
Subject: Re: [PATCH RFC] capabilities: introduce per-process capability bounding set

Posted by [Andrew Morgan](#) on Thu, 20 Sep 2007 04:16:58 GMT

[View Forum Message](#) <> [Reply to Message](#)

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Serge E. Hallyn wrote:

```
> + case PR_GET_CAPBSET:
> +   error = put_user(current->cap_bset, (unsigned long __user *)arg2);
> +   break;
> + case PR_SET_CAPBSET:
> +   if (!capable(CAP_SYS_ADMIN))
> +     return -EPERM;
> +   if (!cap_issubset(arg2, current->cap_bset))
> +     return -EINVAL;
> +   current->cap_bset = arg2;
> +   break;
```

You need to pass the capability magic value in both get and set directions... Otherwise, you'll not be able to tell what vintage of cap_bset you are manipulating.

Cheers

Andrew

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.6 (GNU/Linux)

iD8DBQFG8fQ0QheEq9QabflRApzJAKCUSxj72X4F++kNGy29oO6FE/OGAgCelrBw
dzyfE/XF2FI71WQvIwu/E9s=
=hkFZ

-----END PGP SIGNATURE-----

Containers mailing list

Containers@lists.linux-foundation.org

<https://lists.linux-foundation.org/mailman/listinfo/containers>
