Subject: Re: [RFC][PATCH 4/7] UBC: syscalls (user interface)
Posted by Arnd Bergmann on Fri, 18 Aug 2006 11:40:30 GMT
View Forum Message <> Reply to Message

On Wednesday 16 August 2006 17:39, Kirill Korotaev wrote:

> @@ -304,3 +304,6 @@ SYSCALL_SPU(fchmodat)

> +SYSCALL(sys_getluid)
> +SYSCALL(sys_setluid)
> +SYSCALL(sys_setublimit)
...

> @@ -619,10 +619,16 @@ __SYSCALL(__NR_sync_file_range, sys_sync

> +__SYSCALL(__NR_getluid, sys_getluid)

> +__SYSCALL(__NR_setluid, sys_setluid)

> +__SYSCALL(__NR_setublimit, sys_setublimit)

...
> +/*

> + */
> +asmlinkage long sys_setublimit(uid_t uid, unsigned long resource,

While I don't yet understand what this call does, it looks to me that
the way it's implemented breaks in 32 bit emulation mode on x86_64 and
powerpc.

You either need to pass a pointer a something that is the same on 32 and
64 bit (e.g. __u64 __user *limits), or need to provide a different
entry point for 32 bit applications:

long compat_sys_setublimit(compat_uid_t uid, compat_ulong_t resource,
    compat_ulong_t __user *limits);

You should also add the prototypes to include/linux/syscalls.h.

Arnd <><