Subject: Re: [patch 1/2] [RFC] Simple tamper-proof device filesystem.
Posted by Oren Laadan on Tue, 18 Dec 2007 01:39:47 GMT
View Forum Message <> Reply to Message

I hate to bring this again, but what if the admin in the container
mounts an external file system (eg. nfs, usb, loop mount from a file,
or via fuse), and that file system already has a device that we would
like to ban inside that container ?

Since anyway we will have to keep a white- (or black-) list of devices
that are permitted in a container, and that list may change even change
per container -- why not enforce the access control at the VFS layer ?
It's safer in the long run.

Oren.

Serge E. Hallyn wrote:
> Quoting Tetsuo Handa (penguin-kernel@i-love.sakura.ne.jp):
>> 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).
>
> Sure but that doesn't bother us :)
>
> The admin in the container has his own /dev directory and can do what he
> likes with the devices he's allowed to have. He just shouldn't have
> access to others. If he wants to rename /dev/sda1 to /dev/sda5 that's
> his choice.
>
>>> 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.
>
> Sure but it is worthless alone.
>
> No?
>
> What will keep the container admin from doing 'mknod /root/hda1 b 3 1'?
>
>> But use with MAC (or whatever access control mechanisms that prevent
>> attackers from unmounting/overlaying this filesystem) is recomennded.
>
> -serge
> _____
> Containers mailing list

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

_____

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