电子邮件的安全问题研究电子商务师考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E7_94_B5_E5_AD_90_E9_82_AE_E4_c40_645569.htm 随着互联网的迅速发展和普及，使得通过为一大群顾客和供应商提供一个通用通讯环境的方法可以发挥电子商务的独一无二的潜力。今天，网上有数以千计的面向消费者和面向交易的商务站点，并且这个数目正在快速增长。电子商务成为世界新热点,但其安全性也随着信息化的深入也随之要求愈高了。电子邮件系统的发展面临着机密泄漏、信息欺骗、病毒侵扰、垃圾邮件等诸多安全问题的困扰。人们对电子邮件系统和服务的要求日渐提高，电子邮件系统的安全问题也越来越得到使用者的重视，如果没有采取安全措施,得到的信息就可能被别人破坏过,电子商务往来就不能正常运行。 一、电子邮件系统安全问题研究的必要性 电子邮件系统的功能是办公自动化系统的基本需求，是企业网络的基本应用之一，为企业进行信息交流提供了有力支持。安全的电子邮件系统有效地解决了信息保密，信息完整、身份鉴别，以及密钥的安全存储等问题，安全的电子邮件系统在各行业中的应用和推广，将给相关企业在商业秘密、客户资料、产品研发资料、金融资料、交易谈判、市场与产品计划、财务资料等方面的数据交换提供安全保障。 对于企业和政府用户而言，安全的电子邮件系统为系统用户的身份鉴别，企业商业信息和政府公务文件的收发、传输和存储提供了有效的安全保障，简化了工作流程，提高了工作效率；安全的电子邮件系统提供的强大易用的管理功能，有效地整合了企业内各个组织机构的沟通和管理，实现了

企业机构的一体化管理，提高了管理水平和效率。因此，安全的电子邮件系统在企业信息化建设的深化中，将发挥巨大的推动作用，并获得更多的企业和政府机构用户，在企业信息化和电子商务中赢得可观的市场份额。 二、电子商务中电子邮件面临的安全性问题及解决 1.电子商务中电子邮件面临的安全性问题 电子商务中电子邮件往来将会遇到以下几方面的问题：电子邮件系统的安全漏洞、电子邮件系统的威胁和欺骗、电子邮件系统垃圾、电子邮件系统炸弹、电子邮件系统有关的病毒、匿名转发等等。 2.解决电子商务中电子邮件安全问题的主要技术 (1)防火墙技术 防火墙是位于内部网络或Web站点与Internet之间的一个路由器或一台计算机(堡垒主机),可以使内部网可以与Internet联结又保护内部网免遭外界非法访问。防火墙建立在一个服务器/主机上,是一个多边协议路由器,在通常的配置中,堡垒主机经常作为一个公共的Web服务器,或者FTP服务器,或一个电子邮件服务器使用。通过堡垒主机上进行Http服务器软件,要使用“ 代理 ”服务器,以访问防火墙的另一端的Web服务器。 利用防火墙可以加强安全性合理配置防火墙,可以限制邮件的访问,使之只能发送到有限的几个机器上,并加强对这几个机器的防范,可以将这些机器作为竟如内部网络的网关来控制邮件的出入。因此,用防火墙可所有外部的SMTP联结到一个电子邮件服务器上,这样会有一个集中登录地点,便于追踪不正常的电子邮件,但是防火墙不能识别恶意的Applet和脚本。 (2)PGP加密算法 从本质上来讲,最有效的保护电子邮件系统方法是使用加密签字来验证电子邮件系统信息,通过验证,保证信息确实来自发信任,并且来保证电子邮件系统在传输的过程中没有被修改。最常用的是PGP加密

算法。 利用PGP的数字签字签名可以实现保证电子邮件不被冒发或修改过。PGP对电子邮件的内容计算后得出一个128位的二进制作为描述电子邮件的特征值。如果邮件被改动,这个特征值就不符合邮件的内容。 (3)电子邮件系统炸弹的处理 预防垃圾邮件的方法对电子邮件系统炸弹毫无作用，因为电子邮件系统炸弹发送时,攻击软件会自动的修改发送的地址(Fake IP),这样你收到的电子邮件的发信地址根本就是不存在的,或随时变化的,所以无法提前防范,也不可能根据发信地址追查扔炸弹的人。防治电子邮件系统炸弹的方法是进入一种排斥模式，排斥模式需要你检查收到邮件的源地址。如果发现一个站点,它的用户在用电子邮件站点攻击你,那么你就可以和他们系统管理员联系。 (4)防范电子邮件系统的威胁和欺骗 由于简单的邮件传输协议(SMIP)不能验证系统伪造的电子邮件。如果站点允许与SMIP端口联系,任何人都可以与该端口联系,并且以你虚构某人的名义发出电子邮件。应该经常查看电子邮件的错误信息,这里经常会有闯入者的线索，查看电子邮件信息的表头,它们通常会记录电子邮件到达目的地址前经过的所有“ 跳跃 ”或短暂的停留。应该注意到表头中诸如“ 接到 ”和“ 信息-ID ”信息,并且有电子邮件的发出/收到记录比较,看它们是否响应。 (5)电子邮件系统垃圾的处理 电子邮件系统垃圾已经成为人们最头疼的问题之一,下面介绍几种常见的防垃圾邮件技术。 ①SMTP用户认证 目前常见并十分有效的方法是，在邮件传送代理(Mail Transport Agent，MTA)上对来自本地网络以外的互联网的发信用户进行SMTP认证，仅允许通过认证的用户进行远程转发。这样既能够有效避免电子邮件传送代理服务器为垃圾邮件发送者所利用，又为出差在外或在

家工作的员工提供了便利。如果不采取SMTP认证，则在不牺牲安全的前提下，设立面向互联网的Web邮件网关也是可行的。 ②逆向名字解析 认证的目的都是避免电子邮件传送代理服务器被垃圾邮件发送者所利用，但对于发送到本地的垃圾邮件仍然无可奈何。要解决这个问题，最简单有效的方法是对发送者的IP地址进行逆向名字解析。通过DNS查询来判断发送者的IP与其声称的名字是否一致，如不一致则予以拒收。这种方法可以有效过滤掉来自动态IP的垃圾邮件，对于某些使用动态域名的发送者，也可以根据实际情况进行屏蔽。但是上面这种方法对于借助Open Relay的垃圾邮件依然无效。对此，更进一步的技术是假设合法的用户只使用本域具有合法互联网名称的邮件传送代理服务器发送电子邮件。但是，逆向名字解析需要进行大量的DNS查询。 ③实时黑名单过滤 以上介绍的防范措施对使用自身合法的域名的垃圾邮件仍然无效。对此比较有效的方法就是使用黑名单服务了。黑名单服务是基于用户投诉和采样积累而建立的、由域名或IP组成的数据库，最著名的是RBL、DCC和Razor等，这些数据库保存了频繁发送垃圾邮件的主机名字或IP地址，供MTA进行实时查询以决定是否拒收相应的邮件。然而，目前各种黑名单数据库难以保证其正确性和及时性。 ④内容过滤 即使使用了前面诸多环节中的技术，仍然会有相当一部分垃圾邮件漏网。对此情况，目前最有效的方法是基于邮件标题或正文的内容过滤。其中比较简单的方法是，结合内容扫描引擎，根据垃圾邮件的常用标题语、垃圾邮件受益者的姓名、电话号码、Web地址等信息进行过滤。更加复杂但同时更具智能性的方法是，基于贝叶斯概率理论的统计方法所进行的内容过滤

。内容过滤是以上所有各种方法中耗费计算资源最多的，在电子邮件流量较大的场合，需要配合高性能服务器使用。 ⑤关键字 将一些会在垃圾邮件中经常出现的字符(如：广告、化妆品、发票等)收集起来形成一个大的数据库，当一封电子邮件到来的时候能够对信头、信标题、主题和信体等几部分进行检查，看是否里面有数据库中的字符，如果有就被认为是垃圾邮件，如果没有就判断不是垃圾邮件。主要采用的技术是关键词匹配。 ⑥IP黑/白名单 将经常向你发垃圾邮件的IP地址添加到IP黑名单中，当再从同样的IP地址发来信件都被判定为垃圾邮件。如果IP地址被加入到白名单中，则认为从那里来的任何电子邮件都不是垃圾邮件。后来出现的拒绝发件人、拒绝目的地域也都是类似的技术。 三、结论 通过安全的电子邮件系统，可以把企业尤其是跨地域的大中型企业的所有组织机构安全有效地联系起来，实现企业管理的一体化，提高企业的管理水平和效率，加强企业的市场应变能力，提高企业的整体经济效益，从而促进企业信息化建设的进一步发展。 