Protect system files with UAC Virtualization - Part 1

In this article, I will show you how to use User Account Control Virtualization to protect the system.

Derek Melber

Network administration - *When a user standardizes on a Windows-based computer, it's also time for some actions to be protected. This protection is not always successful because some versions of Windows do not protect the system as well as everyone expected* . Protected actions are changes or writes to system folders and Registry locations. This is absolutely necessary to protect the stability and security of the entire operating system. In this regard, Windows Vista has provided a great solution to help us protect these system areas. Vista uses User Account Control and Virtualization to do so. In this article, I will show you how UAC uses Virtualization to protect the system.

Summary of the history of enterprise application behavior

The Program Files folder (installed at C: Program Files, or still written as% ProgramFiles%) is where most LOB applications (business streams) store executable files for applications. In most cases, the settings for the LOB application are stored in *HKEY_LOCAL_MACHINESoftware* in the Registry. Both of these locations are protected by the operating system by only allowing the system and administrators to have access and write access, and users can read and access at the execution level.

Enterprise stream applications need to be designed to be able to write to specific user application data directories, which will be placed in the user profile. Usually it is *C: UsersAppData* or *% AppData%* . If any settings need to be saved, these settings should be placed in the Registry at *HKEY_CURRENT_USERSoftware* . Both of these locations are created on one user and are protected by only allowing users who have access to the data to record and change.

However, many enterprise applications are not designed to work that way but instead they are designed to store user data in *% ProgramFiles%* and *HKEY_LOCAL_MACHINESoftware* . However, standard users do not have write access to these location locations, location can make many companies can add standard users to the local administrative group to run these applications. Obviously, that is really not safe at all, because users can change anything on their computer.

UAC Virtualization

Because enterprise line applications cannot be changed easily and users still have to run these applications, Vista therefore uses another method to fix this problem. Inside Vista, UAC adds the file system and namespace virtualization feature of the Registry. UAC will virtualize legacy applications and allow standard users to keep a 'standard user', but can still run the application. The inheritance definition in this case includes 32-bit processes, does not run with administrator privileges, does not include the manifest files of Windows Vista. If a certain process or a certain member does not meet the necessary conditions, it will not be processed virtually. In

addition, the following operations and operations are also not:

- Default Vista applications
- Executable files with extensions like .EXE, .BAT, .VBS and .SCR. You can add exceptions to extensions in *HKLMSystemCurrentControlSetServicesLuafvParametersExcludedExtensionsAdd* .
- 64-bit applications and processes
- Applications with directive execution of their executable's Execution Level, like most Vista implementations.
- Processes or applications running with administrator rights.
- Applications run in kernel mode
- Activities do not originate from an interactive login session, like file sharing.
- Applications that modify the registry key have been marked with the ' *Don't_Virtualize registry* ' *flag.*

Virtualization of file system and Registry is not widely implemented. It is limited to some locations, which is necessary for the operating system to run and keep them safe. This is an almost complete list of virtualized locations:

- *Program Files and subfolders*
- *Program Files (x86) on 64-bit systems*
- *Windows and all subfolders, including System32*
- *Users% AllUsersProfile% ProgramData*
- *Documents and Settings (symbolic link)*
- *HKLMSoftware*

Verify UAC Virtualization

When an action is virtualized, its content will be saved in the user profile as we mentioned above. However, do you know how the information is virtualized? Depending on what content is virtualized, there will be instructions within the different interfaces to help you see this.

The first directive that we introduce to you is within Windows Explorer. Depending on the directory and which files are virtualized, you will see additional menu options inside Windows Explorer. Figure 1 shows what Windows Explorer looks like and when you have virtual files in the C: Windows folder.

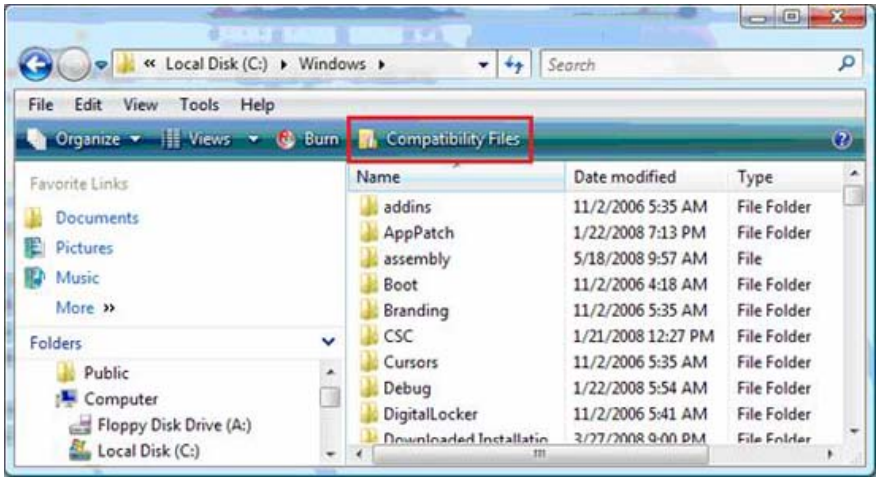

Figure 1: The highlighted red box indicates that these are virtual processed files

Compatibility file options ' *Compatibility Files* ' in Windows Explorer only appear when virtualized files are processed and this new menu option appears only for folders with virtual files and virtual folders.

When the option Compatibility Files is selected, it will direct the Windows Explorer window to the virtualized files and the folder containing it. Figure 2 will show what is inside the problem of virtualizing these files as well as the directories in it.

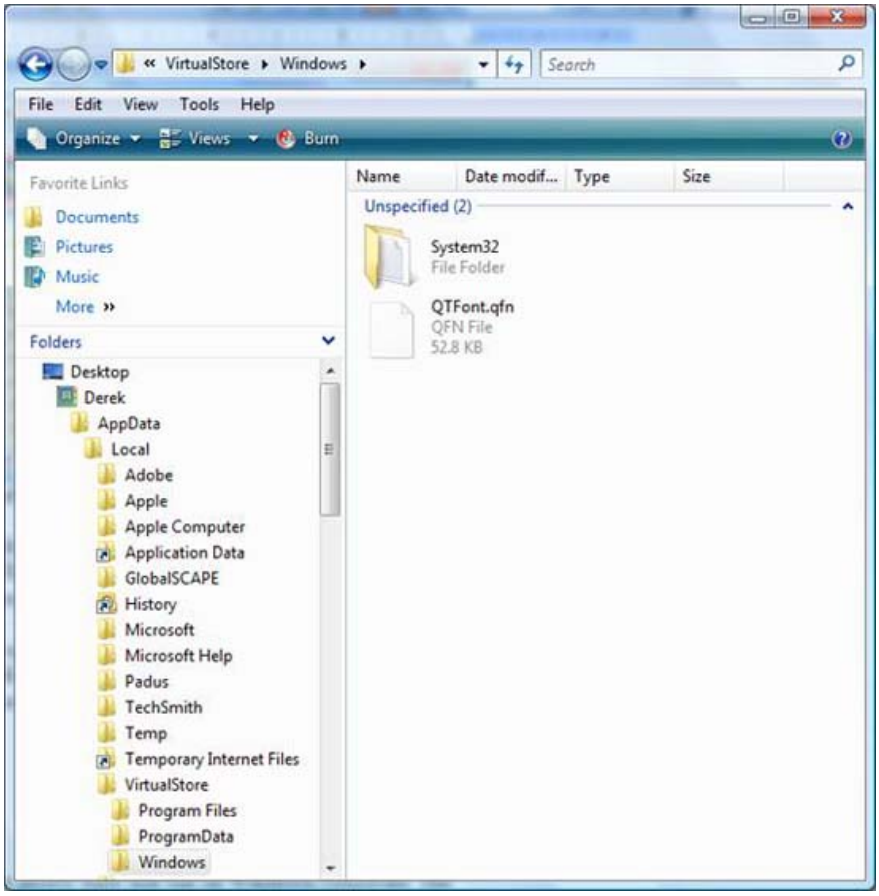

Figure 2: Options menu of compatible files saved in the VirtuaStore folder

As you can see, the menu option of compatible files opens in the VirtualStore folder, this is the folder that is located in the user's profile. As you can see in Figure 2, its name is *AppDataVirtualStore* .

Conclude

Perhaps we all know that applications built to run on Windows computers are also very difficult. The main reason for that is that the applications write to protected system files, folders and Registry locations. However, for Windows, it requires users to obtain local administrator privileges or must be set appropriately. Placing user accounts into the local administrators group to allow users to successfully run their applications is not a good solution at all. Depending on how the application is designed, the UAC virtualization of files and Registry is a great solution. Registry files and entries will be virtualized, by placing themselves in the user's personal profile. This method helps Windows protect the system, the network and still allow users to run their applications.