Subject: Re: [PATCH -utrace] Move utrace into task_struct
Posted by Alexey Dobriyan on Tue, 08 May 2007 14:34:26 GMT
View Forum Message <> Reply to Message

Regardless of future of "struct utrace utrace;" patch looks like there
is another race: engine's flags and ops settings in utrace_detach() and
acting on them in report_quiescent():

```
utrace_detach()    report_quiescent()
---------------    ------------------
[utrace lock held]   [utrace lock is not held]

engine->flags = UTRACE_EVENT(QUIESCE) |
  UTRACE_ACTION_QUIESCE;
     if (engine->flags & UTRACE_EVENT(QUIESCE))
      REPORT(report_quiesce);

rcu_assign_pointer(engine->ops, &dead_engine_ops);
```

At the moment of REPORT call engine's ops are still "live" ptrace ops
which do not have ->report_quiesce callback. So, there will oops while
calling function at NULL address. "Dead" ptrace engine ops do have dummy
callback but it wasn't yet glued.

I hit this once with "struct utrace utrace;" patch applied, but this
bug is also present in stock utrace, I'm sure.