Subject: Re: [PATCH 0/3] capabilities: per-process capbset
Posted by James Morris on Mon, 01 Oct 2007 23:03:38 GMT
View Forum Message <> Reply to Message

On Mon, 1 Oct 2007, Serge E. Hallyn wrote:

> Here is a new per-process capability bounding set patchset
> which I expect to send to linux-kernel soon. It makes
> the capbset per-process. A process can only permanently
> remove bits from it's bounding set, not add them. To
> remove bits, CAP_SYS_ADMIN is currently needed. Maybe
> that's not the best choice, but some privilege should
> probably be required.

I'm not clear on why privilege would required for a process to remove capability bits from its set. (Sure, if running setuid).

Doesn't that just make it more difficult to write safe applications ?

--
James Morris
<jmorris@namei.org>

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