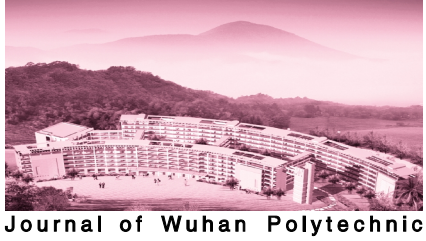

Journal of Wuhan Polytechnic

基于 POSTFIX 的安全电子邮件系统设计与实现

吴　颖

（武汉职业技术学院 艺术设计学院，湖北 武汉 430074）

摘　要：分析了基本的邮件安全技术，以及包括三员分离、密级标示和流向控制在内的安全电子邮件管理技术，最后基于 Postfix 邮件系统开发一套安全电子邮件系统。

关键词：安全电子邮件；Postfix；密级；分级保护

中图分类号：F507.454　　文献标识码：A　　文章编号：1671-931X（2012）05-0073-04

一、概述

电子邮件是互联网的基础应用，但其在传输中使用的基本协议——SMTP 协议不提供加密服务，攻击者可在邮件传输中截获数据或者伪造邮件，电子邮件系统面临安全风险。尤其在党政机关和企业中，许多重要的敏感信息通过邮件系统进行传输，出于对信息安全保密的要求越来越高，需要实现安全的电子邮件系统以满足需求。现在，很多安全领域的技术都应用到电子邮件系统中，例如 PKI 技术、SSL、PGP 和 S/MIME 技术等，解决邮件的加密传输、验证发送者的身份验证、错发用户的收件无效（因为需要用密钥解密）等问题，这些技术提高了电子邮件系统的安全性。但安全是“三分技术、七分管理”，关于电子邮件的安全保密管理容易被忽略，在信息系统等级保护和分级保护中，对电子邮件的保密管理做出了要求。

本文以 Postfix 开源邮件系统为蓝本，分析总结安全电子邮件基本技术手段，在这些基础的安全技术之上，进行扩展和开发，增加“三员分离”、密级标示和流向控制等安全管理手段，实现真正的全方位的安全邮件，满足对安全有严格要求的党政机关和企业的需求。

二、基本电子邮件的安全分析

（一）电子邮件协议概述

1982 年，RFC 822《APRAInternet 文本信息格式标准》成为电子邮件的标准格式，1996 年又发布了 RFC 2045-2049 规定了 MIME 编码格式，使电子邮件系统也可以发送非文本信息。SMTP 协议的最新版本是 RFC 2821，定义了邮件信封格式，邮件信封包含传输和发送邮件所需的信息，收件人不会看到邮件信封，因为它是由邮件传输进程生成的，不是邮件内容的一部分。邮件内容由邮件头（头字段的集合）和邮件正文组成，邮件内容的格式规范的最新版本是 RFC 2822。

一个完整的电子邮件系统主要由用户代理 MUA（Mail User Agent）、邮件传输代理 MTA（Mail Transfer Agent）以及邮件投递代理 MDA（Mail Delivery Agent）组成。MUA 指用于收发 Mail 的程

收稿日期：2012-06-05

作者简介：吴颖（1977-），女，湖北武汉人，武汉职业技术学院教师，研究方向：动画制作技术及计算机技术。

序，MTA 指将来自 MUA 的信件转发给指定用户的程序，MDA 就是将 MTA 接收的信件依照信件的流向（送到哪里）将该信件放置到本机账户下的邮件文件中（收件箱），当用户从 MUA 中发送一份邮件时，该邮件会被发送到 MTA，而后在一系列 MTA 中转发，直到它到达最终发送目标为止。

（二）SASL 认证协议

基本的 SMTP 协议没有验证用户身份的能力。虽然信封上的寄件人地址已经隐含了发信者的身份，但由于信封地址实在太容易假造，为了判断客户端是否有权使用转发服务，服务器端必须确认客户端（寄件人）是否当真是对方所自称的那个人。RFC 2554“smtp service extension for authentication”制定了如何在基本 SMTP 协议上增加验证功能的机制，此机制使得 SMTP 能使用 SASL 协议来验证客户端身份。SASL（Simple Authentication Security Layer）简单认证安全层是用于加强或增加 SMTP 这类协议的一种通用方法。SASL 验证机制规范 client 与 server 之间的应答过程以及传输内容的编码方法，SASL 验证架构决定服务器本身如何存储客户端的身份证书以及如何核验客户端提供的密码。如果客户端能成功通过验证，服务器端就能确定用户的身份，并借此决定用户具有怎样的权限。

（三）端到端安全电子邮件 PGP 和 S/MIME

端到端的安全电子邮件技术，保证邮件从被发出到被接收的整个过程中，内容保密、无法修改、不可否认。现有两套成型的端到端安全电子邮件标准：PGP 和 S/MIME。

PGP 是 Pretty Good Privacy 的简称，其特点是通过单向散列算法对邮件内容进行签名，以保证信件内容无法修改，使用公钥和私钥技术保证邮件内容保密且不可否认。发信人与收信人的公钥都分布在公开的地方，如 FTP 站点，而公钥本身的权威性则可以由第三方、特别是收信人所熟悉或信任的第三方进行签名认证，没有统一的集中的机构进行公钥/私钥的签发。即在 PGP 系统中，信任是双方之间的直接关系，或是通过第三者、第四者的间接关系，但任意两方之间都是对等的，整个信任关系构成网状结构。

S/MIME 是 Secure Multi-Part Intermail Mail Extension 的简称。S/MIME 也是利用单向散列算法和公钥与私钥的加密体系。与 PGP 不同的主要有两点：首先，它的认证机制依赖于层次结构的证书认证机构，所有下一级的组织和个人的证书由上一级的组织负责认证，而最上一级的组织（根证书）之间相互认证，整个信任关系基本是树状的。其次，S/MIME 将信件内容加密签名后作为特殊的附件传送。Microsoft Outlook/Foxmail 都支持 S/MIME。

（四）传输加密与 SSL

端到端安全电子邮件技术一般只对信体进行加密和签名，一些应用环境下会要求信头在传输过程中也能保密，这就需要传输层的技术作为后盾。目前主要有两种方式实现电子邮件在传输过程中的安全，一种是利用 SSL SMTP 和 SSL POP，另一种是利用 VPN 或者其他的 IP 通道技术，将所有的 TCP/IP 传输封装起来。SSL SMTP/POP 即在 SSL 所建立的安全传输通道上运行 SMTP/POP 协议，同时又对这两种协议作了一定的扩展，以更好地支持加密的认证和传输，这种模式要求客户端的 EMAIL 软件和服务器端的 EMAIL 服务器都支持，而且都必须安装 SSL 证书。基于 VPN 和其他 IP 通道技术，封装所有的 TCP/IP 服务，也是实现安全电子邮件传输的一种方法。这种模式往往是整体网络安全机制的一部分。

（五）内容过滤技术

邮件系统都提供一定程度的内容过滤技术，来实现反病毒、反垃圾邮件和邮件过滤自动分类等功能，内容过滤技术可以在 MDA、MTA 和 MUA 等位置进行。通过过滤规则的设置，可以控制各类用户或者各个不同部门邮件的收发权限，功能丰富的产品则可以针对不同的 IP、部门、发件人或收件人、邮件主题、邮件内容、时间等条件进行过滤，从更加细致的角度规划邮件系统收发权限。

三、安全电子邮件管理的设计

（一）“三员”分离管理

按保密规定，管理员分开管理，系统管理员、安全保密管理员和安全审计员的权限设置应相互独立、相互制约。安全保密管理员与安全审计员不得由一人兼任。系统管理员主要负责系统的日常运行维护工作；安全保密管理员主要负责系统的日常安全保密管理工作，包括用户账号管理以及安全保密设备和系统所产生日志的审查分析；安全审计员主要负责对系统管理员、安全保密管理员和操作行为进行审计跟踪分析和监督检查，以及时发现违规行为，并定期向系统安全保密管理机构汇报相关情况。针对“三权分立”的要求，邮件系统中采用分级保护措施，保证了文件基于安全网络内进行数据传输的工作，确保每一个操作行为都有记录，可供查阅与审计。

（二）密级标示管理

实现邮件的安全保密，其基础是对邮件进行密级标识管理，也就是对邮件设置密级，邮件的正文和附件可以分别设置密级，邮件的密级以两者中最高的密级标识。对于附件文档，可以使用第三方密级标志文档开发接口，一般实现对 office 文档的隐示和显示标密（通过加密手段写入 Office 文件头中），并保

证标志与正文的不可分割、不可篡改。

（三）流向控制管理

按照分级保护的要求，低密级用户不能处理高密级数据、高密级数据不能流向低密级、低密级用户不能接收高密级数据。在对邮件进行了密级标识和对用户设置了密级之后，邮件系统中设置流向控制，对于违背流向原则的拒绝投递邮件。

四、基于 Postfix 的安全电子邮件系统的实现

（一）基于 Postfix 的安全电子邮件系统整体架构

Postfix 是目前占主流的电子邮件系统，本质上就是 MTA，基于 Postfix 及其它主流的开源组件，可以建立一套完整的比较安全的电子邮件系统。电子邮件系统采用的部件包括 MTA 为 Postfix，POP3/IMAP 服务采用 DoveCot，WebMail 采用 RoundCube WebMail，认证为 Cyrus-SASL。同时，对其保密管理进行扩展，形成如图 1 所示的安全电子邮件系统。

（二）组织架构管理与身份认证

组织架构支持和身份认证提供电子邮件保密管理的基础，组织机构的树形结构，可以清楚知道组织机构之间的关联及上下级关系，实现 SSO（单点登录），并和其它应用系统集成。一种方法是采用 LDAP+CA 的方式，用户身份信息保存在 LDAP 信息库中，由 CA 对其颁发证书，通过公钥技术可实现数字签名和加密。本文采用 Ucenter 解决方案，在 Ucenter 的数据库集中存储用户信息，邮件系统和其它应用则和 Ucenter 接口（通行证），实现用户管理的同步，具体实现是开发了一个 RoundCube 的 UCenter 插件。

在邮件系统中，管理员通过组织结构树方便、快捷的查找相应用户，可查看用户在系统中运行情况，及有多少封邮件，用了多少空间等等。在用户端体现为组织通讯录，只要用户登录电子邮箱，打开组织通讯录就看到完整的组织联系人信息。联系人按部门分组，方便用户查询组织里所有用户的联络信息。组织通讯录只提供浏览和搜索联系人信息，不提供修改、删除、改名等操作。

（三）密级标示及邮件流转控制

按照 RFC 822 规定，每封邮件都有两个部分：信头和主体。信头是一系列的字段；主体指发送给收件人的数据，包括文本或文件。一个空字符串将两者分开，也就是说一个空字符串标记了信头的结束。信头部分的字段可分为两类：一类是由电子邮件程序产生的，另一类是邮件通过 SMTP 服务器时加上的。可由用户的邮件程序控制的信头字段不是所有的字段都是必须的，实际上可以忽略形成信头这一步骤而只发送正文，让 SMTP 服务器加上必需字段，如 From 邮件作者，Sender 发信人等。除了标准字段外，

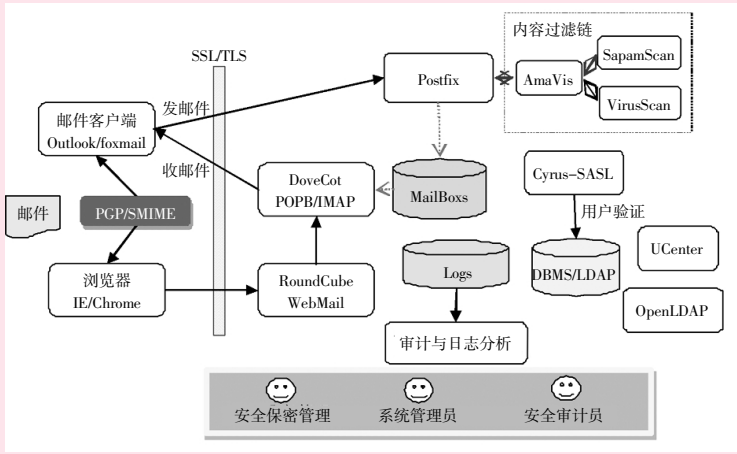

图 1　安全电子邮件系统整体架构示意图

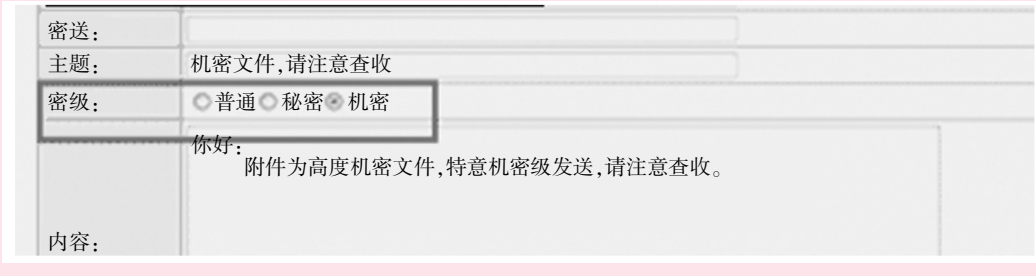

图 2 密级标示示意图

信头还可以包含用户自定义的字段。这些用户自定义的字段名必须由 X 开始。例如：X-SecretLevel，在写邮件的时候，就要明确邮件的密级。对于 Webmail，直接写入在 roundcube 的模版中，而对于 outlook 等客户端，就需要增加一个扩展插件。密级标示如图 2 所示。

有了密级标示和用户的身份信息，系统就基于此对邮件的流转进行控制，主要是发件控制，控制点有两个选择，一是 MUA 层：在用户发送邮件之前，就进行一次邮件检查，查看收件人的密级和邮件的密级是否匹配。遵循邮件发送的规则，低密级用户不能处理高密级数据，高密级邮件不能流向低密级用户。而当前用户的处理邮件最高密级权限由用户自身的权限来定。第二个是 MTA 层：在 Postfix 投递之前进行内容过滤的时候，调用一个密级检查代码模块。本文基于时间选用的是第一种方式。

此外，对于没有标识密级的邮件，有两种处理策略：拒收，退信要求加上密级标头；或者默认为非密邮件。处理策略可以通过 Postfix 中配置一个邮件头过滤规则实现。

（四）日志系统与三员管理

首先是要打开各个组件的 syslog 日志开关，同时，对于 WebMail，还需要自己建立一套日志设施，对用户、管理员的所有操作进行集中处理。其后，三种身份的管理员各司其职。

五、小结与展望

本文介绍了一个较完整的安全电子邮件系统的开发，但目前很多支持还处于基本阶段，需进行完善，如：可考虑引入 IBC 技术，从而省略了双方通信前需要的公钥认证和获取步骤，彻底简化了公钥管理，使得各种使用公钥技术的通信非常容易实现和使用；进一步加强电子邮件保密检查，检查邮箱的往来邮件内容和附件，通过文件导入、添加历史用户和手工录入三种方式设置所要检查的电子邮件地址，还可设置要在邮件内容和附件中查找的涉密信息等；检查邮件服务器，生成检查报告和运行日志，方便查看连接邮件服务器的状态；系统中密级流向控制比较粗，只按密级划分了，没有细化到跨域（跨部门）的问题，简化的方法是一个密级域使用一个邮件域名，然后在 Postfix 中可以在域转发上实施控制。

参考文献：

[1] （美）Kyle D.Dent.Postfix 权威指南[M].南京：东南大学出版社，2006.

[2] （美）Richard Blum.开放源码邮件系统安全[M].北京：人民邮电出版社，2002.

[3] （美）W.R.史蒂文斯.TCP/IP 详解.卷 1：协议[M].北京：机械工业出版社，2008.

[4] 张迎春.多重安全机制在电子邮件系统中的应用[J].计算技术与自动化，2011，(2).

[责任编辑：刘　骋]

On Design and Implementation of Email Security System Based on POSTFIX

WU Yin

(School of Art and Design, Wuhan Polytechnic, Wuhan430074, China)

Abstract: The paper reviews on the fundamental email security technology and email management technology including the separation of administrators, intensive signing and control of flow, based on which, the paper puts forward an email security system based on POSTFIX.

Key words: email security; Postfix; intensive; hierarchic protection