Outsmarting System File Protection
Tested in Windows 2000 sp2, Windows 2000 sp3 with and without IE6 sp1. Should work fine in XP and XPsp1

A lot of people are having troubles with System File Protection (SFP for short). This can be a major pain in the butt unless you know the tricks to it. Having only tweaked Windows 2000 Service Pack 3 I figured out a few things about SFP and replacing files:

1) TaskManger is your best friend when replacing files in 2k/XP.
When you open task manager you can do just about as much as you can do with Explorer just by going File>NewTask(Run..). From here you can either use the Run Dialog to launch programs one at a time, or select 'Browse' and explore. Using right click menu commands to do the bulk of your work (Copy, Paste, Rename). Problem is often times you can't replace items do to the fact that your browse is making calls to things you want to delete.

2) CommandLine or Cmd.exe is like that other friend you have that likes to help out.
One plus this has over TaskMan is you don't use the file you are trying to replace. A minus is that it can be a pain if you aren't an experienced DOS user.

3) Backups are your ace in the hole.
Always back your files up prior to doing anything (sometimes I don't bother and wish I did.). Keep It Simple Stupid applies here. Save yourself a few keystrokes and place your backups in something like C:\back\

4) SafeMode is the rest of the hand.
Windows2000 and XP (I believe) can both be booted into SafeMode. When your computer is first booting up, after your bios screen but before the Windows is Starting screen (I could be slightly wrong here seeing how I don't know the timing for sure.) you hit F4 or F8 to get the SafeMode menu. Select 'SafeMode with CommandPrompt'. Welcome to "DOS" on 2k/XP. Anything that can't be replaced while Windows is running can be replaced here. (url.dll) Syntax would be Copy c:\url.dll "c:\Program Files\Internet Explorer\" quotations allow you to put spaces in the path (I didn't know this)

...

Here we go. System File Protection, of Sytem File Checker is a neato feature of Windows meant to protect Joe Computeruser's PC from being ruined. When a needed System file is being replaced your File Checker says "Wait a minute this isn't mine." While this can be great in the long run, it's not a positive thing in Windows Hacking. The trick is to replace the files it uses to replace files.

...

1) First up you need to find the file you want to hack and then replace. Start>Search>Files and Folders>dllname. It's good to actually search for the file so you can find out all of the locations of all copies. Let the search finish just in case. If you have installed any service packs you will have probably have copies of the file in:

\winnt\servicepackfiles\i386\ (Win2k)
\windows\servicepackfiles\i386\ (XP)

As well as:

\winnt\system32\dllcache\ (hidden folder in Win2k)
\WINDOWS\system32\dllcache\ (hidden folder in XP)
\winnt\system32\ (win2k)
\windows\system32\ (XP)

2) Now that you have all of the locations, write them down on paper or your forehead just to be safe (backwards so it shows up in the mirror).

3) Make a backup (remember K.I.S.S.)

4) Hack your file and save it c:\ for simplicity.

5) Open TaskManger (Right click on your taskbar and select TaskManger)

6) Go to the 'Processes' Tab and find 'Explorer.exe' highlight it and push the 'End Process' button. Say Yeah to the popup.

7) Go to the first tab in TaskManger and select 'File>NewTask>Run>Browse' from this Window navigate to c:\ and higlight your hacked file. Right clic on it and select 'Copy' (don't Cut it.)

8) Nagivate to your Windows directory, open the \servicepackfiles\i386\ folder. Paste your hacked file and replace the copy that is in that folder.

9) Navigate to your respective dllcache folder, paste the file there too.

10) Replace the normail copy in system32 finally (or wherever it might be).

11) Reboot. Don't LogOff , Reboot.

Now chances are this won't go that smoothly. Either the file you want to replace is in use, or your pal and mine SFP will pop-up. It can mess with you in odd ways. I've replaced the servicepackfiles version and the dllcache files, then had SFP grab the normal and replace the other two with it. This can be frustrating. Or maybe the file is in use. This is where the Command Prompt comes into play. If you already replaced the files and rebooted to no change, launch TaskMan again, kill explorer.exe, then go 'File>NewTask>Run>Cmd.exe' Use the DOS commands to try to replace all of the copies of the file in that order using your hacked version in C:\

This is usually where you get the message from SFP telling you it's alive and kicking. You will get a rather urgent looking pop-up telling you that a file that Windows needs is being replaced by a different file. It will then ask you if you want keep the modified files. Say 'yes'. Next it will prompt you to insert your Windows cd to retrieve a copy of the file it needs. Click 'Cancel'. As a good rule of thumb, when you get this message replace what you need then reboot!

If your file still isn't changing, boot into SafeMode with CommandLine. Wait for Windows to take it's sweet time loading. Then just type copy c:\file.dll c:\winnt\servicepackfiles\i386\. Rinse and Repeat. Then reboot. This has worked for me 100% of the time, if followed it will work for you as well.

http://pixelarmy.org