A shell extension is a guest in someone else's house; don't go changing the carpet

devblogs.microsoft.com/oldnewthing/20091202-00

Raymond Chen

A customer was running into this problem with a shell extension:

> I am writing a shell namespace extension. I need to get data from a COM server, which requires impersonation via `CoInitializeSecurity` with `RPC_C_IMP_LEVEL_IMPERSONATE`. As I am just writing an extension into `explorer.exe`, I am not able to call `CoInitialize`, `CoInitializeSecurity` anymore from my extension. Is there a way I can start `explorer.exe` by setting `RPC_C_IMP_LEVEL_IMPERSONATE` in its COM initialization? I was browsing through web, and `explorer.exe` seems to take some settings from registry, but couldn't find anything related to this one.

First of all, who says that the host process is `explorer.exe`? If I open Notepad, then do a File.Open, and then navigate to your shell extension, boom, your shell extension is now loaded into Notepad, and I doubt you told Notepad that you wanted it to initialize COM in a special way, just for you. Same goes for Quicken, Lotus Notes, all those other programs that use the shell. Even if you solved the problem for Explorer, that doesn't solve your problem in general. Second, what if two shell extensions did this? Your shell extension requires `RPC_C_IMP_LEVEL_IMPERSONATE`, but another one requires `RPC_C_IMP_LEVEL_DELEGATE`. Who wins? Or are those shell extensions mutually incompatible? And what about the effect your decision has on the other shell extensions hosted by Explorer? Now they are running with `RPC_C_IMP_LEVEL_IMPERSONATE` even though they didn't ask for it. Will that introduce a security vulnerability? Will those other shell extensions stop working or even crash? A shell extension is a guest in the host process's house. You don't go and change the color of the carpet when you are invited over for dinner.

This question is yet another example of using a global setting to solve a local problem. To solve your local problem (*I need this specific COM interface to run with impersonation*), use a local solution.

Raymond Chen

Follow