

---

Subject: Re: [patch 8/9] unprivileged mounts: propagation: inherit owner from parent  
Posted by [Miklos Szeredi](#) on Tue, 15 Jan 2008 14:37:37 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

> > > On mount propagation, let the owner of the clone be inherited from the  
> > > parent into which it has been propagated. Also if the parent has the  
> > > "nosuid" flag, set this flag for the child as well.

> > >

> > > What about nodev?

> >

> > Hmm, I think the nosuid thing is meant to prevent suid mounts being  
> > introduced into a "suidless" namespace. This doesn't apply to dev  
> > mounts, which are quite safe in a suidless environment, as long as the  
> > user is not able to create devices. But that should be taken care of  
> > by capability tests.

> >

> > I'll update the description.

>

> Hmm,

>

> Part of me wants to say the safest thing for now would be to refuse  
> mounts propagation from non-user mounts to user mounts.

>

> I assume you're thinking about a fully user-mounted chroot, where  
> the user would still want to be able to stick in a cdrom and have  
> it automounted under /mnt/cdrom, propagated from the root mounts ns?

Right.

> But then are there no devices which the user could create on a floppy  
> while inserted into his own laptop, owned by his own uid, then insert  
> into this machine, and use the device under the auto-mounted /dev/floppy  
> to gain inappropriate access?

I assume, that the floppy and cdrom are already mounted with  
nosuid,nodev.

The problem case is I think is if a sysadmin does some mounting in the  
initial namespace, and this is propagated into the fully user-mounted  
namespace (or chroot), so that a mount with suid binaries slips in.  
Which is bad, because the user may be able rearrange the namespace, to  
trick the suid program to something it should not do.

OTOH, a mount with devices can't be abused this way, since it is not  
possible to gain privileges to files/devices just by rearranging the  
mounts.

Miklos

---

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

---