Uninitialized floating point variables can be deadly

devblogs.microsoft.com/oldnewthing/20080702-00

July 2, 2008

Raymond Chen

A colleague of mine related to me this story about uninitialized floating point variables. He had a function that went something like this, simplified for expository purposes. The `infoType` parameter specified which piece of information you're requesting, and depending on what you're asking for, one or the other of the output parameters may not contain a meaningful result.

```
BOOL GetInfo(int infoType, int *intResult, double *dblResult)
{
 int intValue;
 double dblValue;


 switch (infoType) {
 case NUMBER_OF_GLOBS:
  intValue = …;
  break;


 case AVERAGE_GLOB_SIZE:
  dblValue = …;
  break;
 …
 }
 *intResult = intValue;
 *dblResult = dblValue;
 …
}
```

After the product shipped, they started geting crash reports. This was in the days before Windows Error Reporting, so all they had to work from was the faulting address, which implicated the line `*dblResult = dblValue`.

My colleague initially suspected that `dblResult` was an invalid pointer, but a search of the entire code base ruled out that possibility.

The problem was the use of an uninitialized floating point variable. Unlike integers, not all bit patterns are valid for use as floating point values. There is a category of values known as *signaling NaNs*, or `SNaN` for short, which are special "not a number" values. If you ask the processor to, it will keep an eye out for these signaling NaNs and raise an "invalid operand" exception when one is encountered. (This, after all, is the whole reason why it's called a *signaling* NaN.)

The problem was that, if you are sufficiently unlucky, the leftover values in the memory assigned to the `dblValue` will happen to have a bit pattern corresponding to a `SNaN`. And then when the processor tries to copy it to `dblResult`, then exception is raised.

There's another puzzle lurking behind this one: Why wasn't this problem caught in internal testing? We'll learn about that next time.

Raymond Chen

Follow