The hunt for a faster syscall trap

devblogs.microsoft.com/oldnewthing/20041215-00

December 15, 2004

Raymond Chen

The performance of the syscall trap gets a lot of attention.

I was reminded of a meeting that took place between Intel and Microsoft over fifteen years ago. (Sadly, I was not myself at this meeting, so the story is second-hand.)

Since Microsoft is one of Intel's biggest customers, their representatives often visit Microsoft to show off what their latest processor can do, lobby the kernel development team to support a new processor feature, and solicit feedback on what sort of features would be most useful to add.

At this meeting, the Intel representatives asked, "So if you could ask for only one thing to be made faster, what would it be?"

Without hesitation, one of the lead kernel developers replied, "Speed up faulting on an invalid instruction."

The Intel half of the room burst out laughing. "Oh, you Microsoft engineers are so funny!" And so the meeting ended with a cute little joke.

After returning to their labs, the Intel engineers ran profiles against the Windows kernel and lo and behold, they discovered that Windows spent a lot of its time dispatching invalid instruction exceptions. How absurd! Was the Microsoft engineer not kidding around after all?

No he wasn't.

It so happens that on the 80386 chip of that era, the fastest way to get from V86-mode into kernel mode was to execute an invalid instruction! Consequently, Windows/386 used an invalid instruction as its syscall trap.

What's the moral of this story? I'm not sure. Perhaps it's that when you create something, you may find people using it in ways you had never considered.

Raymond Chen

Follow