方可采取几种行动。他们可以将垃圾信息散播者的标识符加入黑名单中，以阻止垃圾信息散播者向其或其他用户发送更多的垃圾信息。他们也可以给予垃圾信息散播者恶评（坏的评分）以反映到信誉系统。报告违法的垃圾信息来处罚垃圾信息散播者也是可能的。然而，正如前面提及的，识别许多 IP 多媒体应用上的垃圾信息散播者并不容易，因为创建新的标识符也不困难。在这一点上，还要求采用有效的认证机制以提高对付接收垃圾信息行动的效力。

9 与垃圾信息相关的安全威胁

本节讨论关于 IP 多媒体垃圾信息中与安全有关的问题。某些安全威胁被定义并按照其对策加以分类。

9.1 与垃圾信息相关的安全威胁

本节讨论出现在 IP 多媒体垃圾信息中的安全威胁。从向网络发送垃圾信息的角度定义安全威胁。在 IP 多媒体环境中，垃圾信息散播者可通过下列技术攻击手段发送垃圾信息。

9.1.1 标识符收集

为了发送垃圾信息，垃圾信息散播者收集标识符以寻找垃圾信息散播的目标。因此，标识符收集是最普通的垃圾信息威胁和基本预备过程。垃圾信息散播者试图收集到尽可能多的标识符，因为从垃圾信息散播者的观点来看，标识符的数量意味着可能攻击的目标的数量。可以通过不同的方法搜集到标识符。可以通过搜索引擎、留言板等等进行收集。还可以采用普通的词或名称收集标识符。有时，还可以通过违法事物处理方式，从通常拥有大量私人信息的客户的公司和学校中收集。

唯一标识符，如 e-mail 地址和 URI 已经在许多 IP 多媒体应用中用于辨别用户。不同于电话业务，IP 多媒体应用中的业务有几个优势，如多路通信、价格低廉等等。尤其在 IP 多媒体环境，对发送垃圾信息的垃圾信息散播者有吸引力。因此，用户应十分小心保护其识别以免暴露给垃圾信息散播者。

9.1.2 垃圾信息发送方假冒地址

假冒地址是电脑数据非法获取技术中的一种，恶意网络入侵者制做了互连网站并引诱用户访问其互连网站，利用 TCP/IP 组织缺陷以获得用户的权力、窃取其个人信息。而且，如果垃圾信息散播者发送伪装成著名公司的垃圾信息，接收方可能认为，这是一个可信任的发送者。垃圾信息被接受的可能性很大。这也称为'假冒地址'。

通过发送方假冒地址方式发送的垃圾信息是一种威胁，垃圾信息散播者伪造 IP 多媒体应用中使用的消息标题字段或发送方标识符，将其伪装成其他人。这种威胁可以扰乱作为众所周知的垃圾信息解决方案的白名单和黑名单。例如，如果垃圾信息散播者将其标识符变为在接收者的伙伴名单或白名单中登记的有效用户，垃圾信息散播者就可以旁路基于白名单的政策。另外，由于多媒体通信的性质，在连接建立之前确定消息是否为垃圾信息非常困难。因此，在这种情况下，接收方除了接收垃圾信息外无能为力。

9.1.3 注册信息监听

监听行为是：垃圾信息散播者在其他用户之间正在进行的连接上偷听。进行监听所用的工具称为网络监听器。

在 IP 多媒体环境中，垃圾信息散播者可能采用网络监听器非法发送垃圾信息。首先，垃圾信息散播者采用网络监听器在有效用户的特定应用注册信息上偷听，并且采用已获得的信息生成假的注册信息。接着，垃圾信息散播者在注册消息中插入攻击者的 IP 地址代替有效用户的 IP 地址。接着，垃圾信息散播者采用假的注册发送垃圾信息。

9.1.4 会话入侵

会话入侵是一种技术手段，某人入侵其他用户之间的通信会话。它也被用于在 IP 多媒体环境中发送垃圾信息。垃圾信息散播者可以在会话中强迫两个用户之间通信中断。在该情形下，用户往往要重新建立先前正在进行的会话。垃圾信息散播者可以入侵会话，并在重新建立会话中插入包括垃圾信息的 RTP 媒体传输。

9.1.5 SQL 注入

SQL 注入是一项电脑数据非法获取技术，通过插入违背请求者意愿的询问语法而导致异常结果。在 IP 多媒体应用环境中，当 HTTP 摘要机制应用于认证时，可使用 SQL 注入。垃圾信息散播者修改认证标题并插入伪造的 SQL 询问。而后，垃圾信息散播者伪造一个 Proxy 服务器中消息的认证标题，HTTP 摘要机制用于认证，并插入伪造的 SQL 询问。如果此项攻击成功完成，垃圾信息散播者就可将自己伪装成认证用户并通过伪造有效用户注册信息的方法发送具有有效授权的垃圾信息。

9.1.6 垃圾信息机器人

垃圾信息机器人是一种程序或代码形式的恶意机器人，它可以通过远端控制和操作但不能由其本身激活。通常，它经由采用 IRC 协议的连接控制。由机器人组成的网络称为僵尸网络（BotNet）。垃圾信息散播者有可能只采用一个命令就控制许多被感染的系统，因为僵尸网络可能被链接在一起。因此，在 IP 多媒体应用中，垃圾信息散播者利用此项技术可以很容易地大量发送垃圾信息。

9.1.7 高速缓冲存储器中毒

高速缓冲存储器中毒为一项攻击技术，将域地址由另一个错误地址替代。高速缓冲存储器中毒可在 IP 多媒体应用中的 ARP 和 NDP 中采用。ARP 用于在 IPv4 网络中将 IP 与 MAC 地址进行匹配，NDP 在 IPv6 网络用于发现邻居。ARP 和 NDP 包转发到一个链路中连接的所有设备。垃圾信息散播者可以使用高速缓冲存储器中毒方法通过包拦截修改 ARP 高速缓冲存储器或 NDP 高速缓冲存储器中的内容。

例如，利用 ARP 高速缓冲存储器中毒，垃圾信息散播者可以伪装成一个网关，在同一链路中使所有的包中途拦截全部的包。因此，如果用户开始一个连接，则垃圾信息散播者可以插入一个准备好的 RTP 垃圾信息在正在进行的会话中。垃圾信息散播者可以改变目标的标识符。如果用户的标识符被改变，用户就可以尝试与其他方（具有由垃圾信息散播者编址的标识符，他已经不是初始方了）建立另外的连接。通过此项攻击，垃圾信息散播者可以向请求连接的用户发送垃圾信息。

9.1.8 选路控制

假设，路由器和用户之间正在进行 IP 多媒体应用通信，垃圾信息散播者通过电脑数据非法获取方法在网络内的通信中扮演一个选路角色。如果一个用户试图建立与属于特定网络的其他用户的连接，垃圾信息散播者便将自己伪装成有效用户来响应请求，并发送垃圾信息给请求连接的用户。

9.1.9 薄弱的管理系统

还可能存在利用业务管理系统的弱点进行的其他威胁。在这种威胁情况下，垃圾信息散播者可改变有效用户的注册信息并发送具有有效用户资格的垃圾信息。

9.2 垃圾信息安全威胁的分类

上述垃圾信息安全威胁可以通过攻击技术分类。已分类的垃圾信息安全威胁示于表 9-1 中。

表 9-1 – 通过攻击技术分类的垃圾信息安全威胁

攻击技术	垃圾信息安全威胁
恶意代码/远端控制	垃圾信息机器人
会话入侵	会话入侵
SQL 注入	SQL 注入
监听	注册信息监听
假冒地址	发送方假冒地址，高速缓冲存储器中毒，选路控制
其他	标识符收集，薄弱的管理系统

恶意代码/远端控制是一种可以轻易地大量转发垃圾信息的技术。垃圾信息散播者可以通过各种方式散布恶意代码，并控制被感染的设备发送垃圾信息。垃圾信息机器人 就是这类示例中的一种。

会话入侵是一种窃取某人会话的电脑数据非法获取技术。通常，它只是通过猜测会话 ID 并采用会话 ID cookie 进行。垃圾信息散播者可以在服务器和用户之间的连接上偷听，没有认证程序或具有服务器授权。

SQL 注入是一种利用数据库弱点的电脑数据非法获取技巧，它可以非法改变正常的 SQL 询问并通过认证过程。通常，此方法用于网站数据非法获取中以窃取用户信息。

监听是一项技术，借此电脑黑客在两个或多个用户之间交换的包上偷听。

假冒地址是一项一个人伪装成其他人的技术。这项技术可以欺骗另一方的机器相信垃圾信息散播者是另一个可信任的人。

9.3 对策

解决上述垃圾信息问题有 3 种对策：认证、授权和安全管理。安全管理为适用于适当的安全配置中的对策，即在系统构建中插入安全补丁以维护、修理和增强用户的安全意识。这些对策如流量控制、加密等。本节针对 3 种主要对策。

对策与垃圾信息安全威胁之间的关系总结于表 9-2。

表 9-2 – 对策与多媒体通信垃圾信息安全威胁之间的关系

威胁 \ 对策	认证	授权	安全管理
标识符收集			X
发送方假冒地址	X		
注册信息监听	X		
会话入侵	X		
SQL注入		X	X
垃圾信息机器人			X
高速缓冲存储器中毒	X		
选路控制	X		
薄弱的管理系统		X	X

认证对策，通过解析假冒地址问题可以解决许多垃圾信息安全威胁。在各种威胁中都采用欺骗手段，如发送方假冒地址、注册信息监听、会话入侵、高速缓冲存储器中毒和选路控制。对于发送方假冒地址，每个发送方在收到消息后通过认证被鉴别。对于注册信息监听攻击，通过认证，未被认证的用户被阻止修改注册信息。对于入侵和高速缓冲存储器中毒攻击，通过认证的用户才可加入到连接中。对于选路控制，只有通过认证的用户可以控制路由器。

然而，在 SQL 注入上的垃圾信息安全威胁不能通过认证对策解决。因此，在这种情况下就要建立授权政策。薄弱的管理系统也可属于此类情况。系统管理器应按照用户账户给予用户不同的访问权限。

最后，某些垃圾信息安全威胁需要周密的安全管理。标识符收集、SQL 注入、垃圾信息机器人和薄弱的管理系统这属于这种情况。垃圾信息散播者可以通过许多通路收集用户的标识符并发送垃圾信息。因此，要求周密的标识符管理。在开发系统时，系统的开发商应重视，因为 SQL 注入威胁有时由错误代码引起。垃圾信息机器人由恶意机器人感染引起。因此，计算机用户在下载文件或访问网站时应该相当小心，并保护其 OS。在薄弱的管理系统中，系统管理者应仔细管理其系统。

10 共知的阻止垃圾信息机制对于IP 多媒体应用的适用性

对于阻止常规电子邮件垃圾信息的各种机制已经进行过许多研究。某些垃圾邮件解决方案也适用于阻止 IP 多媒体垃圾信息。在讨论针对 IP 多媒体垃圾信息的解决方案空间之前，必须分析常规垃圾信息阻止机制，并讨论其对阻止 IP 多媒体垃圾信息的适用性。因此，本节将就其对阻止 IP 多媒体垃圾信息的适用性讨论某些共知的阻止垃圾信息机制。

10.1 识别过滤

10.1.1 黑名单

黑名单表示一个识别名单（对电子邮件来说即为电子邮件地址），列出被怀疑或确定为垃圾信息散播者的名单。黑名单机制即为对源自该名单的消息或呼叫进行过滤。识别的名单

可以是：IP 地址、域名、主叫识别或地址、标题或内容的目录或这些不同类型的某种组合，可以借此来帮助识别垃圾信息。

在基于 IP 的应用中，仅使用黑名单阻止垃圾信息可能是不够的。垃圾信息散播者可以使用其他民众的识别并欺骗接收方。解决这个问题可以在源地址上采用认证机制。本方法的另一个问题是，用户可以很容易地创建新的识别。多种 IP 多媒体应用在通信中采用电子邮件地址。电子邮件地址也可以通过各著名的门户网站轻易创建。一般的非垃圾信息散播用户大多使用来自著名门户网站的地址，因此门户网站的域名不能列入黑名单。为解决这个问题，门户服务提供商对新地址的创建必须增加复杂程度，如果创建新地址所需要的时间很长而且过程很复杂，而为传播垃圾信息而创建的新地址又很可能被域黑名单过滤掉的话，垃圾信息散播者最终会使用其他的方法。因此，当采用其他方法时列黑名单的方法就变为有效了。

只当第一次遇到发起方（源）的识别，并在通信开始时，黑名单方法适用。因此可以将黑名单方法应用于任何类型的采用识别（如源地址）的 IP 多媒体应用。此方法可用于互联网站应用，因为，通过只对非垃圾信息散播者准许通信权，可以适用黑名单方法，即通信的用户不在黑名单中。因此黑名单方法可以用于阻止实时和非实时应用中，采用所有类型识别的 IP 多媒体垃圾信息。

10.1.2 白名单

白名单与黑名单相反。此名单包括被信任的用户信息。从白名单始发的电子邮件将总是被接受。不同于黑名单，采用大量创建电子邮件地址来经常改变其身份对通过白名单检查并无帮助，但它仍然通过假冒地址暴露出来。采用强有力的认证方法，具有假冒地址的垃圾信息很容易地被过滤。

虽然白名单方法几乎可以过滤所有的垃圾信息，但普通人还是需要与未在白名单中的其他人进行通信。如果一个未在白名单中的发送方需要与用户通信，就需要某种类型的授权方法以进入该用户的白名单。用户必须通过识别或某些来自发送方的介绍性注释来认证发送方。用户可以接受或拒绝通信请求。一个被接受的发送方可进入用户的白名单。如果用户必须接受或拒绝每个新的请求，这将很讨厌，因为许多新的请求为垃圾信息。采用此方法的另一个问题是，当用户的环境发生变化时，用户必须配置白名单，这将浪费时间和精力。

白名单的概念经常包括在 IM 系统中，被称为伙伴名单。对于被接受加入伙伴名单的新用户，许多 IM 系统只允许伙伴名单中的用户采用同意方式进行通信。因此借助于强有力的认证机制，它可能是一种有效的阻止 IM 垃圾信息的方法。然而，VoIP 具有与 IM 系统不同的性能。如电子邮件系统，采用其他方法时，白名单作为增补方法可能是有益的，因为用户仍然愿意接受未知用户的呼叫。

白名单方法只能用于通信开始时，因为适用于实时或非实时应用。此方法可用于互联网站应用，因为通过只向在白名单中的用户发放准许通信权的办法，采用白名单方法是可能的。

10.1.3 信誉系统

信誉系统与名单白或黑名单联合使用。如果不在接收方的黑名单或白名单中的发送方希望与接收方通信，信誉得分在接收方的终端中显示。信誉得分帮助接收方决定应该接收还是应该拒绝该呼叫。如果用户接受了通信请求并发现发送方为垃圾信息散播者，他可以向信誉系统举报垃圾信息散播者，并且发送方识别不再加入到用户的白名单中。举报报告在信誉服务器中积累并形成信誉得分。

此方法的问题是：具有负信誉得分的垃圾信息散播者可以改变其识别并采用新身份再开始垃圾信息散播。新身份不具有负得分，通过累积负得分而将一个用户认定为垃圾信息散播者还需要一定的时间。此方法的另一个问题是：某些坏人群体可能通过向无辜受害者给出负信誉得分进行威胁。具有负信誉得分的无辜受害者将很难继续其通过 IP 网络进行的交易。

另一类信誉系统是正信誉系统，接收方为非垃圾信息散播者给出正得分。根据此方法，使用新身份进行垃圾信息攻击就不容易了，因为新身份会很公正地得低分。采用此方法的问题是：几个垃圾信息散播者联合起来彼此给予正得分。然而，这样做就要求垃圾信息散播者形成某种联盟，而此方法成本巨大。因此，与负信誉系统相比，正信誉系统更为有效。

使信誉系统工作，需要集中且完整的控制电信系统。此方法对只受一个服务提供商操作的 IM 应用类型有效。然而，对于 VoIP 应用，假设在多个服务提供商之间提供通信，从不同的服务提供商获得的信誉得分就可能不同，因为没有制定标准。因此，此方法不适用的应用包括，如没有标准化描述系统的 VoIP。

在采用某种类型的发送方身份的应用中也可使用信誉系统，因为可以对身份给出信誉得分。如果发送方已经通过信誉系统，发送方将被加入到接收方的白名单中。因此此方法可以在所有实时或非实时应用中采用。

通过将准许通信权只发给超过一定等级信誉得分的用户，此方法也可以用于互联网应用中。互连网站为每个成员保留记录其先前行为的信誉得分。

10.1.4 信任圈

在信任圈方法中，获得信任的人或获得信任的域组成群体共享其白名单。此办法的方法是，一个人应该信任他信任的朋友信任的人。该群体形成一种获得信任的关系，并且他们也应同意执行一定类型的处罚手段，如果其成员被发现散播垃圾信息的话。

信任圈的另一变化形式是分布式黑名单法，在此方法中，获得信任的人的群体共享其黑名单。此方法在过滤垃圾信息中非常有效。许多根据此方法收集黑名单的服务器在工作，并将收集到的黑名单公布于众。

这类方法适用于可以共享和执行此政策的小的人群或小规模的提供商群体。如果获得信任的圈的规模扩大，在垃圾信息散播达到一定级别时，对所适用的处罚就难以达成共识。

10.2 地址掩蔽

各种 IP 多媒体应用在使用其业务中需要地址。因此，避免将地址公开很重要。但是，当使用基于互联网的业务时，对于新的客户应该暴露地址以便于与所有者联系。垃圾信息散播者将这个弱点用于收集垃圾信息目标地址。垃圾信息散播者扫描各种网页并收集带有“@”和“.”结构的地址。收集到的地址用于垃圾信息散播，并且收集到的地址传播给其他的垃圾信息散播者，因为垃圾信息散播者总是共享目标地址。

地址掩蔽是一种掩蔽某一地址的方法，使垃圾信息散播者不能自动收集到某地址。最简单的方法是将“@”改为 AT 和“.”改为 DOT。在此方法中，地址看似一个普通文本，因此，它可以通过垃圾信息散播者使用的自动地址扫描系统。

地址掩蔽不是一个阻止垃圾信息的方法，但是预防垃圾信息的方法。本方法防止将某地址暴露给垃圾信息散播者为收集地址所用的自动地址收集程序。因此，本方法适用于防止 IP 多媒体应用（使用基于互联网的业务的不同地址）中的垃圾信息。

本节描述地址掩蔽中可能用到的其他技术。

10.2.1 Java 脚本

在 JavaScript 环境中，很容易采用 Java 功能增加“abc@xyz.com”地址类型。网页应以“abc@xyz.com”形式显示，但当使用 JavaScript 中的 document.write() 功能时，非常容易掩蔽电子邮件地址。举例如下。

```
<SCRIPT TYPE="text/javascript">
  document.write('abc@' + 'xyz.com')
</SCRIPT>
```

还可能使用 JavaScript 中的其他功能或方法掩蔽电子邮件地址。但此处是描述在 JavaScript 环境下掩蔽电子邮件地址。因此，当采用 JavaScript 掩蔽地址时，垃圾信息散播者以自动方法收集电子邮件地址应该很困难，即使网页很明显地显示了普通的电子邮件地址。

本方法只能用在 JavaScript 环境中。但是，如果用户想要采用 JavaScript 在互联网网页中表示其联系人 ID 或 VoIP 联系地址，在变为垃圾信息散播者的目标中此方法会提供帮助。

10.2.2 ASCII 代码

ASCII 代码方法是隐藏在 ASCII 代码（为“&#number”）形式出现的重要信息的方法。此重要信息可以是电子邮件地址或电话号码，这就是垃圾信息散播者的目标。网页将不在普通文本中显示而是在图像中显示。因此当网页被下载时，它也只显示 ASCII 代码。如果垃圾信息散播者在其网页搜索工具中具有 ASCII 代码转换功能，则 ASCII 代码很容易被解码。

10.3 人工交互验证

每种通信工具在设计时都面临一个困惑或挑战就是：具有只有人能识别而机器则不行的功能。比如只有人能理解而机器不能明白的文字或数字的图像或声音。这可能是一个隐藏在各种色彩中的图像或隐藏在多种噪声中的声音，这对机器来说就难以识别了。现如今，由于自动图像或声音处理以及人工智能领域的进步，要做到机器不能理解更困难了。

在网络业务的订购阶段，人工交互验证方法是基于互联网的应用中常用的方法，因此非常适用于阻止基于互联网的垃圾信息。此方法也可通过采用声音授权方法用于过滤呼叫垃圾信息。当不在黑名单或白名单中的主叫方开始一次语音呼叫时，接收方自动激活交互式语音响应（IVR）系统，要求主叫方在电话键盘中输入号码，如果主叫方号码输入正确，则主叫方的号码自动加入到用户的白名单中。聊天用户也可通过交互验证方法加入到交谈中。

10.4 内容过滤

按主题线进行内容过滤是阻止垃圾电子邮件信息中最通常和最广泛应用的方法。它对主题线进行扫描，以检查是否包括垃圾信息中通常含有的可疑字。

IM 通信采用短文本消息，因此，本机制可容易地用于阻止 IM 垃圾信息。与扫描电子邮件的主题线的方法相同，每个 IM 的内容部分也可采用相同的技术进行扫描。

然而，这不适用于总是包含音频和/或视频的 VoIP 或其他 IP 多媒体通信。将在呼叫建立之后发送媒体，因此对内容的预先过滤不能显现任何优势。另一方面，虽然以语音或视频邮件形式传播的垃圾信息将被存储在服务器中，但当前用于扫描文字的技术还不能用于阻止垃圾信息。

10.5 通过密钥交换的认证

认证已经能够安全地识别 IP 多媒体消息的发送方，以帮助阻止任何假冒地址类型垃圾信息的攻击。

10.5.1 PKI 和 PGP

鉴别发送方以阻止源自伪装成其他白名单中成员的垃圾信息散播者的连接请求是可能的。公开密钥基础设施（PKI）和最优保密（PGP）是公认的采用公开密钥机制的认证方法。PKI 采用公开密钥机制，其中发送方可以通过被证书机构（CA）鉴定的公开密钥进行鉴别。PGP 使用的计算机程序为认证提供标记功能。在电子邮件系统中，这些机制被用于消息的加密和增加数字签字。这是防止垃圾信息的强有力的机制。

密钥交换机制适用于几乎所有的 IP 多媒体电信系统。它应谨慎用于 IP 会议业务，会议的群密钥被偷窃的风险很高。

PKI 和 PGP 方法可用于几乎所有类型的 IP 多媒体应用，如 VoIP 和 IM。此方法也可用于只允许由被鉴定的用户上传文件或消息的基于互联网的应用。

10.5.2 DKIM [b-IETF RFC 4871]

域密钥识别邮件（DKIM）是一种由 IETF（互联网工程任务组）（可用于电子邮件认证）开发的方法。电子邮件服务器向邮件加入一个加密标志以证实服务器已经实际发送了附属的电子邮件。DKIM 允许一个机构负责由接收方验证的消息。通过采用公开—密钥密码系统和密钥服务器技术，DKIM 定义了电子邮件的域级别数字签字认证框架。一个电子邮件欺诈可能产生的损害不仅伤害到接收方而且也影响企业或机构的信誉。采用 DKIM 方法可以保护企业或机构免于这种伤害。

DKIM 的使用可以防止通过 VoIP 或 IM 进行的欺诈通信。如果所接收的消息或呼叫实际来自于申明的发送方，接收方可以采用发送方的服务器进行检查。认证过程可以在通信开始时进行，因此即使对紧急的实时应用也不会造成影响。

10.5.3 HTTP 认证和 TLS 连接

对具有客户服务器结构的 IP 多媒体应用，使用 HTTP 摘要认证 [b-IETF RFC 5090] 随同 TLS（传送层安全）与服务器相连接是非常有效的。通过 HTTP 摘要认证，域的服务器验证其用户。通常通过用户名和密码，HTTP 摘要认证被用于鉴别 IP 多媒体应用的用户。客户，也就是用户和服务器保持持久的 TLS 连接。通过维持 TLS 与服务器相连接，客户证实服务器身份。服务器采用 TLS 连接上的摘要交换鉴别客户。当一个通过认证的用户发送一个消息到另一个域时，发送的域通过插入签字以证实消息来证明用户。发送和接收的域应形成一个相互的认证从而信任彼此的用户。

此方法可用于鉴别通过 IM 或 VoIP 通信的用户。认证过程可以在通信开始时进行，因此即使对紧急的实时应用也不会造成影响。

10.6 基于网络的垃圾信息过滤

上述讨论的垃圾信息过滤机制已经计划用于电信的服务器侧和客户侧。然而，建立安全网络以防止垃圾信息更是重要的。本节将简要地讨论某些基于网络的垃圾信息过滤方法。

10.6.1 网络实体上的包拒绝

可能对一个路由器或任何网络实体设置某些政策，如 ACL（访问控制表）以删除来自特殊 IP 地址源或 IP 前缀源的可疑垃圾信息包。垃圾信息散播者的来源可能在 ISP 网络内部或 ISP 网络外部。想要保护其网络不受垃圾信息干扰的 ISP 将采用不同的办法来解决上述两个问题。

如果垃圾信息的来源在 ISP 内，ISP 可设置源的网络实体切断垃圾信息源的 IP 连接。垃圾信息散播者将认识到网络连接已经取消并被迫承认其错误行为。然而，应制定一些标准以防止误用。一个人可能不实地控告一个无辜者为垃圾信息散播者而切断其网络连接。一个欺诈者也可能使用无辜者的 IP 地址发送其垃圾信息，因此切断无辜者的网络连接并且在一段时间内散播垃圾信息。

假设 ISP A 网与 ISP B 网相连接，而垃圾信息散播者利用 ISP B 网。如果垃圾信息的来源在 ISP A 网之外，ISP A 必须检查 ISP B 是否正在努力控制其网络内的垃圾信息。如果垃圾信息散播者的 ISP B 没有采取任何措施控制垃圾信息，则 ISP A 必须在 ISP B 的网关中设置对付垃圾信息的政策以防止垃圾信息流入 ISP A 网络。在此种方法中，ISP A 不能阻断网络连接的垃圾信息散播者，但他可以保护其网络。这种方法可以保护并节约其网络资源，此方法的弱点是它可能阻止了无辜用户从 ISP B 连接到其网络。

这个办法另一个问题是，垃圾信息散播者可以频繁地改变其 IP 地址。因此，垃圾信息散播者一侧的 ISP 必须控制和鉴别垃圾信息散播者所采用的 IP 地址以便此方法发挥作用。

在网络实体上的包拒绝方法可用于任何应用，因为此方法无关于 IP 多媒体应用。

10.6.2 分布式黑名单

分布式黑名单是一种寄居在网络内的黑名单，为网络社区所共享。分布式黑名单通常在 DNS 中实现。用户可以将垃圾信息散播的地址加入到分布式黑名单中。当一个 IP 地址出现在分布式黑名单中后，许多网站将拒绝来自该 IP 地址的消息。此方法对 IP 多媒体应用的适用性等同于黑名单法。

10.6.3 垃圾信息防火墙

企业网或 ISP 网络采用垃圾信息防火墙以保护其网络不受垃圾信息干扰。垃圾信息防火墙采用上述提及的许多方法以阻止垃圾信息进入其网络。在受保护的网路中的用户不再受垃圾信息的损害。此方法是黑名单和内容过滤方法的合并，因为当包通过企业网传送时，它保持了黑名单和内容过滤。

垃圾信息防火墙通常用于电子邮件和 IM。此方法可能对 VoIP 业务无效，因为在 VoIP 呼叫开始时，不能捕获任何信息。此方法可用于过滤基于互联网的垃圾信息，因为通过检查内容可能达到过滤的效果。

10.7 在线邮票

在在线邮票方法中，未在接收方白名单中的发送方应不得不购买在线邮票来发送消息。如果未列出的发送方没有在线邮票而发送消息，它将被服务提供商的服务器取消。只有带有在线邮票的未列出消息可以出现在接收方的终端。如果接收方接受此消息，他将向发送方返回在线邮票。发送方的地址便自动地加入到接收方的白名单中。如果接收方确定发送方为垃圾信息，他可以保留在线邮票的钱。垃圾信息散播者应不得不发送大量消息因此就增加了垃圾信息散播的费用。

此方法同样可以用于电子邮件、VoIP 或 IM 业务中。因为发送方只需购买一次在线邮票，它也不是很麻烦或昂贵的方法。因此，当采用适当的发送方身份认证时，它可以有效阻止垃圾信息。

10.8 基于授权的垃圾信息过滤

在过滤垃圾信息中一种重要的阻断构建是：依照用户或网络政策，提供一种机制在网络中命令某些实体"过滤"进入的连接请求。各种实体如用户或系统管理员可创建或修改授权政策。需要网络政策以规定各域之间的通信流。

授权政策可被终端主机采用和/或由网络单元采用。规则制定者可能是拥有该设备的终端用户、VoIP 服务提供商、与终端用户有关的其他人（例如，使用移动电话的孩子的父母）。本节以各种基于授权的垃圾信息过滤机制为基础。

10.8.1 基于同意的通信

基于同意的通信基于消息接收方的直接授权。它与白名单或黑名单联合使用。如果一个不在白名单或黑名单中的主叫方试图与用户通信时，他发送其识别和/或任何短文本到用户以确定自己。主叫方最初被拒绝。然后用户被通知主叫方请求通信。通过检查由主叫方发送的识别和/或短文本，用户或以接受或拒绝主叫方。

此类过滤方法目前应用于各种 IM 业务。它已经被认为在管理白名单中非常有效。通过采用在呼叫开始时获得同意的方法，在处理呼叫垃圾信息中，此方法切实可行。但不适用于

为单向性业务的基于互联网的垃圾信息。它也不适用于涉及多个用户的业务，因为它不能从所有正在进行业务中的所有参与者获得同意。

此方法的问题是，用户可能被过多的同意请求所打扰。因此某些同意请求应被另一个过滤系统所过滤。

10.8.2 基于用户政策的授权

在基于用户政策的授权中，IP 多媒体用户定义一个接受政策来过滤来自不知名发送方的请求。政策为用户终端或应用服务器设置以便自动接受或拒绝请求。在基于同意的通信方法中，政策可适用于垃圾信息源地址、识别和/或由发送方发送的短文本。政策也适用于所接收的图像、声音或文本的内容以自动过滤违背政策的通信请求。所拒绝的请求信息应记录在储藏区，以便于用户还可以返回并检查那些不应该被拒绝的请求。用户可以修改政策以满足其需要。

基于同意的方法的问题是，用户必须应答所有的通信请求。但是，在基于政策的授权方法中，大部的垃圾信息已经被自动过滤了，因此用户不会被太多的同意请求问题所打扰。政策的创建将取决于所采用的 IP 多媒体应用的特性。基于用户政策的过滤方法应规定用于所有可能出现垃圾信息的应用中。

在管理白名单中此方法非常有效。此方法是基于用户的方法，因此它可以用于任何类型的双向业务中，如 VoIP 和 IM 业务。

10.8.3 基于网络政策的授权

网络运营商应采用基于网络政策的授权来过滤垃圾信息从而保护网络。网络政策可用于单个的网络或相邻网络之间。此方法等同于网络实体方法上的包拒绝。

为提供可升级的垃圾信息过滤，网络运营商可下放部分管理权给技术好的终端用户，并使他们能够在到提供商网络的链路上配置网络政策。对有效的用户身份和管理权，必需的认证可在业务路由器中实现。只有有效的用户被授权按照其意愿提供相应的网络政策。

10.9 法律法案和规则

为防止垃圾信息，重要的是设置相关的法律法案和规则来禁止垃圾信息，虽然在这点的效能上还有争议。许多国家已经为受害者设置了法律对讨厌的垃圾信息采取法律行动。大部分情况是，必须将广告插入一个专门的内容组中以便于接收方可以将垃圾信息识别为广告，并且当违犯法则时会受到处罚。

此方法的问题是，本地的反垃圾信息法律执行对外国发送的垃圾信息的处罚上还有一定的困难。必须创建多国间的国际条约以确保此方法有效执行。国际组织包括 ITU-T、OECD、APEC 等等正在致力于定义有效的垃圾信息立法、国际合作和执行。

此方法并非技术方法，它与 IP 多媒体应用的特性无关。

11 关于阻止IP多媒体应用垃圾信息的考虑

利用 IP 网络传播广告不仅经济实惠而且有效。垃圾信息是伴随滥用广告一起出现的问题。一些严重的社会问题也可能随着垃圾信息问题一起出现。这些问题可能是：使网络用户备受折磨的大量广告、欺诈、诱骗。

本建议书已经介绍了各种 IP 多媒体应用垃圾信息的阻止方法。IP 多媒体应用具有各种特性，因为附属它的垃圾信息也有各种特点。只采用一种或两种方法不能阻止所有类型的 IP 多媒体垃圾信息。必须详细研究关于多媒体应用实体各部分的垃圾信息类型，以实际解决或至少减轻垃圾信息问题。因此，分析垃圾信息阻止方法应根据 IP 多媒体应用的特性。本节旨在表达阻止 IP 多媒体应用垃圾信息的某些思考要点。

为有效地阻止 IP 多媒体应用垃圾信息，应考虑业务参与群体的各个方面应采用的不同方法。包括业务用户（和/或业务订户）、服务提供商、网络运营商、公众组织和广告商。因此本节描述了针对上述每个方面阻止 IP 多媒体应用垃圾信息的思考要点。

11.1 业务用户（业务订户）

业务用户和/或业务订户是垃圾信息的实际受害者，应认识到为保护个人权利而阻止垃圾信息的重要性。在打击垃圾信息时，业务用户应对以下一些内容予以考虑，尽管不同手段可能造成这些建议在实施方式上的不同：

- 用户应获得垃圾信息过滤引擎并保持垃圾信息过滤引擎不断更新以阻止不必要的垃圾信息。新的垃圾信息经常出现，因此，过滤引擎应不断更新以控制新的垃圾信息。
- 用户应预订各种垃圾信息过滤表，如黑名单，白名单等等。并时常更新这些过滤表目录。
- 当遇到垃圾信息时，用户应立即将其删除并通知公布此问题以防止出现相同的受害者。
- 用户应参与垃圾信息预防培训，以学习新的垃圾信息和新的阻止技术。垃圾信息的新类型可能出现在伴随新业务的常规业务中。虽然，不需要采用每项阻止技术，但应努力寻求足够的解决方案以控制垃圾信息。
- 用户还应谨慎地保护其私人信息不暴露给垃圾信息散播者。用户不应使用很容易记忆或推测的识别类型或号码。
- 用户应采用保护技术，如阻止来自垃圾信息散播者通信请求的逻辑，并配置一个系统使垃圾信息散播者难以通信。

11.2 服务提供商

服务提供商通过提供服务的高质量获得很大的利益。由于垃圾信息散播者的滥用业务垃圾信息可能严重地损害业务质量。服务提供商应意识到垃圾信息问题的严重性以便保护网络并提供更好的服务。下面是服务提供商在阻止垃圾信息方面可考虑的问题。

- 在开始新的IP多媒体业务之前，服务提供商可分析新的IP多媒体业务或应用作为潜在的垃圾信息目标的可能性。并非每项IP多媒体业务都是垃圾信息散播者的目标。但是，进行垃圾信息分析并寻求解决方案，使垃圾信息的散播困难就增加了新业务成功的可能性。如果一种易受垃圾信息影响的业务没有经过上述分析过程就展开，它可能很难控制垃圾信息，并且在受垃圾信息干扰控制后用户就会忽视这项新的业务。
- 服务提供商可检查组成IP多媒体业务或应用的所有的实体如，用户、网络、业务组成等等，并分析在每种实体中的各种垃圾信息散播方法，以便发现更简单且有效的阻止垃圾信息解决方案。只在 IP 多媒体业务中采用垃圾信息阻止技术是可能的，但从整个网络实体的角度看还有更好的解决方案。
- 服务提供商可执行持续不断的搜索以防止常规应用中出现新的垃圾信息。垃圾信息的新类型甚至可能出现在最老的业务中。服务提供商可能希望观察这种现象并努力寻找解决方案以处理垃圾信息的新类型，即使对于老业务。
- 业务提供可采用各种过滤表，如黑名单和白名单以控制用户对业务的访问。它是防止垃圾信息散播者利用该业务的最好方法，因为垃圾信息散播者只可能滥用该业务。
- 如果业务包括预订过程，服务提供商可使预订的程序困难到足以使垃圾信息散播者无法连接业务。许多垃圾信息散播者使用自动方法或雇用很便宜的员工制造很多对垃圾信息散播很有效的预订。预订过程可包括强有力的认证方法以核实订户，并具有某些方案以防止一个用户的多个预订以及连接业务中的垃圾信息散播者。
- 如果业务保持一个系列的业务用户，服务提供商可采取评估每个业务用户信用度的办法以保证用户不滥用业务或其他业务用户。服务提供商应具有保护技术以防止订户的个人信息不暴露给内部和外部用户。
- 如果业务维持一个储藏室，服务提供商可能希望万维网中的内容得到监视以删除万维网垃圾信息。甚至可以对视频和音频数据进行内容分析以发现不当内容。
- 服务提供商可选择向业务用户提供控制垃圾信息的方法。它可以是过滤引擎、过滤表、政策配置工具、垃圾信息阻止手册或是用户可以采用的阻止垃圾信息的方法。

11.3 网络运营商

垃圾信息会对网络资源造成浪费，特别是如果垃圾信息包含多媒体内容的情况。网络运营商应该努力阻止垃圾信息以保护网络并提供有效的网络服务。下面是网络运营商在阻止垃圾信息方面应考虑的问题。

- 网络运营商可监测网络业务量以发现可能被认作垃圾信息的异常业务量。网络运营商应能够分析异常业务量并采取一个的行动。通过分析网络业务量以捕获垃圾信息并非易事。但是，各种恶意垃圾信息或程序确定可以显示异常业务量的模式。
- 网络运营商可限制垃圾信息散播者业务量或采取停止散播垃圾信息的其他手段。

- 网络运营商可与服务提供商合作共享垃圾信息相关的信息。网络运营商可以真正停止垃圾信息散播业务量，使垃圾信息散播无效。
- 网络运营商可利用各种垃圾信息防火墙保护其网络。
- 网络可只配置获得信任的网络，因此只允许被授权的用户或由获得信任的网络认证的用户可以进行通信。如果网络获得信任的关系，就可能使网络控制业务量和用户。最终，当所有子网络信任来自同类子网络的业务时，可以保护整个网络免受垃圾信息和其他恶意业务量损害。

11.4 公众组织

公众组织可以是一个政府机构或从事垃圾信息控制工作的相关群体组成的私人组织。私人组织可以是营利或非营利的组织，在控制垃圾信息方面拥有有效的解决方案。下面是公众组织在阻止垃圾信息方面应考虑方面。

- 公众组织可拥有一个系统供受害者提交受垃圾信息侵害的报告。该组织可警告或处罚垃圾信息散播者。这可能是一个政府组织或任何强大的有能力有效地警告垃圾信息散播者的私人组织。
- 在阻止垃圾信息方面，公众组织可选择建立一定的培训程序或向IP多媒体业务用户、IP多媒体服务提供商和IP网络运营商提供指导。垃圾信息阻止技巧要求更多的经验，在这方面，新的IP多媒体服务提供商或网络运营商可能不具备。
- 公众组织可以提供黑名单或过滤表使公众共享。公众还可以参与到构建黑名单或过滤表过程中。
- 广告机构可利用无法伪造并经认证的广告批准系统，由于不会被认为是垃圾信息散播者，因此从中受益。

11.5 其他需要考虑的事项

不同于上述内容的其它考虑事项如下：

- 尽管阻止垃圾信息方面的研究取得各式各样的成效，但垃圾信息的问题也许不会因此消失，新的垃圾信息总会出现，新的研究也会针对解决这些新问题而展开。但是，如果对垃圾信息阻止方法的研究事先进行，对更多的应用业务来讲就会有更好的适用环境。
- 各种垃圾信息阻止方法应一起使用。尚未有极好的解决方案可以解决所有的垃圾信息问题。各种方法一起使用来阻止各种类型的、可能出现在各种场合、采用各种技术的垃圾信息。
- 最理想的解决方案应该使垃圾信息的散播更为困难和昂贵。垃圾信息散播者的最终目标是使用便宜和简单的方法做广告。如果垃圾信息的散播太困难并且太昂贵或对散播垃圾信息的处罚太重的话，垃圾信息散播者最终也将停止散播垃圾信息。

参考资料

- [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>>

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	电信系统使用的语言和一般性软件情况