Subject: Re: [NETLINK] Don't attach callback to a going-away netlink socket
Posted by Evgeniy Polyakov on Wed, 18 Apr 2007 09:14:18 GMT

On Wed, Apr 18, 2007 at 01:03:56PM +0400, Pavel Emelianov (xemul@sw.ru) wrote:
> > Yes, you are right, that it will not be freed in netlink_release(),
> > but it will be freed in netlink_dump() after it is processed (in no-error
> > path only though).
> >
>
> But error path will leak it. On success path we would have
> a leaked packet in sk_write_queue, since we did't see it in
> skb_queue_purge() while doing netlink_release().
>
> Of course we can place the struts in code to handle the case
> when we have a released socket with the attached callback, but
> it is more correct (IMHO) not to allow to attach the callbacks
> to dead sockets.

That is why I've asked why such approach is used but not freeing
callback in errror (well, no-dump name is better to describe that path)
path, and more generally, why callback is attached, but not freed in the
function, but instead is freed next time dump started.

--
 Evgeniy Polyakov