Subject: Re: utrace regressions (was: -mm merge plans for 2.6.21)
Posted by adobriyan on Tue, 13 Feb 2007 15:28:13 GMT
View Forum Message <> Reply to Message

On Mon, Feb 12, 2007 at 01:36:34PM -0800, Roland McGrath wrote:
> > We're aware of two regressions compared to mainline if ptrace is utrace:
>
> Thanks very much for bringing these to my attention.
>
> > 1) zero holes for PTRACE_PEEKUSR vanished.
>
> I've fixed this in the current patches.

Looking at mainline x86_64 ptrace code I think hole for u_debugreg[4]
and [5] is also needed.

```
--- a/arch/x86_64/kernel/ptrace.c
+++ b/arch/x86_64/kernel/ptrace.c
@@ -687,6 +687,8 @@ EXPORT_SYMBOL_GPL(utrace_x86_64_native);
 #ifdef CONFIG_PTRACE
 static const struct ptrace_layout_segment x86_64_uarea[] = {
  {0, sizeof(struct user_regs_struct), 0, 0},
+ {sizeof(struct user_regs_struct),
+  offsetof(struct user, u_debugreg[0]), -1, 0},
  {offsetof(struct user, u_debugreg[0]),
   offsetof(struct user, u_debugreg[4]), 3, 0},
  {offsetof(struct user, u_debugreg[6]),
```