Subject: Re: [PATCH] cgroups: implement device whitelist lsm (v3)
Posted by Greg KH on Tue, 18 Mar 2008 06:48:42 GMT
View Forum Message <> Reply to Message

On Mon, Mar 17, 2008 at 09:26:39AM -0400, Stephen Smalley wrote:
> > > The original promise was that LSM would allow kernels to be built that
> > > shed capabilities altogether,
> >
> > I don't remember that, but it's been a long time so it could be true.
>
> "One of the explicit requirements to get LSM into the kernel was to have
> the ability to make capabilities be a module. This allows the embedded
> people to completely remove capabilities, as they really want this. I
> don't think we can ignore this, no matter how much of a pain in the butt
> it is :)" - Greg KH
>
> Quoted from:
> http://marc.info/?l=linux-security-module&m=99236500727804&w=2
>
> Ironically, since that time, capabilities have doubled in size and still
> can't be removed from the core kernel since LSM didn't push the state
> into the security blobs.

Maybe we need to seriously revisit this and perhaps rip capabilities
back out and put it always into the kernel if it's always a requirement.

Comments made 7 years ago might be totally wrong when we have now
learned how this all has worked out...

thanks,

greg k-h

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