Book review: Advanced Windows Debugging (Mario Hewardt and Daniel Pravat)

December 18, 2007

Raymond Chen

Ever so often, somebody sends me a book, and most of the time I glance through it and say, "Eh." But not this time. _Advanced Windows Debugging_ will make you the envy of your friends (if your friends are computer nerds). Even the section with the "Oh come on every moron knows this already" title _Basic Debugger Tasks_ has stuff that I didn't know. Fortunately, you don't have to slog through the stuff you already do know in order to find it, because the nifty new debugger commands are set off in the snippets of debugger conversation. (And by debugger conversation, I mean output of a debugger based on the Windows debug engine, debuggers like `ntsd`, `kd` and `windbg`.) Once you get past the "basics", you still have loads more ahead of you. The book covers debugging scenarios like a corrupted heap, a deadlock, or 100% CPU usage, as well as debugging tasks, like following the trail of an LPC request from the client to the server, peeking at the token count of a semaphore, and reconstructing a partially-corrupted stack—and illustrates each investigation with both discussion and annotated debugger output. All the things that seasoned developers take for granted (because they have become instinctual after years of experience) are spelled out for you. Learn more from the book's web site, not unsurprisingly named advancedwindowsdebugging.com.

I'm keeping this book on my shelf. You can borrow it, but I'm going to insist that you return it when you're done.

Raymond Chen

Follow