Subject: Re: [PATCH] late checking of permissions during PTRACE_ATTACH
Posted by Roland McGrath on Thu, 30 Aug 2007 06:36:49 GMT
View Forum Message <> Reply to Message

Thanks very much for your report. I'm sorry there's been such a delay before I could follow it up.

> ptrace_attach() does permissions check _after_ actual attaching. Given
> that utrace_attach is quite non-trivial operation there is no way such
> ordering should be allowed -- the following program should crash the box
> in less than second.

utrace_attach is intended to be a reasonably cheap operation. Anyway, we are never too concerned about the performance of an error case.

The reason ptrace_attach does utrace_attach first is to preserve the order of error diagnoses. That is, to avoid calling ptrace_may_attach at all if ptrace_attach is going to fail because someone is already attached. This keeps it consistent with vanilla ptrace. In particular, security_ptrace should not be called when ptrace_attach fails for the "already attached" or "already dead" errors. Whether the call succeeds or fails, it may trigger security logging or whatnot that should not be done for these cases.

The utrace_attach, utrace_detach sequence in a failing ptrace_attach is slightly costly. But it a) shouldn't be too bad and b) is just an error case. Moreover, it always ought to work without crashes whether it's a good idea or not!

Your patch fixes what's not itself a problem, and thereby masks the actual problem that needs fixing. Fortunately, I can now reproduce this problem quickly using your test case. This is the utrace_detach bug you previously identified in http://lkml.org/lkml/2007/5/8/244, which is already #1 on the wiki utrace/bugs list. I wasn't using a good test case for it before, but this case hits it. I think some reasonable fixes are straightforward, and now I can try one and test it with some confidence using this test case.

Thanks,
Roland