Subject: Re: utrace regressions (was: -mm merge plans for 2.6.21)
Posted by Roland McGrath on Wed, 07 Mar 2007 09:10:29 GMT

> On Sat, Feb 17, 2007 at 06:35:31PM -0800, Roland McGrath wrote:
> > > Looking at mainline x86_64 ptrace code I think hole for u_debugreg[4]
> > > and [5] is also needed.
> >
> > It's not. The utrace_regset for the debugregs already has that behavior
> > for those two words, so mapping all 8 uarea words to the regset is fine.
>
> Sorry, I don't get it. Choosing segment from x86_64_uarea is done before
> calling regset->set and regset->get as well as before zero-filling. No
> segment for u_debugreg[4] and [5] means -EIO before segment handlers
> will have a chance to be called.
>
> Do you want to consolidate these two?
>
>   {offsetof(struct user, u_debugreg[0]), offsetof(struct user, u_debugreg[4]), 3, 0},
>   {offsetof(struct user, u_debugreg[6]), offsetof(struct user, u_debugreg[8]), 3, 6 * sizeof(long)},

Oops! I was misremembering what was in x86_64_uarea when I wrote that.
I've indeed fixed it to match what I thought it was:

 {offsetof(struct user, u_debugreg[0]),
  offsetof(struct user, u_debugreg[8]), 3, 0},

Thanks,
Roland