Microsoft Mail 安全性探讨

张积友 （广州通信学院计算机教研室 510502）

摘要：本文介绍了 Microsoft Mail 网络安全措施，指出在系统设计时要采用什么样的网络和客户环境才能实现其网络安全。

关键词：Microsoft Mail 网络 安全性

一、引言

随着办公自动化网络的日益普及，Microsoft Mail（以下简称 Mail）这种基于 LAN 的邮件系统也将被越来越多的单位所采用，如何安全地使用 Mail 就成为一个更加突出的问题，应该说微软公司为 Mail 提供了一定的安全措施，首先 Mail 系统为每个 Mail 用户建立了单独的登录 ID 和用户口令，并使用一个固定的密钥和算法来加密邮件、附件和文件夹，保证 Mail 系统访问安全；其次 Mail 系统还充分利用网络操作系统提供的用户权限和控制机制来实现其网络安全，包括利用一个 SECURITY 程序来封锁用户对邮件库的直接存取。但对于 Mail 系统网络安全性的实现是有条件的，做得不好会出现相当大的安全隐患，甚至是灾难性的。

二、Mail 基本工作原理

Mail 是基于 LAN 的能够传输多种媒体文件的文件共享型系统，其硬件构成如图 1，其中文件服务器（File Server）是邮件系统中心，用户（User）之间的通信依靠文件服务器中网络操作系统的拷贝功能，但 Mail 又和具体的网络操作系统相独立，可运行在任何基础结构之上，只要网络操作系统支持 DOS 的重定向功能。

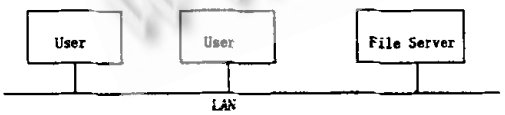

图 1 Mail 系统硬件构成

当我们安装完 Mail 之后，系统将在文件服务器上生成两个目录：一个执行程序目录和一个邮局库目录，这两个目录都必须共享出来，供 Mail 用户访问。其中执行程序目录（以后假定为 MAILEXE 目录）中存放的是管理程序、外部程序和目录同步程序，用户只要有执行权就行；而邮局库目录（以后假定为 MAILDATA 目录）存放的是数据文件，所有 Mail 用户对此目录都要有足够的权力，基本上是全部权力（在有些权力划分较细的网络中可以除掉文件扫描权），才能进行正常的邮件传递。

三、网络安全措施

Mail 用户对于邮局库目录操作权要求很高，而我们又不能进一步将用户权力细分，使得用户只能管理自己的邮件数据，这样就可能出现某个 Mail 用户直接对邮局库目录进行有意无意地删改，扰乱系统的正常运行。要解决这一问题，必须结合具体的网络环境，在此，我们依照文件服务器的操作系统，将网络分为两大类：NOVELL 环境和 Microsoft 兼容的网络环境。

1. NOVELL 网络环境

对于 NOVELL 网络，邮局库目录只是文件服务器中的一个子目录，Mail 用户要通过 MAP 命令将其映射为一个盘，如果我们能够有效控制用户对此目录的直接修改就能基本保证 Mail 系统安全，具体做法是：

（1）以 Supervisor 身份登录并运行 Syscon 程序

（2）将 Mail 用户归为一个组（假定为 MGROUP）

（3）将 MAILDATA 的所有操作权都授给 MGROUP 组

（4）取消其中的文件扫描权（File Scan）

这种方法保证只有 Mail 用户能访问该目录，而且不含有文件扫描权，没有文件扫描权，用户就查不到邮局库中的文件名；用不了 DEL *.* 命令来删除文件，当然也

不可能直接对邮局库进行删改，除非用户知道准确的文件名。存在的不足就是：如果 Mail 系统中含有 Macintosh 用户，就不能取消其文件扫描权。

2. Microsoft **兼容网络环境**

对于 Microsoft 兼容的网络环境，邮局库目录是文件服务器中的一个子目录，要把它以一个特定的名字(假定为 MAILDATA)共享出来

NET SHARE MAILDATA = C: \ MAILDATA

用户访问邮局库目录，就以这个特定的名字和服务器(假定名字为 MAILSERVER)建立连接

NET USE M: \ \ MAILSERVER \ MAILDATA

有些服务器的操作系统还可以为这个共享加上密码(假定密码为 PASSWORD)

NET SHARE MAILDATA = C: \ MAILDATA PASSWORD

用户要访问邮局库目录，就要知道这个特定的密码

NET USE M: \ \ MAILSERVER \ MAILDATA PASSWORD

在这类网络中，访问权限已不再重要了，因为文件扫描权已被其他权力所包含，Mail 用户要拥有的基本上是全部权力，NOVELL 网络上用的那种取消文件扫描权的方式来保证 Mail 系统网络安全的方法已不再有效了，但如果我们能够不让 Mail 用户知道共享名和访问密码，用户就不能直接对邮局库目录进行操作。

对于 3.0 以上版本的 Mail 系统，在服务器程序盘上包含了一个 SECURITY. EXE 程序，系统管理员可以利用它在执行程序目录中生成一个名为 MAIL. DAT 的加密文件，存放在用户的安装程序目录中，当用户安装完成并登陆执行时，Mail 系统自动通过 MAIL. DAT 来建立和邮局库目录的连接并控制访问，用户不需要自己建立和邮局库目录的连接，当然也就不必知道共享名和口令。具体方法如下(这里的共享和连接命令只是一种描述，使用时要结合具体的系统来实现)：

在文件服务器上以系统管理员身份登录：

(1) 将邮局库目录以一个特定的共享名和访问密码共享出来(有的系统不能加 密码) NET SHARE Maildata = c: \ Maildata password。

(2) 将当前目录设为执行程序目录(Mailexe)。

(3) 将包含 SECURITY. EXE 程序的 Mail 服务器盘放入 A 驱动器，并执行

A: \ UTIL \ SECURITY - SMailserver - NMaildata - Ppassword。

(不能加密码就放弃密码项)执行完成，在当前目录生成 MAIL. DAT 文件。

(4) 将所有用户端程序都安装在此目录下，供用户安装时使用。

(5) 将执行程序目录(MAILEXE)对用户设为只读，可执行权。

在用户端：

①对于 MS-DOS 用户。只要简单地将执行程序目录映射为一个盘，并加入搜索路径中，用户就可正常执行 NET USE E: \ \ MAILSERVER \ MAILEXE。或者直接用用户安装盘将执行程序安装在用户端，再将 MAIL. DAT 拷贝到安装目录下，并将此目录设为共享。

②对于 WINDOWS 或 OS/2 Presentation Manager 用户。首先要连接到服务器的执行程序目录，然后在用户本地机上运行该目录下的 SETUP. EXE 程序，安装相应的软件安装完成，Mail. DAT 将自动被拷贝到用户的操作系统目录下，用户无需建立和服务器的连接就可正常运行。

这种方式的网络安全成功的关键在于：对 Mail 用户隐藏邮局库目录共享名和访问口令，由邮件系统自己来处理。因此选择能够给共享目录加上访问口令的服务器操作系统，比只能对共享目录为用户授于某种访问权力的要好，如选择 Windows NT 作为文件服务器，就不如选择 Windows 95，虽然 NT 有很强的用户管理能力，但它只能给对共享目录为用户授于某种访问权力，很难保证网络安全，而 Windows 95 只能为共享加上访问口令的方式，正好迎合 Mail 系统的这种网络安全控制机制。

四、结束语

从以上的分析可以看出，Mail 系统具有一定的网络安全性，但这种安全和具体环境有密切关系，在系统设计时，一定要全盘考虑，使之相互协调才能保证 Mail 系统安全，否则会出现安全漏洞。

(来稿时间：1997 年 7 月)