Why doesn't Windows File Protection use ACLs to protect files?

devblogs.microsoft.com/oldnewthing/20060321-00

March 21, 2006

Raymond Chen

Windows File Protection works by replacing files after they have been overwritten. Why didn't Windows just apply ACLs to deny write permission to the files? We tried that. It didn't work. Programs expect to be able to overwrite the files. A program's setup would run and it decided that it needed to "update" some system file and attempt to overwrite it. If the system tried to stop the file from being overwritten, the setup program would halt and report that it was unable to install the file. Even if the operating system detected that somebody was trying to overwrite a system file and instead gave them a handle to `NUL`, those programs would nevertheless notice that they had been hoodwinked because as a "verification" step, they would open the file they had just copied and compare it against the "master copy" on the installation CD. The solution was to let the program think it had won, and then, when it wasn't looking, put the original back.

Now that Windows File Protection has been around for a few years, software installers have learned that it's not okay to overwrite system files (and trying to do it won't work anyway), so starting in Windows Vista, the Windows File Protection folks have started taking stronger steps to protect system files, and this includes using ACLs to make the files harder to replace. Presumably, they will have compatibility plans in place to accomodate programs whose setup really wants to overwrite a file.

Raymond Chen

Follow