When people ask for security holes as features: Silent install of uncertified drivers

devblogs.microsoft.com/oldnewthing/20050816-08

August 16, 2005

Raymond Chen

Probably the single greatest source of bluescreen crashes in Windows XP is buggy device drivers. Since drivers run in kernel mode, there is no higher authority checking what they're doing. If some user-mode code runs amok and corrupts memory, it's just corrupting its own memory. The process eventually crashes, but the system stays up. On the other hand, if a driver runs amok and corrupts memory, it's corrupting your system and eventually your machine dies.

In acknowledgement of the importance of having high-quality drivers, Windows XP warns you when an uncertified driver is being installed. Which leads to today's topic, a question from a device driver author.

> When I try to install any driver, I get a User Consent Dialog box which tells the user that this is an unsigned driver. Is it possible to author a driver installation package that by-passes this user consent dialog box?

The whole purpose of that dialog is to prevent the situation you desire from happening! [typo fixed 5pm] If you don't want the warning dialog, submit your driver for certification. (For testing purposes, you can sign your drivers with the test root certificate and install the test root certificate before running your setup program. Of course, installing the test root certificate also causes the desktop to read "For test purposes only" as a reminder that your machine is now allowing test-signed drivers to be installed.)

Driver writers, of course, find the certification process cumbersome and will do whatever they can to avoid it. Because, of course, if you submit your driver for certification, it might fail! This has led to varying degrees of shenanigans to trick the WHQL team into certifying a driver different from the one you intend to use. My favorite stunt was related to my by a colleague who was installing a video card driver whose setup program displayed a dialog that read, roughly, "After clicking OK, do not touch your keyboard or mouse while we prepare your system." After you click OK, the setup program proceeds to move the mouse programmatically all over the screen, opening the Display control panel, clicking on the

Advanced button, clicking through various other configuration dialogs, a flurry of activity for what seems like a half a minute. When faced with a setup program that does this, your natural reaction is to scream, “Aaaiiiiigh!”

Raymond Chen

Follow