Subject: Re: [patch 6/9] unprivileged mounts: allow unprivileged mounts
Posted by Miklos Szeredi on Wed, 09 Jan 2008 12:41:40 GMT
View Forum Message <> Reply to Message

> On Tue, Jan 08, 2008 at 12:35:08PM +0100, Miklos Szeredi wrote:
> > Define a new fs flag FS_SAFE, which denotes, that unprivileged mounting of
> > this filesystem may not constitute a security problem.
> >
> > Since most filesystems haven't been designed with unprivileged mounting in
> > mind, a thorough audit is needed before setting this flag.
> >
> > For "safe" filesystems also allow unprivileged forced unmounting.
>
> What about to list "safe" filesystems anywhere in /proc/fs/ ? I think
> it's very important information for admins.

Makes sense. I'll cook up something.

> Note, your patch for mount(8) is always trying to use unprivileged
> mount(2) for non-root users. It's overkill when unprivileged mounts are
> supported for bind mounts and fuse only. It would be nice to check
> if FS is "safe" before switch to unprivileged mode.

I think the little gain in performance is not worth the added
complexity. Especially if the added complexity is in the privileged
part, and itself can be a source of security holes.

> The "safe" definition is also very subjective and it depends on your
> level of paranoia. There should be a way (e.g. /proc) how control and
> modify the list of "safe" filesystems. For example I have no problem
> to mark cifs as "safe" for my home server.

OK, also makes some sense. Pavel's examples do point out that fuse
isn't as safe as I'd like it to be, so perhaps it would make sense to
default to just bind mounts being allowed, and having to explicity
enable unprivileged fuse mounts with a sysctl or whatever.

Miklos

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