Subject: Re: [PATCH 2/2] hijack: update task_alloc_security
Posted by serue on Tue, 27 Nov 2007 16:01:27 GMT
View Forum Message <> Reply to Message

Quoting Casey Schaufler (casey@schaufler-ca.com):
>
> --- Mark Nelson <markn@au1.ibm.com> wrote:
>
> > Subject: [PATCH 2/2] hijack: update task_alloc_security
> >
> > Update task_alloc_security() to take the hijacked task as a second
> > argument.
>
> Could y'all bring me up to speed on what this is intended to
> accomplish so that I can understand the Smack implications?

It's basically like ptracing a process, forcing it to fork, then having
the child execute a file and continue as your child. It takes part of
its state from the current process (stack etc), some from the hijacked
process (namespaces, keys?), and an lsm can decide for itself whose ->security
should be used for the child process.

There are a few reasons to do this. One is to do an admin activity
inside a private namespace, i.e. doing a new mount in a vserver in which
only websphere is running.

Paul has another use for it - basically (iiuc) wanting to be able to
keep a set of namespaces around which he can always enter. For mounts
namespaces that can be accomplished independent of hijack by setting up
a private mount tree and pivot_root()ing into there. But for other
namespaces that isn't an option.

thanks,
-serge

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