Subject: Re: [PATCH] Copy mac_len in skb_clone() as well
Posted by Alexey Kuznetsov on Thu, 15 Mar 2007 16:04:36 GMT
View Forum Message <> Reply to Message

Hello!

> What bug triggered that helped you discover this?  Or is it
> merely from a code audit?

I asked the same question. :-)

openvz added some another fields to skbuff and when it was found
that they are lost while clone, he tried to figure out how all this works
and looked for another examples of this kind.

As I understand, the problem can be seen only in xfrmX_tunnel_input.
If uninitialized mac_len obtained from slab is more than current head room
it could corrupt memory.

Also, it looks like the fix is incomplete. copy_skb_header() also does not
copy this field. But it will be initialized to 0 by alloc_skb in this case
and xfrmX_tunnel_input() just will not copy mac header.

Alexey