反垃圾邮件
相关技术和标准

黄元飞 博士

中国通信标准化协会(CCSA)
网络与信息安全技术工作委员会(TC8)
安全管理工作组组长

垃圾邮件

- 垃圾邮件是指包括下述属性的电子邮件：
  - 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件
  - 收件人无法拒收的电子邮件
  - 隐藏发件人身份、地址、标题等信息的电子邮件
  - 含有虚假的信息源、发件人、路由等信息的电子邮件

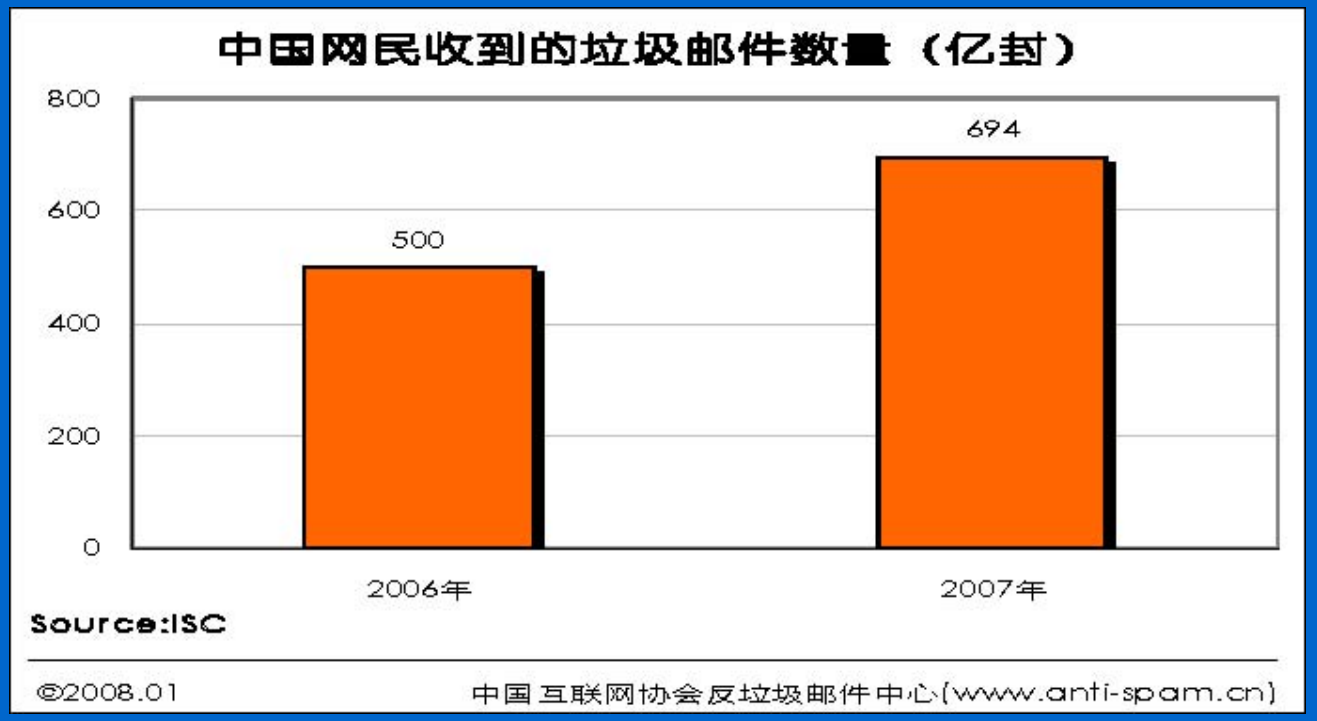
《中国互联网协会反垃圾邮件规范》

全球垃圾邮件泛滥

- 垃圾邮件占全球电子邮件通信量的 60% 以上
- 每天约有 145 亿封垃圾邮件被发出,每年因此耗费205亿$
- 对安全和隐私造成危害:
  - 计算机病毒、木马
  - 钓鱼、诈骗、身份盗窃
  - 僵尸网络
  - 色情、毒品
- 低成本 + 高利润 + 匿名性
  - 所有经济因素都对垃圾邮件制造者有利

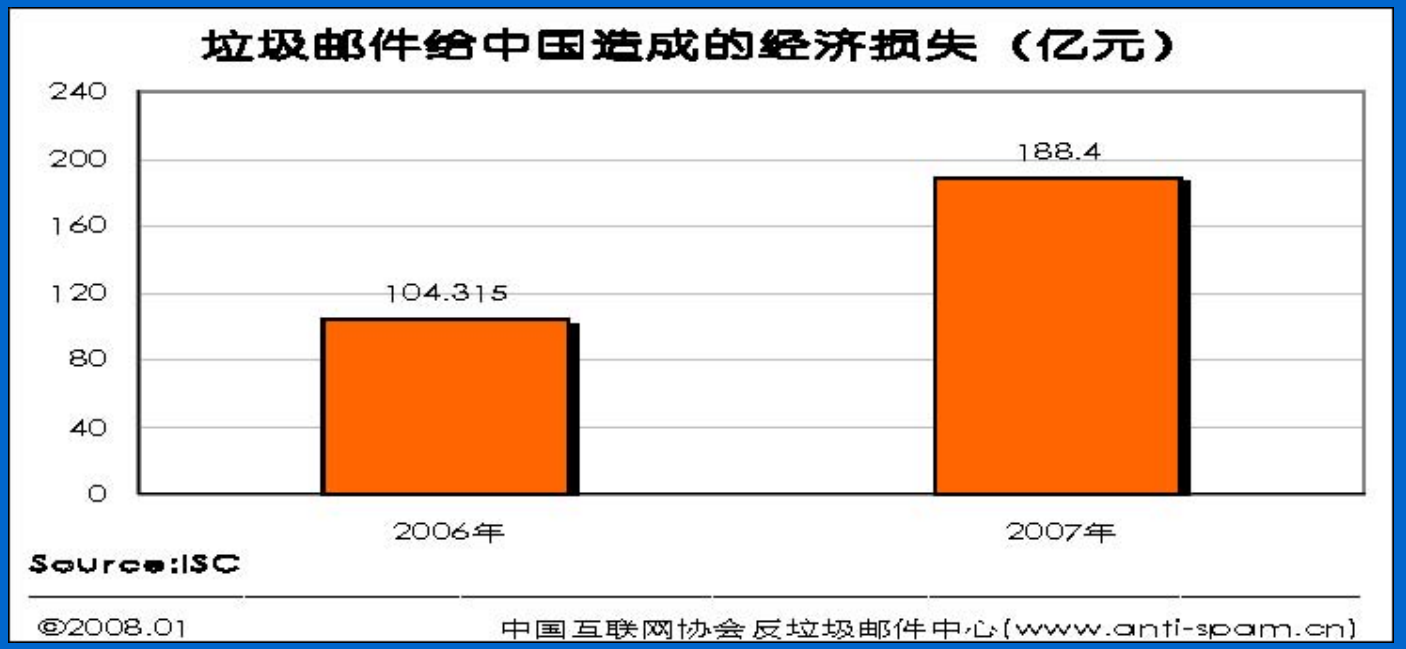
我国垃圾邮件更是泛滥成灾

- 2007年我国网民收到的垃圾邮件总量为694亿封，比2006年的500亿封增长38.8%
- 个人邮箱平均每周收到垃圾邮件的数量为16.71封，收到邮件55.65%为垃圾邮件



我国垃圾邮件更是泛滥成灾

- 2007年垃圾邮件给中国造成的损失达188.4亿人民币，与2006年的104.315亿相比增长了80.6%



面对垃圾邮件，我们该如何办

安全是一个过程，不是一个产品

不能购买了反垃圾邮件软件而认为安全了？

安全是一个妥协的结果

要完全避免垃圾邮件，只有关掉计算机，不再使用电子邮件

现实问题不是如何消除垃圾邮件，

而是如何有效限制垃圾邮件，同时不至于把正常邮件也当成垃圾邮件处理。

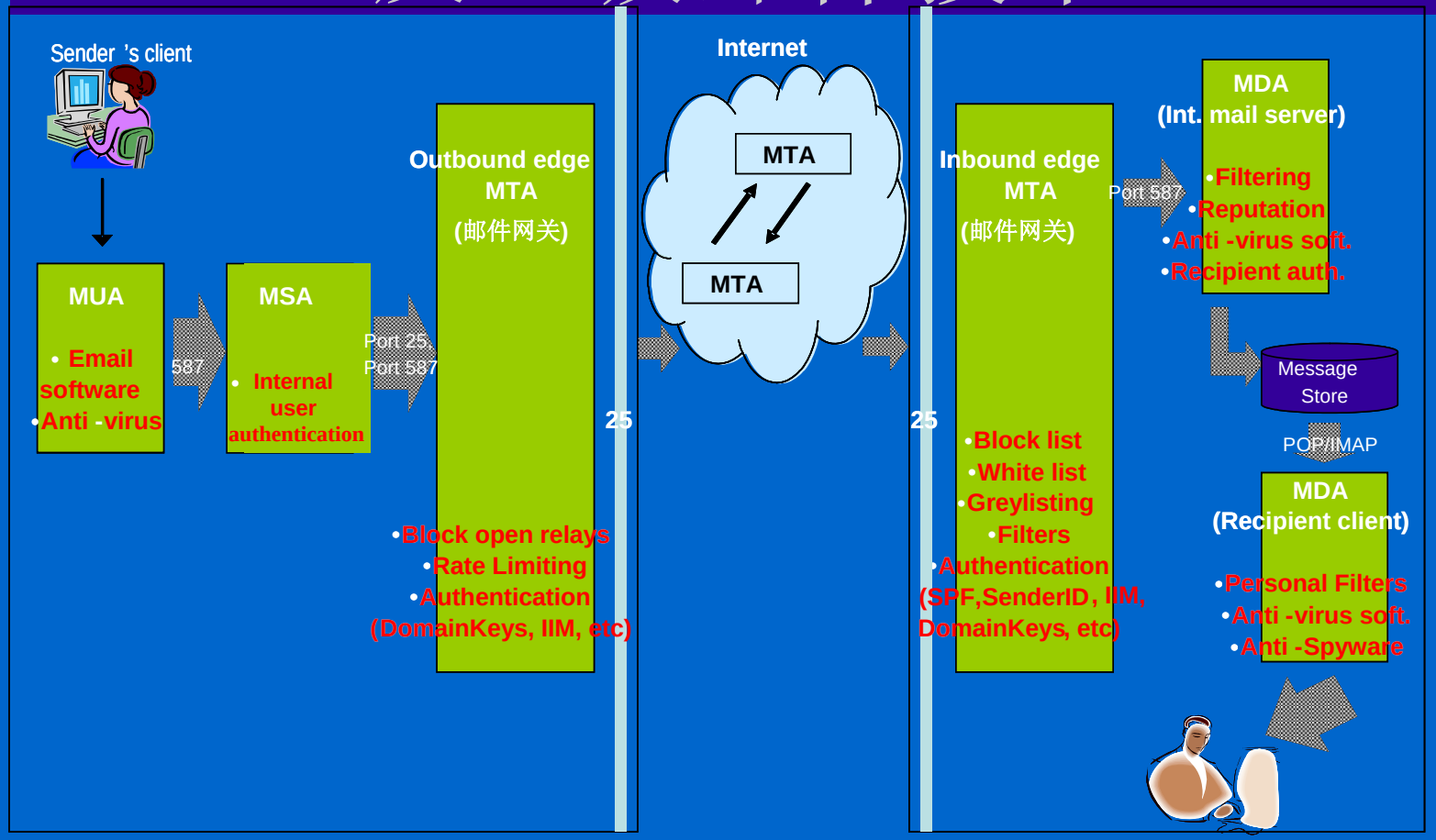
完美解决方案

- 没有漏掉垃圾邮件（false negative）
- 没有误删正常邮件（false positive）
- 低成本
- 不改变现有邮件系统解决方案
- 基于公开的标准

现实并不存在这种完美解决方案

但可以作为评估反垃圾邮件技术好坏的依据

反垃圾邮件技术



MUA-邮件用户代理
MSA-邮件发送代理
MTA-邮件传送代理
MDA-邮件投递代理

- MUA（邮件软件、反病毒）；MSA(内部用户认证)；MTA-Outbound(授限传递、频度限制、认证)；MTA-Inbound(黑名单、白名单、灰名单、内容过滤、认证)；MDA(个人过滤器、反病毒软件、反链接欺骗)

反垃圾邮件技术

- 黑名单
- 白名单
- 灰名单
- 内容过滤
- 认证
- 其他技术

反垃圾邮件技术-黑名单

- 黑名单（Blacklists）
  - 最早出现的一种反垃圾邮件技术，一般的邮件服务器都有该功能
  - 确定已知垃圾邮件制造者及其ISP的域名或IP地址，然后将其整理成黑名单，将黑名单部署在网关处，拒绝任何来自黑名单上的垃圾邮件制造者的邮件
  - 误判率较高

反垃圾邮件技术-白名单

- 白名单（Whitelists）
  - 拒绝接收任何邮件，除非用户的邮件地址在白名单上允许接收
  - 两种使用方式:
    - 一种是用户阻止不在名单上的信件
    - 一种是系统邮件发送者发送信件，要求其回复，以证实确有邮件发送者其人，经过确认后将其列入白名单中

反垃圾邮件技术-灰名单

- 灰名单（Graylists）http://www.greylisting.org/
  - 介于黑名单和白明单之间，通常是新的邮件服务器
  - 当邮件来自一个新的邮件服器时，故意反馈一个临时错误的电子邮件消息
  - 典型的垃圾邮件制造系统(MTA)不会重新发送，而合法的MTA则会从新发送
  - 非常有效，同时配置起来非常简单

反垃圾邮件技术-内容过滤

- **关键字过滤**（Keywords Filters）
  - 基于内容，根据关键词过滤
  - 误判率很高

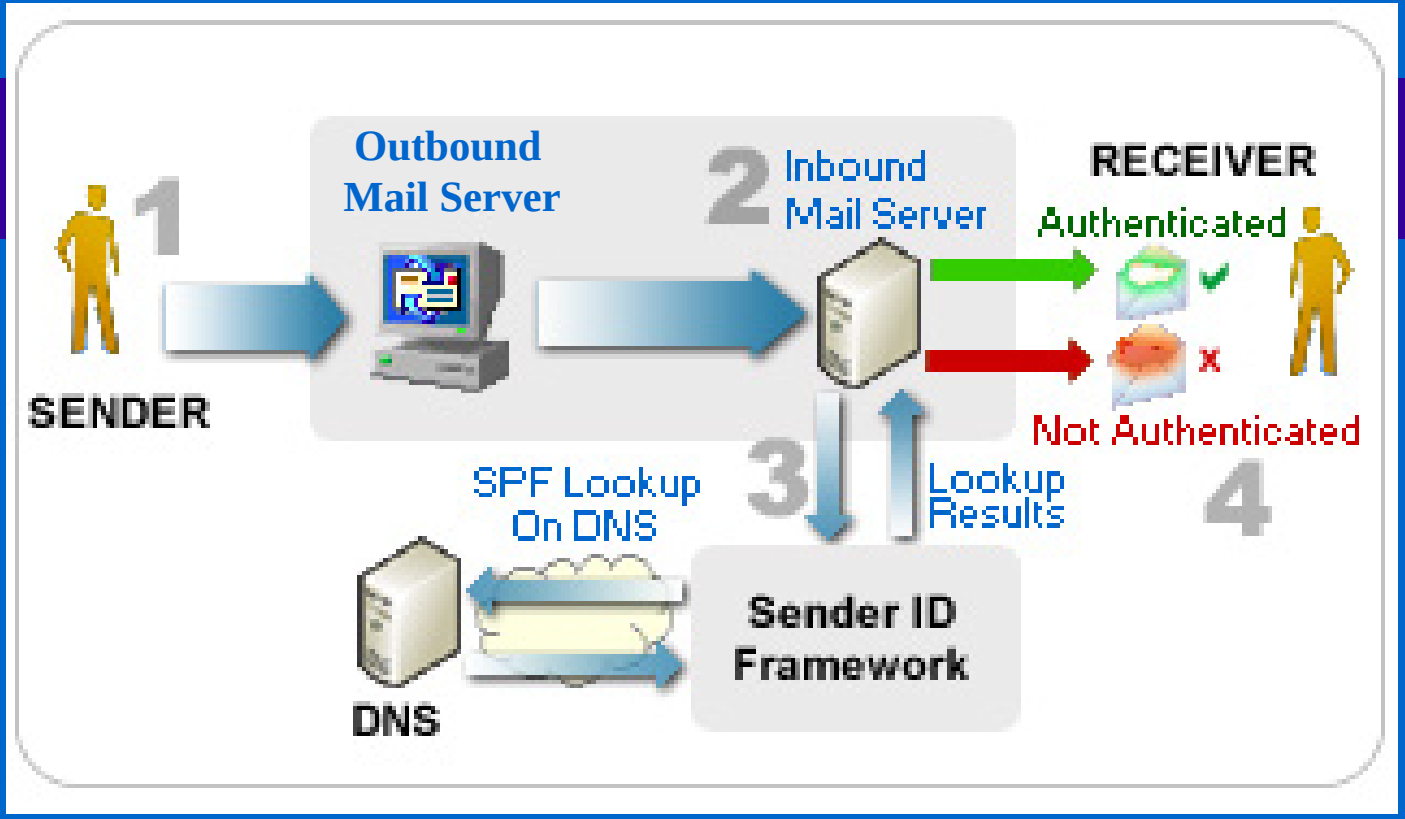
- **启发式(基于策略)的过滤**（Heuristic filters）
  - 通过定义垃圾邮件普遍特征和规则(策略库)，利用这些规则自动识别垃圾邮件
  - 如关键字等规则
  - 比较出名的工具是 ApamAssassin

反垃圾邮件技术-内容过滤

- **贝叶斯过滤**（Bayesian filters）
  http://www.bogofilter.org/
  - 人工智能方法，通过自我学习，过滤垃圾邮件。对于针对个人用户的过滤非常有效
  - 开始：没有任何规则
  - 用户识别垃圾邮件，贝叶斯过滤工具则同时接受训练，逐渐学会识别垃圾邮件
  - 随着经验的增加，贝叶斯过滤工具就能代替用户，识别垃圾邮件
  - 合理的训练方法非常重要

反垃圾邮件技术-认证

- ***Sender Policy Framework (SPF)*** [RFC4408]
  - 原理
    - 域名系统(DNS）解决域名与IP地址之间的映射关系
    - DNS中的邮件转换器MX（Mail exchanger）描述接收邮件的目标服务器的地址
    - SPF 和MX正好相反，在DNS中描述该邮件来自域名内哪台邮件服务器
  - SPF通过DNS传播，并会在ISP中保存，减少访问SPF信息而消耗带宽
  - 工作方式:
    - SPF需要发送方和接收方共同作用
    - SPF发送方需要在DNS中发布自己的SPF纪录
    - 接收方通过SPF纪录，验证电子邮件邮件回复地址，是否与SPF查到的地址相符，若相符，则是合法邮件
  - 不足之处
    - 无法阻止电子邮件内容在传输过程中被篡改，即邮件内容没有完整性认证
    - 垃圾制造者采用合法电子邮件地址发送，或者是一个域名的合法拥有者。该技术就无能为力
  - 该技术主要适用于垃圾邮件发送者采用假的发送地址



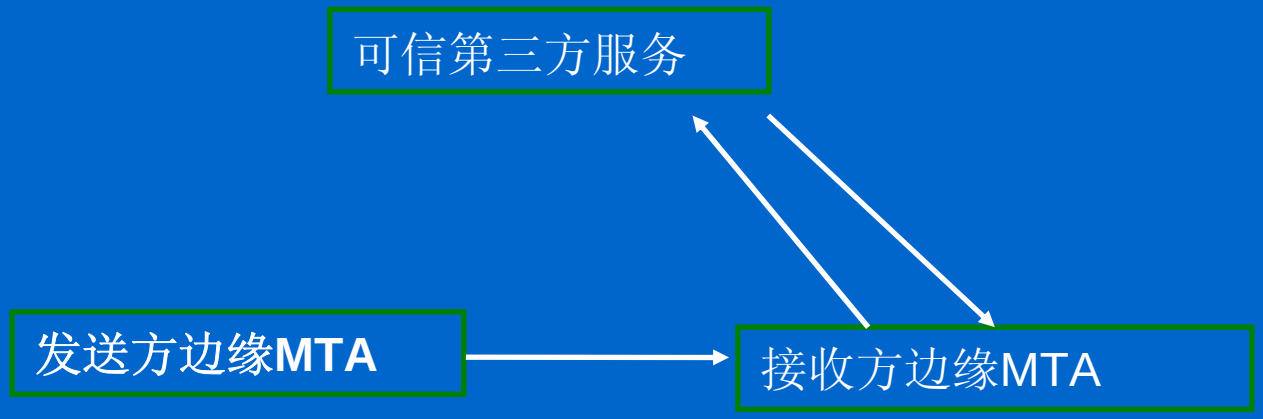
1. 发送者通过发送方邮件服务器发送电子邮件
2. 接收方邮件服务器收到电子邮件
3. 接收方邮件服务器通过电子邮件回复地址，检查哪个域发送该邮件，并检查该域中存放的SPF纪录，接收方邮件服务器确认发送该电子邮件的服务器的IP地址是否在SPF纪录中找得到
4. 如果找得到，则证明是合法邮件，放行。否则，丢弃

反垃圾邮件技术-认证

- ***Sender ID Framework***
  - 在SPF基础上，但在发布SPF纪录和利用SPF纪录判定所接收到的邮件合法性方面做了更多便利的规定，更容易操作。比如允许MUA和MTA利用SPF纪录认证邮件的合法性，帮助管理员发布SPF纪录
  - 该技术已经在Hotmail 和 Sendmail中应用
  - 该技术的缺点和SPF一样
  - 工作原理
    - 域名管理员在域名系统内发布SPF纪录，SPF纪录确认域内合法的邮件服务器
    - 电子邮件接收系统验证收到的邮件是否来自合法的发送方邮件服务器

反垃圾邮件技术-认证

- ***Client SMTP Validation (CSV)***



两个阶段:

1、接收方边缘MTA检查SMTP协商过程中传送的信息，获得发送方电子邮件服务器名字，并通过查询发送方DNS，得到该名字对应的IP地址列表，验证所接收到的电子邮件中，发送方的IP地址是否在列表中。若在其中，则通过验证

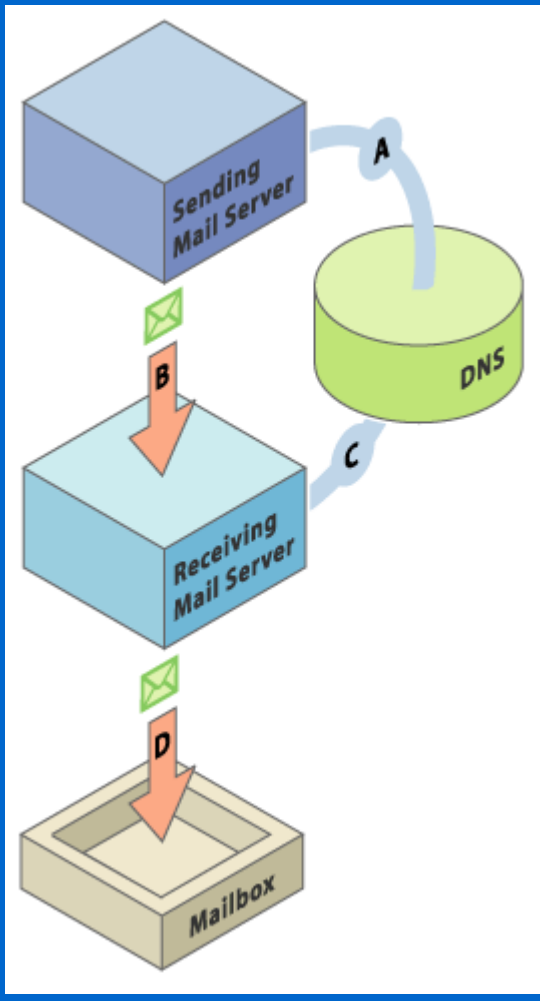
2、接收方边缘MTA可以根据历史积累，自己建立一个信任列表，用来评判后续电子邮件信任度。更好的办法是网络建立可信的第三方服务器，专门提供发送方MTA可信度信息，提供发送方边缘MTA的信任度，供接收方边缘MTA查询和使用。网络管理员有义务向可信第三方提供自己域内可信的MTA。

缺点:

针对的问题和SPF一样，同样的缺点（不能抗邮件内容欺骗）

反垃圾邮件技术-认证

- ***DomainKeys***
  - 雅虎公司提出的一种邮件源头认证技术
  - 能验证邮件发件人是否属于他所声称的邮件域
  - 能保证邮件内容本身的完整性
  - 工作原理:
    - 产生两组钥匙．公钥(public key)和私钥(private key)，公钥将会存放在DNS服务器中，而私钥会存放在寄信服务器中
    - 私钥依附在邮件头中，发送到寄信者的服务器.
    - 收信的服务器，收到夹带在邮件头中的私钥，并在DNS上自己获取公钥．然后进行比对，比较寄信者的域名是否合法，不合法，则很可能是垃圾邮件.

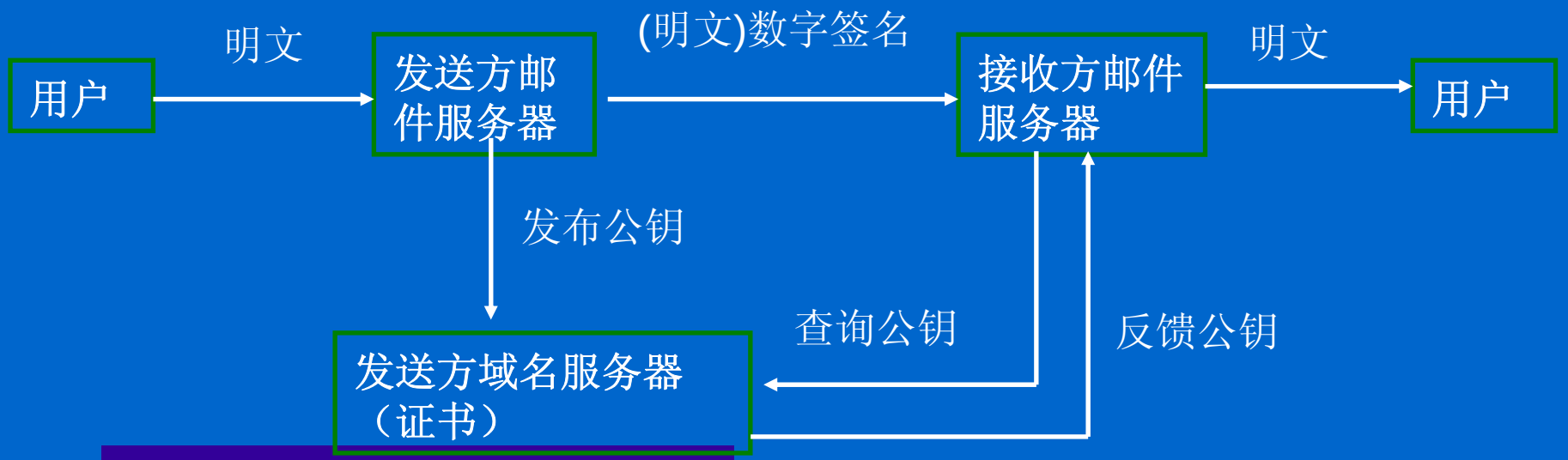


反垃圾邮件技术-认证

- ***Identified Internet Mail (IIM)***
  - 和Domainkeys一样的认证技术，但在密钥管理方面做更多考虑，能够支持域名级和用户级的数字签名。 Domainkeys只提供域名级数字签名
  - 提出Key Registration Server (KRS) 密钥注册服务器来负责公钥证书的管理。通过KRS，可以为日后提供用户级的数字签名提供条件
  - 当用域名级数字签名，并用DNS管理公钥证书，IIM和Domainkeys是一样的

反垃圾邮件技术-认证

- ***DomainKeys Identified Mail (DKIM)*** [RFC 4871]
  - DomainKeys改进协议，结合了DomainKeys和Identified Internet Mail，运作方式基本上与DomainKeys相同
  - Internet-Drafts：
    - draft-ietf-dkim-base-00.txt
    - draft-allman-dkim-ssp-01.txt
    - draft-fenton-dkim-threats-02.txt

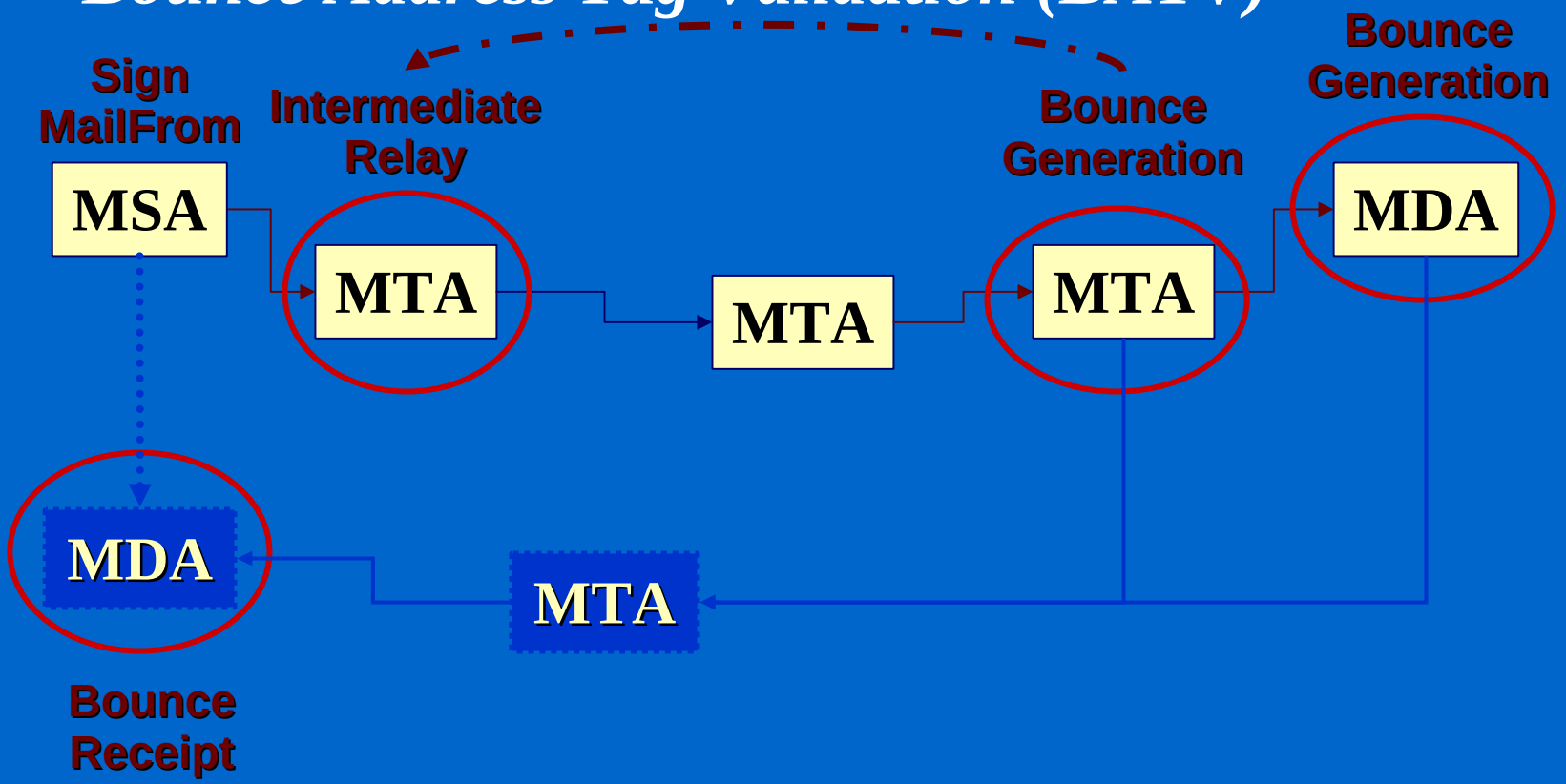


反垃圾邮件技术-认证

- ***Bounce Address Tag Validation (BATV)***
  - 为了对付“发送失败”之类的垃圾邮件或反向散射信息
  - 反弹地址攻击
    - 重定向邮件反馈洪泛：垃圾邮件制造者发送垃圾邮件时，必然包含很多无效的电子邮件地址，发送服务器会收到很多“发送失败”的消息。垃圾邮件发送者为了避免反馈大量的“发送失败”的邮件，必然会采用假的反馈地址
    - 木马：“发送失败”的邮件可能含有木马等有害信息，危害邮件接收者
    - DoS攻击：大量的“发送失败”邮件流会造成邮件接收服务器阻塞

反垃圾邮件技术-认证

- *Bounce Address Tag Validation (BATV)*



反垃圾邮件技术-认证

- ***Bounce Address Tag Validation (BATV)***
  - 接收反馈邮件的代理
    - 判断是否需要将反馈邮件发给用户
    - 采用对称密钥技术
  - 产生反馈邮件的代理
    - 决定是否需要产生反馈邮件
    - 采用公钥技术
  - 对Mail-From地址进行签名（标记）
    - 发送代理对邮件的反馈地址进行签名
    - MAIL FROM mailbox@domain=>
    - MAIL FROM sig-scheme=mailbox/sig-data@domain
  - 对称密钥——用于反馈邮件接收方
    - Sig-data=加密（日期，起始邮件地址）
  - 公钥——用于所有传送点
    - 可以借助DomainKeys 等认证技术

反垃圾邮件技术-其它

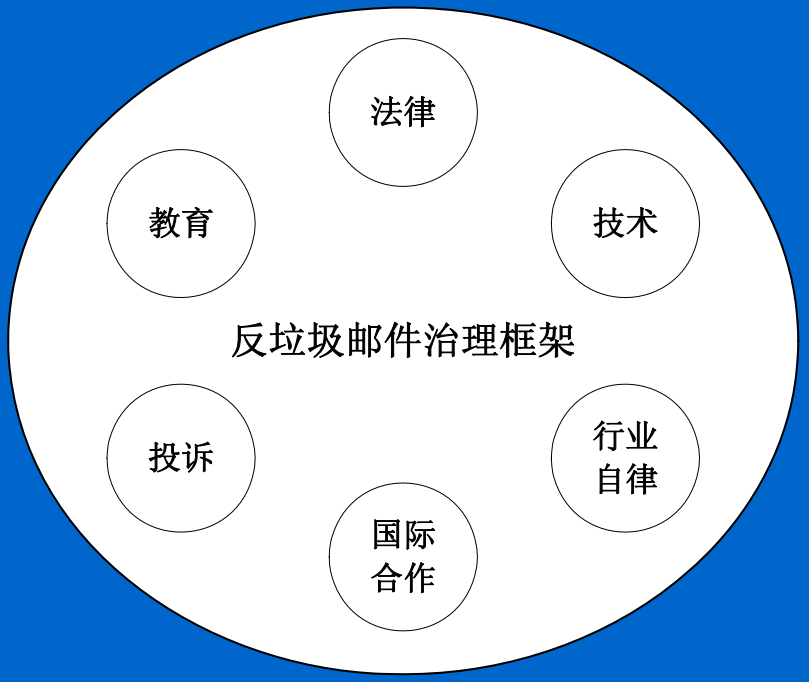
- 关闭开放的中继功能/正确配置中继
- 个人计算机关闭25段口号，改用587端口号
  - 优点：大幅减少垃圾邮件
  - 缺点：用户计算机不能作为服务器使用。限制端到端的服务
- 速度限制（Rate limiting）
  - 邮件服务器限制发送方在一定时间内发送的邮件数量。通过限制速度，并向发送者确认。若获得发送者确认，则是正常邮件。若得不到确认，则可能是计算机染上病毒，自动制造大量垃圾邮件

反垃圾邮件技术-其它

- 监控邮件接收和发送端口，检测大邮件。主要是及时发现异常流量，并采取措施
- 需要遵循以下几个原则：
  - 个人计算机不能安装邮件服务软件
  - 对于包含可执行文件的电子邮件，丢弃
  - 定期对杀毒软件病毒库更新
  - 对于网页服务器或者代理服务器，需要监控运行在上面的Perl、CGI 和其它Scripts程序。这些程序可能被垃圾邮件者利用

反垃圾邮件相关标准-ITU

- ITU-T Q.17/SG17反垃圾信息工作组
  - X.1231 Technical Strategies on Countering Spam
  - X.1240 Technologies involved in countering email spam
  - X.1241 Technical framework for countering email spam



反垃圾邮件相关标准-ITEF

- IETF
  - RFC 2505 Anti-Spam Recommendations for SMTP MTAs
  - RFC 2635 A Set of Guidelines for Mass Unsolicited Mailings and Postings
  - RFC 3685 SIEVE Spamtest and Virustest Extensions
  - RFC 4408 Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1
  - RFC 4686 Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)
  - RFC 4871 DomainKeys Identified Mail (DKIM) Signatures
  - RFC 5016 Requirements for a DomainKeys Identified Mail (DKIM) Signing Practices Protocol

反垃圾邮件相关标准-中国

- CCSA
  - YD/T 1310-2004 《互联网广告电子邮件格式要求》
  - YD/T 1311-2004 《防范互联网垃圾电子邮件技术要求》
    - 垃圾邮件处理系统网络结构
    - 垃圾邮件处理系统参考模型
    - 垃圾邮件处理系统中设备的主要功能
    - 垃圾邮件的主要特征
    - 垃圾邮件判定规则
    - 防范垃圾邮件的主要方法
  - 20079505-T-339 反垃圾信息需求
    - 垃圾邮件
      - 垃圾短信/彩信
      - 垃圾即时消息
      - 垃圾IP电话
    - 垃圾呈现业务
    - 垃圾博客
    - 垃圾新闻消息
    - 垃圾在线游戏

反垃圾邮件相关标准-中国

- MSTL
  - MSTL-JGF-04-013《信息安全技术 反垃圾邮件产品检验规范》
    - 公安部计算机信息系统安全产品质量监督检验中心制定
    - 规范反垃圾邮件客户端产品的安全功能要求和安全保证要求
    - 为办理销售许可证
    - 保证级——EAL2

表 1　信息安全技术 反垃圾邮件客户端产品安全等级划分表

安全功能类	基本要求	增强要求
邮件地址匹配	√	√
关键字匹配	√	√
基于行为识别的过滤功能*	√	√
基于内容学习的过滤功能		√
对垃圾邮件过滤和阻断行为可以进行审计	√	√
垃圾邮件的特征信息可以更新		√
垃圾邮件的过滤强度可设置		√
确保用户信息的安全性	√	√
垃圾邮件过滤动作可设置	√	√
用户配置信息备份和恢复	√	√
管理功能	√	√

a　基本要求：反垃圾邮件（客户端）产品的最低安全要求。

b　增强要求：为进一步提升产品安全功能的附加要求。

* 满足 4.3 中三条以下（包括三条）的为基本级，三条以上为增强级。

反垃圾邮件相关标准-中国

- ISCCC
  - 中国信息安全认证中心《反垃圾邮件产品认证技术规范》
    - 中国信息安全认证中心组织制定，用于产品认证
    - 规定了反垃圾邮件产品的技术要求和测试评价方法

4 安全功能要求
- 4.1 静态黑白名单
- 4.2 实时黑名单
- 4.3 邮件连接地址过滤
- 4.4 邮件内容扫描过滤
- 4.5 动态限制
- 4.6 虚假路由邮件限制
- 4.7 自学习功能
- 4.8 邮件处理
- 4.9 日志功能
- 4.10 升级管理
- 4.11 配置管理

5 自身安全要求
- 5.1 审计数据生成
- 5.2 身份鉴别
- 5.3 用户角色
- 5.4 远程会话保护

6 性能要求
- 6.1 识别率
- 6.2 误报率
- 6.3 最大并发连接数
- 6.4 平均响应时间

7 保证要求
- 7.1 配置管理
- 7.2 交付与运行
- 7.3 指导性文档
- 7.4 测试
- 7.5 脆弱性评定
- 7.6 生命周期支持

8 测评方法
- 8.1 测试环境与工具
- 8.2 安全功能测试
- 8.3 自身安全测试
- 8.4 性能测试
- 8.5 产品保证测试

反垃圾邮件相关研究组织

- Anti-Phishing Working Group
- Authentication and Online Trust Alliance
- Contact Network of Spam Authorities (CNSA)
- Digital PhishNet
- Email Sender and Provider Coalition
- Institute for Spam and Internet Public Policy (ISIPP)
- London Action Plan
- Messaging Anti-Abuse Working Group (MAAWG)
- Spamhaus
- Stop Spam Alliance
- Trusted Electronic Communications Forum (TECF)

具体各个组织的介绍参见ITU-T X.1240

谢 谢！

Email:hyf@cert.org.cn