Verifying that your system files are digitally signed

devblogs.microsoft.com/oldnewthing/20040616-00

June 16, 2004

Raymond Chen

If you want to re-check that the files on your system haven't been tampered with, you can run sigverif (by typing its name into the Start.Run dialog) and tell it to start scanning. (UI note: If you go into the Logging page on the Advanced dialog, you can get trapped where it insists on having a valid log file name even if you didn't ask for logging!) The signature verification process takes a while, so go and do something else while you're waiting. When it's done, you'll get a list of all the system files that are not digitally signed by Microsoft. Just because a file is listed here doesn't mean that it's necessarily bad, however. For example, it might be a video driver or printer driver. (Another UI note: You can't right-click the items in the list to view their properties, say, to see what company issued the files.)

One case when you would want to run sigverif is after you remove the test root certificate which was causing your desktop to say "for test/evaluation purposes only". That way you can find all the uncertified drivers that snuck in under cover of the test signature.

Raymond Chen

Follow