The Itanium's so-called stack

devblogs.microsoft.com/oldnewthing/20050421-28

April 21, 2005

Raymond Chen

Last year I alluded to the fact that the Itanium processor has two stacks. The one that is traditionally thought of as "the stack" (and the one that the `sp` register refers to) is a manually managed block of memory from which a function can carve out space to use during its execution. For example, if you declare a local variable like

```
TCHAR szBuffer[MAX_PATH];
```

then that buffer will go on "the stack".

But not all local variables are on "the stack".

Recall that the Itanium has a very large number of registers, most of which participate in function calls. Consequently, many local variables are placed into registers rather than "the stack", and when a function is called, those registers are "squirreled away" by the processor and "unsquirreled" when the function returns. Where do they get squirreled? Well, the processor can often just squirrel them into other unused registers through a mechanism I won't go into. (Those still interested can read Intel's documents on the subject.) If the processor runs out of squirrel-space, it spills them into main memory, into a place known as the "register backing store". This is another stack-like chunk of memory separate from "the stack". (Here's Slava Oks artistic impression of the layout of the ia64's stacks.)

As already noted, one consequence of this dual-stack model is that a stack buffer overflow will not corrupt the return address, because the return address is not kept on "the stack"; rather, it is kept in the "squirrel space" or (in the case of spillage) in the register backing store.

Another consequence of this dual-stack model is that various tricks to locate the start of the stack will find only **one** of the stacks. Missing out on the other stack will cause problems if you think grovelling "the" stack will find all accessible object references.

The Itanium architecture challenges many assumptions and is much less forgiving of various technically-illegal-but-nobody-really-enforced-it-before shenanigans, some of which I have discussed in earlier entries. To this list, add the "second stack".

Raymond Chen

Follow