

Visual Basic 5.0 和 Access 97 数据库的安全性接口

何建国 (河海大学自动化系 210024)

摘要:本文主要介绍多用户、网络环境下 Visual Basic 5.0 开发 Access 97 数据库应用程序的安全性接口处理机制及其 VB 代码的实现

关键词:数据库, 安全机制 用户级安全 工作组 登录 口令 加密

工业控制系统一般采用分布式、网络化的结构模式,可采用 Visual Basic 作为系统首选的编程语言。现场控制级工控机 IPC 其主要负责处理测控数据,管理信息较少,故采用 Microsoft 公司推出的桌面型小型关系数据库 Access 是完全能满足实际需要的(控制中心则可采用大型数据库语言)。选用 Access 型数据库,使得编程、使用、二次开发都比较容易。Visual Basic 本身目前还没有建立安全数据库的能力,而 Microsoft Access 却完全有建立和维护具有安全性的数据库的能力。如果用 Access 为数据库建立了安全机制,则 Visual Basic 就可使用所有嵌入数据库的安全机制。联合使用 Visual 与 Visual Basic 可建立完备的、安全的客户机/服务器系统。本文主要介绍 Visual Basic 5.0 和 Access 97 开发数据库应用程序的安全性接口处理机制。根据本人的开发经验,要使安全性没有漏洞,概念理解最为重要。

一、Microsoft Access 97 的安全机制

Access 提供了设置数据库安全的两种传统方法:为打开的数据库设置口令,或设置用户级安全,以限制允许用户访问或更改数据库的哪一部分。除这些方法之外,还可将数据库保存为 MDE 文件以删除数据库中可编辑的 Visual Basic 代码以防止对窗体、报表和模块的设计进行修改。在 Access 97 中文版中把“Password”汉化成密码,易和“加密”概念相混淆,在此称为口令。

最简单的方法是为打开的数据库设置口令。设置口令后,打开数据库时将显示要求输入口令的对话框。只有键入正确口令的用户才可以打开数据库,这个方法是安全的(直接查看数据库文件是无法得到口令的),但只应用于打开数据库。在数据库打开之后,数据库中的所有对象对用户都将是可用的(除非定义用户级安全,稍后待述)。对于在某个用户组中共享的数据库或是单机上的数据库,设置口令通常就足够了。如果要复制数据库,

则不要使用数据库口令。如果设置了口令,复制的数据库将不能同步。

设置数据库安全的最灵活和最广泛的方法是设置用户级安全。这种安全类似于很多网络中使用的方法,它要求用户在启动 Access 时确认自己的身份并键入口令。在工作组信息文件中,用户标识为组的成员。Access 提供两种默认的组:管理员组 and 用户组,但也可定义其他的组。实施用户级安全时,数据库管理员或是对象所有者允许个别用户或用户组对数据库中的对象使用指定的权限。例如,用户组的成员可能只允许查看包含单数据的表,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。如果要设置更细致的控制,可以创建自己的组帐号,为其指定适当的权限,然后将用户添加到组中。

二、安全机制的设置

Jet 引擎被 Visual Basic、Access 和其他 Microsoft 产品所共享。Visual Basic 提供了两种与 Microsoft Jet 数据库引擎接口的方法:Data 控件和数据访问对象(DAO)。Data 控件只给出有限的不需编程而能访问现存数据库的功能,而 DAO 模型则是能全面控制数据库的完整编程接口。这两种方法并不是互斥的,实际上,它们常同时使用。Microsoft Jet 数据库引擎将数据访问对象上的这些操作转换为对数据库文件自身的物理操作,来处理所有与各种数据库接口的机制。

1. 添加数据库口令保护数据库

Microsoft Access 设置数据库口令很简单。关闭数据库。如果数据库在网络上共享,应使所有其他用户关闭该数据库。用“独占”方式打开数据库(如 ZL.mdb)。单击“工具”菜单“安全”子菜单上的“设置数据库密码”命令,即可在密码框中,键入自己的口令(如“ZL761227”)。下一次打开数据库时,将显示要求输入口令的对话框。

如果已定义数据库的用户级安全而对数据库不具有管理员权限,就不能设置数据库口令。而且,定义的数据数据库口令是添加到用户级安全上的。

VB Engine 工作区 Workspace 对象的 OpenDatabase 方法可实现在一个指定的工作区中打开一个现有的数据库的功能,而且其可选参数项 Connect 可设置欲打开的数据库类型和口令。以互斥、读写方式打开时,VB 5.0 编程如下:

```
Dim wspHjg AS Workspace
Set wspHjg = DBEngine.Workspace(0)
```

```
Set dbHjg = wspHjg.OpenDatabase("C:/hjg/ZL.mdb", True, False, ";pwd=ZL761227")
```

Access 以不加密形式保存数据库的口令,如果这使口令保护数据库的安全性降低,最好不要采用数据库口令的方式来保护数据库,相反地,可以定义用户级别的安全措施来控制对数据库中敏感数据的访问。

2. 设置用户级安全

Microsoft Access 工作组是在多用户环境下共享数据的一组用户。如果定义了用户级安全,工作组的成员将记录在用户帐号(由用户名和个人 ID(PID)来标识的帐号)和组帐号中,这些帐号则保存在 Microsoft Access 工作组信息文件中。用户的口令也保存在工作组信息文件中。可以为这些安全帐号指定对数据库及其对象的权限。而权限本身则将存储在安全数据库中。

在创建安全帐号之前,应该选择存储这些安全帐号的 Access 工作组信息文件。可以使用默认的工作组信息文件,指定其他的工作组信息文件,或者创建新的工作组信息文件。如果要确保工作组及其权限不可复制,则不要使用默认的工作组信息文件。并且必须确保所选择的工作组信息文件是使用唯一的工作组 ID(WID)创建的。

Access 对象包括:表、查询、窗体、报表、宏和模块。Access 对其所有对象均能设置用户级的许可权限,而由于目前 VB 5.0 只能访问两种 Access 对象(表和查询),其他对象在引用时不支持,所以对基于 VB 的系统其他数据库特权与权限的定义(如访问报表、宏、模块等)是不必要的。

设置数据库用户级安全的流程如下:

(1)新建一个工作组信息文件。在安装 Access 时,安装程序会自动创建使用指定名称和组织信息的 Access 工作组信息文件。自动创建的默认的工作组信息文件为 Windows/System/system.mdw,其中存有默认的所有者帐号、管理员帐号(admin)和空白口令“”。每次启动 Access 时,Access 都将使用默认的工作组信息文件。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创建该工作组信息文件的其他版本,并获得该工作组信息文件中定义的工作组管理员帐号(管理员组的成员)的各种不可撤消的权限。要预防这一点,应使用“工作组管理器”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。

①启动“工作组管理员”。打开文件夹 Program

Files/Microsoft Office/Office,然后双击 Wrkgadm. exe。

②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。

③在“工作组所有权信息”对话框中,键入一个最多为20个字符的数字和字母组合(即WID),然后单击“确定”按钮。

④键入新的工作组信息文件名(如“hjj”),然后单击“确定”按钮。

新的工作组信息文件将在下一次启动 Access 时使用。所有用户以后创建的用户帐号和组帐号或口令都保存在新的工作组信息文件(“hjj. mdw”)中。

(2)要求用户登录到 Microsoft Access。除非激活工作组的登录过程,否则 Access 将在启动时自动使用预定义的“管理员”用户帐号登录所有的用户。向“管理员”用户帐号添加一个口令即可要求工作组的用户进行登录,防止非工作组用户的访问。启动 Microsoft Access,打开数据库。在“更改登录密码”选项卡上,键入新口令(如“oldadmin”)即可。因默认的口令为“”,所以不要在“旧密码”框中输入任何内容。

在这之后,工作组的任何一个成员启动 Microsoft Access 时将显示“登录”对话框。如果当前该工作组中没有定义任何用户帐号,则“管理员”用户就是唯一的合法帐号。

(3)创建管理员的用户帐号,删除管理员组中的“管理员”帐号。在采用安全机制时,管理员(Admin)组和该组中的所有用户都很特殊。数据库和 Admin 组同时创建。一个永久的许可权赋予了该组,对使用该工作组的所有数据库。它们都具有改变数据库对象的许可权的能力。该许可权不能取消,哪怕所有的许可权都从 Admin 组清除了,这个许可权还得保留。在许可权中不能显示该许可权。所以为了安全,应删除管理员组中的“管理员”帐号。由于在管理员组中,至少须含有一个用户,所以应首先创建一个管理员的用户帐号(如:hjj)。但注意,用户组的“管理员”帐号是删除不掉的。

“工具”菜单“安全”子菜单中的“用户与组帐号”命令可用来增加或删除用户与组帐号,并改变其口令。如首先以“管理员”登录,输入新的用户帐号(如“hjj”)和个人标识符 PID(如“ABC123”),并使其加入管理员组,退出 Access。输入的 Personal ID 不是密码。Access 将使用 PID 和用户名作为加密算法的种子,为用户帐号产生安全标识号(SID)。再以“hjj”登录,创建新的登录口令(如

“hjj640704”),并把“管理员”从管理员组中删掉。

(4)改变数据库及其对象的所有者。可以更改数据库对象的权限的人员有:创建数据库时所使用的工作组信息文件的管理员组成员;对象的所有者;对对象具有管理员权限的用户。所有者即为拥有数据库或数据库对象最高控制权的用户帐号。创建数据库或数据库对象时登录的用户帐号就是“所有者”(如目前为默认的“管理员”)。组帐号不能拥有数据库,但是可以拥有数据库对象(在该组中的所有用户都拥有该对象时)。拥有数据库对象的帐号对该对象具有不可撤除的权限,而且可指定他人对该对象的权限,同时数据库所有者在任何情况下都可以打开其数据库。至目前为止,可以更改数据库对象的权限的人员有:工作组信息文件的管理员组成员“hjj”和数据库对象的所有者“管理员”,所以必须改变数据库及其对象的所有者为所要求的用户“hjj”。

对整个数据库设置安全性,是转移所有对象包括数据库本身的所有权的最简单的方法。要对整个数据库设置安全性,最佳方法是使用“用户级安全性向导”(应以新所有者“hjj”登录)。该向导可以新建一个数据库并将所有的对象导入其中,然后通过取消用户组对新数据库对象的所有权限,为选定对象类型设置安全,然后加密新数据库。原有数据库没有进行任何更改。表之间的关系和所有的链接表在新的数据库中都将重建。经过运行“用户级安全性向导”,现在,只有工作组管理员组成员可以访问新数据库中设置了安全的对象。“用户”组则不具备对这些对象的权限。

(5)创建、设置用户与组的权限并设置登录口令。多用户、网络环境下要限制用户和/或组对这些对象的访问必须为其设置权限。管理工作组最简单的方法就是为组而不是单个用户指定权限,然后通过将用户添加到组中或从组中删除的方式来更改单个用户的权限。用户帐号一定要设置登录口令,改变无口令的默认设置,以保证数据库的安全性。用户要登录到 Access,需要在“登录”对话框中键入用户名称和口令,且只拥有与其帐号相联系的权限。

经过以上五个步骤,即可生成安全数据库。如再给数据库加上口令(如“ZL761227”),可进一步增强安全性。若是在第四步之前就给数据库加上口令,经第四步后打开新数据库就不需要口令了。

(6) VB 5.0 代码编程。Visual Basic 5.0 使用

Workspace 工作区对象在 Access 数据库寻址。VB 5.0 的 DBEngine 对象启动时会自动创建一个默认的工作区 Workspace(0) 并把“DefaultWorkspace”和“Admin”设置为其“Name”和“UserName”属性的默认值, DefaultPassword 设置成“”, 即无口令。任何数据访问调用都激活工作组信息文件, 所以应首先告诉 Microsoft Jet 工作组信息文件的地点, 这可通过设置 DBEngine 的 SystemDB 属性来实现。

VB 5.0 可以利用 DBEngine 对象的 DefaultUser 和 DefaultPassword 属性来实现安全数据库的代码登录。

```
DBEngine. SystemDB = " c:/windows/system/hjg.
mdw"
```

```
DBEngine. DefaultUser = "hjg"
```

```
DBEngine. DefaultPassword = "hjg640704"
```

```
Se wspHjg = DBEngine. Workspaces(0)
```

```
Set dbHjg = wspHjg. OpenDatabase (" C:/hjg/zl.
mdb", True, False, ";pwd = ZL761227") '当数据库设密
码时, 应加";pwd = ZL761227"。
```

VB 5.0 也可利用 DBEngine 对象的 CreateWorkspace 方法来实现安全数据库的代码登录。DBEngine. SystemDB = "c:/windows/system/hjg. mdw"

```
Set wspHjg = DBEngine. CreateWorkspace (" default-
workspace", "hjg", "hjg640704")
```

```
Set dbHjg = wspHjg. OpenDatabase (" C:/hjg/hjg.
mdb", True, False, ";pwd = ZL761227") '当数据库设密
码时, 应加";pwd = ZL761227"。
```

3. 加密或解密数据库

除了安全性系统外, Jet 引擎还提供了一种加密数据库的方法。对数据库进行加密将压缩数据库文件, 并使其无法通过工具程序或字处理程序查看数据库内容的方法。加密数据库更多的是为了数据的完整性, 而不是数据的安全。数据库解密则为加密的反过程。

在 Access 能容易地设置数据库的加密和解密。在 VB 5.0 中, 首次创建数据库时, 可以使用 CreateDatabase (name, locale, options) 方法的 options 部分指定加密, 并且其 locale 部分可为新创建的数据库生成一个口令。

```
DimDim wspHjg As Workspace
```

```
Dim dbHjg As Database
```

```
Set wspHjg = DBEngine. Workspaces(0)
```

```
Set dbHjg = wspHjg. CreateDatabase (" c:/hjg/zl.
mdb", dbLangChineseSimplified & ";PWD = ZL761227",
dbEncrypt) '生成一口令为“ZL761227”的加密数据库。
```

在已经创建数据库之后, 可以使用 CompactDatabase (DBEngine. CompactDatabase olddb, newdb, locale, options, password) 方法来添加或删除加密, 并且其 locale 部分也可为新创建的加密或解密数据库生成一个口令。若加密或解密前的数据库已有口令, 则应由其 password 部分给出。

```
DBEngine. CompactDatabase (" c:/hjg/zl/mdb", c:/
hjg/zl. mdb", dbLangChineseSimplified, dbEncrypt) '数
据库加密。
```

```
DBEngine. CompactDatabase (" c:/hjg/zl. mdb", "c:/
hjg/zl. mdb", dbLangChineseSimplified & ";PWD =
ZL761227", dbEncrypt) '数据库加密, 并增加一口令
“ZL761227”。
```

```
DBEngine. CompactDatabase (" c:/hjg/zl. mdb", "c:/
hjg/zl. mdb", dbLangChineseSimplified, dbDecrypt, ";PWD
= ZL761227") '为一个已有口令“ZL761227”的数据库解
密。
```

如果已经定义了用户级安全, 则要加密或解密数据库, 必须使数据库中所有的表具有“修改设计”权限。否则将不能执行加密或解密操作。加密数据库不会限制授权用户或组对对象的访问。数据库加密后, 对速度的影响大约 10% 到 15%。

4. 其他安全措施

通过 Access 隐藏数据库窗口中的对象也可以很容易地达到简单保护数据库安全的作用。另一种方法是使应用程序在启动时提示用户输入一个名字和口令。可是, 这类安全性对应用程序的数据只提供很弱的保护。在这类安全性保护下, 可以很简单地获得数据的访问。

参考文献

- [1] (美) Mike Mckelvy & Ronald Martinsen, Visual Basic 5 开发使用手册, 机械工业出版社, 1998。
- [2] (美) Dan Rahmel & Ron Rahmel, 用 Visual Basic 4 开发客户机/服务器应用程序, 机械工业出版社, 1997。

(来稿时间: 1999 年 4 月)