

---

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 question 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>

---