Subject: Re: [PATCH 1/6] user namespace : add the framework
Posted by akpm on Mon, 16 Jul 2007 01:31:32 GMT
View Forum Message <> Reply to Message

On Mon, 4 Jun 2007 14:40:24 -0500 "Serge E. Hallyn" <serue@us.ibm.com> wrote:

> Add the user namespace struct and framework
>
> Basically, it will allow a process to unshare its user_struct table, resetting
> at the same time its own user_struct and all the associated accounting.
>
> A new root user (uid == 0) is added to the user namespace upon creation. Such
> root users have full privileges and it seems that theses privileges should be
> controlled through some means (process capabilities ?)

The whole magical-uid-0-user thing in this patch seem just wrong to
me.

I'll merge it anyway, mainly because I want to merge _something_ (why oh
why do the git-tree guys leave everything to the last minute?) but it strikes
me that there's something fundamentally wrong whenever the kernel starts
"knowing" about the significance of UIDs in this fashion.

It worries me.
_____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers