Subject: Re: [PATCH 2/9] security: Make capabilities relative to the user namespace.
Posted by David Howells on Wed, 23 Feb 2011 11:40:09 GMT
View Forum Message <> Reply to Message

Serge E. Hallyn <serge@hallyn.com> wrote:

> int (*capable) (struct task_struct *tsk, const struct cred *cred,
> - int cap, int audit);
> + struct user_namespace *ns, int cap, int audit);

Hmmm... A chunk of the contents of the cred struct are user-namespaced. Could you add the user_namespace pointer to the cred struct and thus avoid passing it as an argument to other things.

In fact, I think you probably have to do this so that cachefiles, for example, can override the user namespace when it operates on behalf of a process that's in another namespace.

In fact, looking later on in your patch, I see:

> - || (cap_capable(current, current_cred(), CAP_SETPCAP,
> + || (cap_capable(current, current_cred(),
> + current_cred()->user->user_ns, CAP_SETPCAP,

so the user_ns _is_ already available through the creds. So is there really a need to pass it as an argument to anything that already takes a cred?

> * @cred contains the credentials to use.
> + * @ns contains the user namespace we want the capability in
> * @cap contains the capability <include/linux/capability.h>.

That should be tabbed to match the lines either side.

David

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