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

Source: https://www.google.com/map
WebGL is popular

WebGL adoption rate by top 100 websites

Not using
47.0%

Using
53.0%
WebGL is popular

Browser support rate (48.8 million visitors)

Support 96.0%

Does not support 4.0%

WebGL recap
First, a quick recap on OpenGL

- Native app
- GL libs
- Kernel mode GPU driver
- GPU hardware

- User space
- Kernel space
- Hardware
First, a quick recap on OpenGL

Native app
  function call
  GL libs

Kernel mode GPU driver

GPU hardware

user space
kernel space
kernel space
hardware
First, a quick recap on OpenGL
Use the same design for WebGL?
Web apps are not trusted

- Web app
- GL libs
- Kernel mode GPU driver
- GPU hardware

- Buggy
- Malicious
- Compromised

- user space
- kernel space
- hardware
GPU driver is buggy

- Web app
- GL libs
- Kernel mode GPU driver
- GPU hardware

- Buggy
- Malicious
- Compromised

user space
kernel space
hardware
Kernel driver is compromised

- Web app
- GL libs
- Kernel mode GPU driver
- GPU hardware

- Buggy
- Malicious
- Compromised

user space
kernel space
hardware
Current WebGL design

Browser

Web app

Kernel mode GPU driver

GPU Process
Checks
GL libs

user space
kernel space
hardware
Current WebGL design

- Web app
- Browser
- IPC
- GPU Process
  - Checks
  - GL libs
- Kernel mode GPU driver
  - user space
  - kernel space
  - hardware

GPU hardware
Security checks in GPU Process

- Web app
  - Browser
  - Kernel mode GPU driver
    - GPU hardware

- GPU Process
  - Checks
  - GL libs

- user space
- kernel space
- hardware
TCB of current WebGL Design

- Web app
- Browser
- GPU Process
  - Checks
  - GL libs
- Kernel mode GPU driver
- GPU hardware

- 158,000 LoC (GPU Process)
- 457,000 LoC (GL libraries)
- 123,000 LoC (GPU driver)
Vulnerabilities in GPU process

- Kernel mode GPU driver
- GPU hardware
- Checks
- GL libs
- Web app
- Browser

CVE-2014-1556
CVE-2015-7179
CVE-2013-2874
CVE-2017-5031
CVE-2014-1502
Kernel driver is compromised

- Kernel mode GPU driver
- GPU hardware
- Web app
- Checks
- GL libs

CVE-2011-2601*
Chrome 153469
Chrome 483877*
CVE-2011-2367
CVE-2011-3653

*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

<table>
<thead>
<tr>
<th></th>
<th>High performance</th>
<th>Known vulnerabilities</th>
<th>Zero day vulnerabilities</th>
<th>System UI freeze</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
CVE-2014-3173, read of GPU graphics memory

We type some private notes in terminal:
CVE-2014-3173, read of GPU graphics memory

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
Sugar’s design

- Web app
  - GL libs
  - vGPU driver

- GPU Process
  - GL libs

- Kernel mode
  - GPU driver

- vGPU

- GPU hardware

- Function call

- User space

- Kernel space

- Hardware
Sugar’s design

- Web app
- GL libs
- vGPU driver

Browser

- GPU Process
- GL libs

Kernel mode
- GPU driver

vGPU

user space

kernel space

hardware

function call
Sugar’s design

- Web app
- GL libs
- vGPU driver

- GPU Process
- GL libs

Browser

- User space
- Kernel space
- Hardware

vGPU

GPU hardware
Sugar’s design

- Web app
- GL libs
- vGPU driver

Browser

- GPU Process
- GL libs

Kernel mode
- GPU driver

vGPU

- GPU hardware

virtual graphics plane

primary graphics plane
Why is Sugar secure?
Web app process is untrusted

- Web app
- GL libs
- vGPU driver

- GPU Process
- GL libs

Browser

- User space
- Kernel space
- Hardware

- vGPU
- GPU hardware
Web app process is sandboxed

- **Web app**
  - GL libs
  - vGPU driver

- **GPU Process**
  - GL libs

- **Browser**
  - user space
  - kernel space
  - hardware

  **vGPU**
  - GPU hardware
vGPU is isolated

Web app
  GL libs
  vGPU driver

Browser

GPU Process
  GL libs

Kernel mode
  GPU driver

vGPU

GPU hardware

user space

kernel space

hardware
Sugar’s TCB is small

34,400 LoC (GPU virtualization)

vGPU

Web app
GL libs
vGPU driver

GPU Process
GL libs

Kernel mode GPU driver

Browser

user space
kernel space
hardware
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

- **Kernel mode**
  - GPU 1 driver
  - GPU 2 driver

- **User space**
  - Hardware
  - Web app
  - GL libs

- **Kernel space**
  - Kernel mode
  - GPU 1 driver
  - GPU 2 driver

Photo credit: https://www.amd.com/zh-tw/products/graphics/desktop/6000/6990
Many computers have two GPUs

dell.com/Inspiron15

store.hp.com/envy

apple.com/macbook-pro
Intel’s 8th Generation Core Processors with Radeon RX Vega M Graphics

Sugar’s implementation
WebGL in web app process

Reuse most of GPU process code

WebKit / Blink
WebGL frontend
WebGL backend
GL libs
vGPU driver

Ported from GPU process
vGPU driver as a library

We modify GL libs to issue function calls instead of syscalls
Register: trap and emulate

- Web app
- GL libs
- vGPU driver

Browser

- Mapped registers

- GPU Process
- GL libs

Kernel mode
- GPU driver

vGPU

GPU hardware

- user space
- kernel space
- hardware
Register: trap and emulate

GPU virtualization layer will emulate

Web app
GL libs
vGPU driver

Mapped registers

Browser

GPU Process
GL libs

Kernel mode
GPU driver

vGPU

GPU hardware

user space

kernel space

hardware
Interrupt: deliver as signal

Browser

- Web app
- GL libs
- vGPU driver

GPU Process
- GL libs

Kernel mode
GPU driver

Interrupt
vGPU

GPU hardware

user space
kernel space
hardware
Interrupt: deliver as signal

The virtualization layer delivers as a signal

Web app
GL libs
vGPU driver

Browser

Kernel mode
GPU driver

vGPU

GPU hardware

user space
kernel space
hardware
Interrupt: deliver as signal

- Web app
- GL libs
- vGPU driver

Browser

Keyboard mode
- GPU Process
- GL libs

vGPU

- Interrupt
- GPU hardware

Signal

user space
kernel space
hardware
DMA overview
DMA overview

- vGPU
- Page table
- DMA
- Main memory
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