Subject: Re: [patch 0/8] mount ownership and unprivileged mount syscall (v4)
Posted by Karel Zak on Wed, 25 Apr 2007 09:23:56 GMT
View Forum Message <> Reply to Message

On Wed, Apr 25, 2007 at 09:18:28AM +0200, Miklos Szeredi wrote:
> > > The following extra security measures are taken for unprivileged
> > > mounts:
> > >
> > > - usermounts are limited by a sysctl tunable
> > > - force "nosuid,nodev" mount options on the created mount
> >
> > The original userspace "user=" solution also implies the "noexec"
> > option by default (you can override the default by "exec" option).
>
> Unlike "nosuid" and "nodev", I don't think "noexec" has real security
> benefits.

Yes. I agree.

> > It means the kernel based solution is not fully compatible ;-(
>
> Oh, I don't think that matters. For traditional /etc/fstab based user
> mounts, mount(8) will have to remain suid-root, the kernel can't
> replace the fstab check.

Ok, it makes sense. You're right that for the mount(8) is more
important the fstab check.

Please, prepare a mount(8) patch -- with the patch it will be more
clear.

> We could add a new "nosubmount" or similar flag, to prevent
> submounting, but that again would go against the simplicity of the
> current approach, so I'm not sure it's worth it.

The "nosubmount" is probably good idea.

The patches seem much better in v4. I'm fun for the feature in the
kernel (and also for every change that makes mtab more and more
obsolete :-).

   Karel

>
> Miklos
> -

> To unsubscribe from this list: send the line "unsubscribe linux-fsdevel" in
> the body of a message to majordomo@vger.kernel.org
> More majordomo info at http://vger.kernel.org/majordomo-info.html

--
Karel Zak <kzak@redhat.com>

Red Hat Czech s.r.o.
Purkynova 99/71, 612 45 Brno, Czech Republic
Reg.id: CZ27690016

_____
