Subject: Re: [patch 8/8] allow unprivileged fuse mounts
Posted by Miklos Szeredi on Sun, 22 Apr 2007 07:22:44 GMT
View Forum Message <> Reply to Message

> > + /*
> > +  * For unprivileged mounts use current uid/gid.  Still allow
> > +  * "user_id" and "group_id" options for compatibility, but
> > +  * only if they match these values.
> > +  */
> > + if (!capable(CAP_SYS_ADMIN)) {
> > +  d->user_id = current->uid;
> > +  d->user_id_present = 1;
> > +  d->group_id = current->gid;
> > +  d->group_id_present = 1;
> > +
> > + }
>
> CAP_SETUID is the appropriate capability...
>
> This is not a dimension we have not fully explored.
> What is the problem with a user controlled mount having different
> uid and gid values.
>
> Yes they map into different users but how is this a problem.
> The only problem that I can recall is the historic chown problem
> where you could give files to other users and mess up their quotas.
>
> Or is the problem other users writing to this user controlled
> filesystem?

Yes.  Or even just a suid process trying to access the user controlled filesystem.  See Documentation/filesystems/fuse.txt for the gory details.

Eric, thanks for the detailed review :)

Miklos