Just follow the rules and nobody gets hurt

devblogs.microsoft.com/oldnewthing/20031104-00

November 4, 2003

Raymond Chen

You may have been lazy and not bothered calling VirtualProtect(PAGE_EXECUTE) when you generated some code on the fly. You got away with it because the i386 processor page protections do not have a “read but don’t execute” mode, so anything you could read you could also execute.

Until now.

Starting with Windows XP Service Pack 2, on processors which support it (according to the web page, currently AMD K8, Itanium, and AMD64), the stack and heap will not be executable. If you try to execute the stack or the heap, an exception will be raised and the code will not execute. In other words, execute page protection will soon be enforced, now that processors exist that support it. (Actually, I believe Windows XP for Itanium already used this new protection level, so those of you who have been playing around with your Itanium may have seen this already.)

If you were a good developer and followed the rules on page protections, then this has no effect on you. But if you cheated the rules and took advantage of specific hardware implementation details, you may find yourself in trouble. Consider yourselves warned.

Raymond Chen

Follow