On 11/23/06, Pavel Emelianov <xemul@openvz.org> wrote:
> You mean moving is like this:
>
> old_bc = task->real_bc;
> task->real_bc = new_bc;
> cmpxchg(&tsk->exec_bc, old_bc, new_bc);
>
> ? Then this won't work:
>
> Initialisation:
> current->exec_bc = init_bc;
> current->real_bc = init_bc;
> ...
> IRQ:
> current->exec_bc = init_bc;
> ...
>   old_bc = tsk->real_bc; /* init_bc */
>   tsk->real_bc = bc1;
>   cx(tsk->exec_bc, init_bc, bc1); /* ok */
> ...
> Here at the middle of an interrupt
> we have bc1 set as exec_bc on task
> which IS wrong!

You could get round that by having a separate "irq_bc" that's never
valid for a task not in an interrupt.

Paul