一种为DOS扩充密码功能的方法*

涂星原 李 鹏

(郑州工学院计算中心)

摘 要: 本文给出了一种扩充 *PC* 机 *DOS* 操作系统，使其具有数据保密功能的方法，分析了扩充的方案和策略。扩充后的 *DOS* 与原 *DOS* 完全兼容。

关键词: 数据保密 文件管理

中国图书分类号: TP31

随着计算机在数据处理领域日益广泛的应用，出现了数据保密问题。解决好计算机系统中保密这个瓶颈问题，将会推动计算机在数据处理领域中更加广泛的应用。

目前PC机在国内非常普及，许多企、事业单位已用计算机进行管理。但是PC机上数据保密性问题的解决一直不尽人意。常常采用对文件独立进行加、解密的软件来实现数据保密，每当使用数据之前，先用软件解密，待使用完毕后，再用软件加密。给使用者带来许多的不便，同时也会因为使用者的不慎，如忘记进行加密等，给窃密者以可乘之机。

本文给出了一种对DOS进行扩充，具有数据保密功能，又与原DOS兼容的方法。

1 DOS结构及其文件管理概述

DOS由BIOS（基本输入／出部分）和DOS功能服务组成，采用分层结构，示于图0。高层部分调用低层部分，低层部分不能调用高层部分。

DOS服务功能调用BIOS，BIOS调用ROS，DOS服务功能不能直接调用ROS。DOS支持的结构良好的软件也只调用DOS服务功能，而不能直接调用BIOS或ROS。

磁盘文件管理是DOS的核心，它负责把磁盘空间分配给文件使用，使用文件目录和文件分配表管理文件。DOS提供两组文件管理功能：一组是文件控制块（FCB）方法，根据FCB对文件进行操作；另一组是句柄（handle）方法，根据文件所分配的句柄（一个16位的字）进行文件操作。

DOS提供的文件管理功能包含：创建、打开、删除，关闭文件，文件改名，FCB方式的文件顺序读／写、随机读／写、块读／写等，句柄方式的文件读／写、移动文件指针、复制句柄、修改文件属性、加载一个文件等功能。

由DOS支持的任何软件，对文件的操作都是通过调用DOS提供的这些文件管理功能实现的。

* 收稿日期：1990-05-20

2　总体方案设计

根据DOS内部结构的分层性，以及应用软件通过调用DOS服务功能来完成文件的操作这两个特点，本方案采用：在应用软件层和DOS服务功能层之间插入一个对文件加密、解密管理的C__D管理层（Code__decode manager），它完全接管DOS的中断，根据文件是否需要加、解密处理、调用DOS服务功能和加、解密算法来完成文件的操作，改造后的层次关系示于图1.

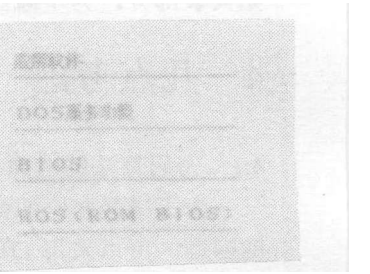

图1 原DOS分层结构示意图

本方案选用口令字作为C__D管理层的密码算法的密钥，对数据进行加／解密．文件名后加一特别标记（不妨定为字符串′IJH′）作为需进行数据的密码变换（加／解密）处理的文件标记．对于文件的句柄，把句柄的最高位（第15）位置1作为需要进行数据的密码变换处理的文件标记(因为在DOS中正常的文件句柄的第15位总为O）这样，就区分出了对哪些文件的操作需要进行数据的密码变换处理，对哪些文件的操作不需要数据的密码变换处理．访问一个文件时，若它的句柄的第15位为1或文件名之后有字符串′IJH′，就进行数据的密码变换处理，若没有这些标记，对这些文件的访问就不作数据的密码变换的处理．

C__D管理层的执行过程为:

判断所申请的服务是否文件管理，若否，则直接调用DOS服务功能：若是，判断有无需要密码变换的标记，若没有标记，也直接调用DOS服务功能，若有密码标记，就调整标记，调用DOS服务功能和进行数据的密码变换处理，恢复标记．

标记的调整和恢复分别是为了调用DOS服务功能和从C__D管理层返回时不破坏文件需要数据的密码变换处理（保密文件的加／解密）的标记．标记的调整和恢复可分为三种情况：对于句柄，调整标记是指清除第15位，恢复标记是指置第15位；对于表示路径和文件名的字符串，调整标记是指去掉文件名后的′IJH′串，恢复标记是指把′IJH′加到文件名之后；对于FCB，调整标记是指去掉FCB的文件名域中的′IJH′串，恢复标记是把′IJH′串加到FCB的文件名域中．

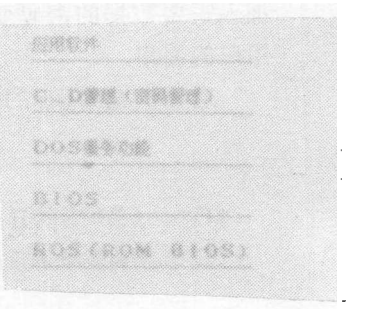

图2 改造后的DOS分层结构示意图

C__D管理层的总体结构框图见图2.

C__D管理层功能服务的结构框图略．

3　系统安排

为完成C__D管理层接管DOS的中断（与应用软件的接口），需要在DOS安装完成之后，安装C__D管理层．C__D管理层的安装由C__D管理层的初始化安装部分完成，其框图如图3示．

为把C__D管理层与DOS结合成一体，而成为一个具有密码变换功能的操作系统，应把C__D管理层放在IBMDOS.COM文件中（联接在IBMDOS.COM之后），并修改

IBMDOS.COM 的初始化部分，使得 DOS 初始化部分完成之后，执行 C_D 管理层的初始安装部分。为了减少对 IBMDOS.COM 的改动，C_D 管理层可以选择驻留在高段。

4 几点考虑

4.1 密码算法的考虑

为了增强密码的强度，增加破译的困难，可以采用 DES.RSA 或活门背包等目前尚无有效解法的密码算法，参见[1]。同时，由于访问文件时，每次访问数据的字节数目不同，故而密码算法要处理好数据短块的加/解密问题。

4.2 总体效果的考虑

安装了 C_D 管理层之后，C_D 管理层就完全接管了 DOS 的中断，使得改造后的系统支持对文件的保密性访问。只有知道口令字，访问保密文件时，才能获得正确的数据。并且，DOS 支持的命令均不需要任何改动。访问保密文件时，只需要在文件名之后加入需要数据的密码变换处理标记，仍按 DOS 提供的方法调用系统服务功能，这方便了用户的使用。

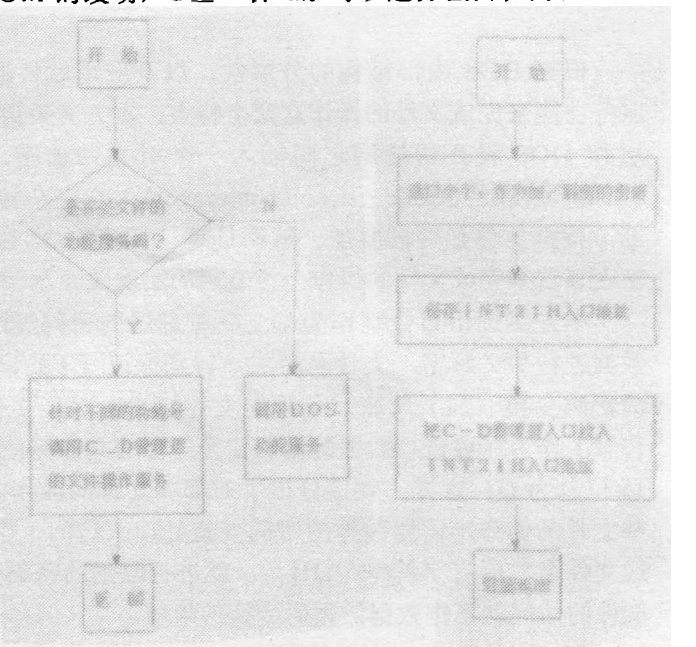

图 3 C-D 管理层的总体结构框图

图 4 C-D 管理层安装部分示意图

这种扩充 DOS 的方案也可以推广到其它不具备密码功能的操作系统上。

参 考 文 献

〔1〕 〔美〕卡尔 H·梅尔等著.刘景伊等译.密码学.国防工业出版社，1980.7

〔2〕 华佳等译.磁盘操作系统 DOS3.10 技术手册.微型计算机增刊，1987.8

An Approach Add Data-security To DOS

Tu Xing Yuan Lipeng

(ZhengZhou Institute of Technology)

Abstract: In this paper, a mothed is pressented by which the operating system DOS can be expanded to the extent which have the function of data-security and is compatible with DOS.Furthermore,the expanding strategy is discussed in detail.for the benefit of furthere investigation.

keywords: data security, file management