

Re: IoSkipCurrentIrpStackLocation() design flaw?

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2006-09/msg00854.html>

- *From:* BubbaGump <bubbagump2685@xxxxxxxxxxxx>
 - *Date:* Thu, 21 Sep 2006 11:50:58 -0400
-

On Thu, 21 Sep 2006 06:37:08 +0400, "Maxim S. Shatskih"
<maxim@xxxxxxxxxxxxxxxx> wrote:

— For instance, the basic problem with my original question about IoSkipCurrentIrpStackLocation() was a race that if not handled with both an outer reference and an inner remove lock could cause arbitrary code to be executed or an IRP to be lost and never completed. —

Such races are the headache of the originator of the IRP, not of the drivers below which execute this IRP.

I should be clear to differentiate my objection to whether originators should do this from my question about whether all current originators do. The problem isn't just proposing a set of conventions. It's figuring out what conventions have been established over the years. The remove lock discussion in the WDM book mentioned a few odd cases in this area.

I want to know what to do in my own driver not just so that I can blame the OS or someone else when it crashes, but so that I can predict some reasonable possibilities for what they might do and prevent the crash from ever happening.