Subject: Re: [PATCH 4/8] user ns: hook permission
Posted by ebiederm on Wed, 24 Jan 2007 17:06:03 GMT
View Forum Message <> Reply to Message

"Serge E. Hallyn" <serue@us.ibm.com> writes:

> From: Serge E. Hallyn <serue@us.ibm.com>
> Subject: [PATCH 4/8] user ns: hook permission
>
> Hook permission to check vfsmnt->user_ns against current.

This looks wrong on several levels.
- This should ultimately be inside generic_permission instead of
  permission as there are some distributed filesystems that know how to cope with
  multiple mount namespaces simultaneous.

- As implemented the test is not what I would expect. I would
  expect comparisons of uid X == uid Y and gid X == gid Y to
  be replaced by comparing the tuples of uid namesspace and uid.
  Which would allow access to world readable/writeable files,
  and it would allow users with CAP_DAC_OVERRIDE to be able to access
  everything.

All we are really saying as I understand a user namespace is that
instead of uid's uniquely identifying a user the pair the pair uidns,
uid is uniquely identifies a user.

Because you didn't pick what I would consider the obvious choice
you now need an extra mount flag to disable the uid namespace all
together, so you can transition through the intermediate uid namespace
state. That really feels wrong.

All mounts should have an associated uid namespace and the only
way you should be able to ignore that is to access filesystems
that can cope with multiple uid namespaces simultaneously.

Eric

_____
Containers mailing list
Containers@lists.osdl.org
https://lists.osdl.org/mailman/listinfo/containers