Subject: Re: [PATCH 2/9] security: Make capabilities relative to the user namespace.
Posted by Daniel Lezcano on Fri, 18 Feb 2011 23:44:50 GMT
View Forum Message <> Reply to Message

On 02/17/2011 04:03 PM, Serge E. Hallyn wrote:
> - Introduce ns_capable to test for a capability in a non-default
> user namespace.
> - Teach cap_capable to handle capabilities in a non-default
> user namespace.
>
> The motivation is to get to the unprivileged creation of new
> namespaces. It looks like this gets us 90% of the way there, with
> only potential uid confusion issues left.
>
> I still need to handle getting all caps after creation but otherwise I
> think I have a good starter patch that achieves all of your goals.
>
> Changelog:
> 11/05/2010: [serge] add apparmor
> 12/14/2010: [serge] fix capabilities to created user namespaces
> Without this, if user serge creates a user_ns, he won't have
> capabilities to the user_ns he created. THis is because we
> were first checking whether his effective caps had the caps
> he needed and returning -EPERM if not, and THEN checking whether
> he was the creator. Reverse those checks.
> 12/16/2010: [serge] security_real_capable needs ns argument in !security case
> 01/11/2011: [serge] add task_ns_capable helper
> 01/11/2011: [serge] add nsown_capable() helper per Bastian Blank suggestion
> 02/16/2011: [serge] fix a logic bug: the root user is always creator of
> init_user_ns, but should not always have capabilities to
> it! Fix the check in cap_capable().
>
> Signed-off-by: Eric W. Biederman<ebiederm@xmission.com>
> Signed-off-by: Serge E. Hallyn<serge.hallyn@canonical.com>
> ---

Acked-by: Daniel Lezcano <daniel.lezcano@free.fr>