计算机应用系统安全结构体系的探讨

广州铁路局电子计算所　　王秀华

摘要：应用系统的安全性，是软件研制中必须解决的一个首要问题。本文首先分析了现有计算机应用系统结构体系在安全方面的局限性，然后提出一种新的结构体系，并阐述了它的主要特点及所采取的技术方法，论证了这些方法的实用性、通用性和安全性能。

一、引言

如何保证应用系统的安全是推广计算机应用过程中必须解决的一个首要问题，对计算机应用系统的威协主要来自自然因素和人为因素两个方面，后者又包括两个部分，一是无意行为，另一为有意行为。目前，各国用计算机犯罪的案例已经屡见不鲜，计算机病毒的产生及其所造成的巨大损失，已经在人们心理上投下了一块极大的阴影，防碍了计算机应用的普及和发展，计算机网络的发展，也要求系统的安全性能得到保障，为此，计算机专家在系统硬件和软件方面采取了很多的方法，以阻止系统遭到破坏，并防止一些保密资料被盗窃。经过实践证明，取得良好的效果。

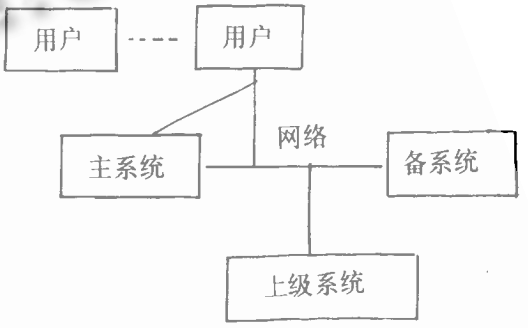
但是，在应用系统方面，由于人们在开发应用软件过程中，对应用系统的安全性缺乏整体的考虑，所以，和计算机系统相比，应用系统更容易被人破坏，系统资料缺乏应有的保护手段，因此，成为整个系统安全的薄弱环节。

本文介绍作者在 DEC 公司的 VAX II 上，开发车站运营管理信息应用系统过程中，为保证应用系统数据和软件安全所采用的各种手段和方法，并进一步讨论如何在多用户和网络环境下，建立安全应用系统结构体系的方案，该方案在广州北站实现一年多来，已经取得良好的效果。

二、现有应用系统的安全性分析

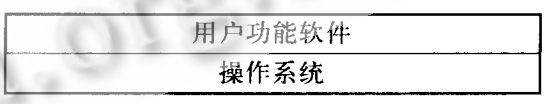
1.现有应用系统的硬件结构

在大型的计算机应用场合，应用系统一般具有如下拓扑结构：



2.现有应用系统的软件结构

应用系统软件一般以操作系统作为运行平台，使用者在用户环境中工作，通常采用下列结构：



3.现有应用系统的安全性分析

下面几条原则可以作为衡量系统安全性的标准：

(1)对系统中的重要用户，必须设置口令，核对口令以后，该用户才能进入

(2)系统必须管好每一个用户的权限，严格控制一些特权用户的使用。

(3)对网络用户和任务实施管理和监督。

(4)对远程终端实施管理和监督。

(5)对最终用户命令权限进行管理，不允许一些最终用户任意执行系统和应用软件。

(6)对重要数据进行加密和解密操作。

(7)实现双机间的数据互为备份和设备高速切换。

按照上面的标准,在现有应用系统结构中,存在下面几个难以解决的问题:

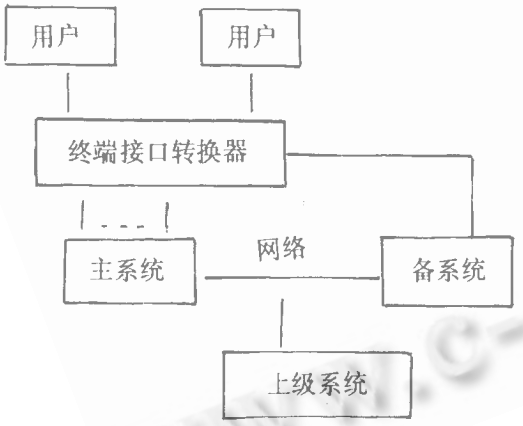
(1)用户口令保密性能极差。由于用户必须掌握口令才能使用计算机,而最终用户人员多,范围广,所以,使得口令保密性能极差,容易被其他人员获取而操作该用户,从而使系统的安全性能降低。

(2)对远程终端难以实施有效的管理和监督。任何人员,只要掌握口令以后,可以在远程终端中进入某个用户,并应用该用户的特权,完成任意的操作,从而有可能破坏该用户的安全,或者窃取该用户的机密。对诸如此类的问题,系统却难以及时发现并制止。

(3)不能实现双机间的互为备用和切换。由于用户设备是直接和主机相连,当主机故障时,用户设备难以迅速的切换到备用机上,这种结构还给主机系统的日常维护等工作带来困难,降低了应用系统的安全性。

三、新系统的结构

1.新应用系统的硬件结构



2.新应用系统的软件结构

终端I/O管理
命 令 处 理
进 程 管 理
用户功能软件
操作系统

四、新应用系统的安全性分析

1.新系统的工作原理

和现有系统的软件结构不同,在新系统的软件结构中,增加了终端I/O管理、命令处理和进程管理软件,由它们负责完成用户命令的输入、输出、检查、记录和执行,并对用户功能软件进行管理。在新系统中,设置一个管理用户,在它启动管理程序后,自动的完成其它终端用户初始化过程,并根据用户终端的内部定义,显示相应的菜单,避免了用户输入密码的登入过程,并且规定用户只能执行菜单的功能。

管理程序还负责完成系统内部的通讯、定时器的设置、文件的自动整理等功能。管理程序使用了许多的系统资源和技术,如窗口、邮箱、中断、I/O缓冲、事件标记、锁同步管理、进程管理及状态查询等。

在硬件结构上,增加了终端接口转换器,使用户设备独立于主机系统,可以根据需要实现双机间的高速转换。用户功能软件完成数据修改以后,向管理程序发出数据备份请求,由管理程序启动备份程序完成数据备份工作。通过这种方法,实现了双机间的互为备份要求。

2.新系统的安全性分析

(1)不存在用户口令保密问题。新的软件结构已经不需要用户自行完成登入过程,取而代之的是管理程序自动启动用户菜单系统。整个启动过程对用户是透明的,用户只需等待菜单出来以后,才能使用计算机系统,因而保证了系统的安全。

(2)能对远程终端实施有效的管理和监督。新的软件结构中,限制远程终端进行登入操作,并对远程终端用户的功能表进行了严格的规定,用户一般不能越权执行其它命令,为系统数据和软件的安全提供了保障。

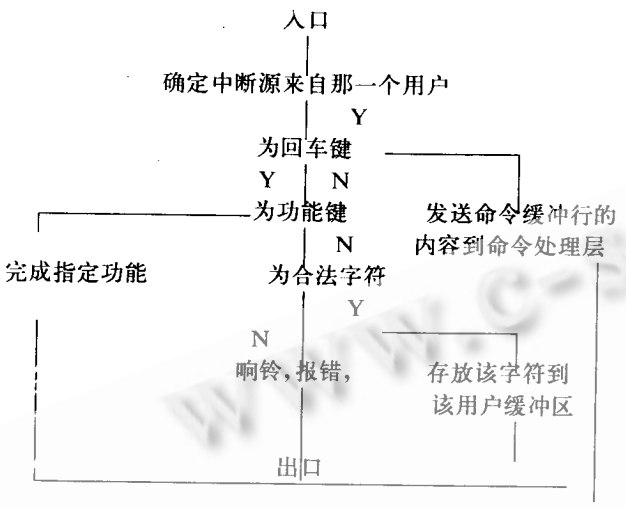
(3)能够实现双机间的高速切换。由于在软件和硬件方面采取了有效的措施,系统备分和切换得到了较好的解决,也为系统的日常维护代来了方便。

(4)限制网络上用户的使用。重要用户一般不准网络用户注册。如果网络任务确需进入该用户,必须核对口令,而该口令以加密形式存储在系统文件中,所以,其他人员很难通过网络打入该应用系统。

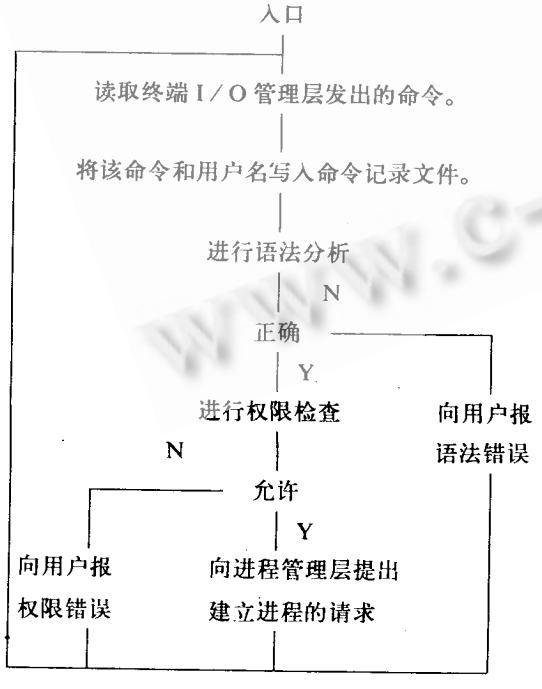
五、新应用系统的实现方法

1.管理软件的实现算法

(1)终端 I/O 管理。终端 I/O 管理以中断方式管理多个终端用户的输入和输出操作，当用户输入一个字符时，系统转入中断状态，执行以下中断服务程序：

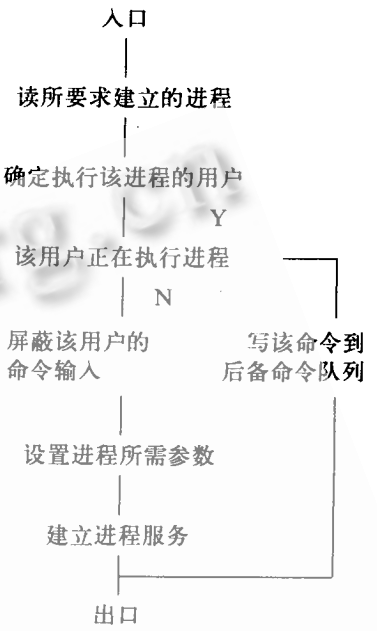


(2)命令处理层。命令处理层包括对命令进行语法检查和权限检查，命令处理层应用邮箱技术，读取终端 I/O 管理层发出的命令。

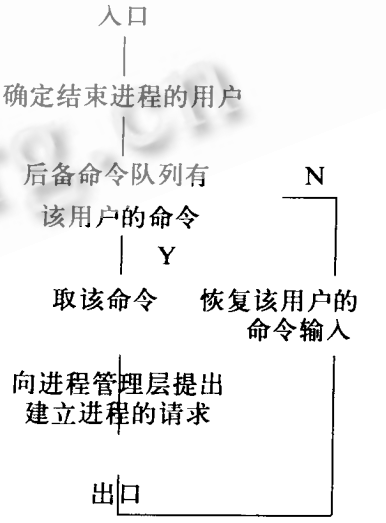


(3)进程管理层。进程管理层包括进程的创建和结束处理，该层采用中断方式工作，进程管理层建有一个后备命令队列，当进程不能建立时，暂存到该队列中。

进程建立处理：

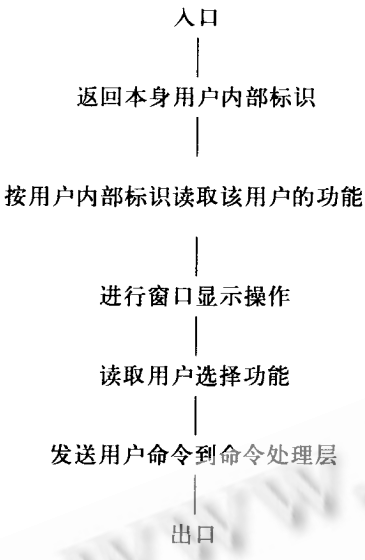


进程结束处理：



(4)菜单管理。菜单管理为全屏幕功能，用户可以使用键头选择所需的功能，也可以直接输入功能的编号，菜单为一个单独的进程，它将用户的功能符号发送到命令

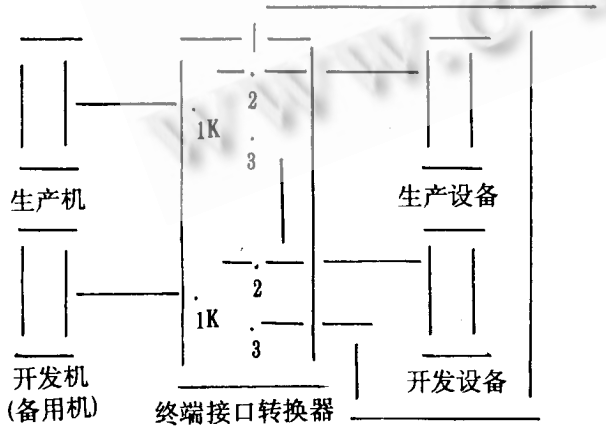
处理层，菜单程序将程序和数据分开，对所有的用户作统一处理，它按以下流程工作：



(5)数据实时备份管理。数据实时备份管理负责在备用机完成主机同样的数据修改工作。它接收用户功能软件发出的修改数据请求，应用网络通信技术，在备用机上，启动统一的备用软件，完成对数据的实时修改和更新工作。

2.用户终端设备的高速切换

用户终端设备的高速切换主要由终端接口转换器完成。终端接口转换器将主计算机和备用计算机的生产和开发管理功能有机的结合起来，实现二者功能上的高速转换。其原理结构如下：



终端接口转换器由一套电子线路所组成，接收RS-232的输入信号，根据控制信号的设置，将输入信号引到所需的输出端口进行放大，然后转换为RS-232输出信号。

在上图中，K为受控制信号控制的电子线路开关，具体工作过程如下：在开关打在2时，生产设备接到生产机，开发管理设备接到开发机；当生产机故障时，将开关打到3，生产设备接到开发机，开发管理设备接到生产机，从而实现了生产设备双机间的迅速切换。在生产机准备就绪后，又可以投入使用，这样，为系统安全提供了可靠的设备保障。

六、结束语

由于在新系统的结构体系中，引入了管理程序概念，使用户摆脱了复杂的系统登入过程，也避免了一些不利于安全的环节，通过屏蔽用户不必要的系统和应用软件使用，限制远程用户和网络用户的访问手段和权限，从而大大地提高了整个应用系统的安全性能。而双机间的切换过程简单易行，为系统的故障处理和日常维护提供了强有力的技术保障，满足了用户的安全要求。

本文所介绍的方法通用性强，能够被推广应用到其它的计算机应用系统中，和传统的结构体系相比，新的结构体系更加先进可靠。

由于笔者水平和经验的不足，在本文的论述过程中，难免存在许多问题，请学者和专家给予指正。

参考文献：

1.*VMS* 系统维护手册
2.*DECNET* 网络维护手册
3.*VMS* 系统服务参考手册
4.*VMS* 运行时间库参考手册
5.*VAXII FORTRAN* 语言参考手册
6.*VMS* 程序设计支持手册
7.*VMS* 程序员指南
8.广州北站运营管理系统可行性报告
9.广州北站运营管理系统系统设计报告