Subject: Re: [patch 1/2] [RFC] Simple tamper-proof device filesystem.
Posted by serge on Tue, 18 Dec 2007 02:53:33 GMT
View Forum Message <> Reply to Message

Quoting Tetsuo Handa (penguin-kernel@i-love.sakura.ne.jp):
> Hello.
>
> Serge E. Hallyn wrote:
> > But your requirements are to ensure that an application accessing a
> > device at a well-known location get what it expect.
>
> Yes. That's the purpose of this filesystem.
>
>
> > So then the main quesiton is still the one I think Al had asked - what
> > keeps a rogue CAP_SYS_MOUNT process from doing
> > mount --bind /dev/hda1 /dev/null ?
>
> Excuse me, but I guess you meant "mount --bind /dev/ /root/" or something
> because mount operation requires directories.

Nope, try

```
touch /root/hda1
ls -l /root/hda1
mount --bind /dev/hda1 /root/hda1
ls -l /root/hda1
```

But I see tomoyo prevents that

> MAC can prevent a rogue CAP_SYS_MOUNT process from doing
> "mount --bind /dev/ /root/".
> For example, regarding TOMOYO Linux, you need to give
> "allow_mount /dev/ /root/ --bind 0" permission
> to permit "mount --bind /dev/ /root/" request.

Ok, that answers my question. Thanks.

(I won't go into "who gets to say allow_mount" :)

> Did you mean "ln -s /dev/hda1 /dev/null" or "ln /dev/hda1 /dev/null"?
> No problem. MAC can prevent such requests too.

Then it sounds like this filesystem is something Tomoyo can use.

thanks,
-serge

_____

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

Subject: Re: [patch 1/2] [RFC] Simple tamper-proof device filesystem.
Posted by Tetsuo Handa on Tue, 18 Dec 2007 03:40:25 GMT
View Forum Message <> Reply to Message

Hello.

Serge E. Hallyn wrote:
> Nope, try
>
> touch /root/hda1
> ls -l /root/hda1
> mount --bind /dev/hda1 /root/hda1
> ls -l /root/hda1

[root@sakura ~]# touch /root/hda1
[root@sakura ~]# ls -l /root/hda1
-rw-r--r-- 1 root root 0 Dec 18 12:04 /root/hda1
[root@sakura ~]# mount --bind /dev/hda1 /root/hda1
[root@sakura ~]# ls -l /root/hda1
brw-r----- 1 root disk 3, 1 Dec 18 2007 /root/hda1

Oh, surprising.
I didn't know mount() accepts non-directory for mount-point.
But I think this is not a mount operation
because I can't see the contents of /dev/hda1 through /root/hda1 .
Can I see the contents of /dev/hda1 through /root/hda1 ?

> Then it sounds like this filesystem is something Tomoyo can use.

I had / partition mounted for read-only so that the admin can't do
'mknod /root/hda1 b 3 1' in 2003, and I named it
"Security Advancement Know-how Upon Readonly Approach for Linux" or SAKURA Linux.
This filesystem (SYAORAN) is developed to make /dev writable and tamper-proof
when / partition is read-only or protected by MAC.
TOMOYO is a pathname-based MAC implementation, and
SAKURA and SYAORAN were merged into TOMOYO Linux. ;-)

Regards.

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