Defrauding the WHQL driver certification process

devblogs.microsoft.com/oldnewthing/20040305-00

March 5, 2004

Raymond Chen

In a comment to one of my earlier entries, someone mentioned a driver that bluescreened under normal conditions, but once you enabled the Driver Verifier (to try to catch the driver doing whatever bad thing it was doing), the problem went away. Another commenter bemoaned that WHQL certification didn't seem to improve the quality of the drivers. Video drivers will do anything to outdo their competition. Everybody knows that they cheat benchmarks, for example. I remember one driver that ran the DirectX "3D Tunnel" demonstration program extremely fast, demonstrating how totally awesome their video card is. Except that if you renamed TUNNEL.EXE to FUNNEL.EXE, it ran slow again. There was another one that checked if you were printing a specific string used by a popular benchmark program. If so, then it only drew the string a quarter of the time and merely returned without doing anything the other three quarters of the time. Bingo! Their benchmark numbers just quadrupled. Anyway, similar shenanigans are not unheard of when submitting a driver to WHQL for certification. Some unscrupulous drivers will detect that they are being run by WHQL and disable various features so they pass certification. Of course, they also run dog slow in the WHQL lab, but that's okay, because WHQL is interested in whether the driver contains any bugs, not whether the driver has the fastest triangle fill rate in the industry. The most common cheat I've seen is drivers which check for a secret "Enable Dubious Optimizations" switch in the registry or some other place external to the driver itself. They take the driver and put it in an installer which does not turn the switch on and submit it to WHQL. When WHQL runs the driver through all its tests, the driver is running in "safe but slow" mode and passes certification with flying colors.

The vendor then takes that driver (now with the WHQL stamp of approval) and puts it inside an installer that enables the secret "Enable Dubious Optimizations" switch. Now the driver sees the switch enabled and performs all sorts of dubious optimizations, none of which were tested by WHQL.

Raymond Chen

Follow