Subject: Re: Containers don't handle keys, but should they?
Posted by serue on Fri, 14 Mar 2008 16:17:11 GMT

View Forum Message <> Reply to Message

Quoting David Howells (dhowells@redhat.com):
> Serge E. Hallyn <serue@us.ibm.com> wrote:
>
> > It looks like maybe just adding a struct user_namespace * to a struct key
> > should suffice.
>
> That's not quite sufficient. The per-UID key_user structs also need to be
> differentiated. Unfortunately, I can't just merge it into user_struct as I
> then end up with a reference loop user_struct -> uid_keyring -> user_struct.
>
> Rooting the key_user trees in user_namespace will probably do the trick.
>
> A couple of questions:
>
> (1) A process may inherit a session keyring over clone(). Should this be
>   discarded if CLONE_NEWUSER is set? Or would I need to copy it?

Someone else may have stronger feelings about this. Personally so long
as a container setup program has a way of discarding the keyring
manually I think that's fine.

> (2) In a recent patch, I've given the root user its own quota limits. Is UID
>   0 always the root user in any container? Or would it make more sense
>   just to scrap the per-root quota limits?

Yeah uid 0 may not have a bunch of privileges, but it is still the root
user.

thanks,
-serge