Subject: Re: [NETLINK] Don't attach callback to a going-away netlink socket
Posted by Evgeniy Polyakov on Wed, 18 Apr 2007 08:17:07 GMT
View Forum Message <> Reply to Message

On Wed, Apr 18, 2007 at 12:16:18PM +0400, Pavel Emelianov (xemul@sw.ru) wrote:
> Sorry, I forgot to put netdev and David in Cc when I first sent it.
>
> There is a race between netlink_dump_start() and netlink_release()
> that can lead to the situation when a netlink socket with non-zero
> callback is freed.

Out of curiosity, why not to fix a netlink_dump_start() to remove
callback in error path, since in 'no-error' path it removes it in
netlink_dump().

And, btw, can release method be called while socket is being used, I
thought about proper reference counters should prevent this, but not
100% sure with RCU dereferencing of the descriptor.

--
Evgeniy Polyakov