用 VB5.0 操纵安全的 Access 数据库

林　民　赵希武　（内蒙古师范大学 计算机系　010022）

摘要：本文详细介绍了创建安全的 Access 数据库的意义和具体步骤。

关键词：安全　密码　工作组管理员　工作空间

目前，在基于 Foxpro 或 Access 这些桌面数据库管理系统开发数据库应用软件时，往往只注重软件的界面及业务功能的实现，而数据安全性方面考虑比较少，很多软件虽然设有登录用户名及口令，实际上只能对不熟悉 Foxpro 或 Access 的非法用户有一定限制作用，而对熟悉这些数据库管理系统的非法用户来说可以轻易破解，或不使用应用软件直接打开库文件操作数据，因此，这些应用系统的数据都存在轻易被人破坏和篡改的危险。特别是在数据被共享的网络化环境中，这种潜在的危机更加严重。事实上 Access 数据库提供了很完善的数据安全机制，可以创建真正意义上的安全数据库。下面具体说明有关的操作方法。

1. Microsoft Access 提供两种设置数据库安全的方法

(1)为打开的数据库设置密码。设置密码后，打开数据库时将显示要求输入密码的对话框。只有输入正确密码的用户才能打开数据库。Mcrosoft Access 对密码进行了加密，直接查看数据库文件是无法得到密码的，因此是安全的。但这种方法只在打开数据库时检查密码，数据库打开之后，数据库中的所有对象对用户都将是可用的。另外，设置了密码的数据库将不能实现同步复制。这种方法适用于安全性要求不高的共享数据库或是单机上的数据库。

(2) 设置用户级安全，以限制用户访问或更改数据库的某部分。这是一种类似于网络中使用的安全方法，首先创建一个工作组信息文件，在工作组信息文件中，用户被标识为组的成员，可以为组和用户授予权限，规定他们如何使用数据库中的对象。Microsoft Access 提供了两个默认的组："管理员组"和"用户组"。例如在一个名为"销售管理"数据库中，可以设定"用户组"的成员能查看、输入或修改"顾客"表中的数据，但不能更改表的设计。或者只允许查看包含定单数据的表，而不能访问"工资"表。"管理员组"的成员则对数据库中的所有对象都具有完全的权限。要设置更细致的控制，可以创建自己的组帐号，定义其他的组，为其指定适当的权限，然后将用户添加到组中。工作组信息文件设置完成后，用户在启动 Microsoft Access 时将显示对话框要求输入用户名及密码。只有工作组信息文件中的合法用户才能打开数据库，并且对数据库对象只具有预先设定的操作权限。从以上说明可以看出，设置用户级安全是设置数据库安全的最灵活和最广泛的方法。

2. 设置用户级安全的具体步骤

(1)新建一个工作组信息文件

①退出 Microsoft Access。

②启动"工作组管理员"。在 Win95 (Win NT4.0)下打开安装 Microsoft Access 的文件夹(默认文件夹是 Program Files \ Microsoft Office \ Office)，然后双击 Wrkgadm.exe。

③在"工作组管理员"对话框中，单击"创建"按钮，然后键入相应的名称和组织名。

④在"工作组 ID 号"文本框中，键入一个最多为 20 个字符的数字和字母组合，然后单击"确定"按钮。应确保书写正确的名称、组织和工作组 ID 号，包括字母大小写(对所有三项输入)，并将其放置在安全的地方。如果要重新创建工作组信息文件，必须使用相同的名称、组织和工作组 ID 号。如果遗忘或丢失这些输入项，则不可恢复，因而也就无法再访问原数据库了。

⑤键入新的工作组信息文件名，然后单击"确定"按钮。工作组信息文件默认保存在 c: \ windows \ system 文件夹中。要使其他用户加入新工作组信息文件定义的工作组，可将该文件复制到共享文件夹中。新的工作组信息文件将在下一次启动 Microsoft Access 时被使用。所有创建的用户帐号和组帐号和密码都保存在新的工作组信息文件中。特别注意的是 在安装 Microsoft Access 时，安装程序会自动创建使用默认名称和组织信息的工作组信息文件 system.mdw。因为这些信息通常很容易确定，所以不具有授权的用户也很可能再创建这个工作组信息文件，并获得该工作组信息文件中定义的数据库管理员的各种权限。要预防这一点，完全确保数据库的安全，请不要使用这个默认的工作组信息文件，应新建一个工作组信息文件并为其指定工作组 ID (WID)。这样

只有知道 WID 的人才可以创建工作组信息文件的副本。

(2)创建新的用户帐号作为管理员帐号,移去管理员组中的"管理员"帐号。重新启动 Microsoft Access ,确保以"管理员"身份登录。选择"工具"菜单"安全"子菜单中的"用户与组帐号"命令;单击"用户"选项卡上的"新建"按钮;在"新用户/组"对话框中,键入新的用户帐号名称和个人 ID (PID)。将该用户帐号添加到管理员组中,而把"管理员"帐号从管理员组中移去。例如,要为名为"销售管理"的数据库设置安全性,可以创建新的帐号"销售管理员",并为帐号设置密码,然后将此帐号添加到管理员组中,而把"管理员"帐号从管理员组中移去。这是由于"管理员"帐号对 Microsoft Access 的每份副本都是相同的,任何一个使用 Microsoft Access 副本的用户都可以使用"管理员"帐号登录而对数据库中的对象具有所有的权限。因此,只有定义新的管理员和数据库所有者帐号(或者以一个帐号同时作为管理员和所有者帐号),然后将"管理员"帐号从管理员组中移去,这样才能保证数据库的安全性。

(3)重新启动 Microsoft Access 并以新的管理员身份(例如"销售管理员")登录,打开要设置安全的数据库。单击"工具"菜单"安全"子菜单中的"用户级安全性向导"命令,根据向导对话框中的提示完成各个步骤。

"用户级安全性向导"将创建一个新的数据库,并将原有数据库中所有对象的副本导出到新的数据库中,取消"用户组"的所有权限,并保持其他帐号设定的权限不变,然后加密新数据库。这样,数据库就完成了安全设置。现在,只有在步骤(2)中加入到"管理员组"中的帐号可以访问新数据库中设置了安全的对象。"用户"组不再有对这些对象的访问权限。如果在安全性方面只需要有"管理员组"和"用户组",就直接这两个默认建立的组,只是再给"用户组"指定适当的权限即可,而不必再创建额外的组了。所有新添加的用户帐号都会自动添加到"用户组"中而具有了"用户组"的权限。如果要更细地控制不同的用户权限,可以创建新组,为它们指定不同的权限集合,然后将用户帐号添加到适当的组中。为了简化权限管理,建议对组而不直接对用户指定权限,然后将用户添加到适当的组中,用户自然具有了组的权限。例如,为"销售管理"数据库设置安全性时,可以为经理建立一个"经理"组,为销售人员建立一个"销售员"组以及为雇员建立一个"职员"组。然后可以将具有最少限制的权限赋给"经理"组,将具有较多限制的权限赋给"销售员"组,而将具有最多限制的权限赋给"职员"组。当为新雇员创建用户帐号时,可将其添加到适当的组中,以使该雇员就拥有对应于该组的权限。在建立了用户和组帐号之后,可以选择"工具"菜单"安全"子菜单上的"用户和组帐号"命令,然后单击"打印用户和组"按钮来打印该工作组中所有帐号的报表,显示每个用户从属的组和每个组包含的用户。

下表总结了可以指定的各种用户权限类型:

权限	说明	权限有效的对象
打开/运行	允许打开数据库、窗体或报表或者运行宏。	对数据库、窗体、报表和宏有效。
独占打开	允许以独占访问方式打开数据库。	数据库
读取设计	允许在"设计"视图中查看对象。	表、查询、窗体、报表、宏和模块
修改设计	允许查看、修改或删除对象的设计。	表、查询、窗体、报表、宏和模块
管理员	①对于数据库,允许设置数据库密码、复数据库以及更改启动属性。 ②对于数据库对象,具有完全访问的权力,包括指定权限的能力。	数据库、表、查询、窗体、报表、宏和模块
读取数据	允许查看数据。	表和查询
更新数据	允许查看和修改数据,但不允许插入或删除。	表和查询
插入数据	允许查看和插入数据,但不允许修改或删除。	表和查询
删除数据	允许查看和删除数据,但不允许修改或插入。	表和查询

此外,表中有些权限自动地隐含其他的权限。例如对表的"更新数据"权限自动隐含"读取数据"和"读取设计"权限,因为只有具有这两项权限才能修改表中的数据。"修改设计"和"读取数据"权限则隐含了"读取设计"权限。对宏的"读取设计"权限隐含了"打开/运行。

(来稿时间:1999 年 5 月)