**用户权限的提升：**

*UAC(User Account Control，用户帐户控制)是微软为提高系统安全而在Windows Vista中引入的新技术。要关闭它，可以进行如下操作：  
  
1、开始——运行，或者WIN+R键打开运行对话框，输入Gpedit.msc打开“组策略”。  
2、依次定位：“计算机配置”——“Windows设置"——“安全设置”——“安全选项”。  
3、在“安全选项”中找到“用户帐户控制: 管理审批模式下管理员的提升提示行为”选项，双击它。在弹出的窗口，点击右侧的向下箭头，修改为“不提示，直接提升”后确定"，就不会再弹出提示框了!*

**进程权限的检查：**

**//pElevationType：当前的权限类型：**

typedef enum {

TokenElevationTypeDefault = 1,

TokenElevationTypeFull,

TokenElevationTypeLimited

} TOKEN\_ELEVATION\_TYPE , \*PTOKEN\_ELEVATION\_TYPE;

TokenElevationTypeDefault：进程以缺省的用户身份运行，或者没有使用UAC功能，简单来说，就是用户没有启动UAC功能，那么程序使用的令牌，一定不是Filter Token。

TokenElevationTypeFull：进程的权限已经被提升，进程令牌没有使用filter令牌

TokenElevationTypeLimited：进程使用的令牌是Filter令牌。此时通过GetTokenInformation函数，并使用TokenLinkedToken标志，来获取原令牌。

**//pIsAdmin：是否是管理员。**

BOOL GetProcessElevation(TOKEN\_ELEVATION\_TYPE\* pElevationType, BOOL\* pIsAdmin)

{

HANDLE hToken = NULL;

DWORD dwSize;

// Get current process token

if (!OpenProcessToken(GetCurrentProcess(), TOKEN\_QUERY, &hToken))

return(FALSE);

BOOL bResult = FALSE;

// Retrieve elevation type information

if (GetTokenInformation(hToken, TokenElevationType,

pElevationType, sizeof(TOKEN\_ELEVATION\_TYPE), &dwSize))

{

// Create the SID corresponding to the Administrators group

BYTE adminSID[SECURITY\_MAX\_SID\_SIZE];

dwSize = sizeof(adminSID);

CreateWellKnownSid(WinBuiltinAdministratorsSid, NULL, &adminSID,

&dwSize);

if (\*pElevationType == TokenElevationTypeLimited)

{

// Get handle to linked token (will have one if we are lua)

HANDLE hUnfilteredToken = NULL;

GetTokenInformation(hToken, TokenLinkedToken, (VOID\*)

&hUnfilteredToken, sizeof(HANDLE), &dwSize);

// Check if this original token contains admin SID

if (CheckTokenMembership(hUnfilteredToken, &adminSID, pIsAdmin))

{

bResult = TRUE;

}

// Don't forget to close the unfiltered token

CloseHandle(hUnfilteredToken);

}

else

{

\*pIsAdmin = IsUserAnAdmin();

bResult = TRUE;

}

}

// Don't forget to close the process token

CloseHandle(hToken);

return(bResult);

}

1. 先通过GetTokenInformation函数来确定，当前程序的令牌是否为Filter Token。
2. 如果是，那么通过GetTokenInformation函数，来获得Filter Token的原始令牌。
3. 在获得原始令牌后，通过CheckTokenMembership函数，确认在原始令牌中，有管理员的帐号，如果有，那么说明启动当前程序的账户是管理员帐号，否则就不是。

CheckTokenMembership确认一个SID是否在一个Token中可用。

1. 如果不是Filter Token，那么直接使用IsUserAnAdmin函数，来确定启动当前程序的帐号，是否为管理员帐号。