Subject: Re: [patch 1/2] [RFC] Simple tamper-proof device filesystem.
Posted by Tetsuo Handa on Tue, 18 Dec 2007 02:26:21 GMT
View Forum Message <> Reply to Message

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.
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.

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

Regards.