

questions about fb_pan_display ioctl

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2003-08/8295.html>

From: Arvind Sankar (*arvinds_at_MIT.EDU*)

Date: 08/30/03

Date: Sat, 30 Aug 2003 13:02:47 -0400
To: linux-fbdev-devel@lists.sourceforge.net

I was looking through the source, and am mightily confused as to how this works.

1. The FBIOPAN_DISPLAY ioctl does not error-check var.
2. fb_pan_display uses info->var to bounds-check var->?offset.
3. fb_pan_display modifies info->var, but var is what is returned by the ioctl.
4. The function pointer info->fbops->fb_pan_display takes its args in the opposite order to fb_pan_display! Who came up with this?
5. vesafb_pan_display uses var to bounds-check var->?offset, which is
 - (a) pointless, since fb_pan_display has bounds-checked it already.
 - (b) buggy, since var has never been error-checked, so var->yres could be anything.
6. How does wrapping work, when fb_pan_display has already made sure that yoffset cannot cause display to go beyond yres_virtual? The checks in vesafb_pan_display do this only when ywrap is disabled, but fb_pan_display always does it.
7. vesafb never uses more than 16mb of video ram, so wrapping can never happen on boards with more than 16mb of ram, no?

All these comments refer to 2.6.0-test4. Point 6 should apply to all the fb devices, not just vesafb.

In 2.4.22, there is no fb_pan_display, but vesafb_pan_display is the same, so it turns out that wrapping is allowed, but subject to the issues in 5(b) and 7. The issue in 7 is actually worse, because unless the vram option is passed, the video size is computed from the mode resolution, so it has nothing to do with the actual amount of accessible video memory.

-- arvind

-

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@vger.kernel.org

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>