防范垃圾邮件安全机制

杨晓雪

（武汉软件工程职业学院，湖北 武汉 430000）

摘 要：防范垃圾邮件除可保护邮件传输的安全外，还可保护邮件服务器的安全。除一般的服务器安全配置与防护外，更要加强邮件服务器抵御邮件攻击、垃圾邮件和病毒邮件的能力。

关键词：垃圾邮件；防范；安全机制

中图分类号：TP393.098 **文献标识码：**A **文章编号：**1003-9767（2015）08-083-02

1 垃圾邮件的特征

垃圾邮件 SPAM，又称“不请自来的商业电子邮件”。垃圾邮件主要由以下的一个或多个特征：邮件内隐藏有病毒、木马等破坏性程序，或者含有大量广告甚至色情图片，反动信息；收件人无法拒绝收取邮件，邮件自动打开；邮件看不到发件人，或者发件人为虚假信息；内容篡改、伪造或者篡改发件人。

在实际当中，垃圾邮件的特征是根据环境和应用场景而言的，没有统一的标准，通常具有一个或多个特征，用户使用免费邮箱防范垃圾邮件的效果不良，甚至某些免费邮箱就是垃圾邮件的制造方，垃圾邮件的发送者轻松通过多种途径获得用户的邮件地址，如穷举、猜测和自动收集程序等。人们在上网的过程中也不可避免的要对外公布自己的邮箱地址，一些人便收集这些信息后出售。

2 垃圾邮件的危害

垃圾邮件的泛滥已经让互联网不堪重负，垃圾邮件的负面影响主要由以下几个方面。

2.1 占用网络资源

数量众多的垃圾邮件会占用服务器存储空间，上传下载垃圾有限会占用网络带宽，影响网络服务形象。如果使用邮件服务器发送垃圾邮件，邮件服务器在互连网上会被列入黑名单，影响甚至破坏服务器对外提供正常的服务。所以对于邮件服务器而言，要在内外两个方向上防范垃圾邮件。

2.2 暴露隐私

如果邮箱收到大量垃圾邮件的时候，第一反应就是，自己的邮件地址不安全了，很可能被出卖了。另外，下载和处理这些邮件会耗费收件人大量的时间、精力和金钱。当大量垃圾邮件充满邮箱的时候，会导致正常的邮件无法接收，影响工作的正常进行。

2.3 被黑客利用，成为攻击工具

黑客把病毒和恶意代码隐藏在垃圾邮件中，用户一旦打开这些邮件，就会激活隐藏的病毒或木马程序，不仅危害用户自己的计算机，更有可能被利用成为病毒的传播中介。另外，黑客还会利用邮件系统对目标主机发起垃圾邮件攻击，占用服务器资源，导致当机。

2.4 传播负面信息

一些别有用心的人会利用垃圾邮件向广大群众传播色情反动的信息，在社会上兴风作浪，尤其对未成年人，影响更大。

3 垃圾邮件的防范措施

为了减少垃圾邮件带来的危害，就需要借助和综合运用各种技术手段来防范垃圾邮件的传播，一开始我们只能通过将收到垃圾邮件的地址被动的设置到收件黑名单，到现在的使用智能信息过滤技术，自动过滤掉符合垃圾邮件特征的邮件。再到目前的多种组合算法，反垃圾邮件技术经历了一个不断发展完善的过程，已经抵御

作者简介：杨晓雪（1982-），女，湖北武汉人，硕士，讲师。研究方向：网络安全。

了一大部分垃圾邮件的侵害。目前存在的反垃圾邮件技术主要有以下几种。

3.1 IP 阻断列表与黑白名单技术

这种封禁技术是将那些垃圾邮件服务器的 1P 地址（通过技术或人工手段确认的）列入一个黑名单（Black List），通过定期或实时发布这种黑名单，并提供黑名单查询服务，让合法的邮件服务器知道应当拒收哪些邮件源所发来的邮件。白名单（White List）是一个可信任的邮件服务器 IP 地址的列表。

现在有很多组织都在做垃圾邮件的黑白名单，比如 Spamhaus、Barracuda 等。如果给国外朋友发邮件后收到了有如下内容的退信：554 Scr vi ce unavailable;Client host[rmil.dormin.cdu.cn] blocked using Barracuda Reputation。

3.2 评分过滤器计算邮件垃圾邮件的可能性及概率

它首先对正常的邮件和垃圾邮件进行分类，提取它们的特征值，学习两种邮件的特征，对每个特征值进行给分，正常邮件和垃圾邮件的特征值和分数都各自有特点。如果收到一个邮件，就对其提取特征值，用之前学习到的特征值和分数对其进行赋分。在垃圾邮件中出现特征串赋予一个正分数，如果在正常邮件中也检测到了这个特征串，就赋予一个负分数，用来降低得分，最后根据总分来判断其偏属于哪个类别，是正常邮件还是垃圾邮件。贝叶斯算法计算的特征值通常来自：邮件的内容单词；邮件的发送者和传输路径等；其他的附加信息如附加网页等；Meta 信息，比如特殊短语出现位置等。通过不断的分析，过滤器也自我更新，这样贝叶斯过滤器就有了自适应能力。另外，用户也可以手工操作，以适应一些临时出现的特殊情况。

基于过滤器原理的反垃圾邮件系统也有其局限性。目前垃圾邮件的发送工具也不是静态的，它们会很快适应过滤器，并通过一些技术手段绕过过滤器，如改变拼写和插入句子等。另外还有误报问题，把正常邮件当做垃圾邮件来处理。

还有一种近年来用得比较多的“基于行为模式识别模型”垃圾邮件识别方法，该方法利用概率统计数学模型对垃圾邮件进行判定。这种方法的特点是，在分析时不单单对其邮件内容本身进行判定，还会对与邮件相关的各类因素综合进行判定。这些相关的因素有发送邮件的时间、频率、身份验证等等。

4 结 语

反垃圾邮件的方法不仅仅局限于以上介绍的两种，在互连网应用当中通常综合运用各类方法来防范垃圾邮件的干扰，目前的技术尚不能 100% 自动防御垃圾邮件，常有误判、漏判事件发生，在垃圾邮件的防范问题上仍是一个重要的技术课题。

参考文献

[1] 王斌，潘文锋 . 基于内容的垃圾邮件过滤技术综述 [J]. 中文信息学报，2005（5）：19-21.

[2] 郑炜，沈文，张英鹏 . 基于改进朴素贝叶斯算法的垃圾邮件过滤器的研究 [J]. 西北工业大学学报，2010（3）：12-13.

[3] 张玉红，徐旸 . 治理垃圾邮件的有效途径 [J]. 哈尔滨工业大学学报，2005（8）：24-26.