Sugar: Secure GPU Acceleration in Web Browsers

Zhihao Yao, Zongheng Ma, Yingtong Liu, Ardalan Amiri Sani, Aparna Chandramowlishwaran

Trustworthy Systems Lab, UC Irvine

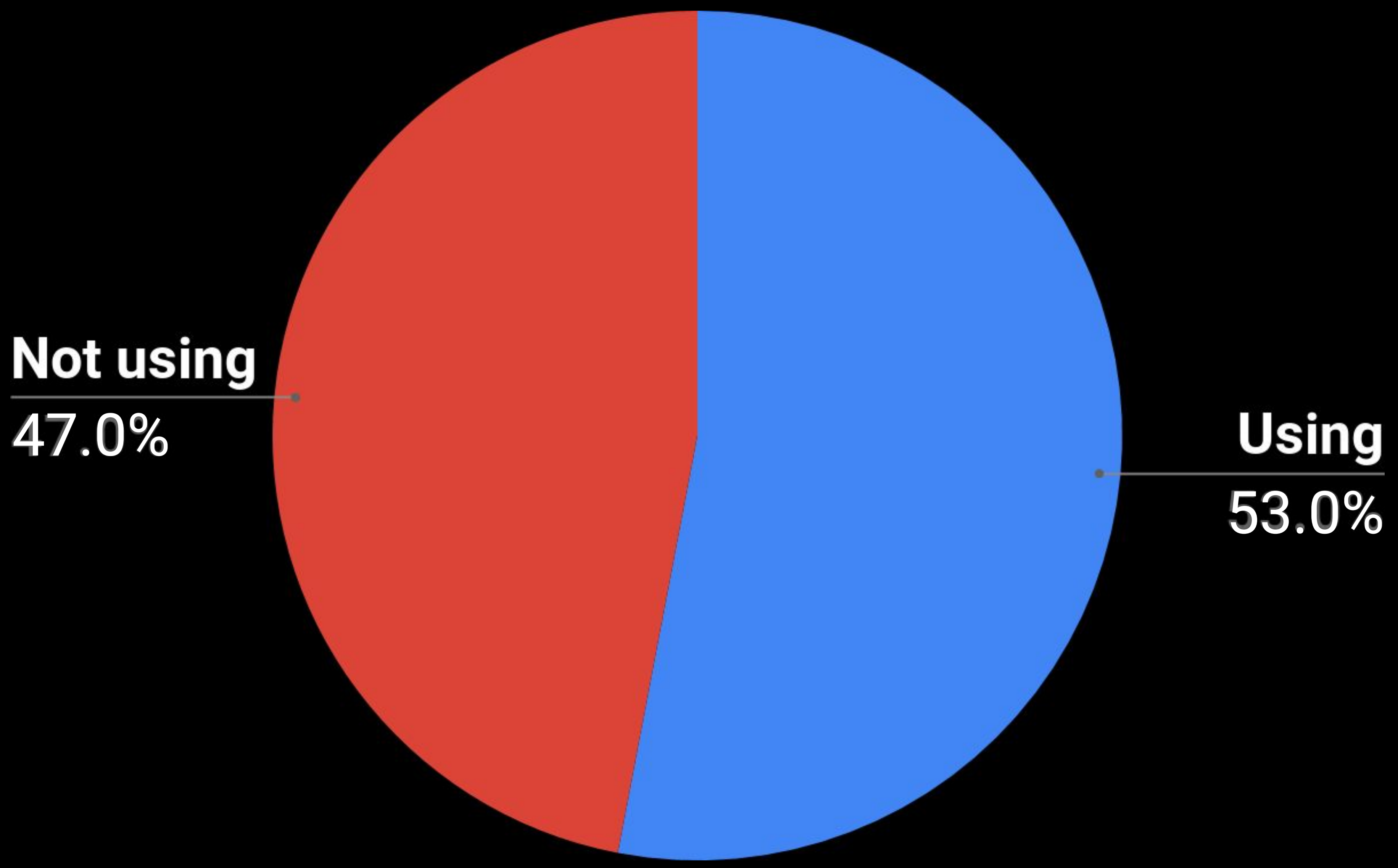
WebGL was released in 2011

Search Google Maps
Z
Fort Point
Golden Gate Bridge
Welcome Center
Fort Point
Rock
Map
Google
2D
Imagery ©2017 Google, Landsat / Copernicus, Data SIO, NOAA, U.S. Navy, NGA, GEBCO, Data LDEO-Columbia, NSF, NOAA, Map data ©2017 Google
United States
Terms
Send feedback
200 ft

Source: https://www.google.com/map

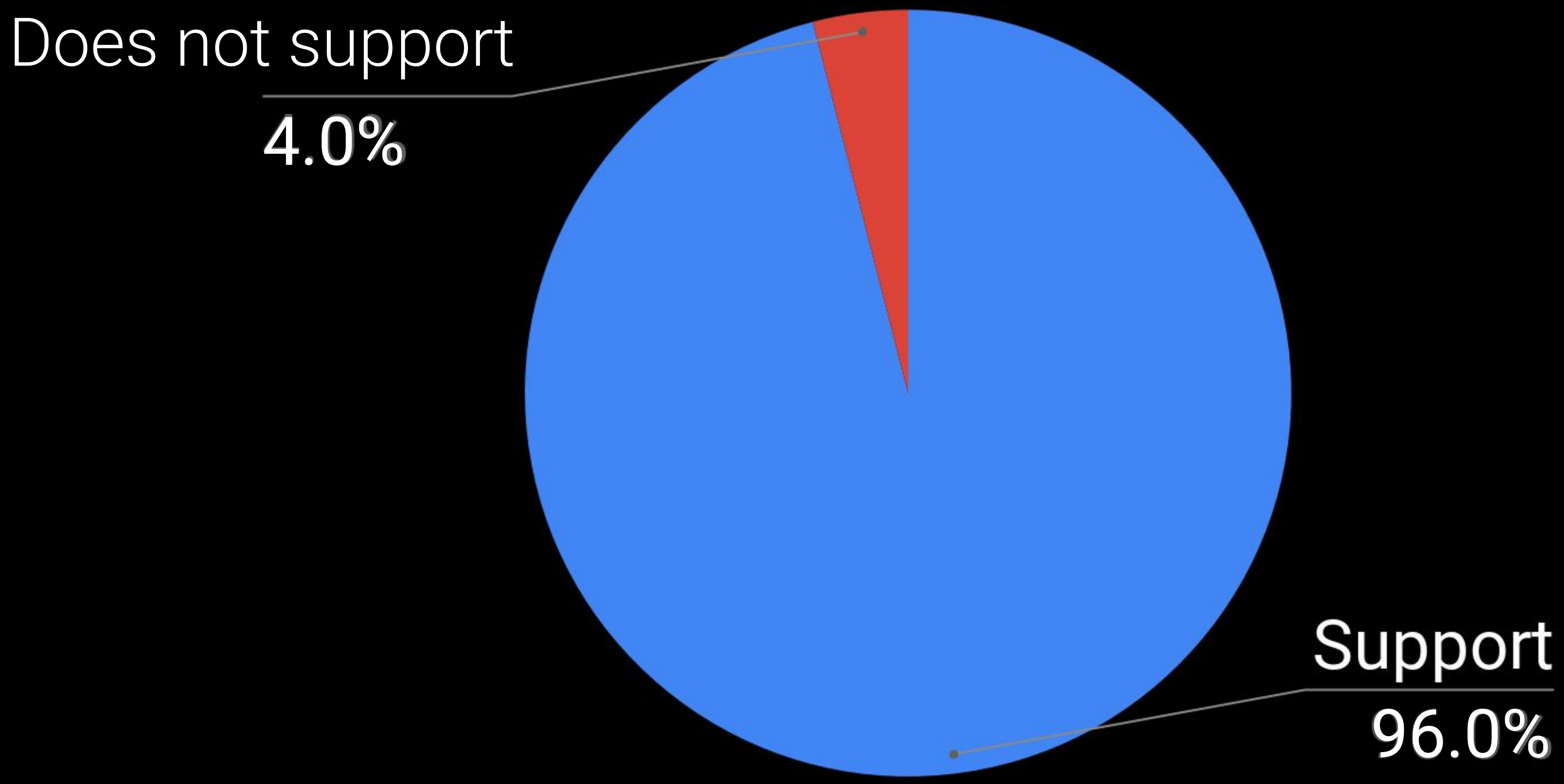
WebGL is popular

WebGL adoption rate by top 100 websites

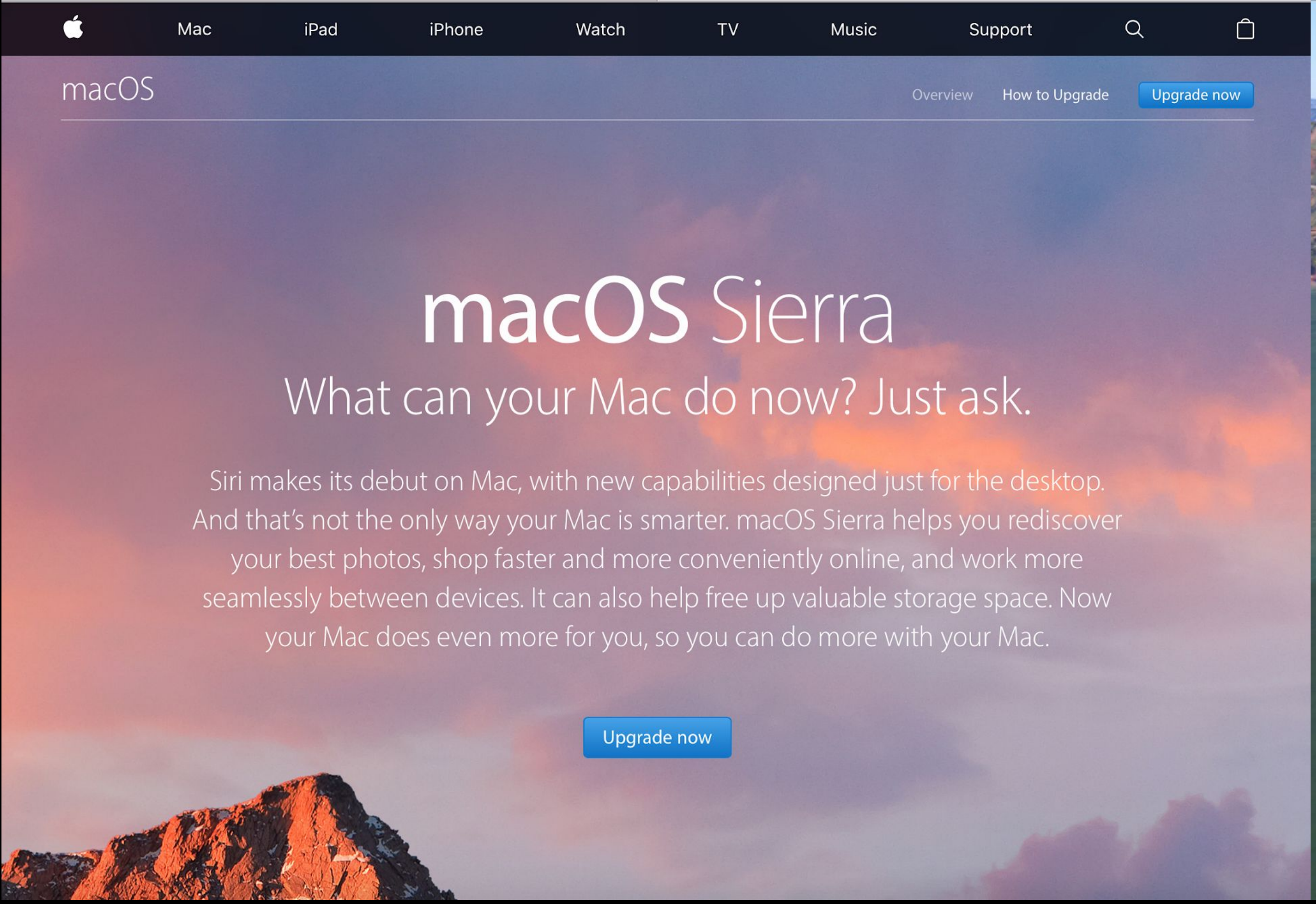


WebGL is popular

Browser support rate (48.8 million visitors)



Source: http://webglstats.com (2017)

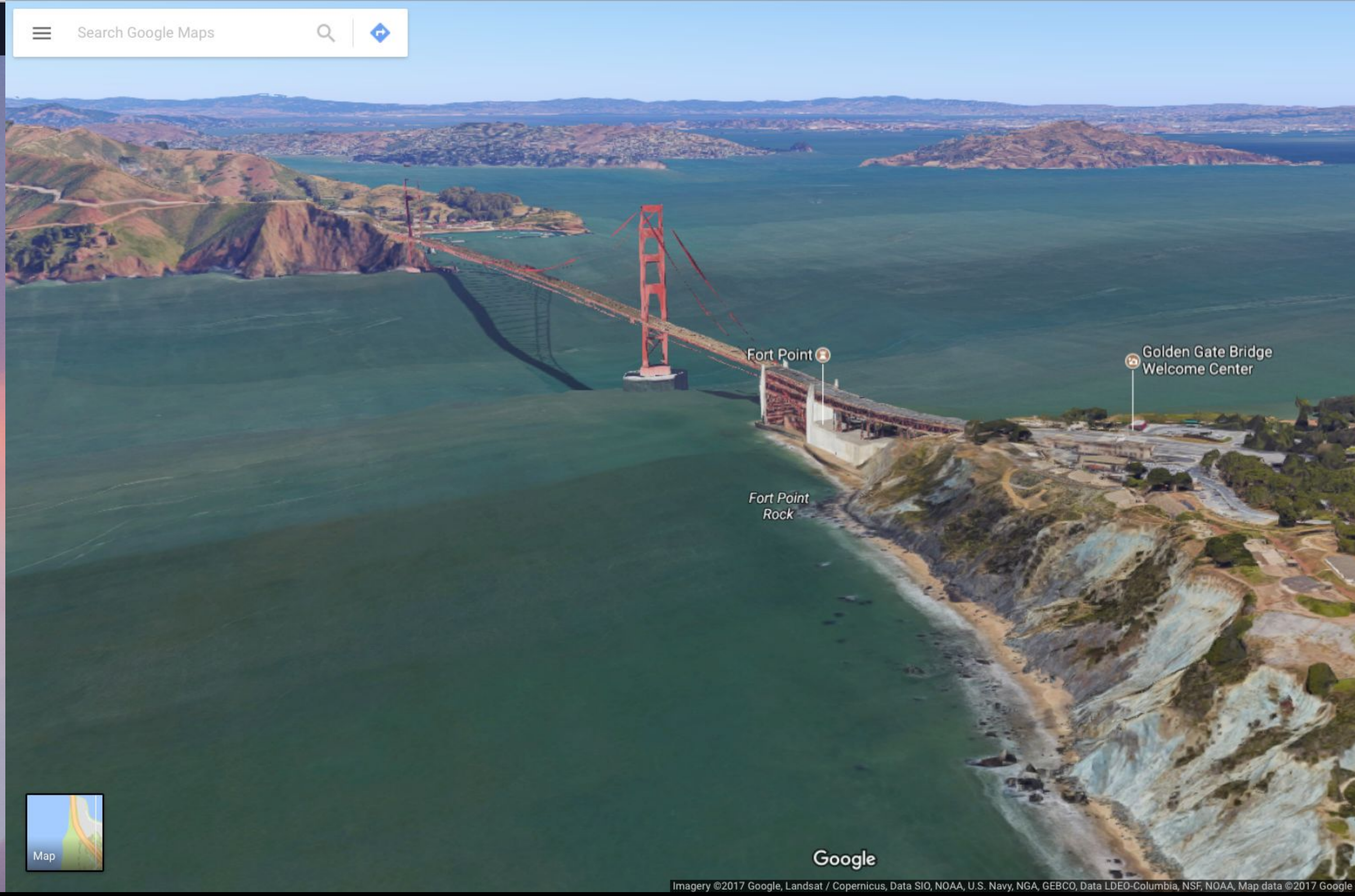


macOS Sierra

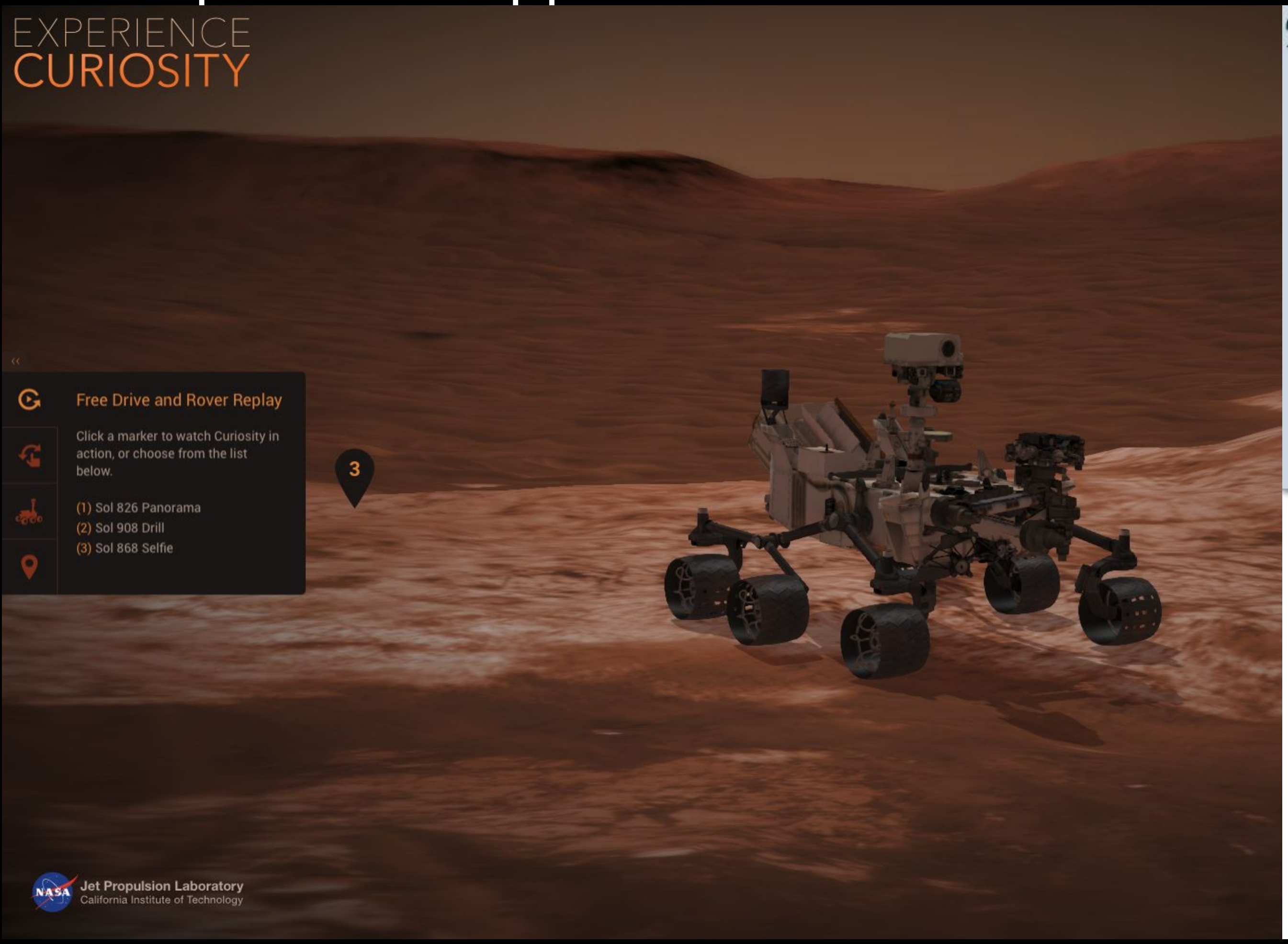
What can your Mac do now? Just ask.

Siri makes its debut on Mac, with new capabilities designed just for the desktop. And that's not the only way your Mac is smarter. macOS Sierra helps you rediscover your best photos, shop faster and more conveniently online, and work more seamlessly between devices. It can also help free up valuable storage space. Now your Mac does even more for you, so you can do more with your Mac.

https://www.apple.com/macos/sierra/


Search Google Maps
Fort Point
Golden Gate Bridge Welcome Center
Fort Point Rock
Map
Google
Imagery ©2017 Google, Landsat / Copernicus, Data SIO, NOAA, U.S. Navy, NGA, GEBCO, Data LDEO-Columbia, NSF, NOAA, Map data ©2017 Google

https://www.google.com/map



Free Drive and Rover Replay

Click a marker to watch Curiosity in action, or choose from the list below.

(1) Sol 826 Panorama
(2) Sol 908 Drill
(3) Sol 868 Selfie

https://eyes.nasa.gov/curiosity/

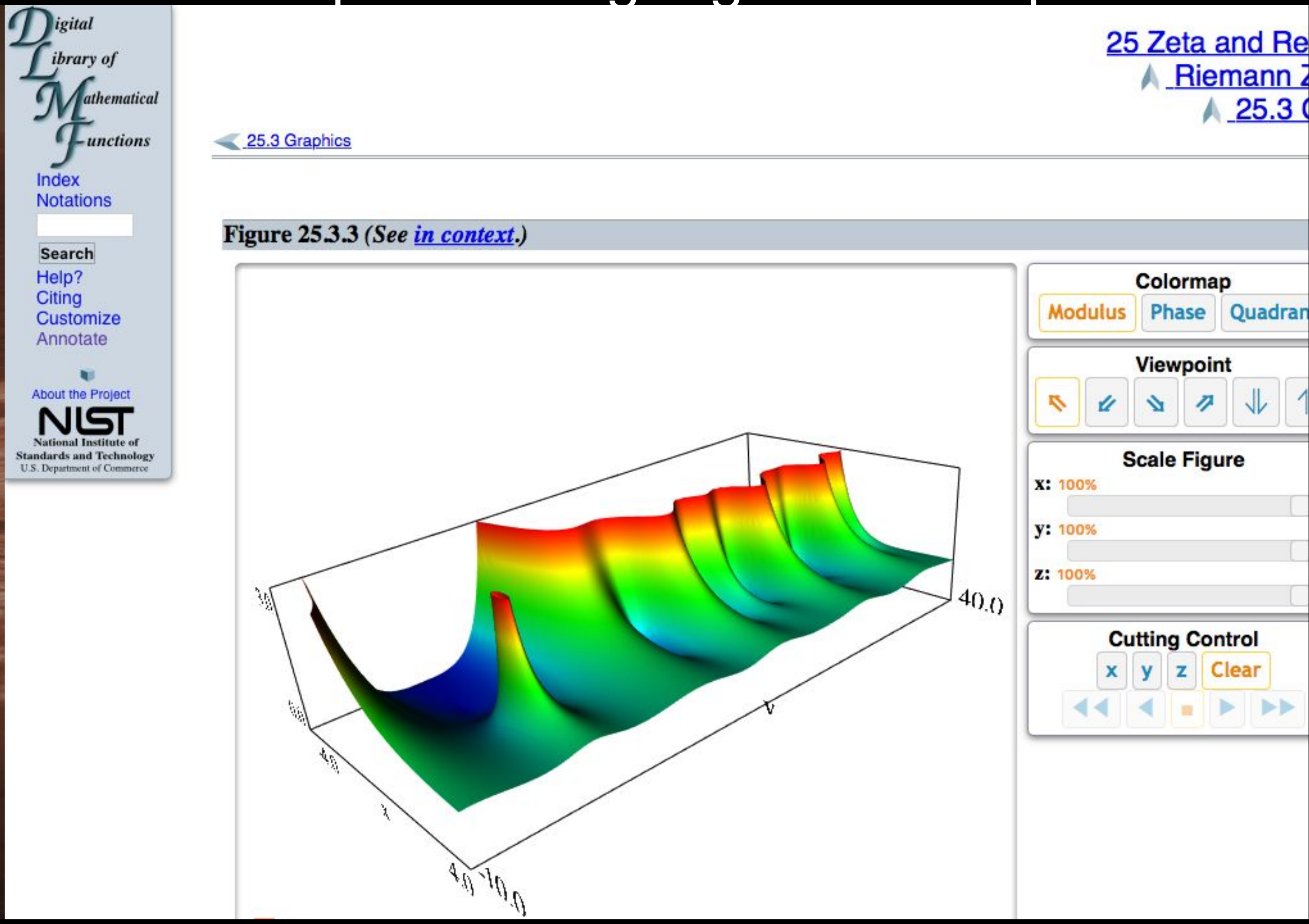
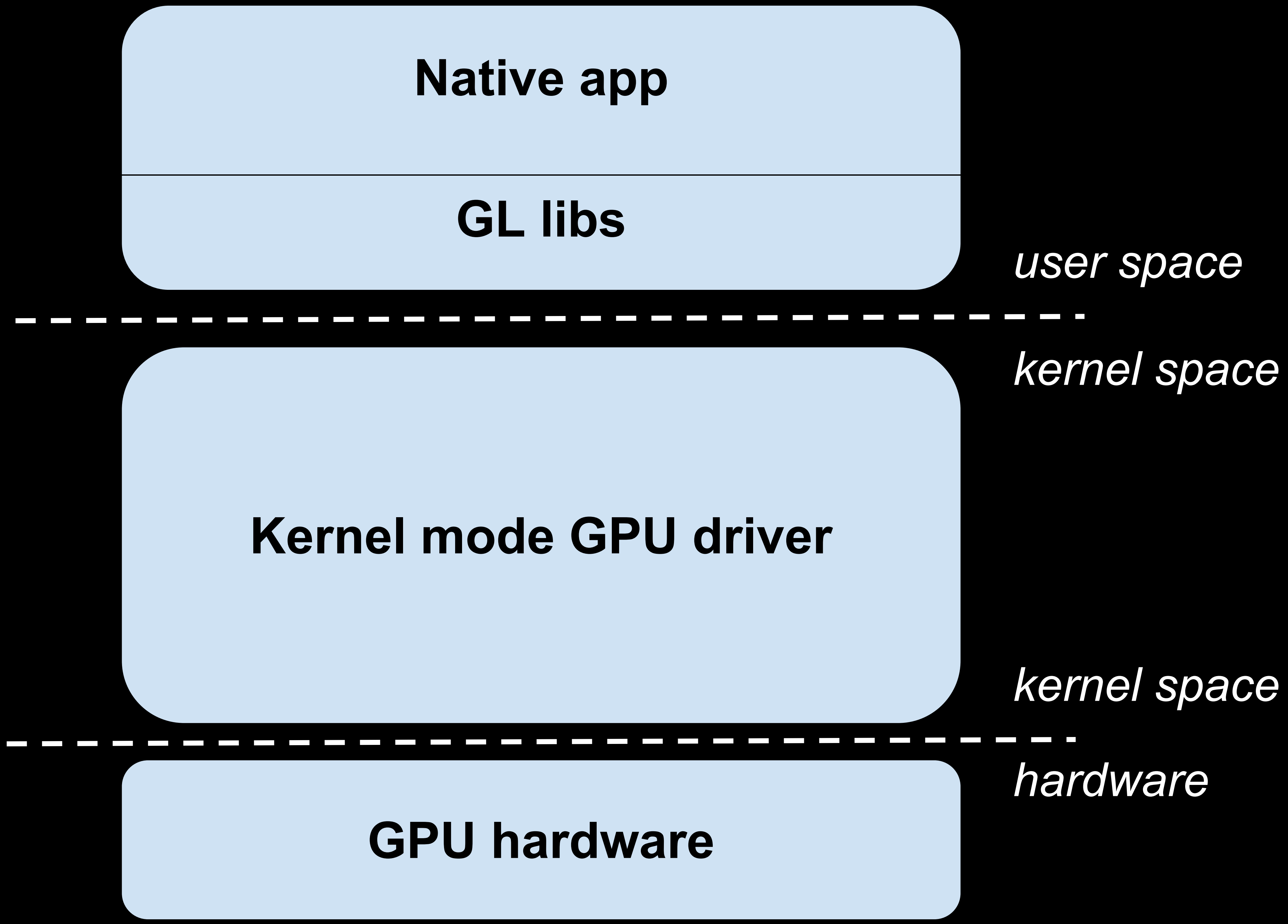

Digital Library of Mathematical Functions
Index
Notations
Search
Help?
Citing
Customize
Annotate
About the Project
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
25 Zeta and Re
Riemann Z
25.3 G
25.3 Graphics

Figure 25.3.3 (*See in context*.)

http://dlmf.nist.gov

WebGL recap

First, a quick recap on OpenGL



Native app

GL libs

user space

kernel space

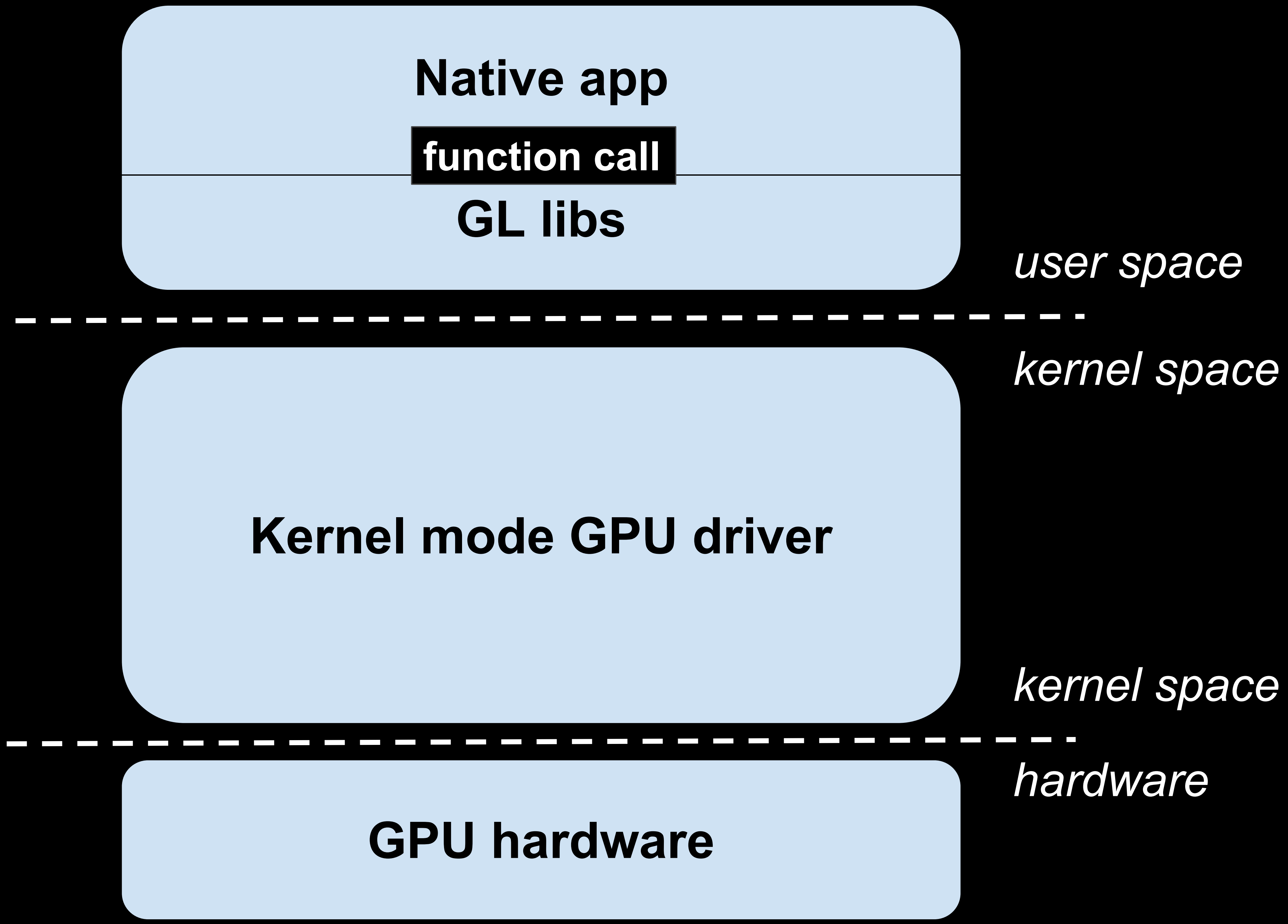
Kernel mode GPU driver

kernel space

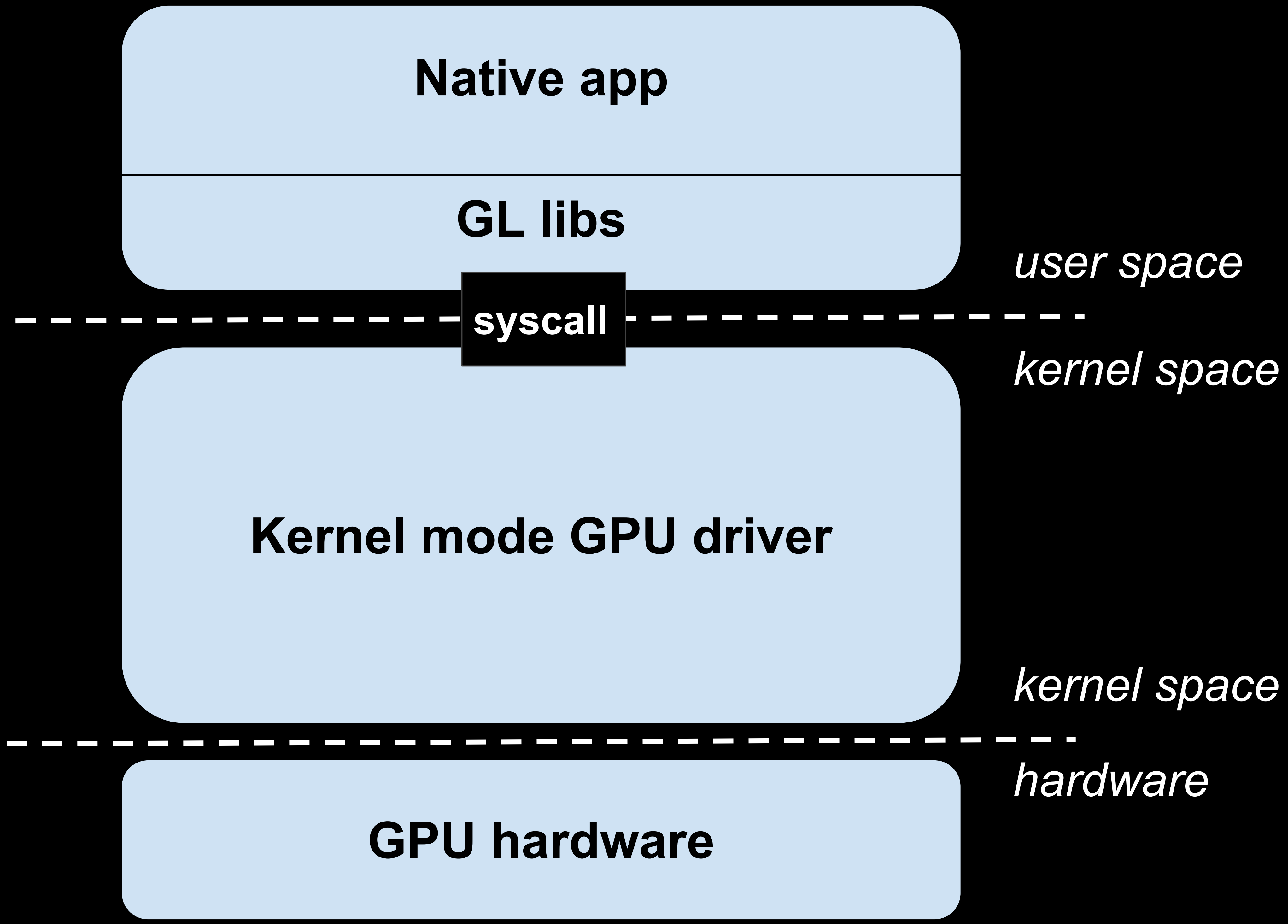
hardware

GPU hardware

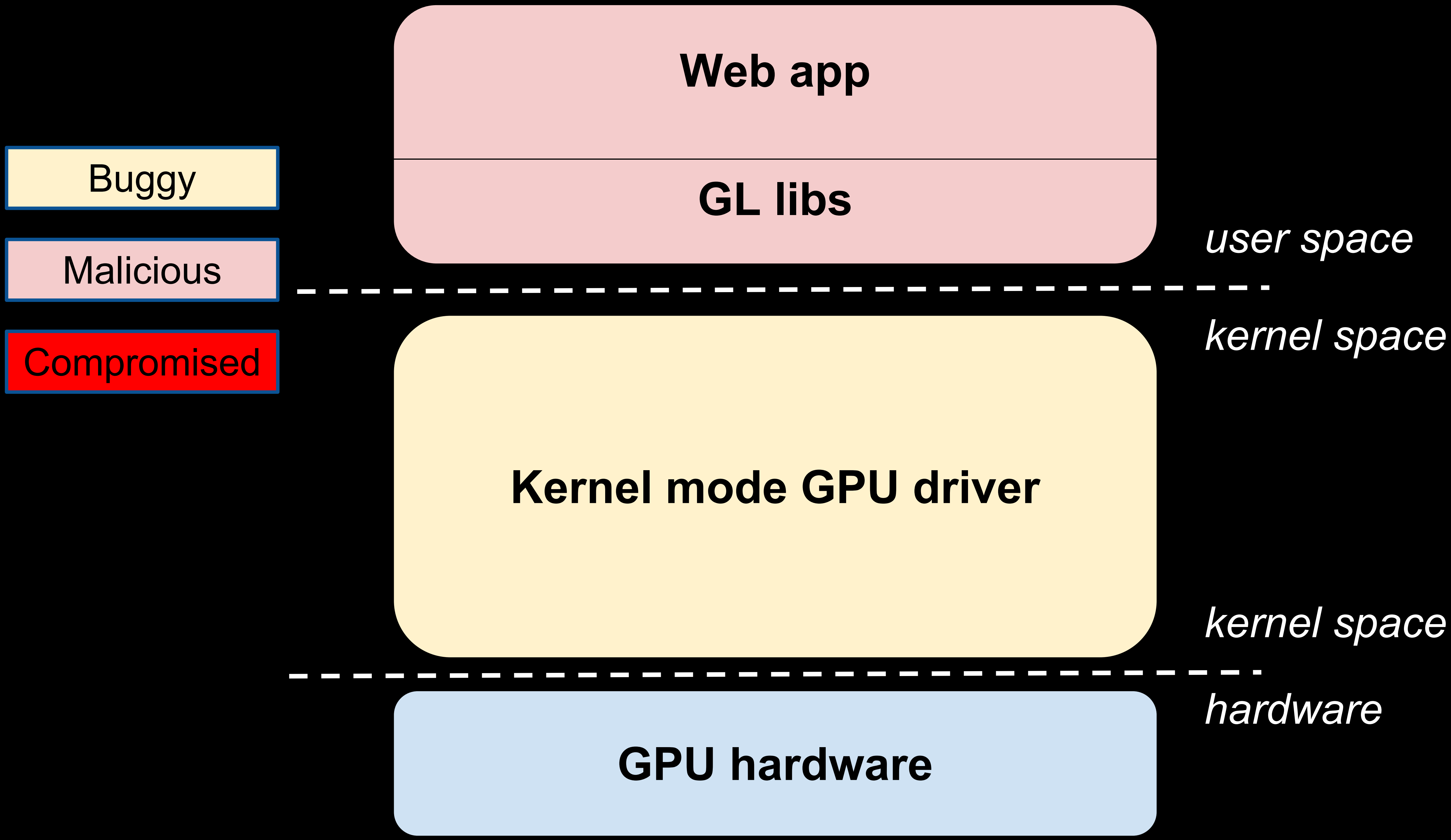
First, a quick recap on OpenGL



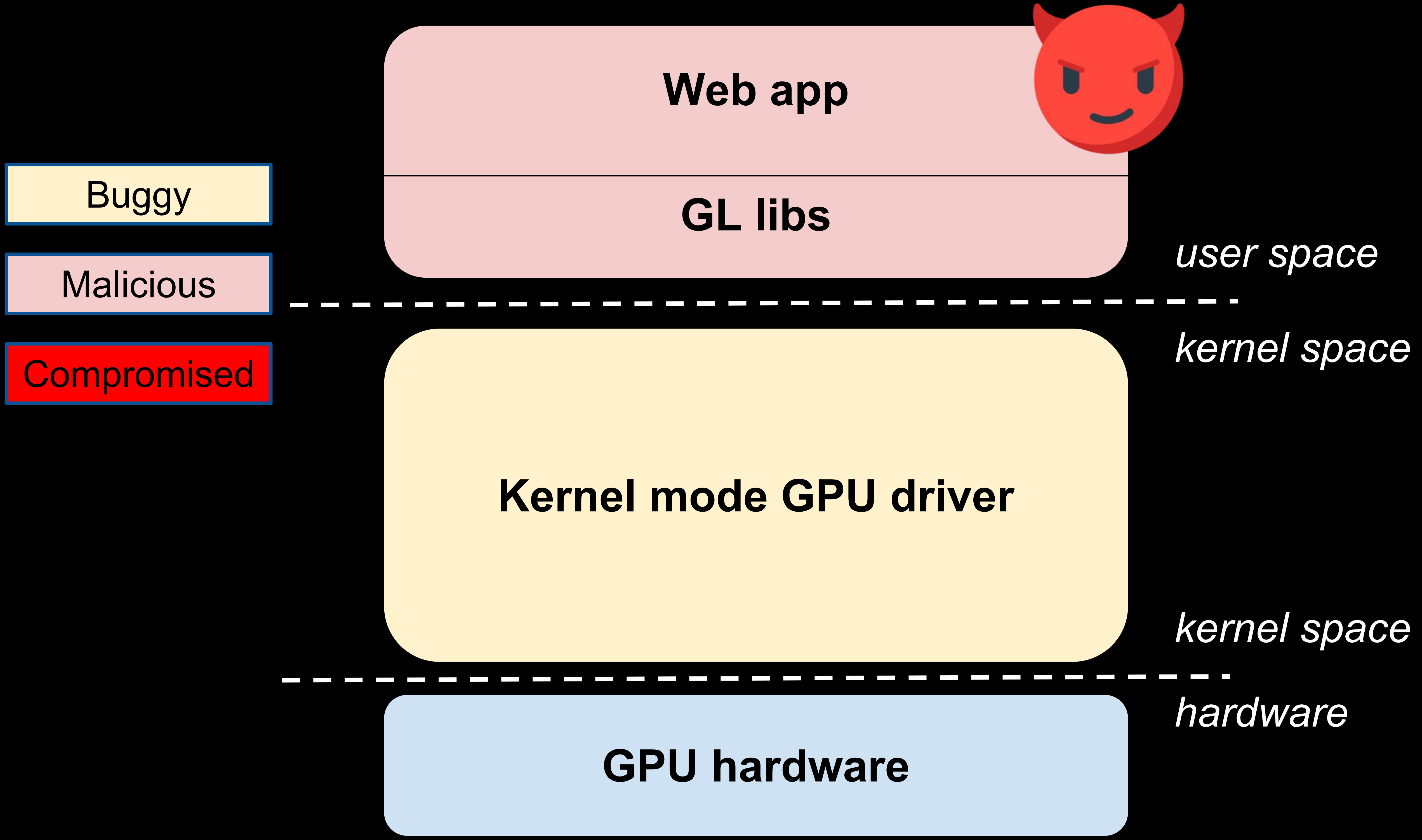
First, a quick recap on OpenGL



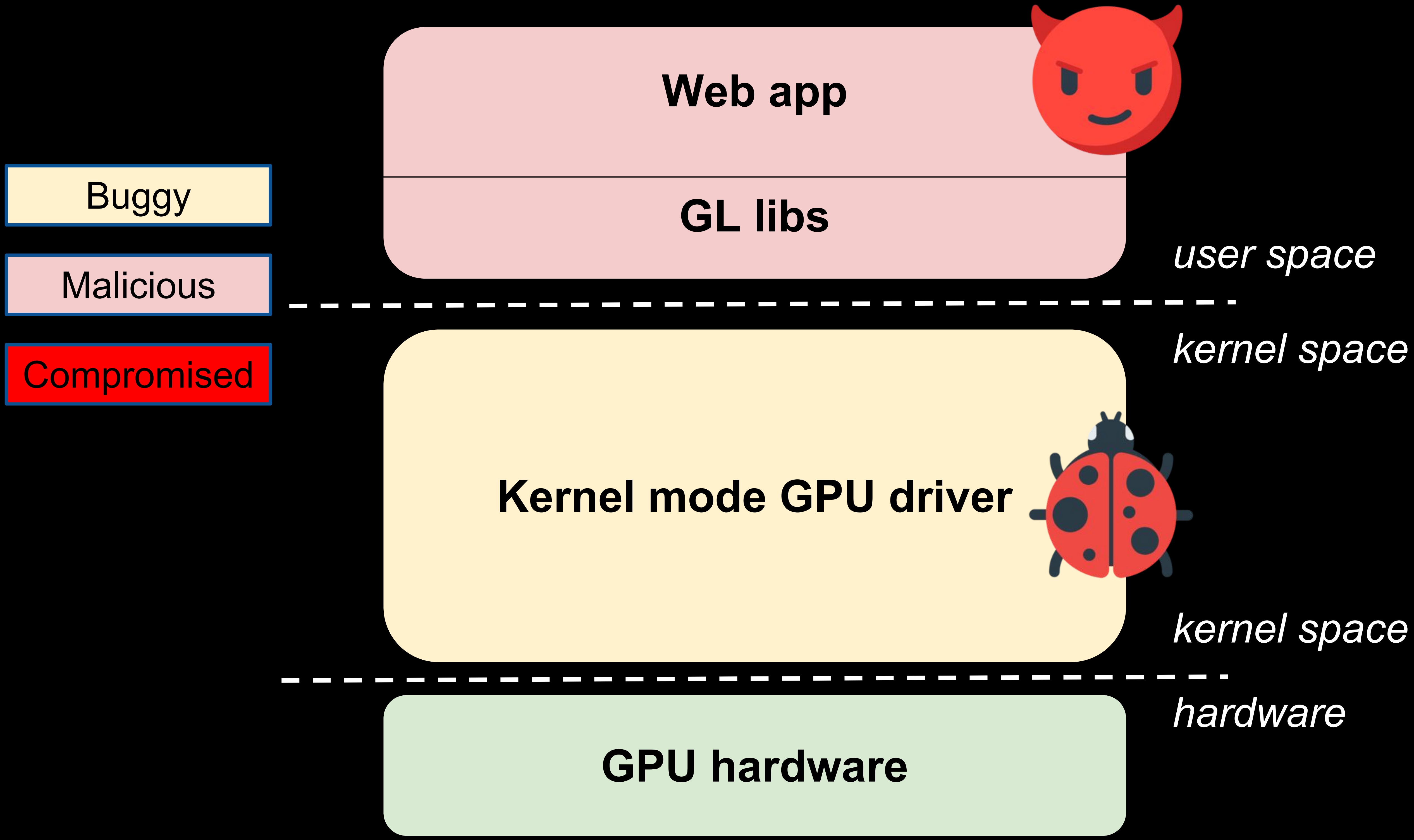
Use the same design for WebGL?



Web apps are not trusted



GPU driver is buggy



Buggy

Malicious

Compromised

Web app

GL libs

user space

kernel space

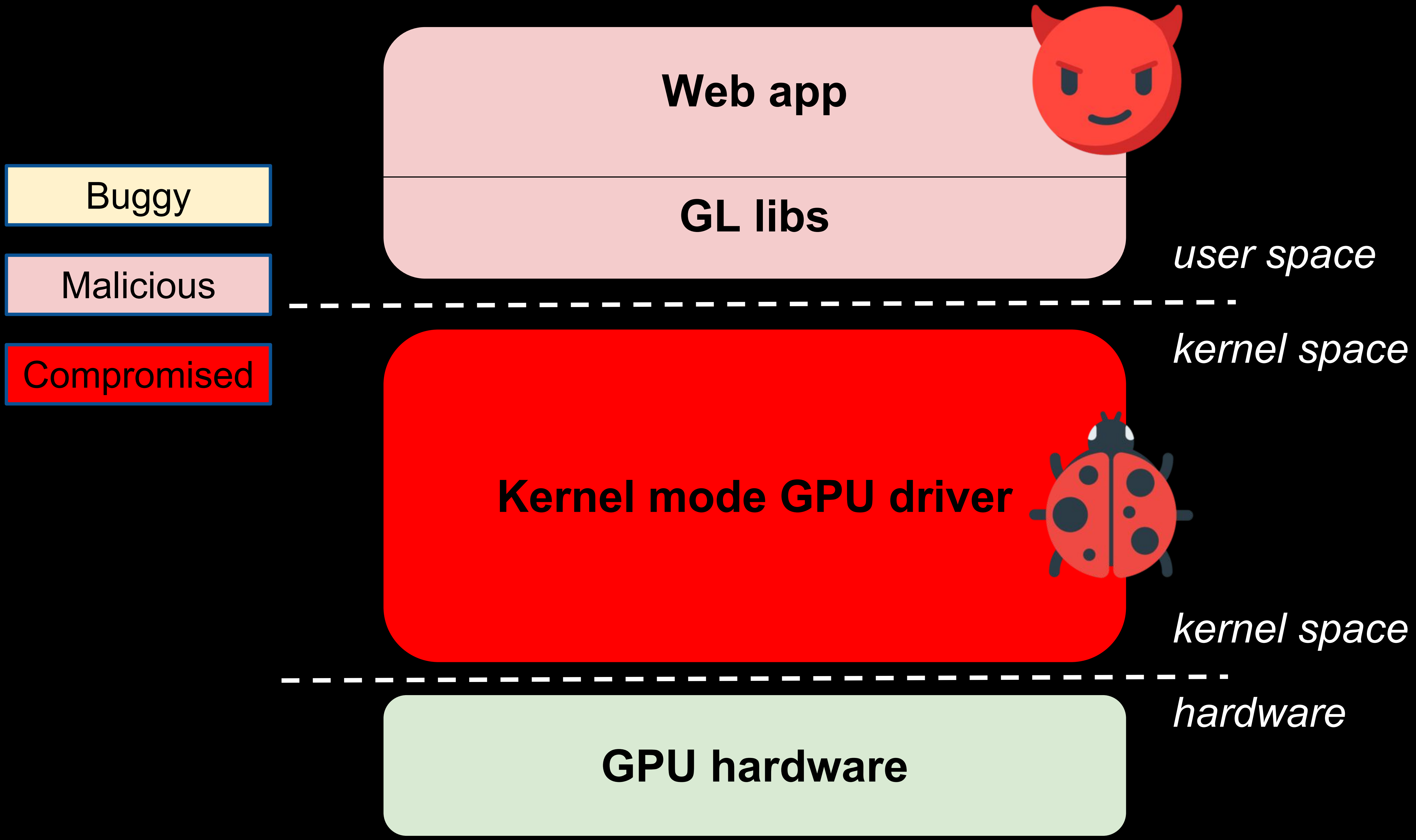
Kernel mode GPU driver

kernel space

hardware

GPU hardware

Kernel driver is compromised



Buggy

Malicious

Compromised

Web app 😈

GL libs

user space

kernel space

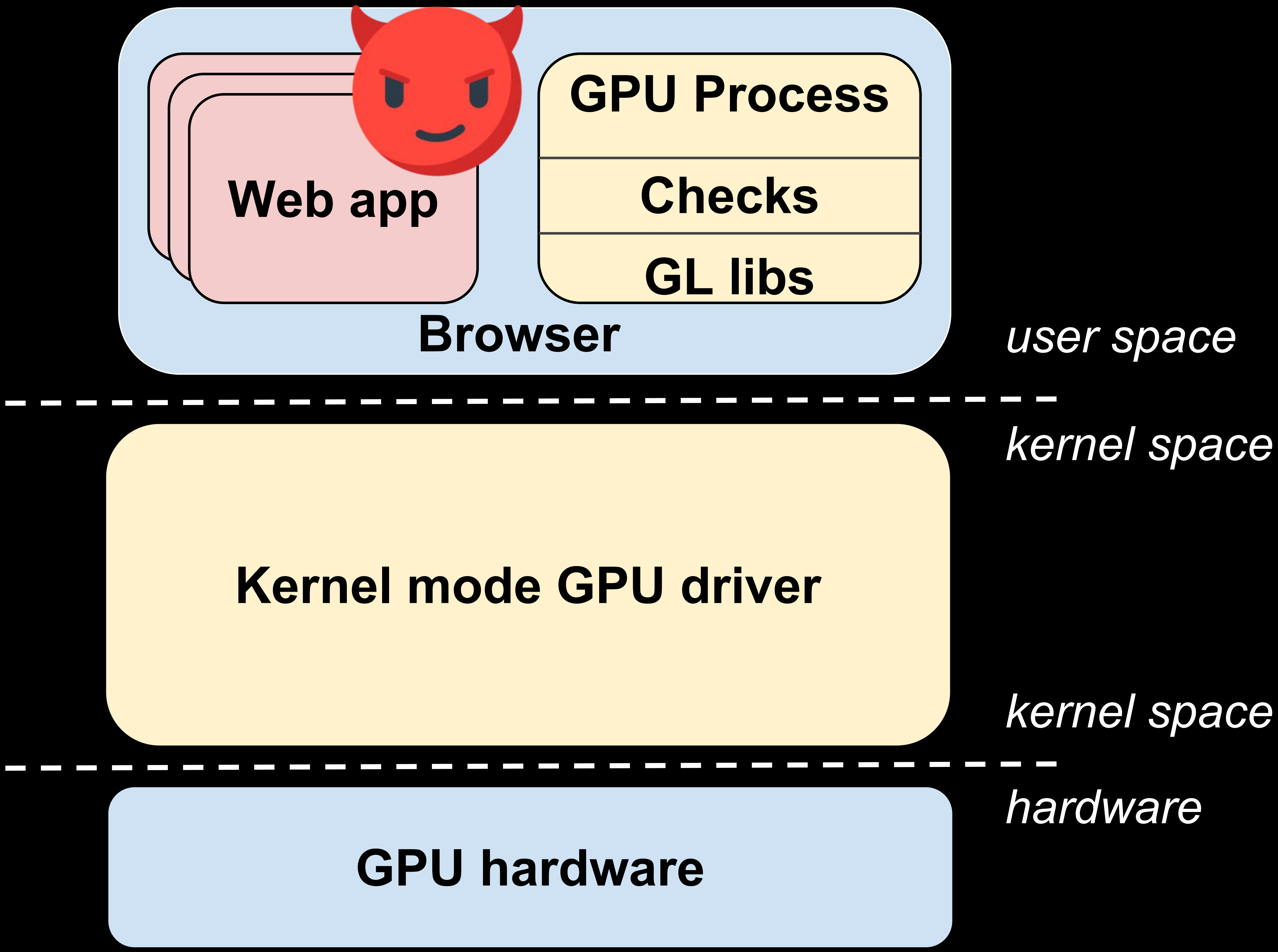
Kernel mode GPU driver 🐞

kernel space

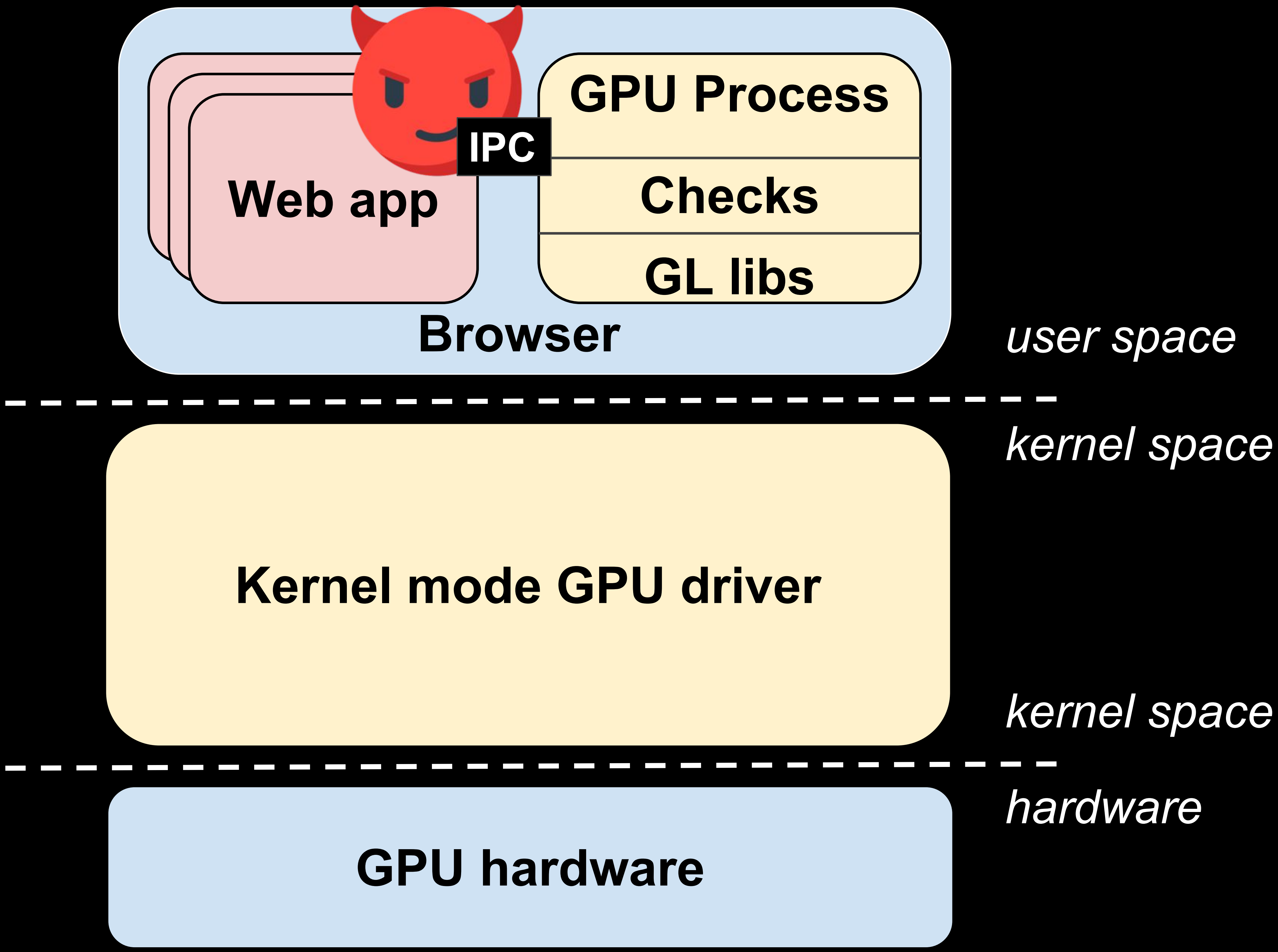
hardware

GPU hardware

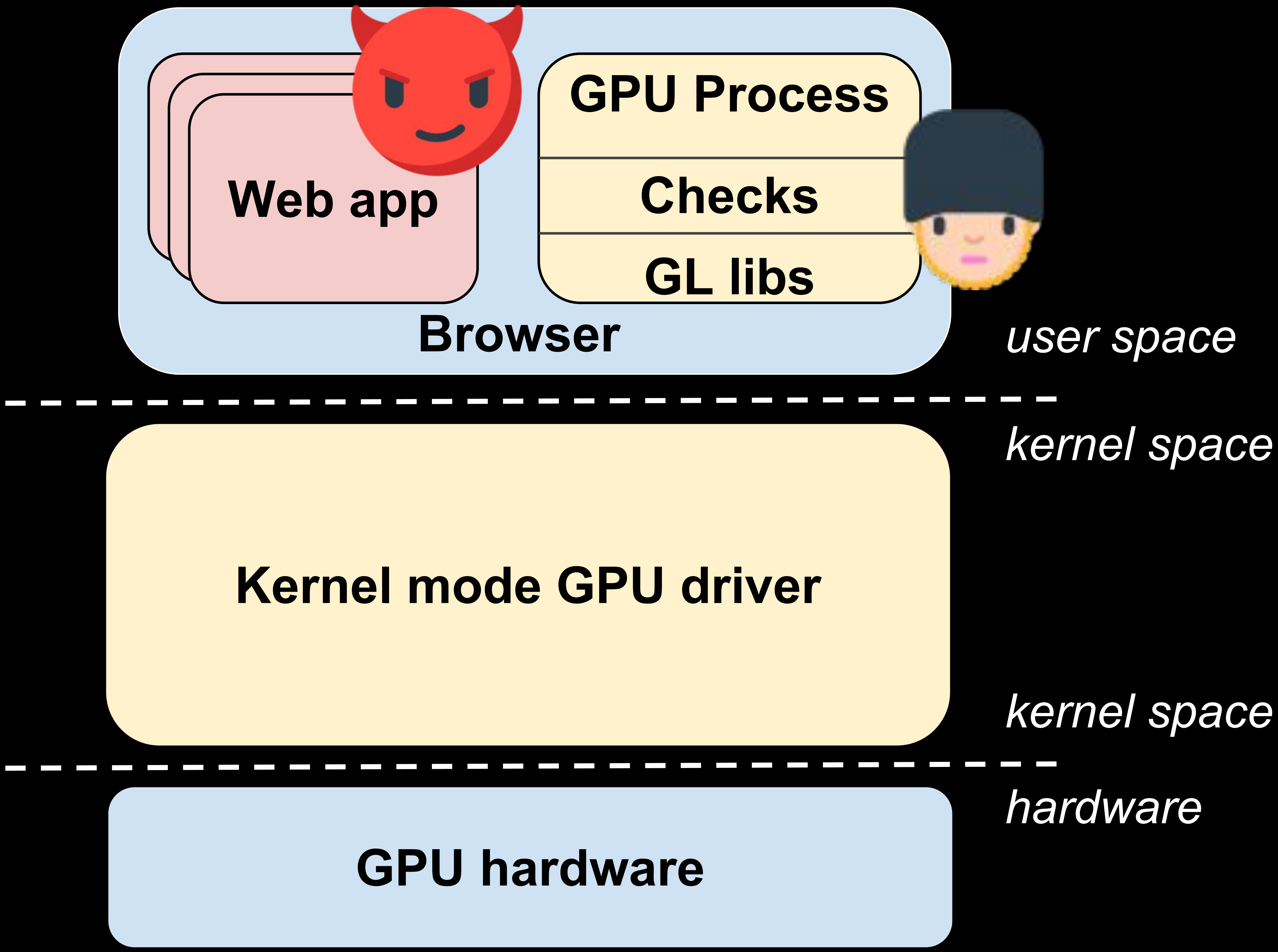
Current WebGL design



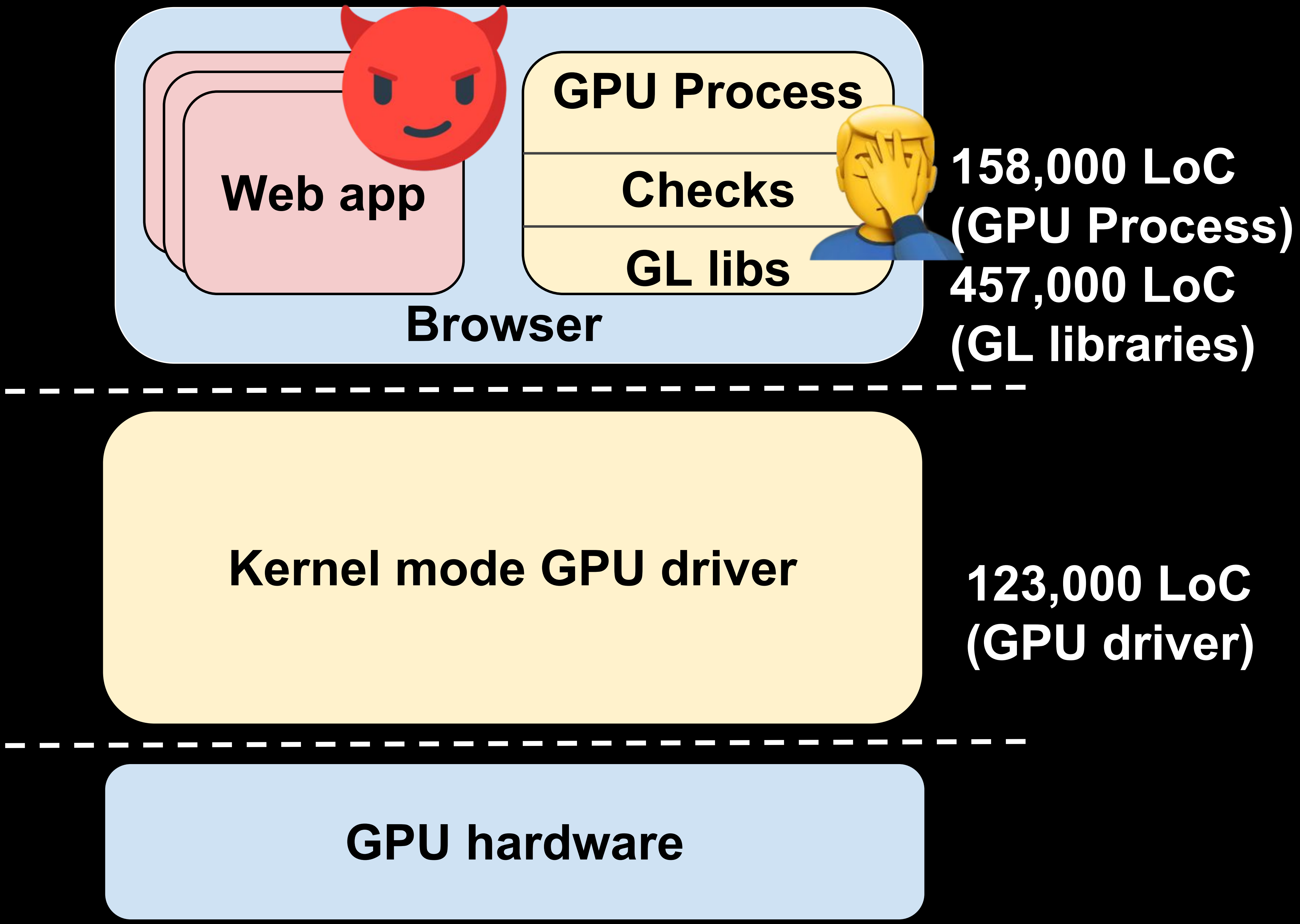
Current WebGL design



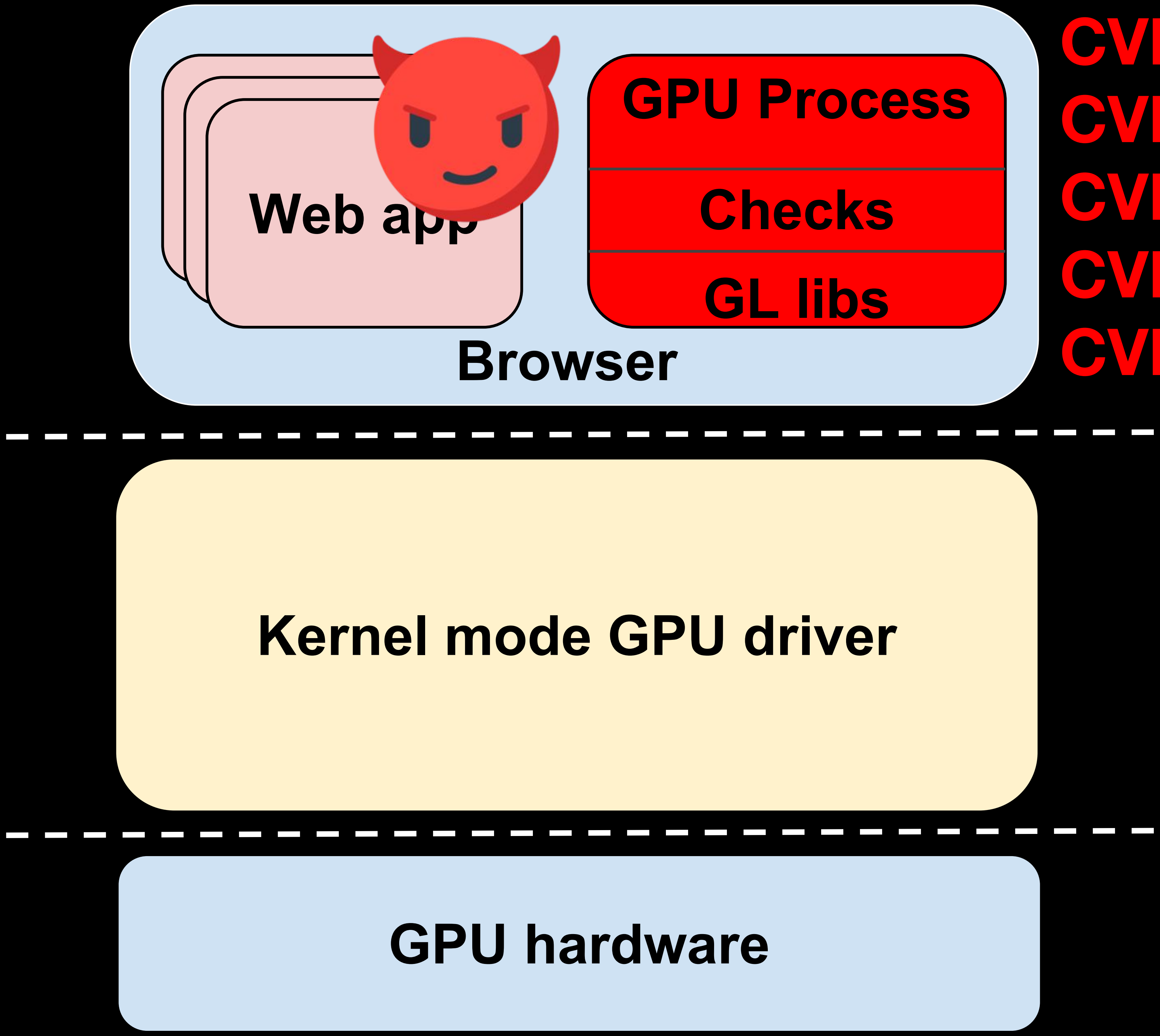
Security checks in GPU Process



TCB of current WebGL Design

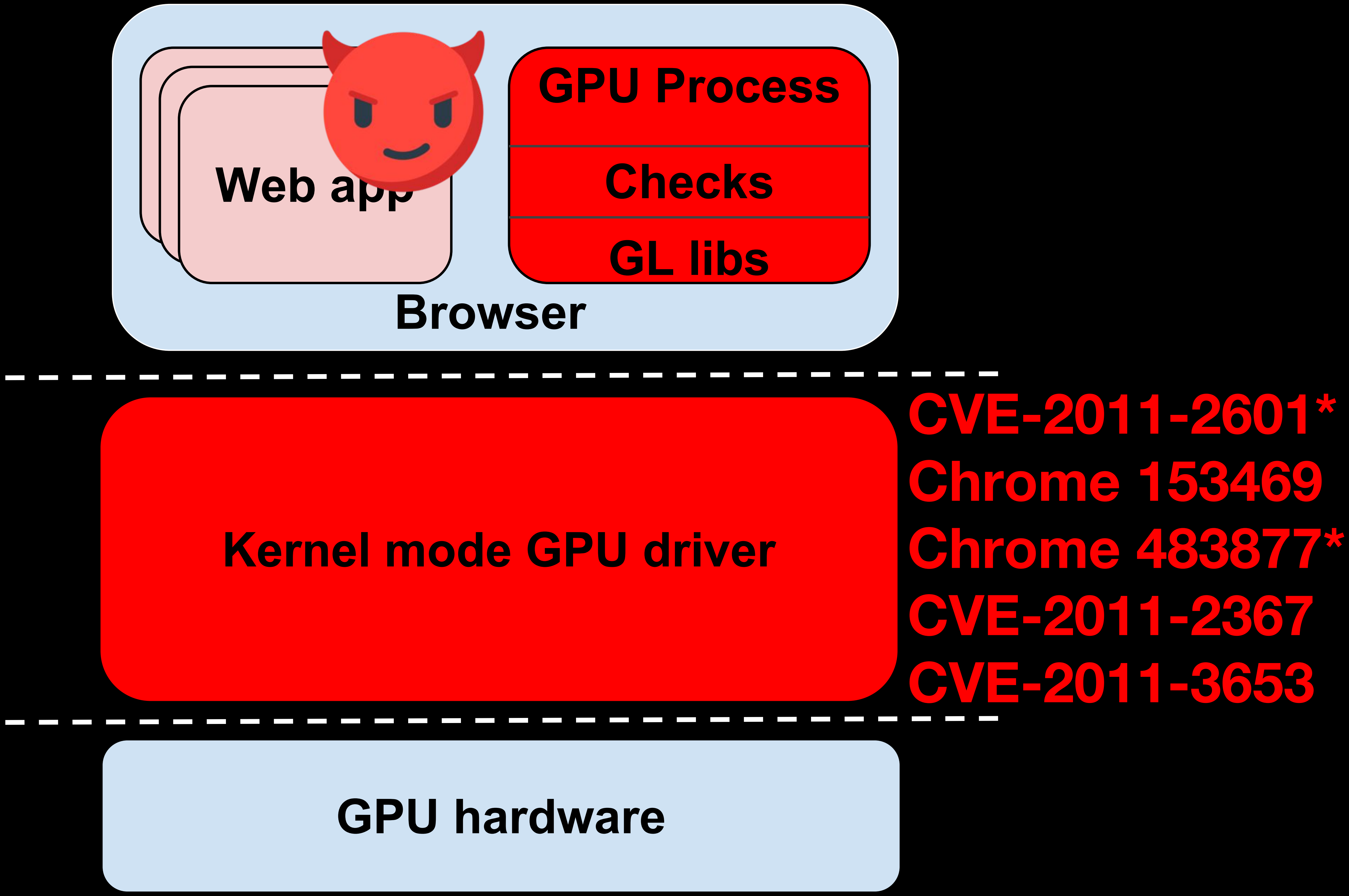


Vulnerabilities in GPU process



CVE-2014-1556
CVE-2015-7179
CVE-2013-2874
CVE-2017-5031
CVE-2014-1502

Kernel driver is compromised



*Not yet fixed

Vulnerability examples

CVE-2014-1556	execute arbitrary code
CVE-2015-7179	execute arbitrary code
CVE-2013-2874	read browser UI
CVE-2017-5031	read GPU process memory
CVE-2014-1502	use of cross-origin contents
Chrome Issue 593680	browser hang
Chrome Issue 83841	leak system username
CVE-2011-2601*	system UI freeze
Chrome issue 153469	kernel panic
Chrome issue 483877*	system UI freeze
CVE-2011-2367	read of GPU memory
CVE-2011-3653	read of GPU memory
CVE-2014-3173	read of GPU memory

*Not yet fixed

Our WebGL vulnerability study

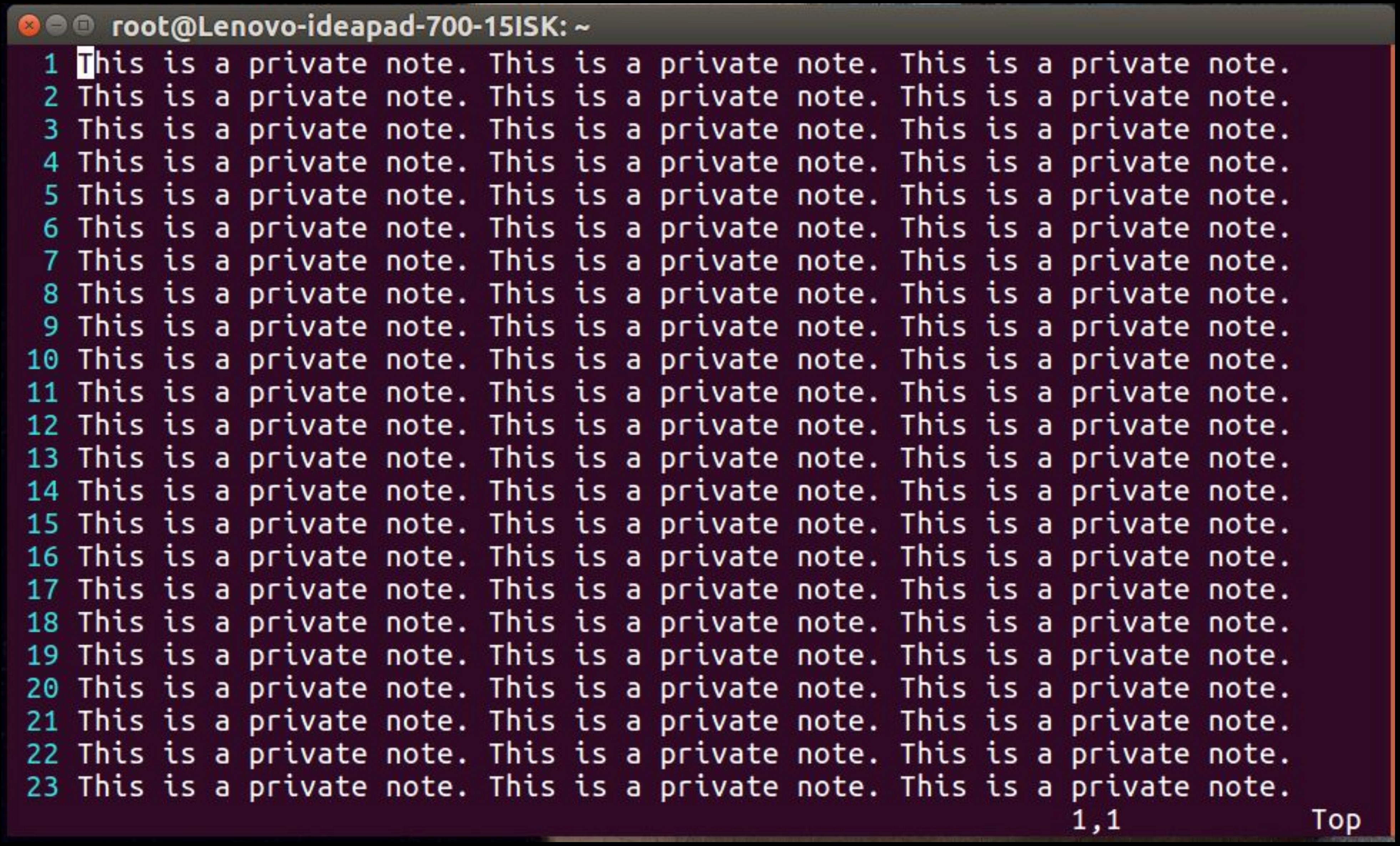
https://trusslab.github.io/sugar/webgl_bugs

Current WebGL design

High performance	Known vulnerabilities	Zero day vulnerabilities	System UI freeze
✓	✓	✗	✗

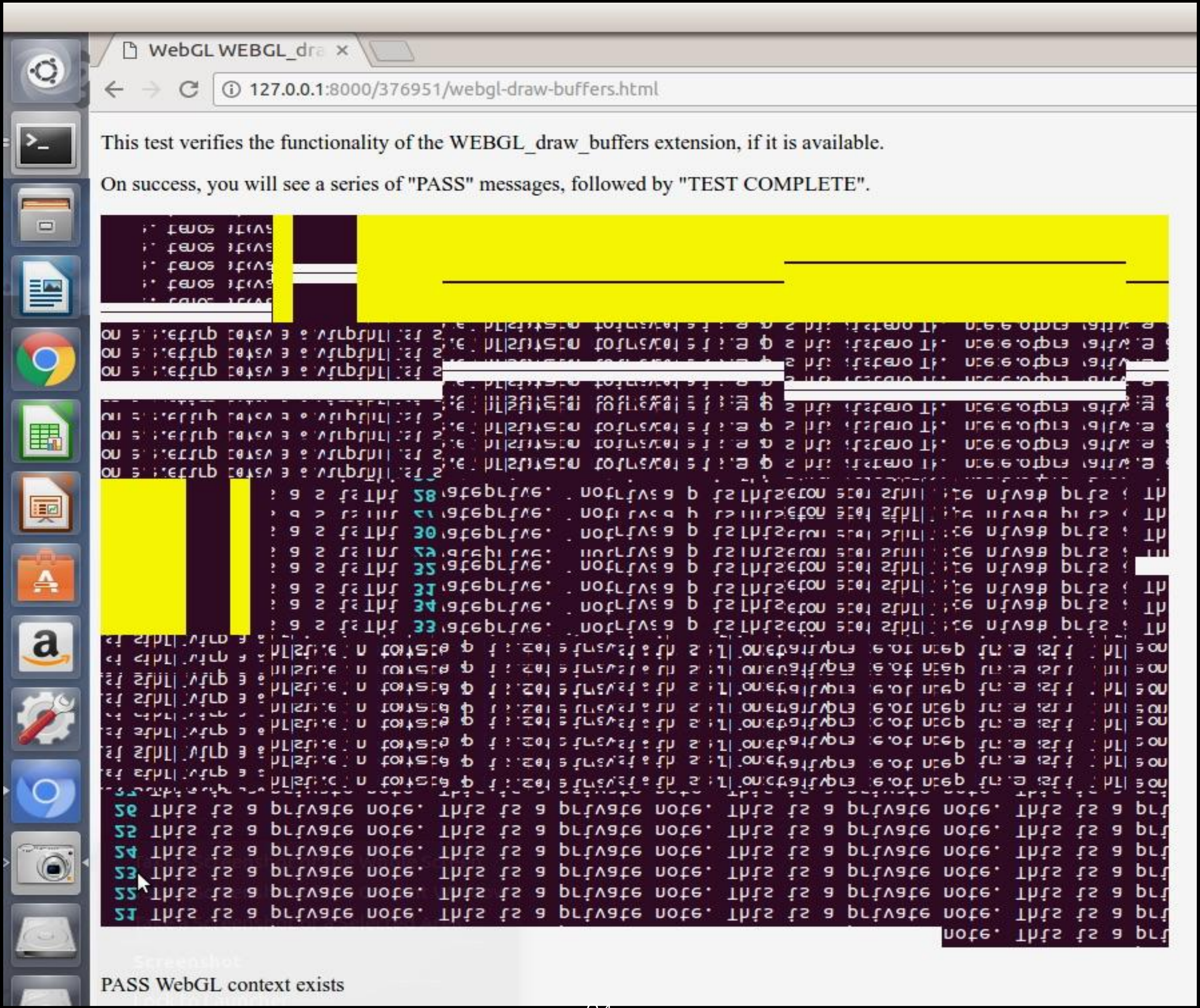
CVE-2014-3173, read of GPU graphics memory

We type some private notes in terminal:



```
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
This is a private note. This is a private note. This is a private note.
                                                       1,1           Top
```

CVE-2014-3173, read of GPU graphics memory



127.0.0.1:8000/376951/webgl-draw-buffers.html

This test verifies the functionality of the WEBGL_draw_buffers extension, if it is available.

On success, you will see a series of "PASS" messages, followed by "TEST COMPLETE".

PASS WebGL context exists

Overview of Sugar

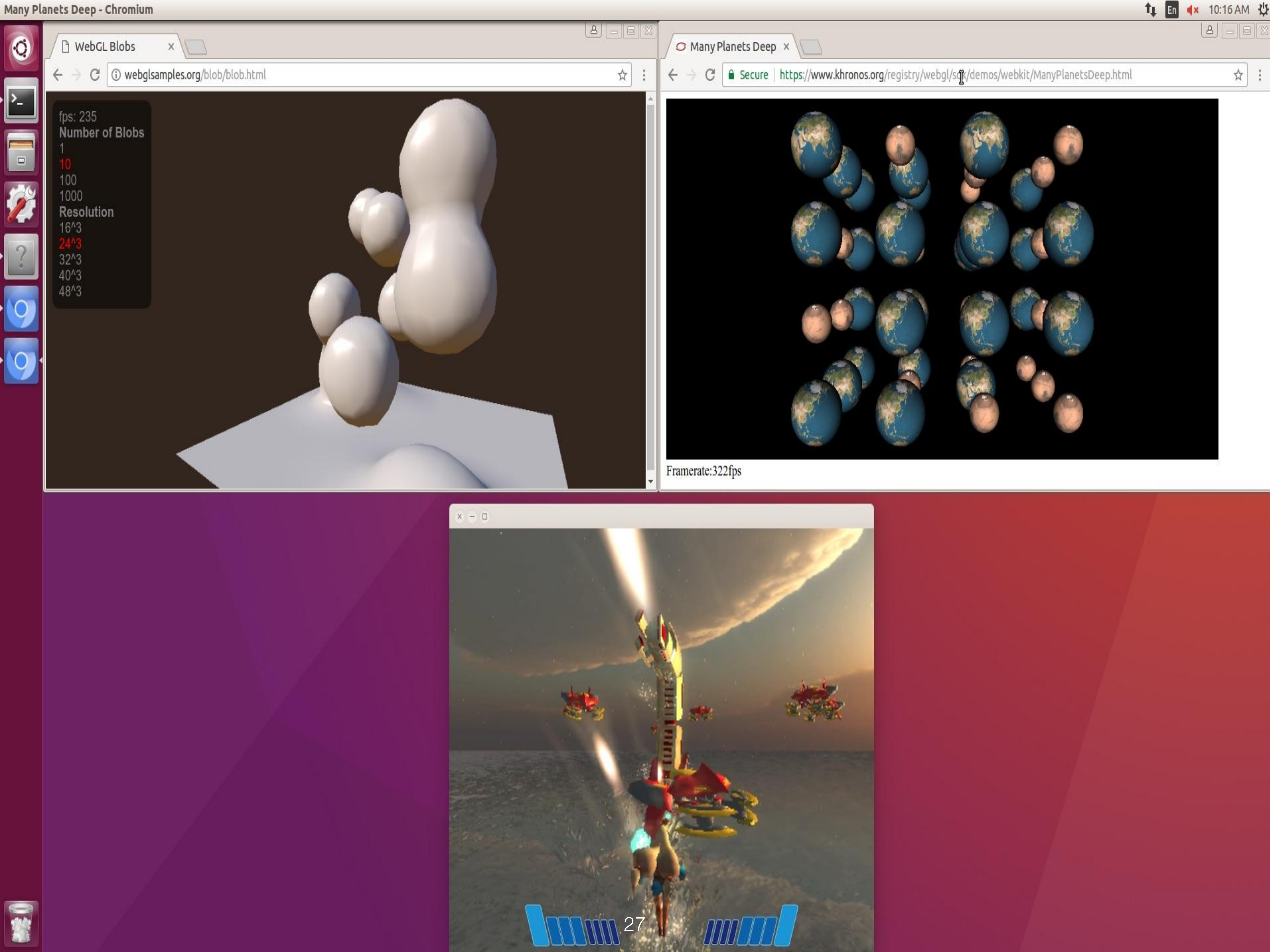
Key idea:

- **Use GPU virtualization to give an untrusted web app a separate vGPU**

Intel GPU virtualization

- **We build a prototype on Intel GPU virtualization**
- **Intel GPU virtualization is available since the 4th generation Core processors** [1]

[1] https://www.usenix.org/conference/atc14/technical-sessions/presentation/tian
Photo credit: https://www.intel.com/pressroom/archive/releases/2008/20081117comp_sm.htm



Many Planets Deep - Chromium

10:16 AM

WebGL Blobs

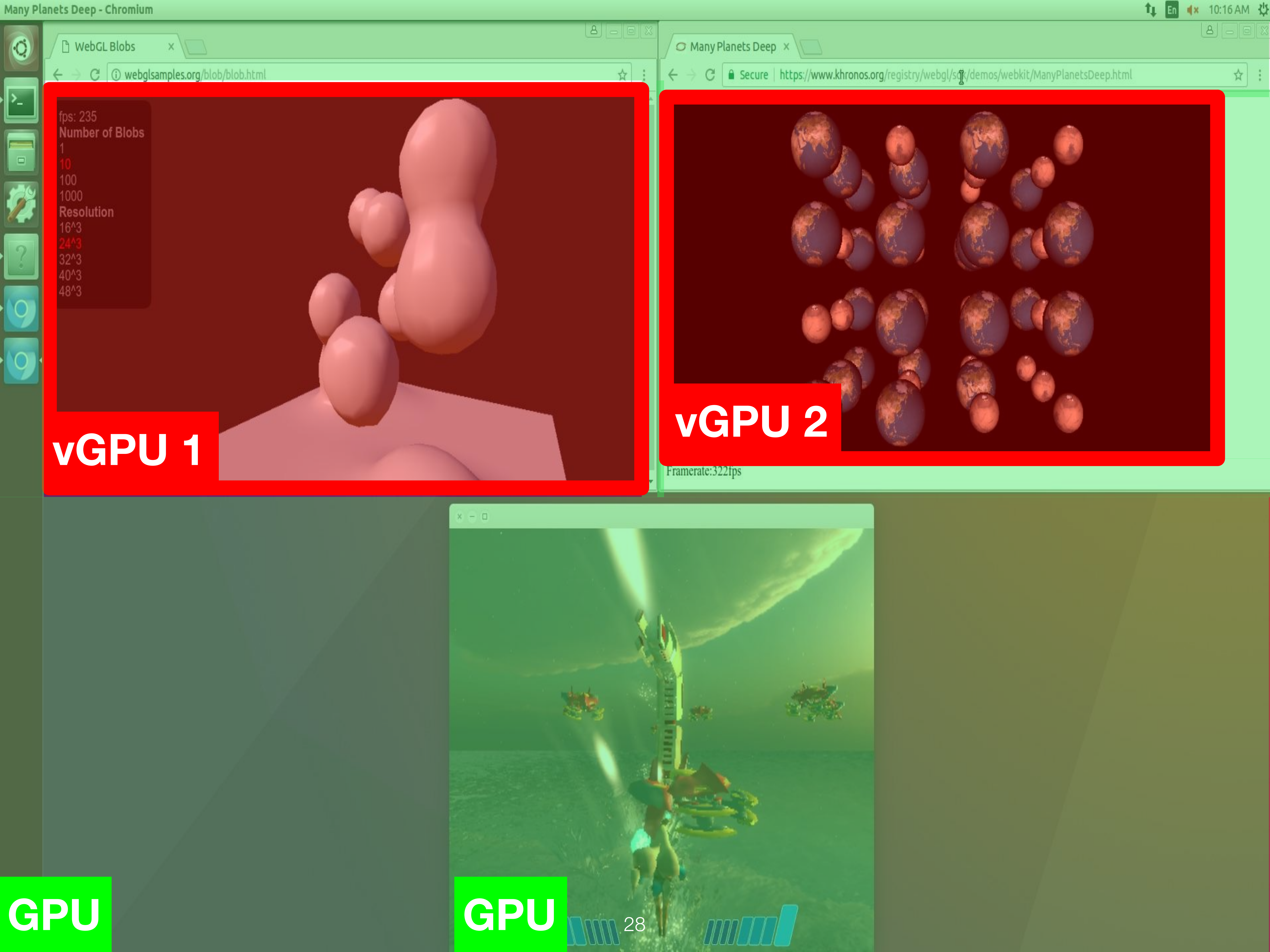
webglsamples.org/blob/blob.html

fps: 235

Many Planets Deep

Secure https://www.khronos.org/registry/webgl/sdk/demos/webkit/ManyPlanetsDeep.html

Framerate:322fps



Many Planets Deep - Chromium
En
10:16 AM
WebGL Blobs
webglsamples.org/blob/blob.html
Many Planets Deep
Secure
https://www.khronos.org/registry/webgl/sdk/demos/webkit/ManyPlanetsDeep.html

```
fps: 235
Number of Blobs
1
10
100
1000
Resolution
16^3
24^3
32^3
40^3
48^3
```

```
Framerate:322fps
```

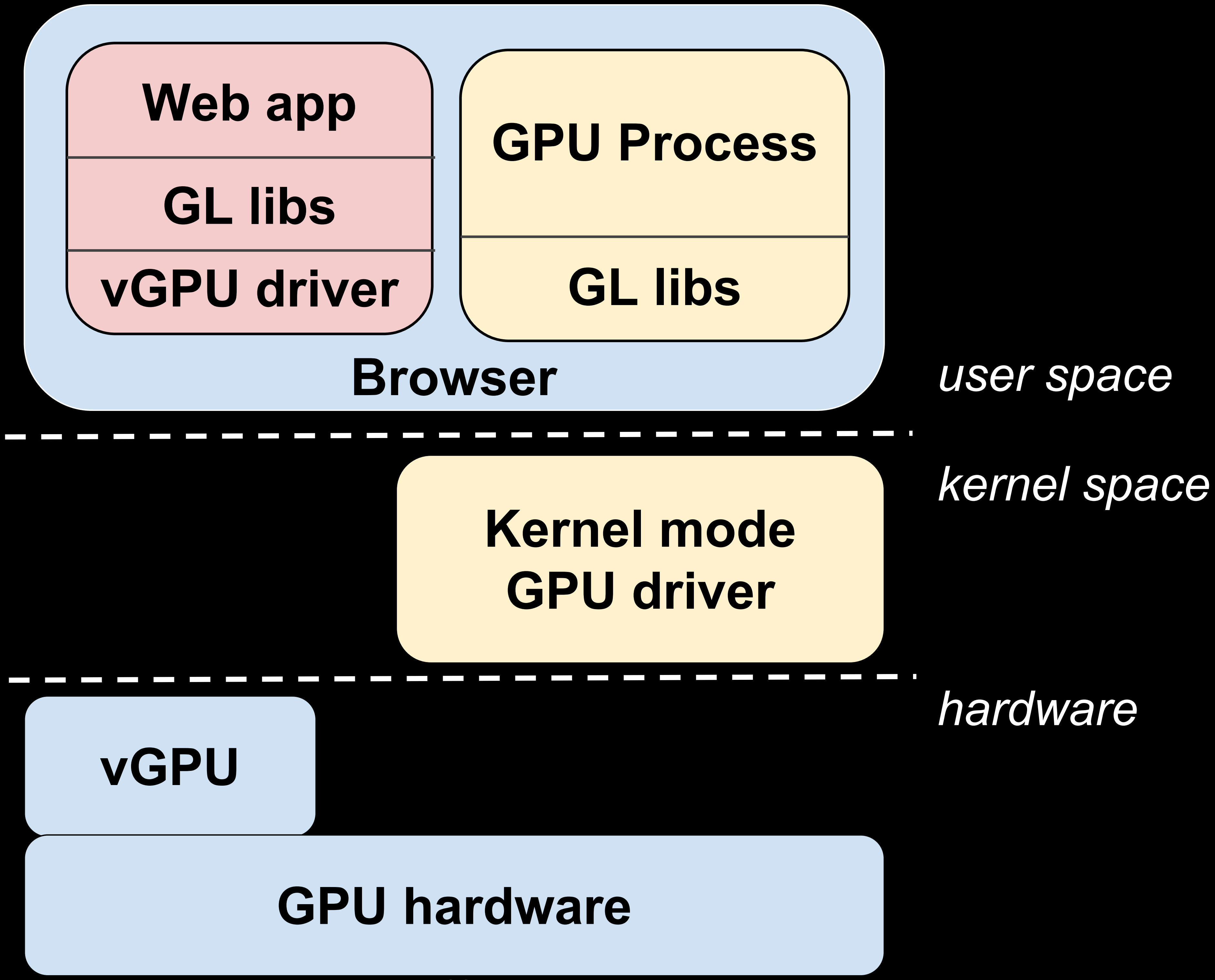
vGPU 1

vGPU 2

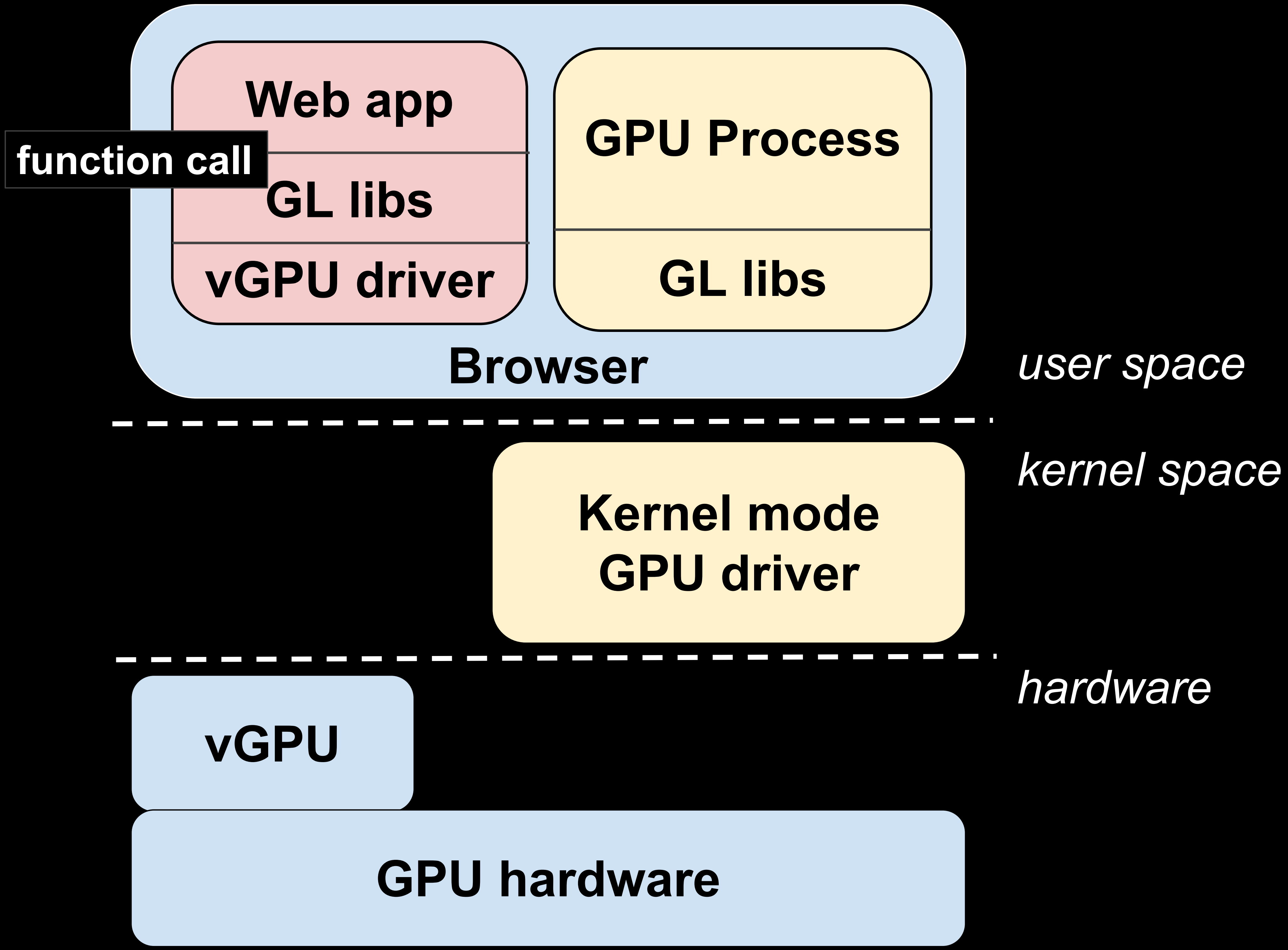
GPU

GPU

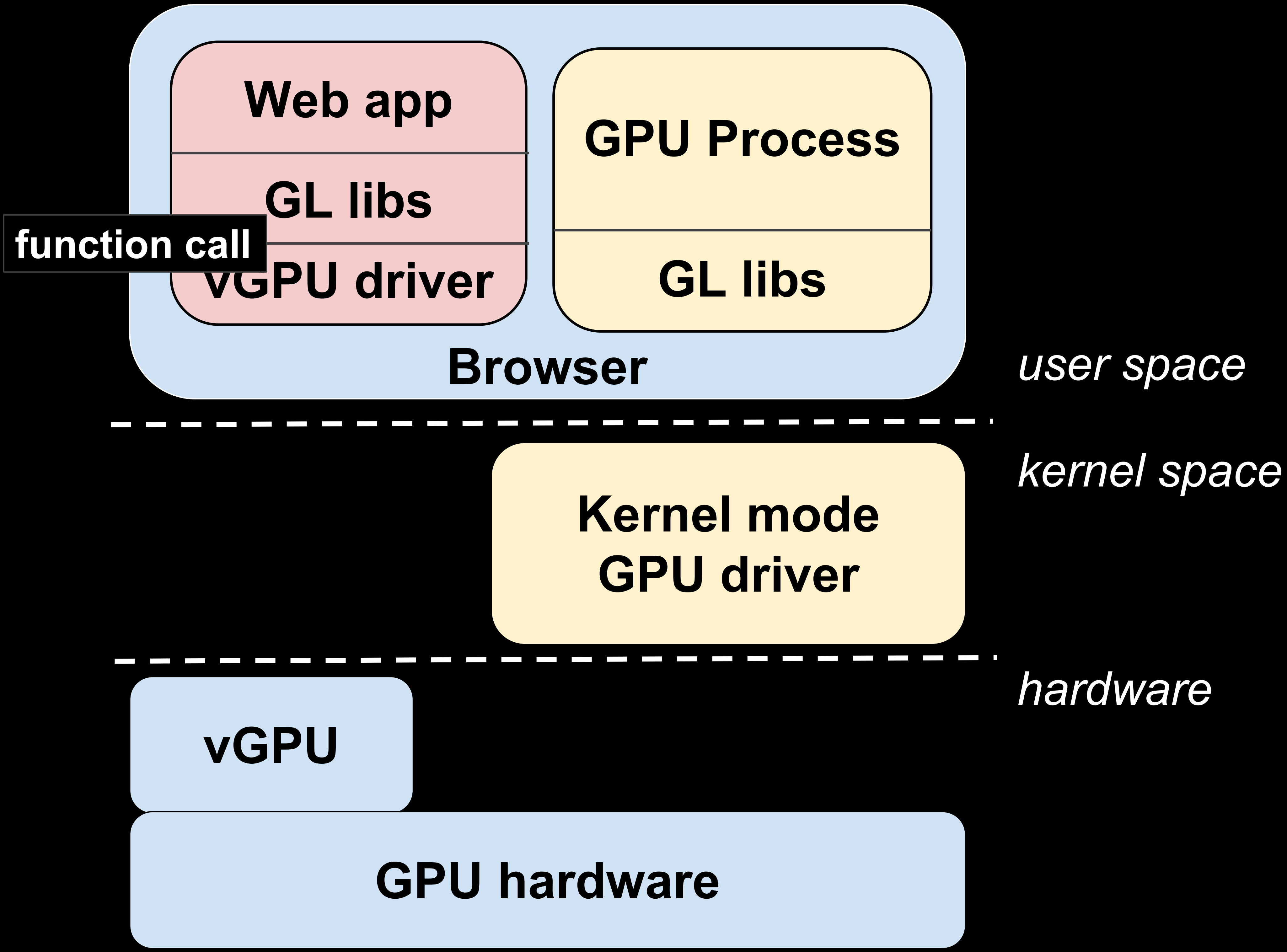
Sugar's design



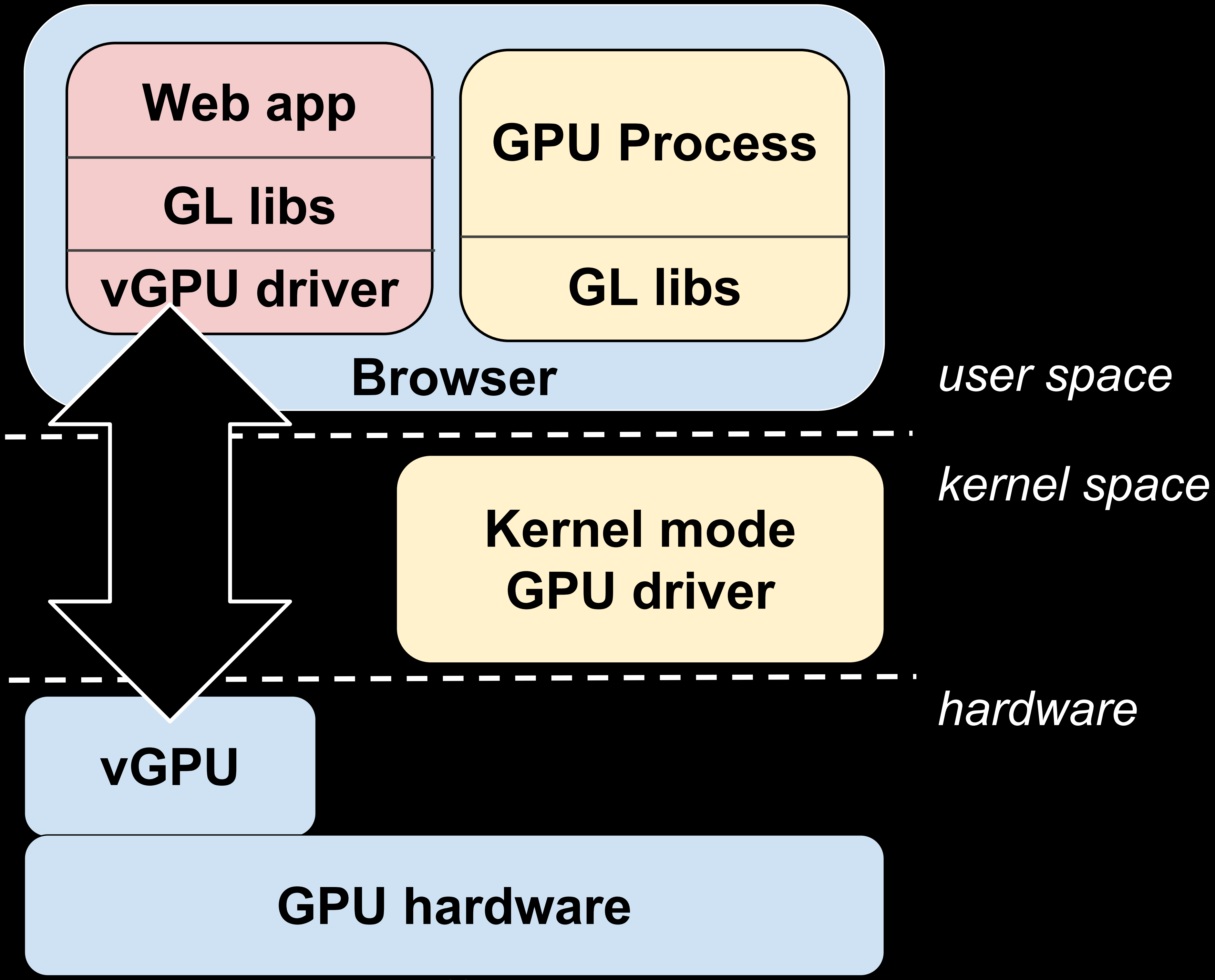
Sugar's design



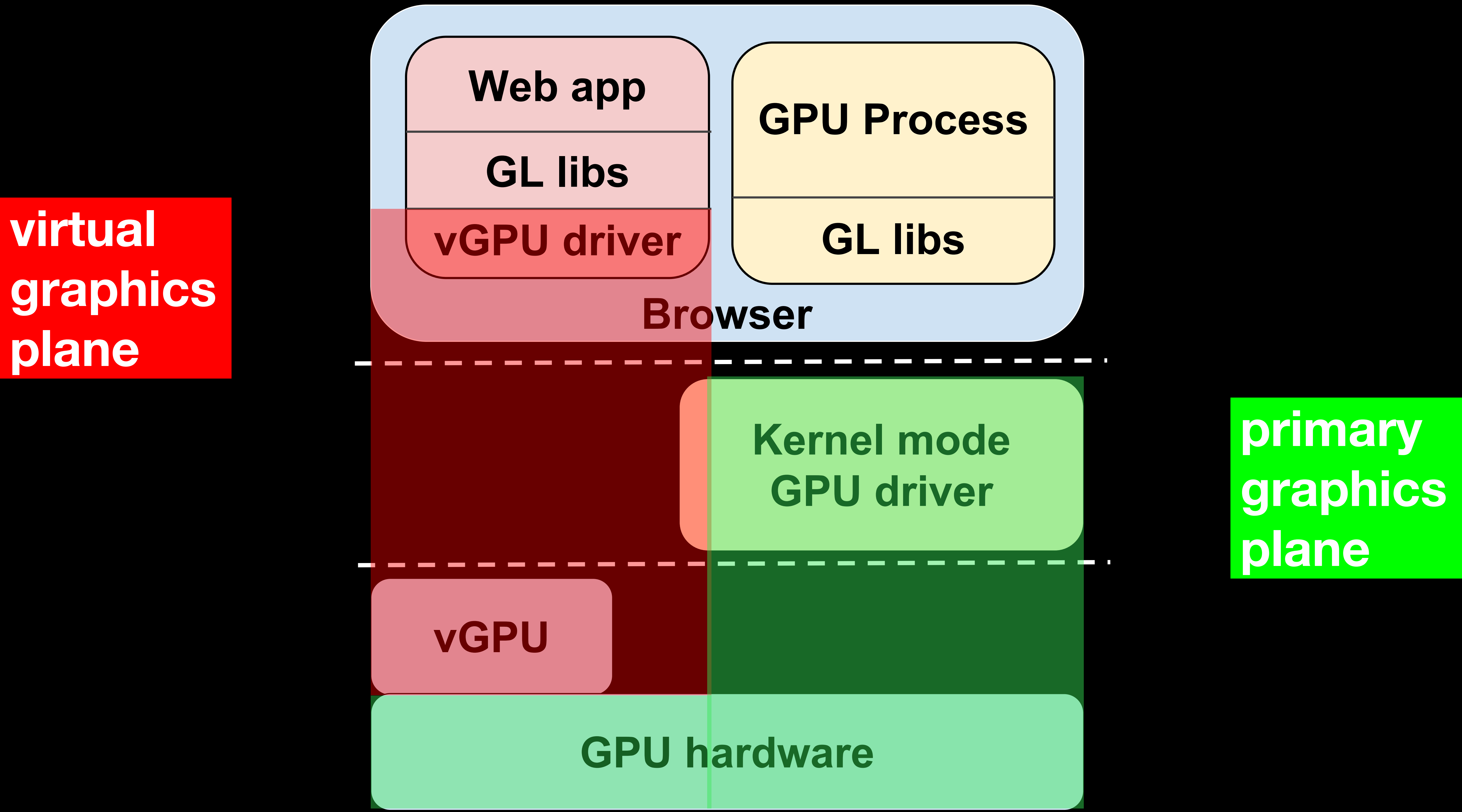
Sugar’s design



Sugar's design



Sugar’s design



virtual graphics plane

Web app

GL libs

vGPU driver

GPU Process

GL libs

Browser

Kernel mode GPU driver

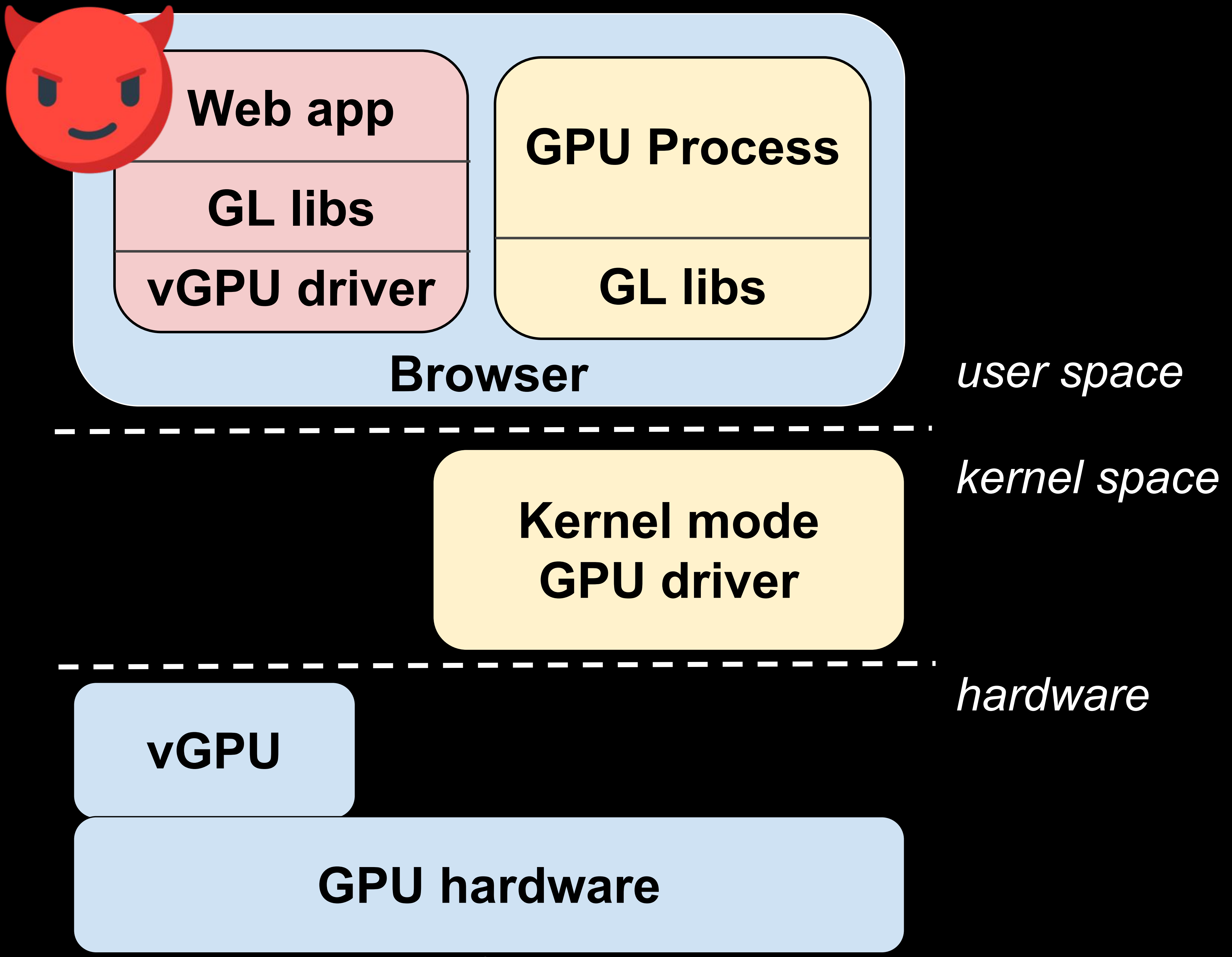
vGPU

GPU hardware

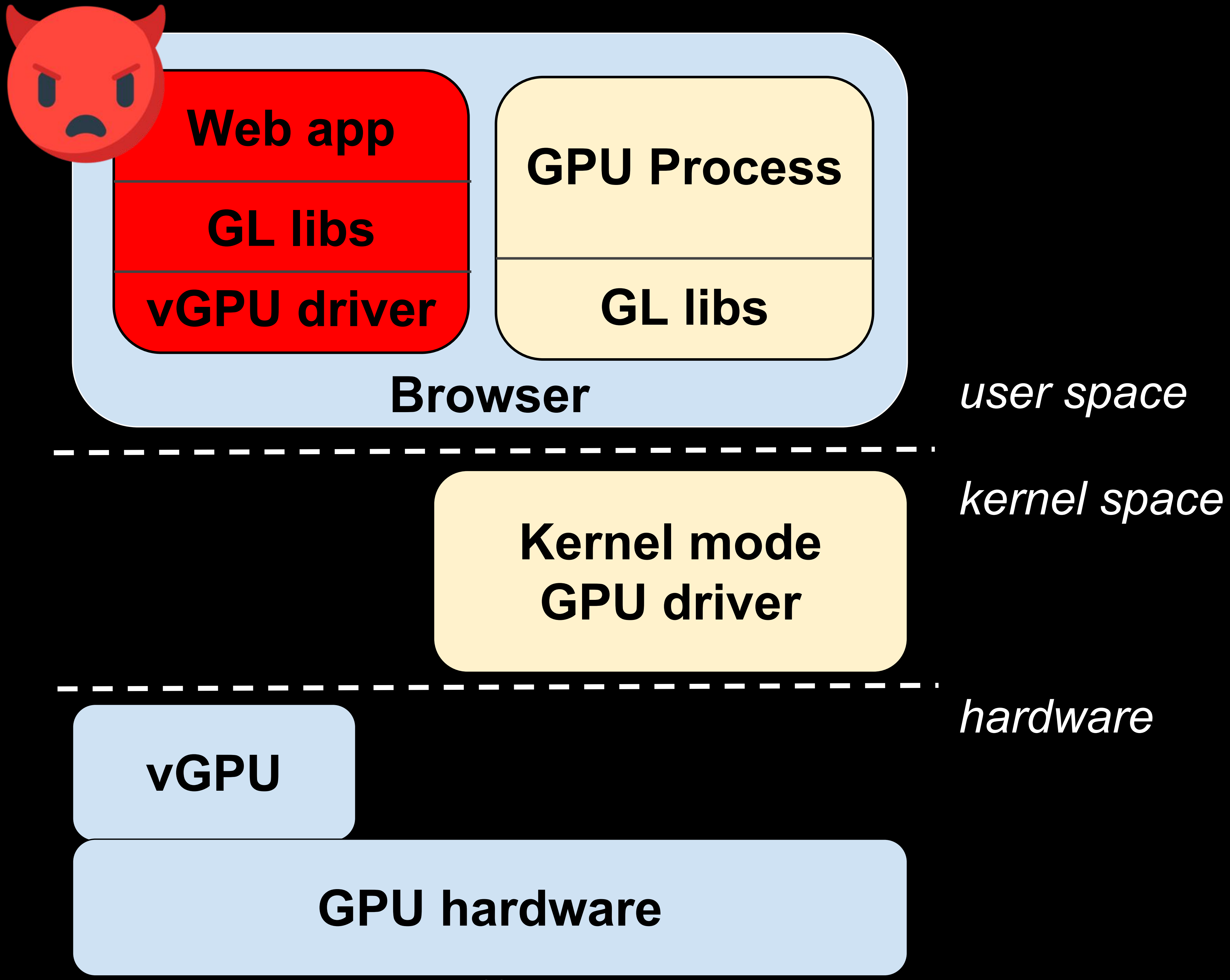
primary graphics plane

Why is Sugar secure?

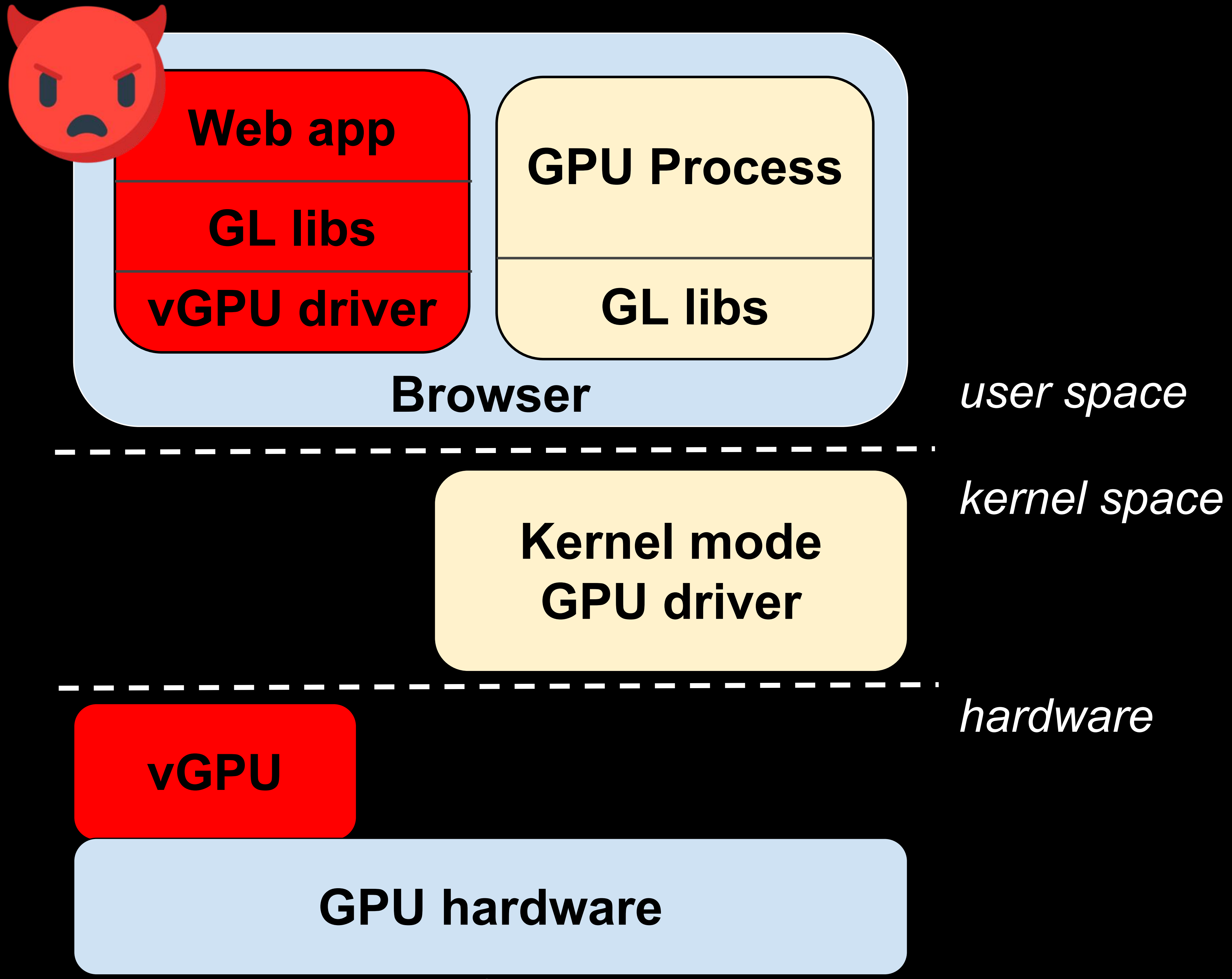
Web app process is untrusted



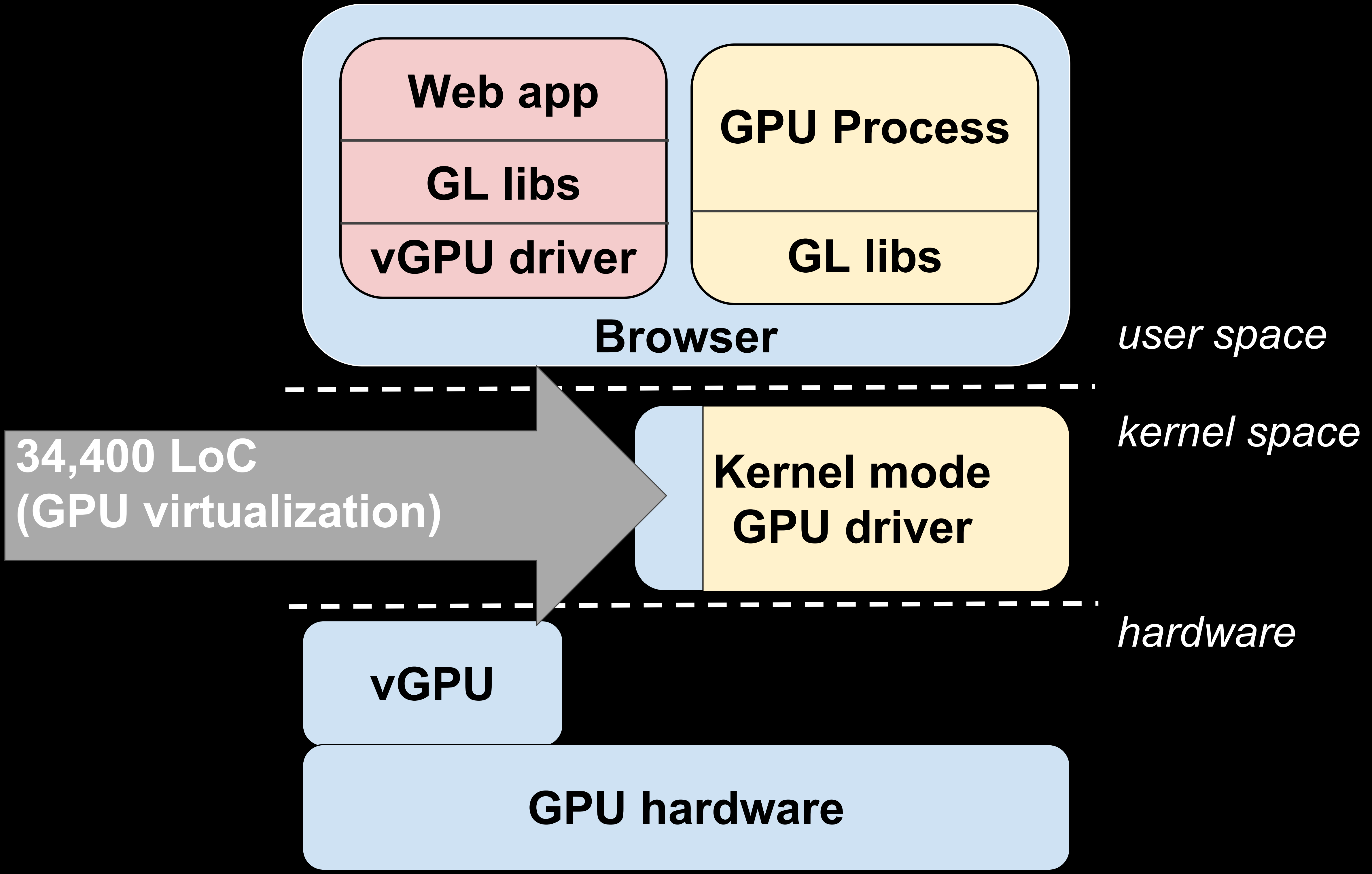
Web app process is sandboxed



vGPU is isolated



Sugar’s TCB is small



Vulnerability examples

CVE-2014-1556	execute arbitrary code
CVE-2015-7179	execute arbitrary code
CVE-2013-2874	read browser UI
CVE-2017-5031	read GPU process memory
CVE-2014-1502	use of cross-origin contents
Chrome Issue 593680	browser hang
Chrome Issue 83841	leak system username
CVE-2011-2601*	system UI freeze
Chrome issue 153469	kernel panic
Chrome issue 483877*	system UI freeze
CVE-2011-2367	read of GPU memory
CVE-2011-3653	read of GPU memory
CVE-2014-3173	read of GPU memory

*Not yet fixed

Limitation of this Sugar design

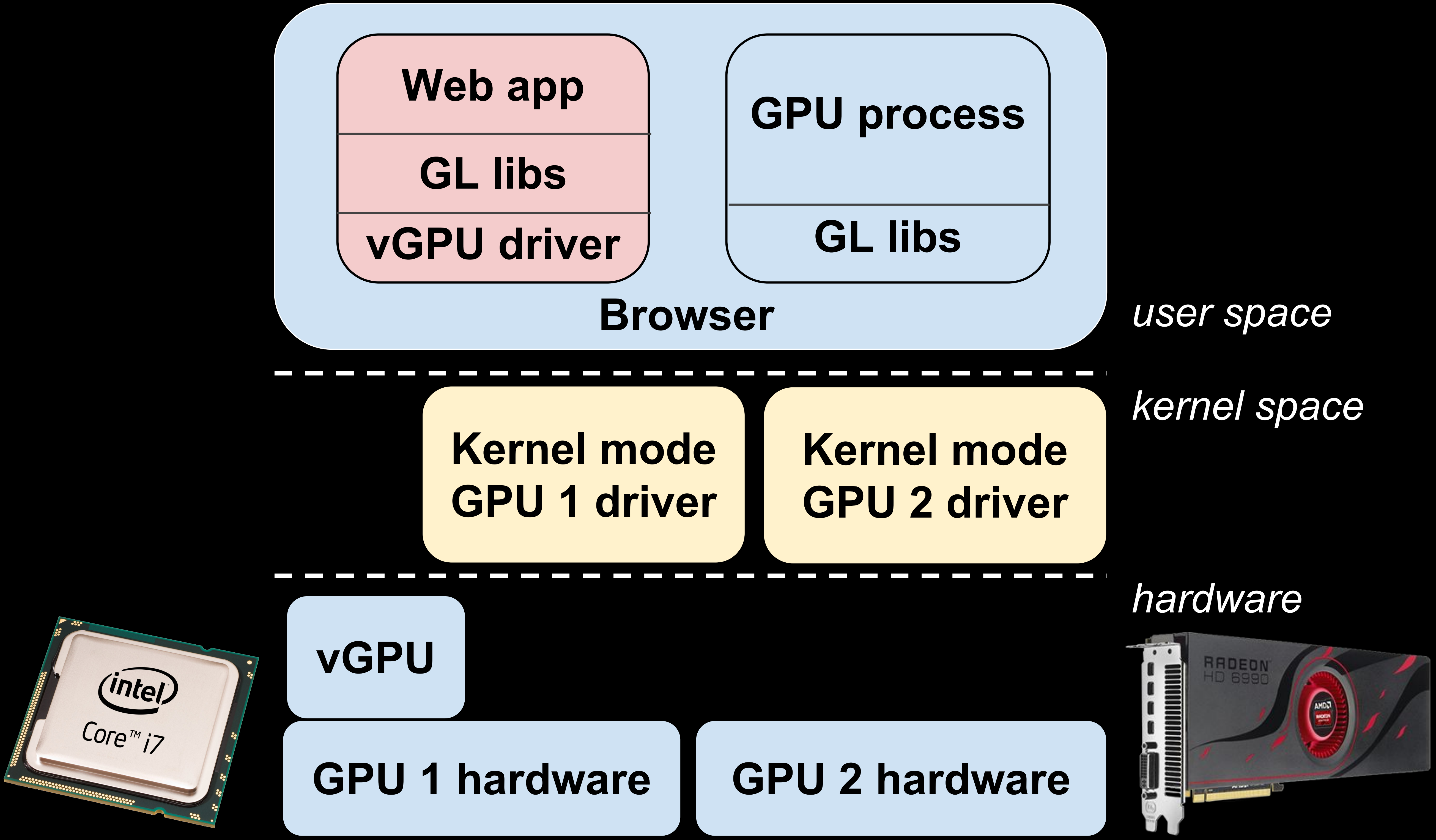
Intel vGPU hang will cause a real GPU hang

Dual-GPU Sugar

Key idea: Use two GPUs to fully isolate the virtual graphics plane and the primary graphics plane.

- Solves system UI freeze
- Provides better performance isolation

Dual-GPU Sugar’s design



Browser

Web app

GL libs

vGPU driver

GPU process

GL libs

user space

kernel space

Kernel mode GPU 1 driver

Kernel mode GPU 2 driver

hardware

vGPU

GPU 1 hardware

GPU 2 hardware

Photo credit: https://www.amd.com/zh-tw/products/graphics/desktop/6000/6990

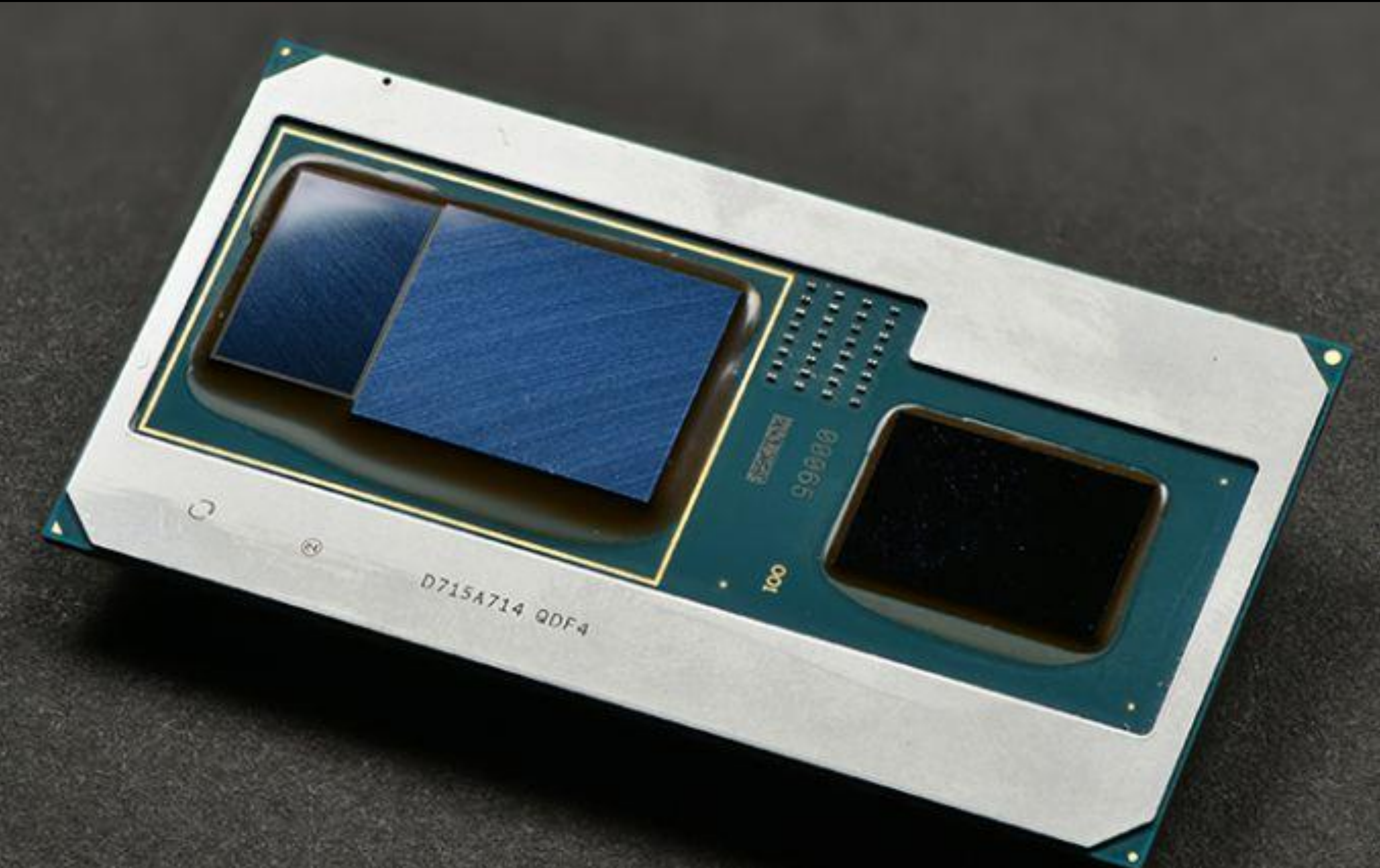
Many computers have two GPUs

dell.com/Inspiron15

apple.com/macbook-pro

store.hp.com/envy

Intel’s 8th Generation Core Processors with Radeon RX Vega M Graphics

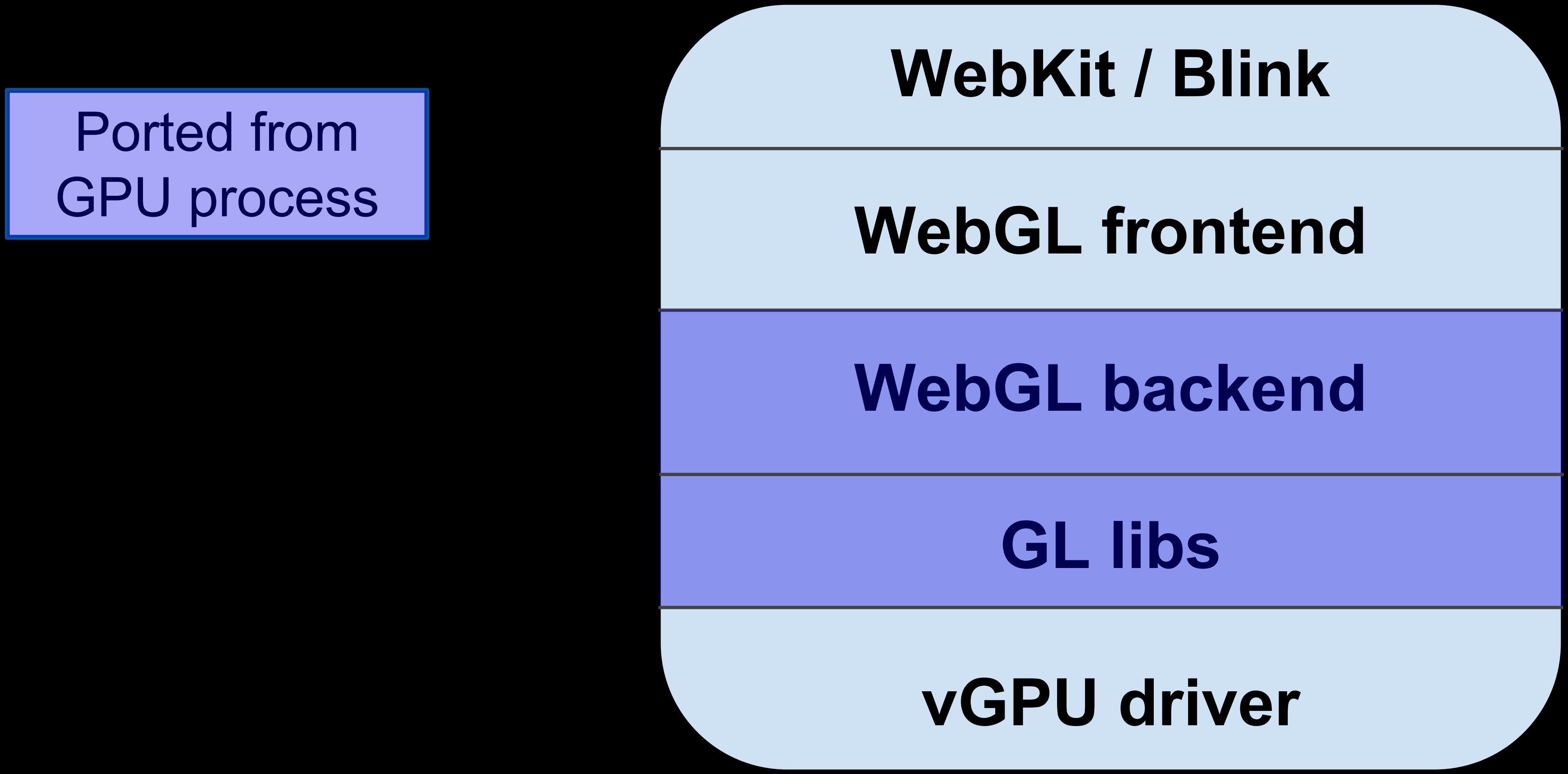


Source: https://newsroom.intel.com/news/8th-gen-intel-core-radeon-rx-vega-m-graphics

Sugar’s implementation

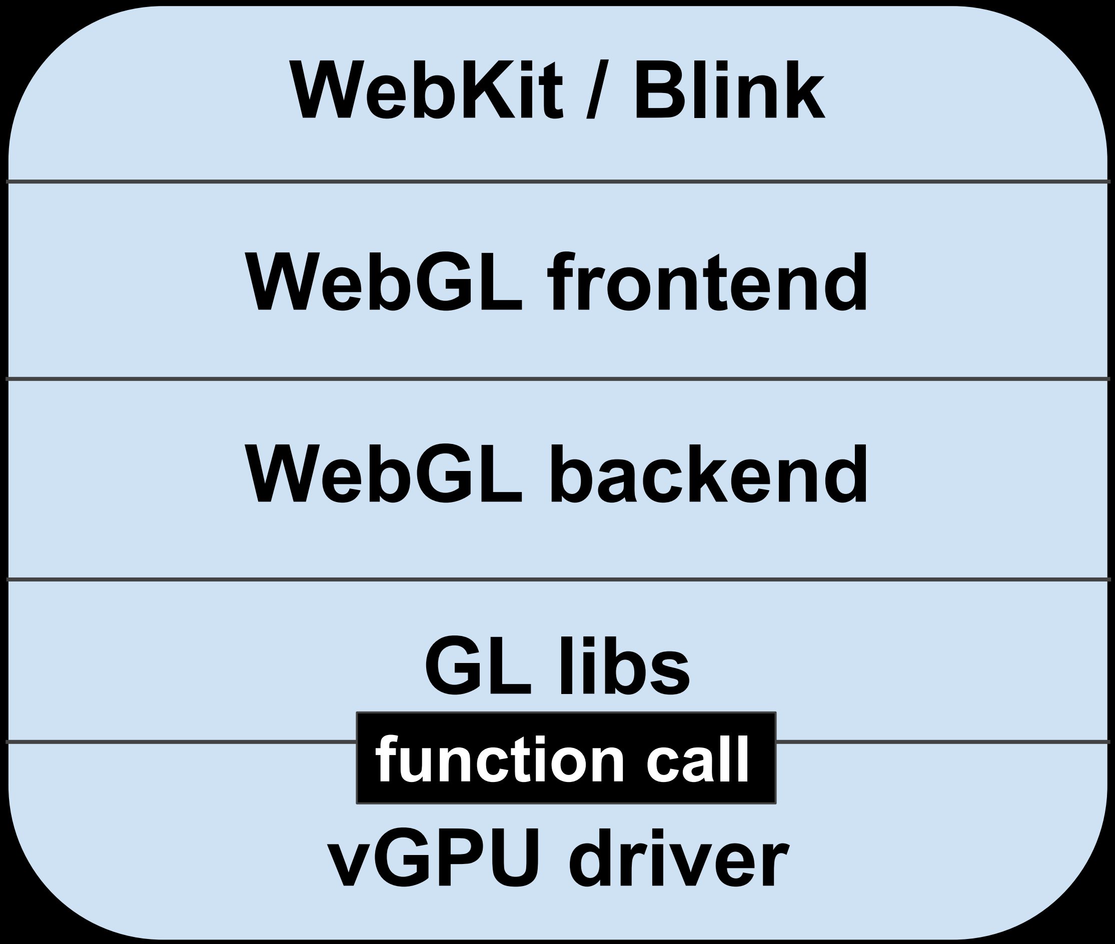
WebGL in web app process

Reuse most of GPU process code

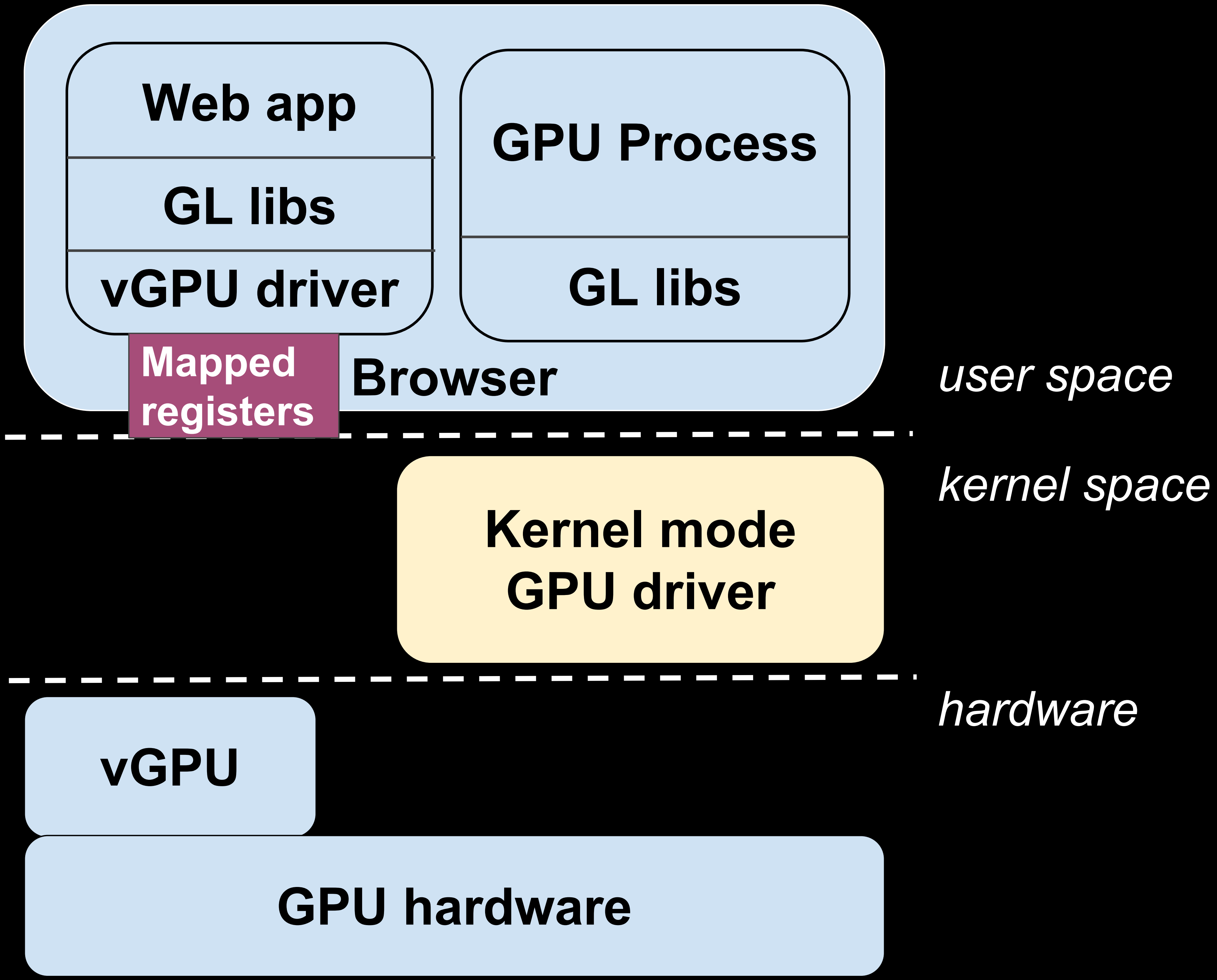


vGPU driver as a library

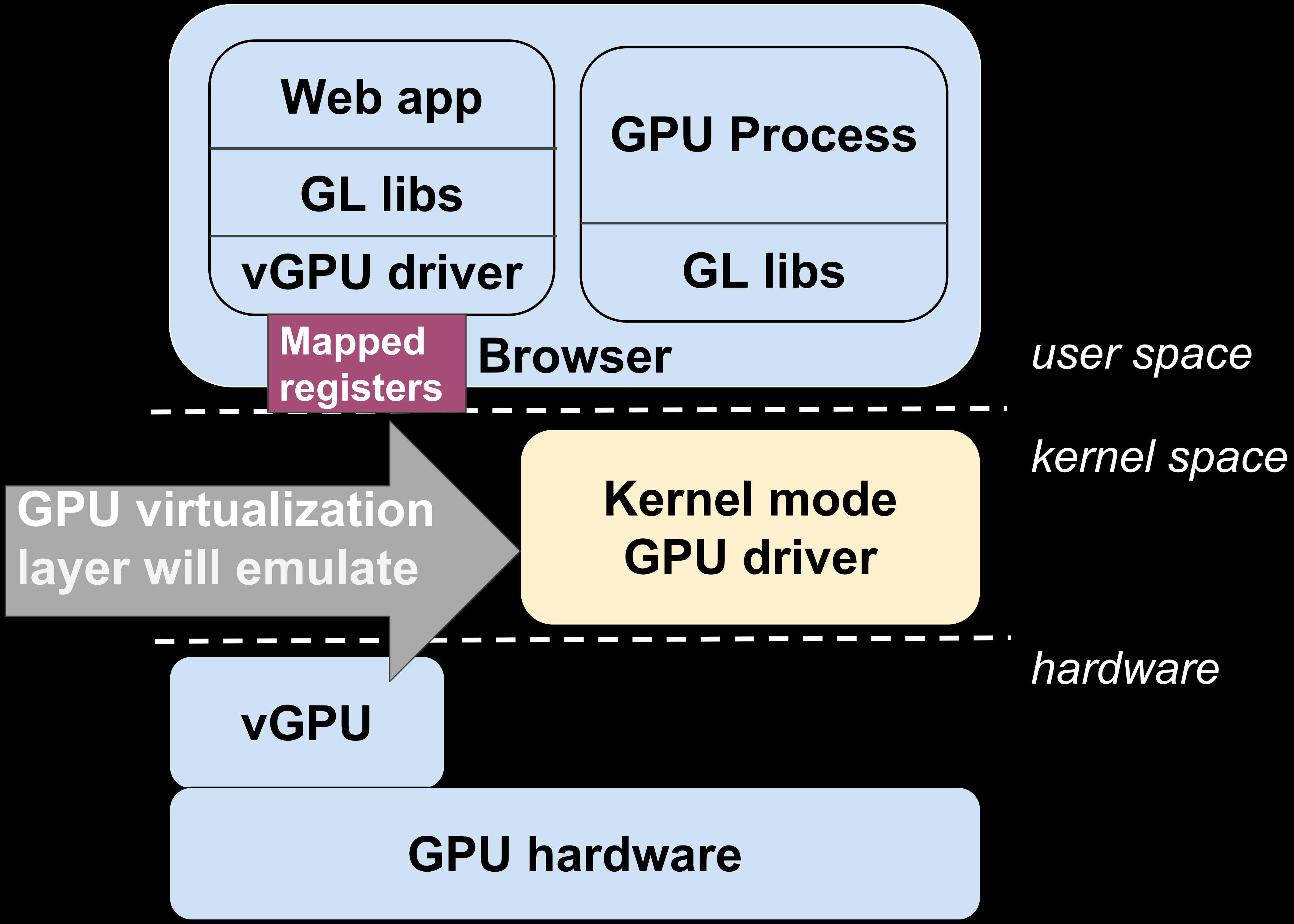
We modify GL libs to issue function calls instead of syscalls



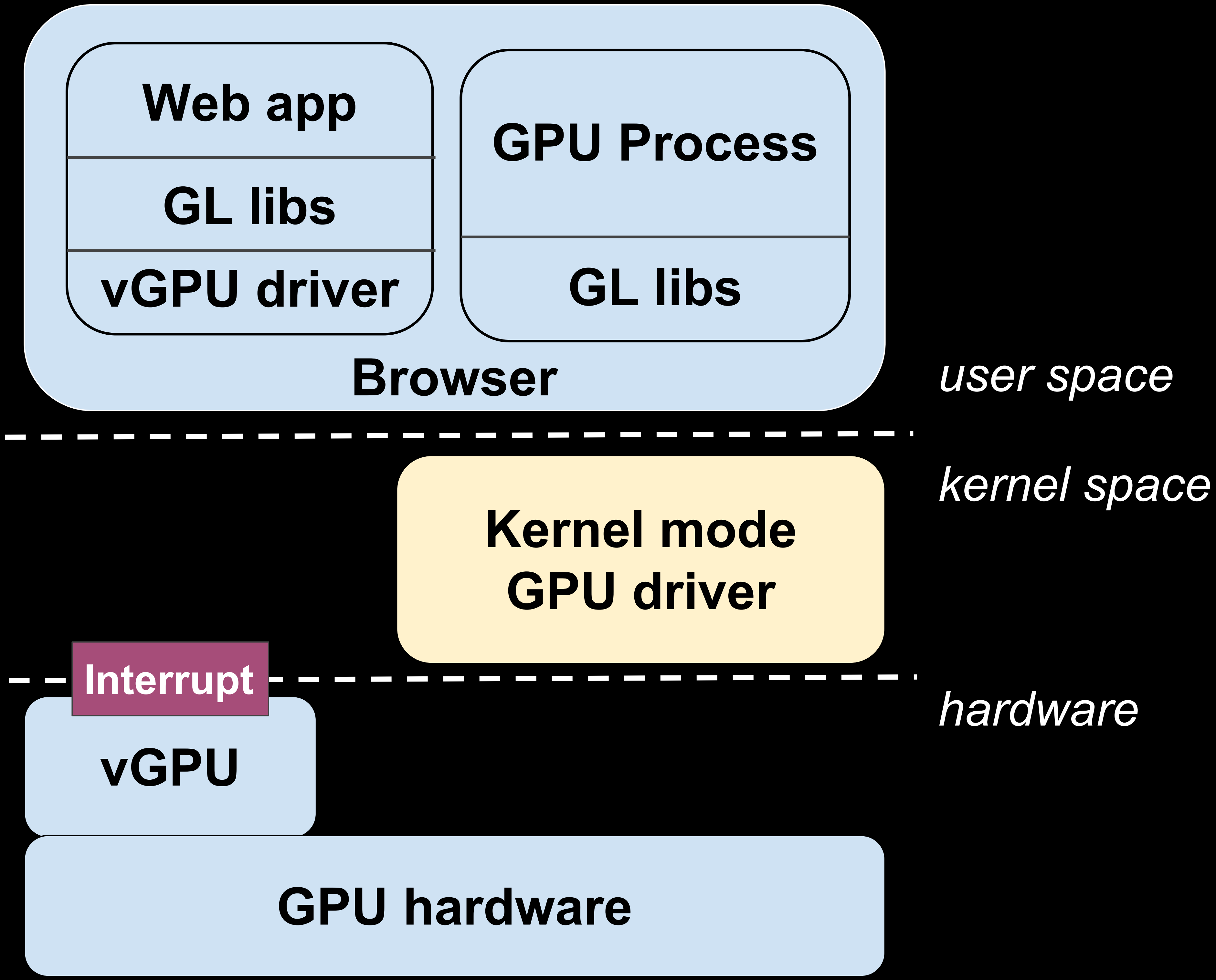
Register: trap and emulate



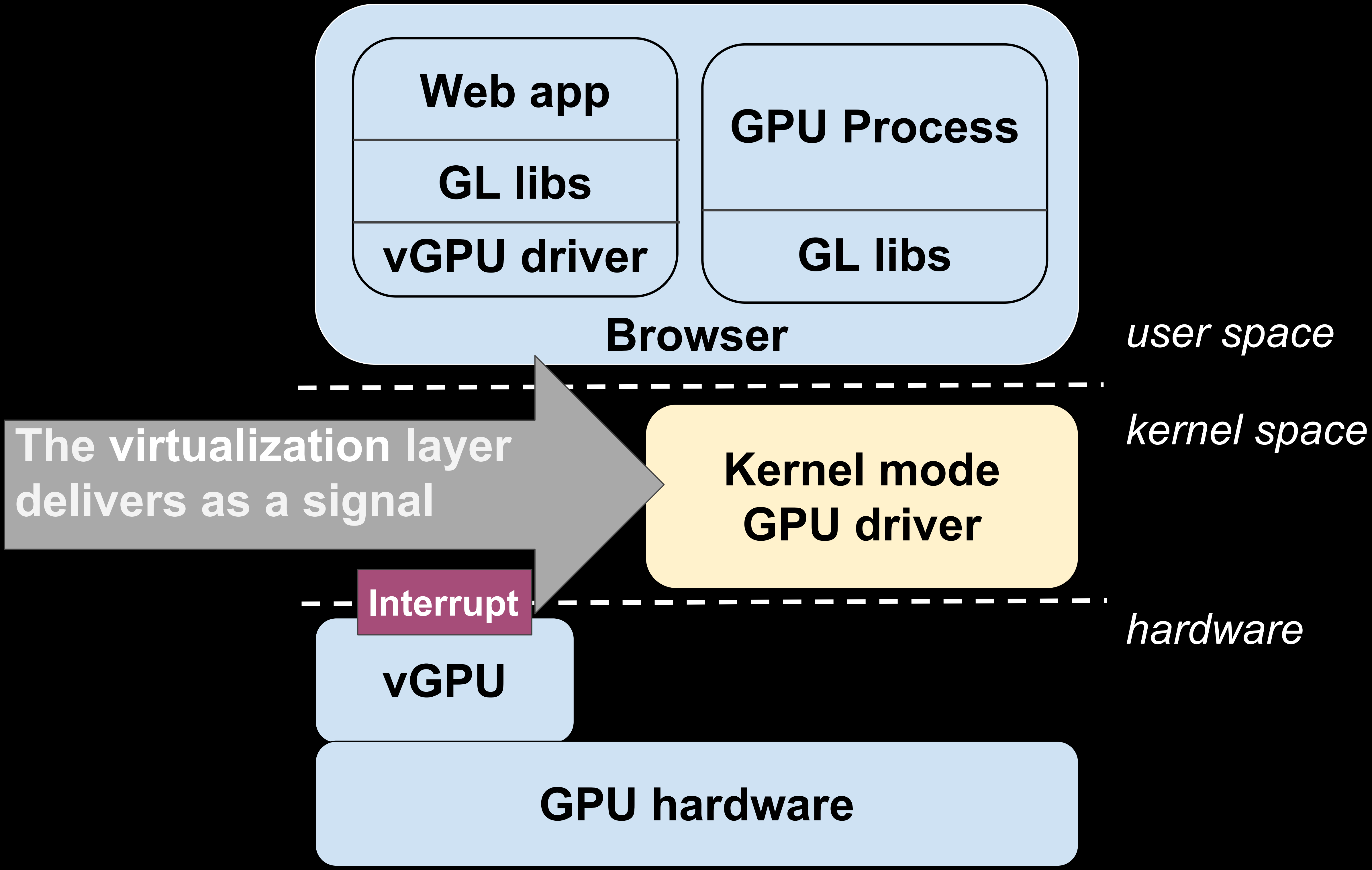
Register: trap and emulate



Interrupt: deliver as signal



Interrupt: deliver as signal



Web app

GL libs

vGPU driver

GPU Process

GL libs

Browser

user space

kernel space

The virtualization layer delivers as a signal

Kernel mode GPU driver

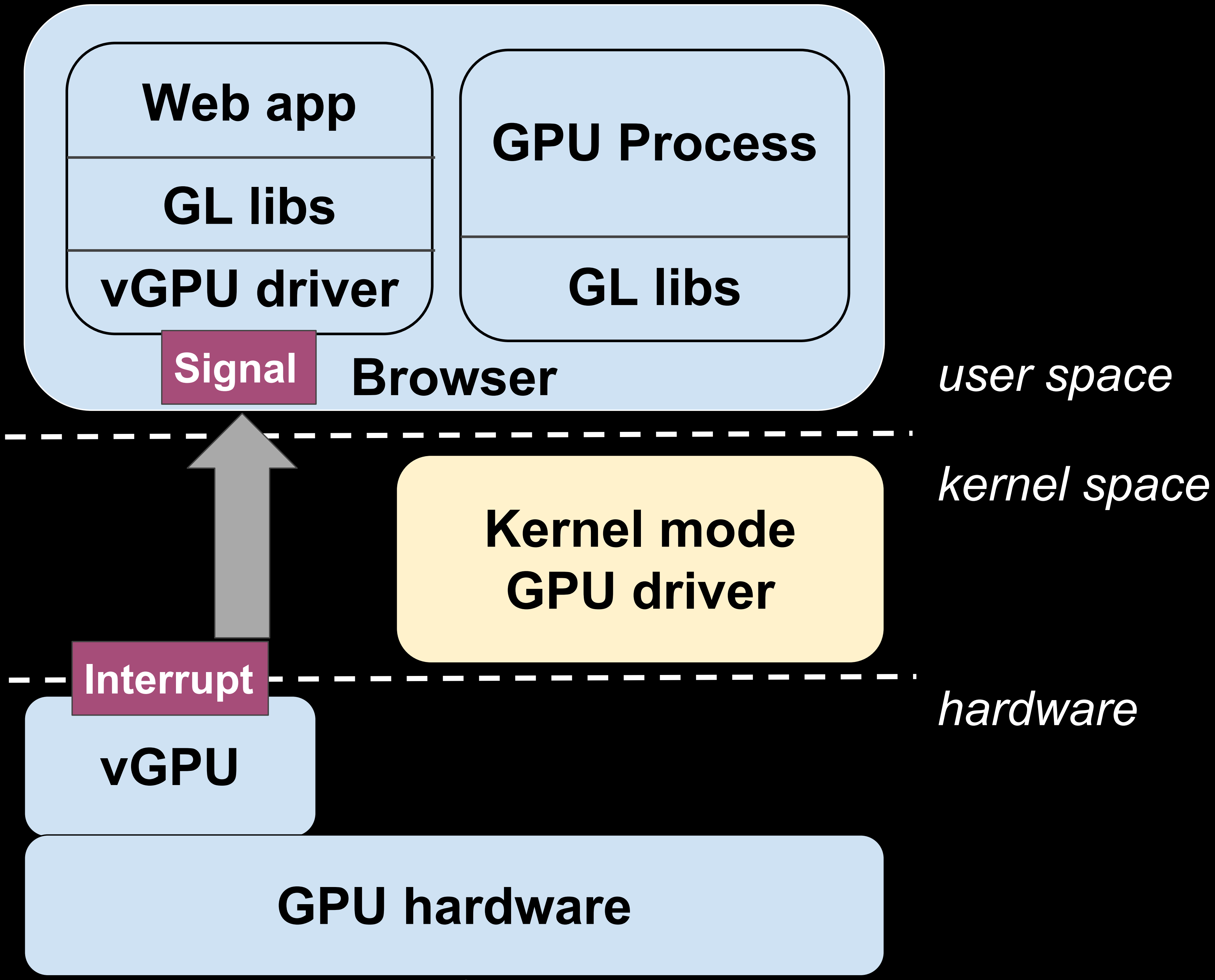
Interrupt

hardware

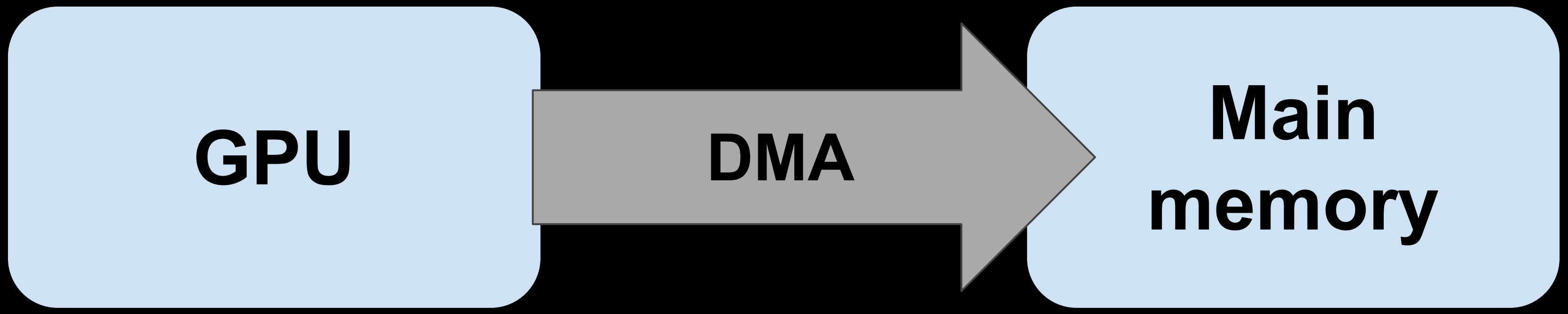
vGPU

GPU hardware

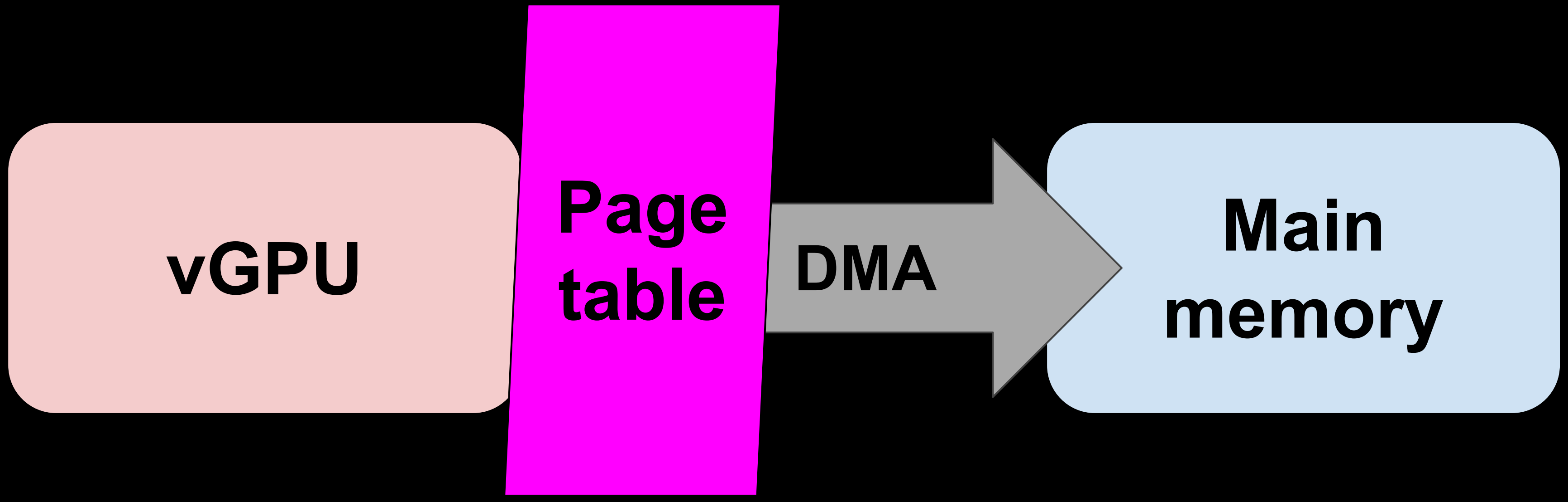
Interrupt: deliver as signal



DMA overview



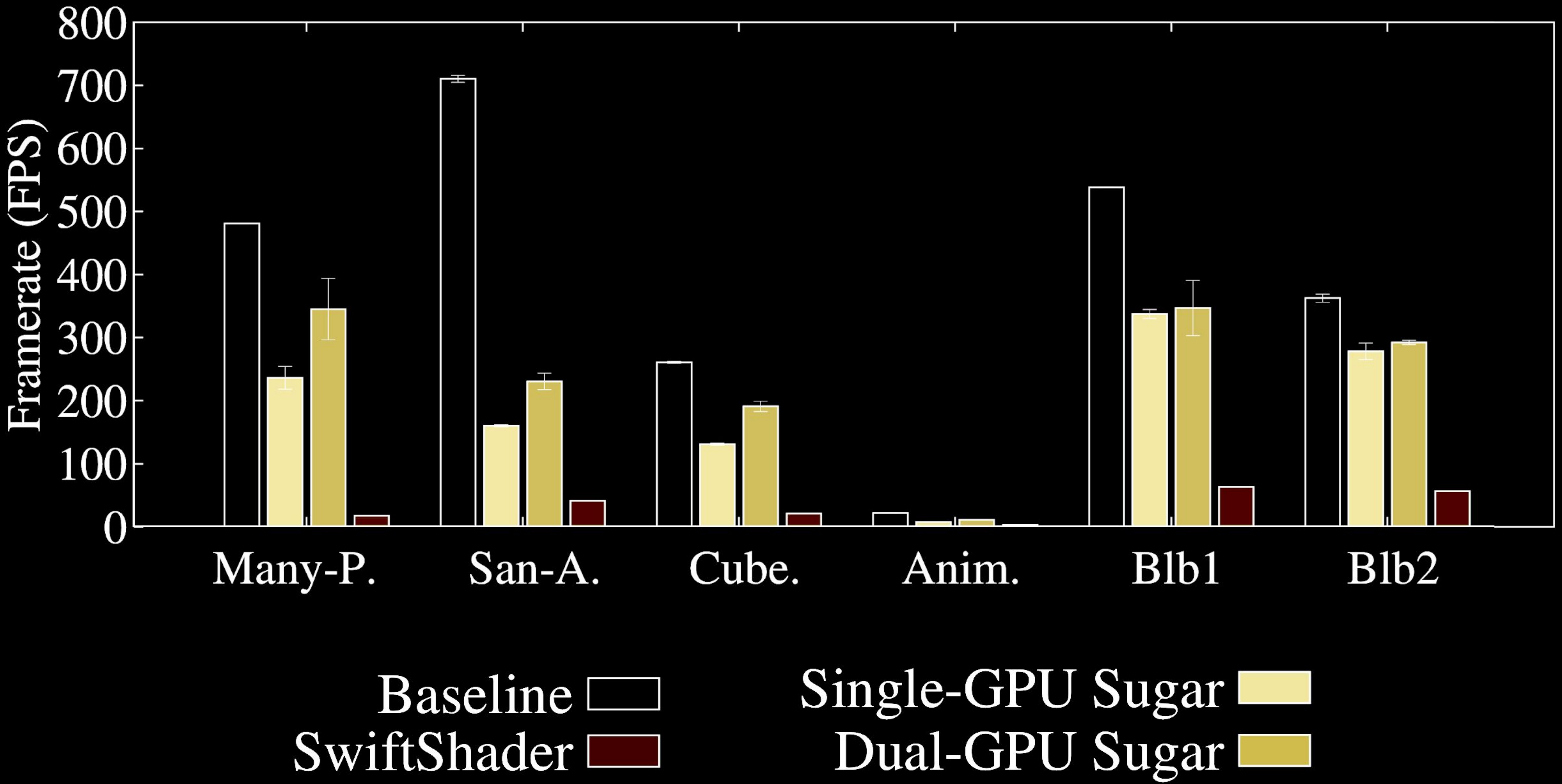
DMA overview



Evaluations

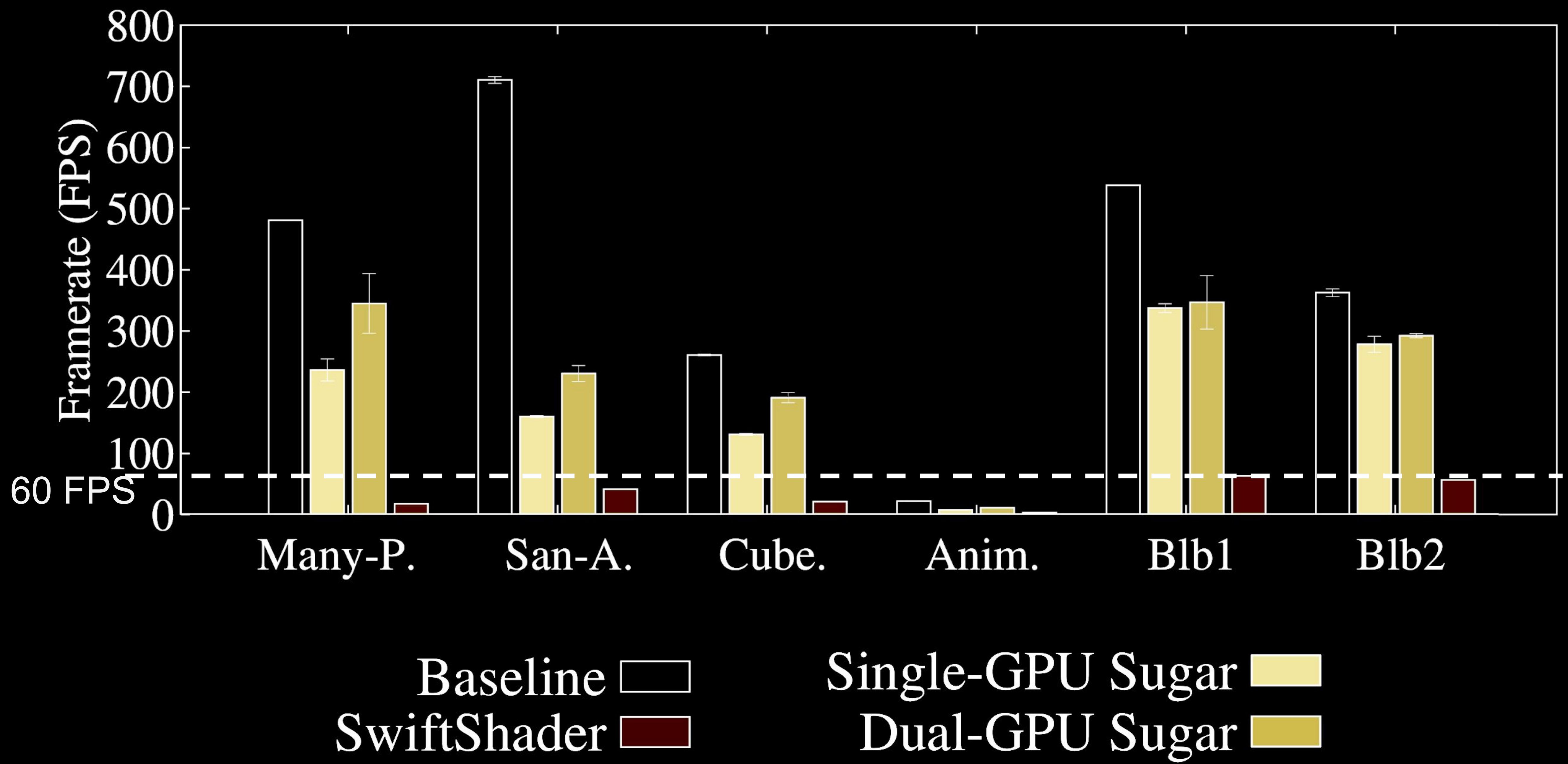
Sugar's performance is good

under the same WebGL benchmarks that Chrome uses



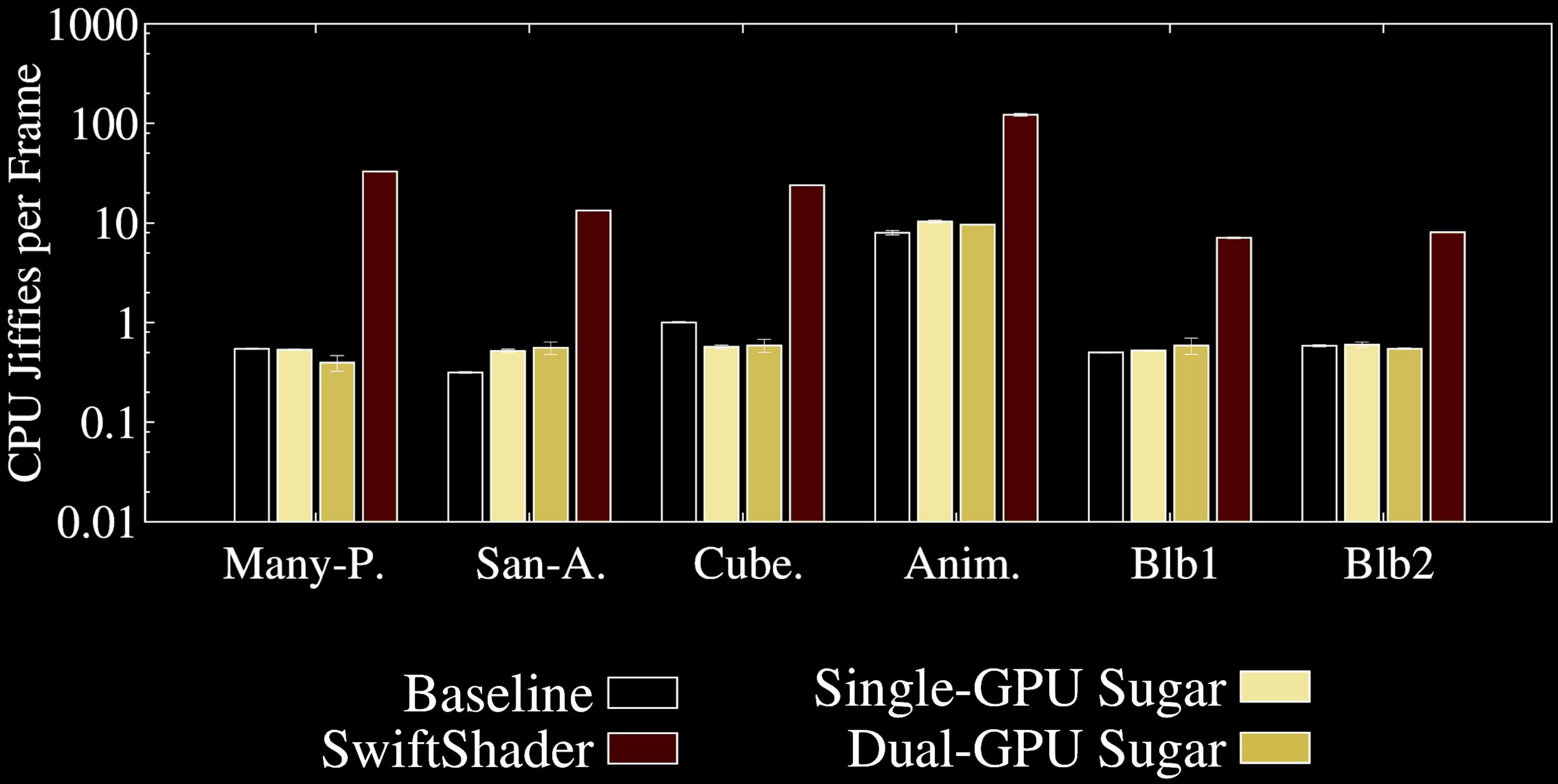
Sugar’s performance is good

under the same WebGL benchmarks that Chrome uses



Sugar’s CPU overhead is low

Sugar is better than CPU rendering by 375% on average



Summary

- Sugar leverages modern GPU virtualization solutions to isolate WebGL

- Sugar addresses this by repurposing Intel vGPU driver to a library

Thank you!

Sugar is open source: https://trusslab.github.io/sugar