Answers to exercise from Scrollbars Part 11

devblogs.microsoft.com/oldnewthing/20030917-00

September 17, 2003

Raymond Chen

Exercise: Why do we use the formula `c = a + (b-a)/2` instead of the simpler `c = (a+b)/2` ?

Answer: To avoid integer overflow in the computation of `a+b` .

Here, `a` and `b` are window coordinates, and the window can be anywhere. If the window were placed at extreme coordinates like (MAXLONG,MAXLONG), then the arithmetic would overflow and the "midpoint" would be incorrectly computed.

Note that the alternate formula `a+(b-a)/2` is also subject to overflow, this time in the computation of the value `b-a` . However, in our case, `b-a` is the width of our window, which is something that we can control.

Integer overflow was one of the Windows 95 application compatibility bugs that I had to deal with. There was a DOS game that wanted to do a binary search, and instead of using indices, they attempted to average the two pointers together:

```
BYTE *low = ...;
BYTE *high = ...;
BYTE *mid = ((UINT)low + (UINT)high)/2;
```

This worked as long as the game was being run under an operating system without virtual memory, because the "low" and "high" pointers would both be comparatively small numbers (nobody had machines with 2GB of RAM), so the sum `low+high` would not overflow.

Windows 95 ran these DOS games, but under a DPMI server that supported virtual memory. The DPMI specification permits the server to put memory anywhere, and we put our memory at the high end of the address space.

This program then overflowed in its attempt to average the two pointers and crashed.

So be careful how you average two values together. It's harder than you think.

Raymond Chen

Follow