第 3 卷◆第 1 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

综合多种技术构建高效垃圾邮件防御体系的研究

李剑飞
福建省莆田市城厢区财政局
DOI:10.12238/acair.v3i1.11872

[摘　要] 在互联网快速发展的背景下,垃圾邮件问题日渐严峻,为企业和个人造成严重困扰。本文基于此,探讨构建高效垃圾邮件防御体系的措施,重点介绍关键字绑定技术、回馈流量控制法,旨在结合应用上述两种方法显著提升识别与拦截垃圾邮件的能力,保证邮件系统安全与稳定。
[关键词] 垃圾邮件；技术拦截；邮件安全；邮件防御
中图分类号：F618.1　文献标识码：A

Research on Building an Efficient Junk Email Defense System by Integrating Multiple Technologies

Jianfei Li
Finance Bureau of Chengxiang District, Putian City, Fujian Province

[Absrtact] With the rapid development of the Internet, the problem of spam has become increasingly serious, causing serious problems for enterprises and individuals. Based on this, this article explores measures to build an efficient spam defense system, with a focus on keyword binding technology and feedback traffic control methods. The aim is to significantly improve the ability to identify and intercept spam by combining the above two methods, ensuring the security and stability of the email system.
[Key words] spam; Technical interception; Email security; Email Defense

伴随着互联网技术推进并融入人们的日常工作和生活,电子邮件已经成为人们沟通和交流的重要通信工具。但是,由于隐私信息保护不当、数据信息泄漏等原因,导致垃圾邮件问题日益严重,为个人用户和企业机构带来困扰[1]。垃圾邮件占用大量存储空间,甚至携带钓鱼链接、恶意软件等,对网络安全和个人信息安全产生严重危害。由此,构建高效、健全的垃圾邮件防御体系十分关键。

1 邮件安全现状

邮箱是内外部交流与商务沟通的重要工具,经常会在商务及日常工作中通过邮件进行信息数据的传递,这其中不乏有客户信息、财务数据、产品参数、核心代码等敏感数据,一旦这些信息被盗取、泄露,将导致企业或者个人在公众的威信和信任度下降,严重的将直接造成巨额经济财产损失。正是因为邮件数据价值高且储存较为集中,加之安全意识薄弱,防护能力低下等特点,便成为了黑客及不法分子瞄准的目标,这也是邮件被频繁攻击的主要原因。在公共网络或网络安全性较差的环境中使用电子邮件,黑客能够轻易的入侵到wifi等联网设备并监控网络流量,如果收发邮件没有加密或者使用SSL的简单信道加密,黑客可窃取电子邮件数据包,并通过简单的技术手段还原邮件正文和附件。犯罪分子一旦掌握了来往邮件信息,通过对邮箱内来往邮件地分析,了解邮箱持有者与相关人员的业务往来情况,随时都有可能发动诈骗攻击,同时也存在商业机密被剽窃的风险。商务密邮利用加密客户端对邮件数据进行加密保护后发出,确保“一邮一密”从源头上控制信息外泄,当数据经过wifi或其他中介服务时,数据均保持密文形式,用户无需担心数据拦截引发的数据泄露。

2 关键字绑定技术

2.1明文关键字绑定

作为最为基础的关键字绑定技术,明文关键字绑定是在收件人邮箱地址后添加特定后缀,从而放行邮件,例如“ever@gmail.com|123456”。当收件服务器接收邮件时,会对收件地址中是否包含关键字进行检查,若包含则默认邮件合法,给予放行。明文关键字绑定技术操作简单,不必使用任何形式的复杂验证,在某些场景下极为实用。但是,由于关键字以明文的方式显示,容易被垃圾邮件发送者抄袭并伪造,增加安全隐患。垃圾邮件发送者在掌握合法关键字后,会使用明文关键字绕过检查系统发送垃圾邮件[2]。用户在使用明文关键字技术时应时刻保持谨慎,或可以与其他技术手段相结合。

2.2 Captcha图片测试绑定

为补足关键字绑定技术存在的缺陷,Captcha图片测试绑定

技术应运而生。Captcha(CompletelyAutomatedPublicTuringtesttotellComputersandHumansApart)多表现为一张包含有图案或者扭曲文字的图片,是要求用户输入图片中的图案或者文字完成真人身份验证,区分用户是否为人类。在Captcha图片测试绑定技术支持下,邮件发送方在发送邮件之前,应通过系统自动生成的特定关键字、图片测试,并将关键字与邮箱地址相结合,ever@gmail.com#http://captcha.com这个表示发件人发邮件时,要向http://captcha.com申请captcha图片测试挑战,通过之后,captcha.com网站会释出绑定的关键字,如123456,收件服务器会预先准备好,以接纳发往ever@gmail.com#123456的邮件。发件人在发邮件的时候,使用新收件地址,待收件服务器在接收到邮件后,会对其地址中是否包含准确的关键字展开校查。如果包含且关键字是通过Captcha图片测试获得的,则默认该邮件是合法的,予以放行。Captcha图片测试绑定技术在使用中,可加大垃圾邮件发送者的邮件发送难度,实现垃圾邮件防御体系安全性提升的目标。但是,这种处理方法在具体应用中同样存在不足,即Captcha图片测试会增加正常用户的困扰和不便。另外,在计算机技术更迭的支持下,部分高等级自动化工具已经可以破解简单的Captcha图片测试,绕过防御机制。所以,用户使用Captcha图片测试绑定技术时,要适当性的选择合适的Captcha图片测试难度和更新频率[3]。

2.3动态字符串绑定

动态字符绑定技术相对于前两种技术而言更为先进,在发件人和收件服务器之间构建共享的秘密(即原始字符串),并与发件时间等信息相结合,生成动态结果串,经过类似2-factorauthenticator的运算,形成123456的结果动态串,然后发件时,收件服务器据此做过滤运算审查,通过的,则予以放行。发件人应用动态字符串绑定技术中,要在邮件发送前与收件服务器进行一定的交互操作,获得当前有效的动态结果串。邮件发送者在实施交互操作时,可采取基于密码学的挑战-应答协议等多种方式实现。一旦发件人成功得到动态结果串,其便采用这个结果串构造邮件收件地址,并传输到接收服务器。收件服务器在接收到邮件信息后,会快速检查是否包含有正确的动态结果串,若是包含则放行。动态字符串绑定技术通过引入时间因素,可进一步强化安全性能,避免垃圾邮件发送者预测或者伪造有效的收件地址。由于动态结果串处于不断变化的状态,所以即使是某个被破解或者泄漏,也不会大规模影响整个垃圾邮件的防御体系[4]。

3 回馈流量控制法

3.1限流机制

在回流控制法技术支持下,邮件服务器构建智能识别和反馈机制,即当某个邮件服务器(如C服务器)识别来自上游服务器(如A服务器)的垃圾邮件时,会即刻向该上游服务器的直接下游服务器(如B服务器)发送包含垃圾邮件的来源信息、垃圾邮件的特征及建议的限流措施等限流指令。B服务器在接收到限流指令后,按照指令中的建议控制A服务器邮件的接收速率、增加邮件审查力度,甚至暂停接收A服务器的邮件。B服务器还会继续传递限流指令到上游服务器(如A服务器的上游服务器),形成逐级反馈的限流网络。整个邮件传输链条上的服务器都能参与到垃圾邮件防御中,共同构建强大的垃圾邮件防御体系。此限流机制并非一成不变,会根据垃圾邮件的特征、来源及传播趋势等因素动态调整。例如,某个服务器频繁发送垃圾邮件时,上游服务器会对其采取更严格的限流措施；当该服务器减少或停止发送垃圾邮件时,上游服务器也会相应放宽限流措施。

3.2限流程度调整

在回馈流量控制法中,限流程度的调整是垃圾邮件防御体系的核心环节,直接影响其效果和稳定性。因此,必须依据垃圾邮件的比例、来源、特征及传播趋势,对限流程度进行科学测算与动态优化。

具体调整原则如下：首先,根据垃圾邮件比例,对高比例发送垃圾邮件的服务器采取严格限流,低比例时则适当放宽。其次,考虑垃圾邮件特征,对危害更大的类型,如含恶意链接或病毒的邮件,实施更严格的限流。再者,依据传播趋势,对突然大量发送垃圾邮件的服务器迅速采取严格限流,传播得到遏制时则适当放宽。在实施调整时,需注意避免误伤正常用户,不断完善识别算法和限流机制,确保其准确性和稳定性[5]。同时,限流程度应随垃圾邮件传播趋势和防御效果动态优化,定期评估并调整限流措施。

4 综合应用与效果评估

4.1具体措施与实施过程

回馈流量控制法的融合实施侧重流量监控与分析,实时监测邮件服务器入站和出站流量,识别异常模式,设定阈值动态调整策略。根据监控结果,自动调整邮件处理策略,平衡审查与邮件延迟,维护邮件系统流畅与安全。对于确认的垃圾邮件来源,实时更新黑名单并回馈至前端过滤系统,建立白名单机制保护信任邮件。

在综合防御体系的深度集成与优化过程中,关键字绑定技术与回馈流量控制法无缝融入邮件服务器过滤系统,成为提升安全防护效能的关键一环。设计的API接口或高效中间件技术,实现防御体系内各组件间的数据共享与实时通信,即时传递与处理信息。为持续保持防御体系的高效与适应性,定期全面回顾与分析防御体系数据至关重要。细致评估过往防御效果,并根据最新安全威胁趋势灵活调整流量监控阈值及处理策略参数,使防御体系始终紧跟安全威胁变化,达到最佳防御效果。开展安全培训、模拟攻击演练等形式多样的用户教育活动,让用户更好地理解安全威胁,掌握基本防御技能。鼓励用户积极报告实际使用中遇到的误判或漏判案例,这些反馈信息将被用于不断优化防御体系的算法与规则,形成闭环改进机制。

4.2优势

在增强安全性上,回馈流量控制法发挥重要作用。该方法实时监控邮件服务器入站和出站流量,迅速识别异常流量模式,如

短时间内大量相似邮件爆发性增长,这通常是垃圾邮件攻击的前兆。设定合理阈值和动态调整策略,系统能对超出正常范围流量进行及时限制或隔离,有效防御大规模垃圾邮件攻击,保护邮件系统稳定运行,降低潜在安全风险。

面对不断变化的垃圾邮件攻击手段和邮件量波动,体系动态调整机制能根据实际情况灵活应对。无论攻击强度增加还是邮件量激增,系统都能自动调整流量监控阈值及处理策略参数,确保在不同情境下保持高效防御,为用户提供持续稳定邮件服务。

4.3效果评估

在实际测试阶段,精心选择部分用户进行小范围测试至关重要。这一步骤允许在不影响大部分用户前提下,收集数据和反馈。测试期间,评估防御体系的初步效果,重点关注垃圾邮件拦截率、用户满意度及系统资源占用等指标。这些数据提供防御体系性能的第一手信息,有助于后续针对性优化。持续跟踪并记录防御体系运行数据,包括每日拦截的垃圾邮件数量、误判率及用户反馈次数等。这些数据整理成详细报告,使我们能清晰了解防御体系整体表现及存在问题。定期分析报告,能发现防御体系中的薄弱环节,为后续优化提供指导。基于数据分析结果,定期调整防御策略,以适应不断变化的垃圾邮件攻击手段。这包括更新关键词库频率、调整流量监控阈值设置等。深知只有不断进行优化,才能提升防御体系的有效性。同时,引入A/B测试等方法,对比不同策略效果,科学指导优化方向。这种方法允许在实际环境中测试不同策略表现,从而选择最优方案。建立高效用户反馈处理机制,对用户报告的误判、漏判案例进行快速响应。这既解决用户问题,也提供宝贵改进意见。将用户反馈视为对防御体系的直接评价,并据此进行针对性优化。

5 结语

本文围绕垃圾邮件防御体系,重点讨论限流程度调整与综合应用、效果评估两大方面。在限流程度调整中,强调科学测算与动态优化,依据垃圾邮件比例、特征、来源及传播趋势灵活调整,注重避免误伤正常用户。综合应用方面,深入阐述关键字绑定技术与回馈流量控制法的实施过程与优势,包括构建智能关键词库、语义与上下文分析、建立个人行为模式、实时流量监控与分析等。效果评估部分,涵盖实际测试、数据统计、持续优化及用户反馈循环等环节,保障防御体系的有效性与稳定性。整体而言,本文提出的垃圾邮件防御体系,综合运用多种技术与策略,实现对垃圾邮件的高效识别与拦截,保障邮件系统流畅与安全,提升用户信任度与满意度。未来,将持续优化防御体系,应对不断变化的垃圾邮件攻击手段。

[参考文献]

[1]付晶.计算机网络技术与信息安全分析[J].集成电路应用,2022,39(06):168-169.

[2]赵宇轩.基于CNN的异常邮件检测技术研究与实现[D].中国电子科技集团公司电子科学研究院,2022.

[3]车敏贤.CM公司企业邮件系统产品营销调研报告[D].华南理工大学,2021.

[4]杨言.互联网域间路由劫持及其防御研究[D].清华大学,2020.

[5]任永琼,季文文.人工智能在计算机网络技术中的应用分析[J].数字技术与应用,2020,38(05):102-103.

作者简介：

李剑飞(1975--),男,汉族,福建省莆田市人,大学本科,助理工程师,会计师,经济师。