

## Re: The dangers of replacing malloc()

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/performance/2003-06/0121.html>

---

**From:** D. J. Bernstein (*djb\_at\_cr.yp.to*)

**Date:** 06/28/03

Date: 28 Jun 2003 06:11:33 -0000

To: freebsd-performance@freebsd.org

Terry Lambert writes:

> *My argument in this case is that the valloc() interface is not  
> portable, and you should not use it.*

kqueue isn't portable, so you're saying nobody should use that, right?

Or do you admit that it's actually a good idea for people to use kqueue,  
with a compile-time fallback to poll or select? Great.

Now, what happens when some other system decides to emulate kqueue (not  
a huge surprise), using valloc (or some future xyzalloc), which in turn  
uses sbrk directly (as valloc already does on a huge number of systems,  
and as xyzalloc will probably do), rather than calling malloc?

That's right: it obliterates the data that I obtained from sbrk in my  
malloc replacement. Kaboom. This is exactly the failure mode I explained  
before. This is why the weak linking of the system's malloc is useless  
for experienced programmers who care about portability.

(Since you asked: My valloc-uses-sbrk-directly demonstration was under  
Linux, exactly as I said; specifically, Debian. Are you really so naive  
as to think that all the Linux functions are listed in the manual?)

---D. J. Bernstein, Associate Professor, Department of Mathematics,  
Statistics, and Computer Science, University of Illinois at Chicago

---

freebsd-performance@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-performance>

To unsubscribe, send any mail to "freebsd-performance-unsubscribe@freebsd.org"