Subject: Re: [PATCH 4/4] The control group itself
Posted by serue on Tue, 15 Jan 2008 17:49:41 GMT

View Forum Message <> Reply to Message

Quoting Paul Menage (menage@google.com):
> On Jan 15, 2008 6:44 AM, Serge E. Hallyn <serue@us.ibm.com> wrote:
> >
> > I don't think so... Wouldn't really make sense for the cgroup
> > infrastructure to presume to know what to enforce, and I don't see any
> > checks around the _write functions in cgroup.c, and no capable() calls
> > at all.
>
> The cgroup filesystem can provide simple unix-level permissions on any
> given file. Am I right in thinking that having an entry in the mapper
> doesn't automatically give privileges for a device to the members of
> the cgroup, but they also have to have sufficient privilege in their
> own right? If so, that might be sufficient.

Oh, well actually I think what we'd want is to require both
CAP_NS_OVERRIDE and either CAP_MKNOD or CAP_SYS_ADMIN. So it's probably
fine to leave this as is for now, and after I resend the patchset which
pushes CAP_NS_OVERRIDE (which is in a 4-patch userns patchset I've
been sitting on) the extra checks can be added.

> One other thought - should the parse/print routines themselves do a
> translation based on the device mappings for the writer/reader's
> cgroup? That way you could safely give a VE full permission to write
> to its children's device maps, but it would only be able to add/remap
> device targets that it could address itself.

Oh, well if we do this then we can just as well use the translation
functions to not allow a VE to add to its own set of devices, right?

Then maybe capable(CAP_NS_OVERRIDE|CAP_SYS_ADMIN) would only be required
to add devices.

Though there *is* some bit of danger to removing devices from a
privileged daemon, isn't there? Though I can't think of examples
just now. (Sorry, piercing headache, can't think quite right, will
think about this later)

-serge

____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers