Subject: Re: [patch 1/2] [RFC] Simple tamper-proof device filesystem.
Posted by Tetsuo Handa on Tue, 18 Dec 2007 00:03:23 GMT
View Forum Message <> Reply to Message

Hello.

Serge E. Hallyn wrote:
> CAP_MKNOD will be removed from its capability
I think it is not enough because the root can rename/unlink device files
(mv /dev/sda1 /dev/tmp; mv /dev/sda2 /dev/sda1; mv /dev/tmp /dev/sda2).

> To use your approach, i guess we would have to use selinux (or tomoyo)
> to enforce that devices may only be created under /dev?
Everyone can use this filesystem alone.
But use with MAC (or whatever access control mechanisms that prevent
attackers from unmounting/overlaying this filesystem) is recomennded.

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