Subject: Re: [PATCH 5/9] Allow ptrace from non-init user namespaces
Posted by David Howells on Wed, 23 Feb 2011 17:11:01 GMT
View Forum Message <> Reply to Message

Serge E. Hallyn <serge@hallyn.com> wrote:

> +int same_or_ancestor_user_ns(struct task_struct *task,
> + struct task_struct *victim)
> +{
> + struct user_namespace *u1 = task_cred_xxx(task, user)->user_ns;
> + struct user_namespace *u2 = task_cred_xxx(victim, user)->user_ns;

Hmmm. task_cred_xxx() uses task->real_cred, which is correct for victim (the
object), but normally you'd use task->cred for task (the subject). However,
in this case, I think it's probably okay.

David

_____