Subject: Re: [PATCH] capabilities: introduce per-process capability bounding set (v2)
Posted by serge on Fri, 28 Sep 2007 19:45:41 GMT
View Forum Message <> Reply to Message

Quoting Serge E. Hallyn (serue@us.ibm.com):
> Two comments on this patch.
>
> One issue that is buggine me is when capabilities are not in the
> kernel, we get no warning of that. You can do PR_SET_CAPBSET,
> and PR_GET_CAPBSET shows the right results after. But you are in
> no way constrained by that bset.
>
> It's not clear how to fix that, because of the weird ways in which
> commoncap.c is included in the kernel. There is no config variable
> you can rely on to know whether it is included or not. All values
> for cap_bset are valid so I can't rely on an invalid value to mean
> we're not using it. So the only options that come to mind are to
> create a a global variable using_capabilities, and define an
> __init function in security/commoncap.c that sets that to one. That,
> or really tweak security/Kconfig so we can in fact know when commoncap
> will be defined.
>
> Secondly, after setting the bcap, the current process'
> capabilities are not reduced. It takes effect after future
> execs. Is that deemed counterintuitive? Or will it be
> sufficient to properly document that in the prctl manpage?
>
> thanks,
> -serge

fwiw if anyone was actually thinking about these, I've
addressed both in a new patchset. Unfortunately adequate
testing will have to wait until next week so I'll send the
set out after that.

thanks,
-serge

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