文章编号：1005－8893（2005）02－0050－04

企业邮件监控策略研究及实现*

王洪元[1]，张　鸣[2]
（1. 江苏工业学院 计算机科学与工程系，江苏 常州 213016）

摘要：随着 Internet 网络的普及与发展，电子邮件正在成为信息资料获取、协作和支持的一种重要手段。遥志邮件服务器系统是一个基于 Web 的 C/S 结构的电子邮件收发系统。某企业已建有电子邮件系统网络，并采用了经授权的遥志邮件服务器软件。然而在企业实际使用的过程中，需要对原系统的功能进行扩展。针对企业提出的要求，根据 CMAILSERVER 自身的特点，提出了基于 ASP 的邮件监控的方法，且完善了其它的功能，给出了具体的解决方案。

关键词：电子邮件系统；ASP；监控
中图分类号：TP 393　　文献标识码：A

某企业安装授权北京遥志公司邮件服务器系统。随着邮件使用者的增多，该企业领导希望能对与非本地邮箱交流的邮件进行隐蔽性监控。笔者通过分析发现，北京遥志公司的 CMAILSERVER 邮件服务器系统可以将所有发送和接收的邮件都保存到相应的地址中，但是其并没有实现隐蔽性：选项是公开化的，且选项仅提供了对所有邮件的监控功能。

针对企业的要求及 CMAILSERVER 的特征，本文对遥志邮件服务器系统 CMAILSERVER 的邮件监控提出了新的策略，主要实现了如下功能：①CMAILSERVER 整体管理隐蔽；②每个帐号对非本地邮箱的发出邮件和收到邮件监控；③监控邮件的按邮箱分类。

1　CMAILSERVER 系统分析

遥志邮件服务器系统是北京遥志公司的一套比较完善的邮件服务器系统，对其进行功能扩展与改造，存在着源代码不可知等困难。通过对原 CmailServer 系统进行分析，发现以下问题：

（1）CmailServer 自身已经带有监控邮件的功能，能够把帐号接收和发出的邮件都得到并发送到指定的邮箱，然而这个功能不具备隐蔽性：由于企业自身的特点，决定服务器不只是一个管理员在管理。这些功能即使系统管理员不使用，也有可能其他人会进行恶意使用。因此，这个选项必须屏蔽。

（2）在 CmailServer 中，服务器设置内容都是通过与 CMAILSERVER 执行程序相同目录下的名为 config. ini 文件进行读取和保存的。相应的“所有的邮件都保存到此地址”、“保存发送的邮件”、“保存接收的邮件”3 个属性的设置在 config. ini 文件中可发现其保存项分别见图 1。随便修改这些值会引起不良后果，因此需要确保这些属性值不可更改。

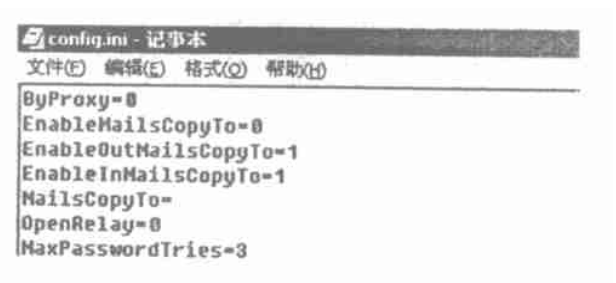

图 1　config. ini 中配置列表

Fig. 1　Config list in config. ini

（3）CmailServer 安装后，会自动分配一个名

* 收稿日期：2005－03－03

作者简介：王洪元（1960－），男，江苏常熟人，博士，副教授，主要研究方向：计算机技术应用；2－本院计算机系 2004 年毕业生。

为Admin的帐号邮箱名，这是系统管理员级别的邮箱。

(4) 系统对使用客户共作3级，分别为帐号，域管理员，系统管理员。3种身份标识所能使用的权限也不一样。帐号只能管理自己的帐号，进行收发邮件，而域管理员即网络管理员，除了一般帐号有的权限，它还拥有对其他帐号的管理的权限，能管理使用者，添加删除帐号，并且限定每个帐号的邮箱大小等功能。而系统管理员享有最高层次的管理权限，不仅能管理每个帐号，还可以对邮件服务器的一些设置进行修改、管理。

(5) CmailServer采用了WEBMAIL方式查看邮件，WEBMAIL方式是基于ASP进行开发的，使用的主要是VBscript方式。

(6) 每次CmailServer后，都会自动在注册表中加入开机启动的信息。这样就不利于加入的修改程序的运行。

2 解决方案

2.1 CMAILSERVER整体管理隐蔽性策略

(1) 对1(1)的选项屏蔽问题，通过使用VC++的资源修改方式，使选项不可见。

(2) 针对config.ini中的设定，为保正选项不选择，通过VC++的方式修改文件内容，在每次启动CmailServer时都将其内容设定为0(0为不选定，1为选定)。每次修改完config.ini文件后，再调用CmailServer，这样能保证选项不选择，并且即使有人中途修改也无效，因为config.ini只有在修改后再执行才有效。

(3) 对1(6)的解决方案是：每次启动后都对注册表修改，把原CmailServer注册信息删除，并将要加入的执行程序信息加入，加入的执行程序中调用原有的程序，并修改。由此制作一个DLL文件，所有程序修改信息加入其中，而另使用API建立EXE程序调用此DLL文件。注册表中的信息就加入此EXE执行信息[1-4]。

2.2 对发出和收到邮件的监控策略

在ASP中进行收发邮件要使用CMAILSERVER的2次接口，这个接口提供了丰富的编程资源。这里主要用了POP3接口(CMailCOM.POP3.1)和SMTP接口(CMail-COM.SMTP.1)。分析WEBMAIL，发现可以从邮件的发出和收到中截取。对于发出邮件的监控，WEBMAIL中有“发出”按钮，一旦这个按钮响应事件，邮件就发出，因此可以对按钮的响应事件进行修改，使之发送的同时，另外将该邮件发一份到Admin这个帐号。在发出该邮件到Admin之前，先分析接收邮件的地址是否是来自同一局域网，不是就将邮件发送到Admin这个帐号，否则就只需要和原程序一样，直接发到目的地即可。而对于帐号接收邮件的监控，每个邮件都有是否阅读的标记，在帐户login进入收发邮件页面后，对没有阅读的新邮件进行分析，发送者是否是同一局域网的，不是就将邮件发送到Admin帐户中。使用这种方法，将监控邮件送入Admin帐号有一个特点是信件独立，这样可以使系统管理员的邮件独立，随意查阅、删除，而不受一般帐号查阅、删除自己邮箱邮件的影响。同样的一份内容邮件，在帐户和邮箱中是分别存储的，存储为两封独立的邮件。

具体流程如图2。

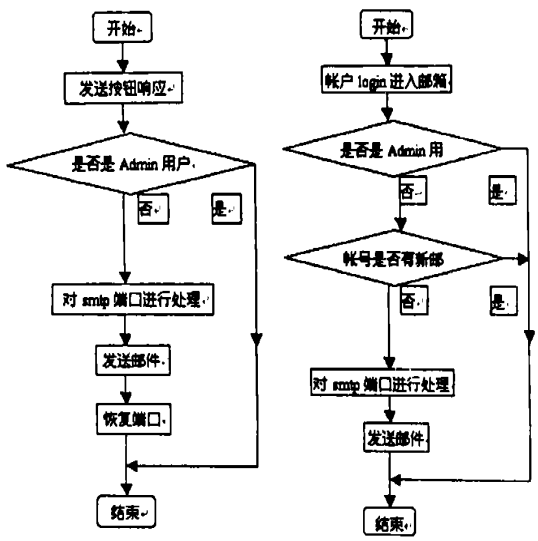

图2 收到和发出邮件的监控

Fig. 2 Monitoring mails received or delivered

2.3 监控邮件的分类

为了方便公司监控人查阅邮件，必须对帐户收到、发出邮件进行分类。选择按照帐号进行分类，每个帐号发出的邮件和收到的邮件放在1个文件夹里，这个文件夹是虚拟的，如图3。当系统管理员用帐号进入后，就会在WEBMAIL的页面中的文件夹里产生以相应帐号名命名的子文件名，并把每个帐号的邮件存入其中。应用CMAILSERVER的2次开发接口—帐号申请和设置接口，读取每个帐

号及相关信息。和建立其它的子文件夹如草稿夹、收藏夹等一样，通过读帐号端口，每读出一个帐号就建立相应的文件夹。当用户点击某个帐户的文件夹后，就会产生事件响应，开始进行对事件处理，处理内容为对 Admin 邮箱中的邮件进行分析，判断每个邮件的收件人或发件人与此帐户名是否一致，若一致便把邮件显示到邮件列表中来。当用户选择查看邮件列表中某个邮件时，调出该邮件，这种调出方式和原有的邮件调出显示内容的方式是一致的，只是对 Admin 中的邮件进行选择显示时的分类，而没有实实在在的这些文件夹，所以称这些文件夹是虚拟的，它们是在打开 WEBMAIL 页面后才产生的。在传送相应的帐户给另一个 ASP 处理时，采用了一个隐藏的按钮，这样可以使按钮的 name 成为一个公共变量，而进行方便的数据传输。具体流程见图 4。

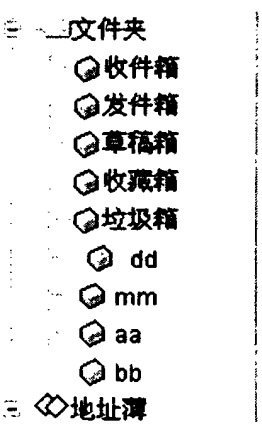

图 3 分类虚拟文件夹

Fig. 3 Virtual classification files

在每个帐户登录时都会首先有个基本信息页面。为了方便系统管理员查阅，决定对这个信息表改进，使系统管理员登陆后的信息页面能够看到每个帐户，并且准确地显示每个帐户里的邮件数，以及新邮件数。方法仍然是通过读出帐户端口的每个帐号，并相应显示，同时对 Admin 帐号里的邮件进行分类统计，按照每个邮件的收件人和发件人的不同，对相应帐号进行计数，同时对相应帐号的未读邮件进行计数。注意，从帐号端口取出各个帐号时也能取出相应帐号的邮件数，但是这个邮件数指的是该帐号的实际邮件数，是这个帐号的收到的邮件数，而对 Admin 进行计数的邮件数，是指的该帐号被 Admin 监控的收到的邮件数和发出的邮件总数。相应地，其中的未读邮件数也是指被 Admin 监控的收发的邮件中系统管理员未查阅的邮件数。具体流程见图 5。

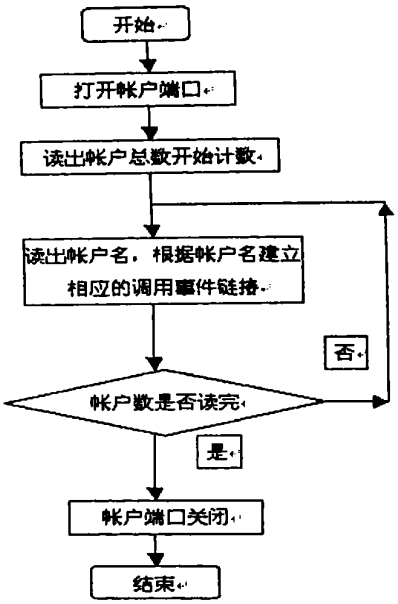

图 4 邮件分类流程

Fig. 4 The flowchart of mail classification

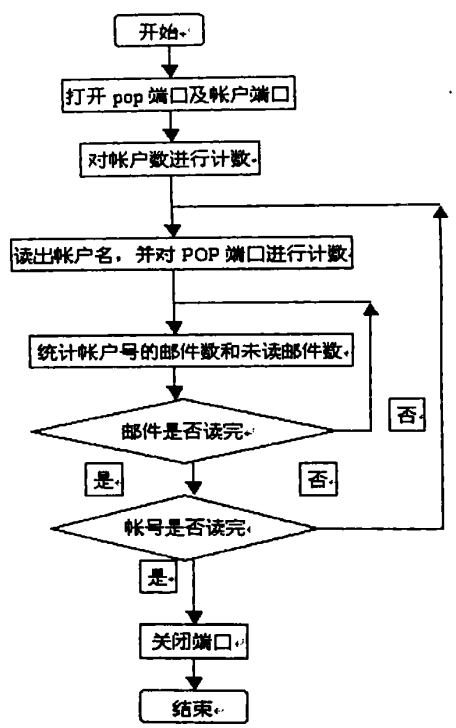

图 5 信息页面显示流程

Fig. 5 The display flowchart of information pages

3 结 论

本文针对用户实际需求，提出并实现了 CMAILSERVER 邮件监控新策略。采用本文策略的邮件监控系统已在企业中正常运用 1 年多，具有

高的实用价值和推广价值。但本系统还存在着一定的不足，由于对邮件监控策略的修改是在 WebMail 下，要限制使用 FoxMail，Outlook 等代理软件，这还有待于行进一步的开发和完善[5~8]。

参考文献：

[1] 清宏计算机工作室. VC++编程技巧多媒体与系统篇 [M]. 北京：机械工业出版社，2001.

[2] Mickey Williams. Windows 2000 编程技术内幕 [M]. 北京：机械工业出版社，1999.

[3] 朱琳杰，刘东红，王海涛. Windows 9X/NT/2000 注册表使用及编程指南 [M]. 北京：电子工业出版社，2000.

[4] 乔林，杨志刚. Visual C++6.0 高级编程技术 [M]. 北京：中国铁道出版社，2000.

[5] 胡珊，顾其威. 企业电子邮件系统安全性技术研究及实现 [J]. 小型微型计算机系统，2003，24（1）：157－160.

[6] 刘嘉勇，刘渊，方勇等. 邮件监听与阻断系统研究 [J]. 计算机工程与应用，2003，8：171－173.

[7] 周家庆. 电子邮件的自动截取与分析系统的设计与实现 [J]. 浙江师范大学学报（自然科学版），2003，26（1）：35－38.

[8] 尤枫，薛峰，赵恒永. 基于 S/MIME 协议的电子邮件安全研究与实现 [J]. 北京化工大学学报（自然科学版），2004，31（4）：44－49.

Research on and Implementation of the Strategy of Monitoring E－mail for Enterprises

WANG Hong－yuan[1]，ZHANG Ming[2]

（1. Department of Computer Science and Technology，Jiangsu Polytechnic University，Changzhou 213016，China）

Abstract：With the popularization and development of Internet，email has become an important means for information obtaining，cooperation and supporting. In line with the requirements of the enterprise that has constructed authorized Youngzsoft E－mail system，a new strategy based on ASP for monitoring E－mail is developed in this paper. It is showed by real application that the strategy is convenienct and valuable.

Key words：E－mail system；ASP；monitor