

Re: Start a new process WITH a visible window from a service?

Re: Start a new process WITH a visible window from a service?

Source: <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.language/2006-01/msg00254.html>

- *From:* adebaene@xxxxxxxxxxxxxxxxxxxx
 - *Date:* 9 Jan 2006 07:01:57 -0800
-

Mikael a écrit :

- > Hello!
- > I have written a simple service from which I would like to initiate a new
- > process that is started as a new window, visible for the user!!
- > I have tried CreateProcess with new process and SW_SHOWNORMAL/SW_SHOW e.t..c.
- > flag active!! Process starts BUT no window appears?
- > I also tried the ShellExecuteEx function with appropriate startup parameters
- > but process still starts with NO visible window.
- > I made the test using "Notepad.exe" as the visible editor that is to be
- > started!!
- >
- > How can I start a new VISIBLE process from my installed service?
- > Should code example would really help! :)

You need to understand some security context before putting together a solution, and the concepts would be better explained in microsoft.public.win32.programmer.kernel... Anyway :

– Each process has an associated user (owner), and when you create a child process with CreateProcess, it inherits the same owner as yours. A service typically runs under a "user" account with high privileges : SYSTEM.

– Each process also run inside a Desktop, which is hosted by a Window Station. A Desktop Station is basically a screen, keyboard and mouse. What you see on screen at one given time is a Desktop.

– Window Station and Desktop are a security boundary, because processes that run inside the same Window Station / Desktop can interact one upon another (by sending WM messages, hooking with SetWindowsHookEx, using the clipboard to paste something into another app, etc...). When the GUI subsystem was first written, there was no worry about security as today, so the whole GUI subsystem is inherently unsecure (Google for "shatter attack" if you want a concret example).

– For this reason, it is considered best security practice that all

Re: Start a new process WITH a visible window from a service?

Re: Start a new process WITH a visible window from a service?

apps running on one given Desktop are all owned by the same user. This also matches with what the user expects from a typical "Desktop" experience where it controls and "owns" everything that appears on the screen.

– Services are running in their own Desktop Station / Desktop (which is why you didn't see the notepad on screen in your test : it was displayed on another, invisible Desktop : The services desktop).

Given all of this, your best bet it to :

– Switch to the currently opened user desktop within your service (see `SetProcessWindowStation / SetThreadDesktop`). Note that the definition of "currently opened user desktop" can be quite difficult to cope with if you are envisaging the Remote Desktop / Fast User Switching capability of Windows XP and up. Also, do not forget to revert to your own Desktop when you're done.

– Use `CreateProcessAsUser` to launch the child process under the correct security account. Obtaining the user token can be challenging in itself.

Conclusion : It is most of the time a bad idea to try this from a security point of view, and it can become really difficult to get it right if FUS/Remote Desktop comes into play. Therefore, this kind of stuff is best avoided unless absolutely necessary.

You should instead envision another architecture. For example, you could write a user mode, GUI, app that is launched when the user log-in (through Startup folder in Start button Menu, registry "Run" key, etc...). This user-mode app connect with your service (using sockets, events, COM objects, .NET remoting, whatever other IPC mechanism you like...) and do whatever the service wants it to do on the user Desktop.

Arnaud
MVP – VC

-
- Prev by Date: [***Re: #define xxxxx***](#)
 - Next by Date: [***Re: Start a new process WITH a visible window from a service?***](#)
 - Previous by thread: [***Fast way to allocate buffer for producer/consumer scenario***](#)
 - Next by thread: [***Re: Start a new process WITH a visible window from a service?***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)