
Subject: Re: [PATCH 1/1] capabilities: introduce per-process capability bounding set (v8)

Posted by [Andrew Morgan](#) on Tue, 20 Nov 2007 05:37:03 GMT

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

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

Hash: SHA1

Andrew Morgan wrote:

```
>> + current->cap_effective = cap_intersect(current->cap_effective,  
>> + current->cap_bset);  
>> + current->cap_permitted = cap_intersect(current->cap_permitted,  
>> + current->cap_bset);  
>> + current->cap_inheritable = cap_intersect(current->cap_inheritable,  
>> + current->cap_bset);  
>
```

```
> You might want to replace the above three lines with a restriction  
> elsewhere on what CAP_SETPCAP can newly set in  
> commoncap.c:cap_capset_check().  
>
```

```
> That is, CAP_SETPCAP permits the current process to raise 'any' pl  
> capability. I suspect that you'll want to prevent raising any bits not  
> masked by this:
```

```
>  
> pl' & ~(pl | (pP & cap_bset)).
```

On second thoughts, I really meant this:

```
diff --git a/security/commoncap.c b/security/commoncap.c  
index 302e8d0..b28c0c1 100644  
- --- a/security/commoncap.c  
+++ b/security/commoncap.c  
@@ -133,6 +133,12 @@ int cap_capset_check (struct task_struct *target,  
kernel_cap_t *cap_inheritable) {  
    /* incapable of using this inheritable set */  
    return -EPERM;  
}  
+ if (!cap_issubset(*inheritable,  
+                 cap_combine(target->cap_inheritable,  
+                             current->cap_bset))) {  
+     /* no new pl capabilities outside bounding set */  
+     return -EPERM;  
+ }  
  
    /* verify restrictions on target's new Permitted set */  
    if (!cap_issubset (*permitted,
```

Cheers

Andrew

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

Version: GnuPG v1.2.6 (GNU/Linux)

iD8DBQFHQnJ8QheEq9QabfIRAI2rAJ4jH+I36N1+cHV+1A3DJpXs+UNsFgCgkg8H

xOU/7dCrEq02xk9EgcRarg0=

=FbqU

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

Containers mailing list

Containers@lists.linux-foundation.org

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