Subject: Re: LSM and Containers
Posted by Crispin Cowan on Wed, 24 Oct 2007 23:21:44 GMT
View Forum Message <> Reply to Message

Peter Dolding wrote:
> The other thing you have not though of and is critical. If LSM is the
> same LSM across all containers. What happens if that is breached and
> tripped to disable. You only want to loss one container to a breach
> not the whole box and dice in one hit. Its also the reason why my
> design does not have a direct link between controllers. No cascade
> threw system to take box and dice.
>
Sorry, but I totally disagree.

If you obtain enough privilege to disable the LSM in one container, you also obtain enough privilege to disable *other* LSMs that might be operating in different containers. This is a limitation of the Containers feature, not of LSM.

The purpose of LSM would be to manage privilege such that you cannot do damage, and in particular, any LSM that fails to prevent an attacker from disabling the LSM itself has failed, either in design, or in having an inadequate policy in place.

> The more I look at it more holes I find why the current LSM model just
> cannot keep on existing with Containers. Its not the best option.
> Hacking it to work with containers is only creating risks of more
> problems. The LSM model as also breed that problem of not sharing
> security tech advantages to everyone. Ie if they don't use our LSM
> they don't need/deserve our defense.
>
Again, I completely disagree.

Well, I agree that the hacking you proposed to permit different LSMs in different containers is a bad idea, so lets not do that :)

I see no need to support different LSMs in different containers. The complexity of such a feature would be very high. The utility strikes me as being very low; people who want that degree of separation of containers should be using Xen or KVM, not Containers.

> Different LSM per container from a security point of view appears
> critical. Sorry to say redesign from the ground up time everyone.
> Its a round peg into a square hole yes you can bash it in but it will
> never fit right.
>
I have no idea how you can support such assertions. Absolutely not. It is quite clear that the way to address security for containers is to

enhance individual LSM modules to be container-aware so that you can have separate policies in the separate containers. That is in keeping with the spirit of sharing the kernel, and providing separate instances to the users.

> ps sorry for going on so long I just see this as a major problem. If
> you have a solution to it tell me. Since a cut line has be put
> somewhere with containers.
>
Where as I see it as a very minor problem, and very easy to fix without any re-design of LSM, or of Containers. It only requires container-aware LSM modules.

Crispin

--
Crispin Cowan, Ph.D. http://crispincowan.com/~crispin/
Itanium. Vista. GPLv3. Complexity at work

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