

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)
> Security (<https://www.bleepingcomputer.com/news/security/>)
> Researchers use GPU fingerprinting to track users online

Researchers use GPU fingerprinting to track users online

By
Bill Toulas
(<https://www.bleepingcomputer.com/author/bill-toulas/>)

January 30, 2022

10:12 AM

0



A team of researchers from French, Israeli, and Australian universities has explored the possibility of using people's GPUs to create unique fingerprints and use them for persistent web tracking.



The results of their large-scale experiment involving 2,550 devices with 1,605 distinct CPU configurations show that their technique, named 'DrawnApart,' can boost the median tracking duration to 67% compared to current state-of-the-art methods.

This is a severe problem for user privacy, which is currently protected by laws that focus on acquiring consent to activate website cookies.



These laws have led unscrupulous websites to collect other potential fingerprinting elements such as the hardware configuration, OS, timezones, screen resolution, language, fonts, etc.

This unethical approach is still limited because these elements change frequently, and even when they're stable, they can only put users into a rough categorization rather than create a unique fingerprint.

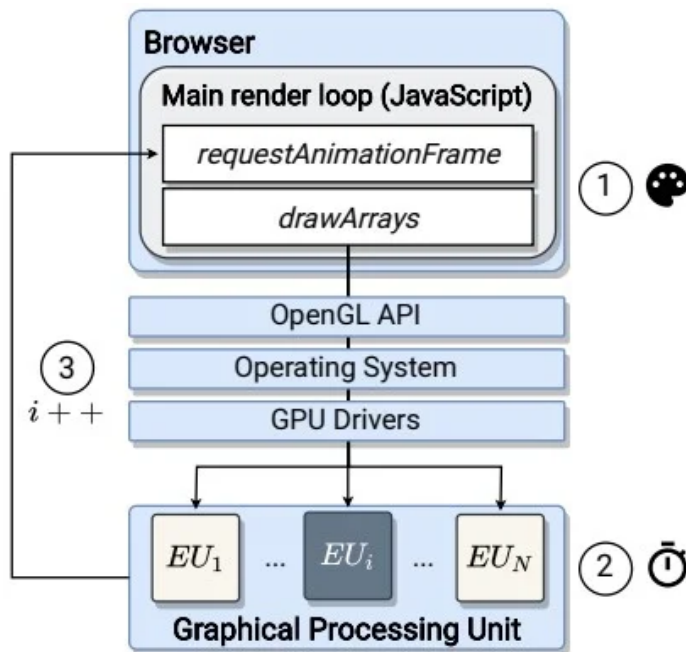
Fingerprinting identical GPUs

The researchers considered the possibility of creating distinctive fingerprints based on the GPU (graphics processing unit) of the tracked systems with the help of WebGL (Web Graphics Library).

WebGL is a cross-platform API for rendering 3D graphics in the browser, and it's present on all modern web browsers.

Using this library, the DrawnApart tracking system can count the number and speed of the execution units in the GPU, measure the time needed to complete vertex renders, handle stall functions, and more.





Fingerprinting the GPU for persistent tracking

Source: Arxiv.org

DrawnApart uses short GLSL programs executed by the target GPU as part of the vertex shader to overcome the challenge of having random execution units handling the computations. Hence, the workload allocation is predictable and standardized.

The team developed both an on-screen measurement method that executes a small number of computationally intensive operations and an offscreen method that puts the GPU through a lengthier and less intensive test.

```

1 function render_loop() {
2   if (point_index < point_count) {
3     // Stall the current point
4     gl.uniform1i(shader_stalled_point_id,
5       point_index);
6     gl.drawArrays(gl.POINTS, 0, point_count);
7     // Save the rendering time
8     var dt = performance.now() - prev_time;
9     prev_time = performance.now();
10    trace.push(dt);
11    // Prepare to stall the next point
12    point_index++;
13    requestAnimationFrame(render_loop);
14  } else {
15    // Finish and send the trace to the server
16    send_trace();
17  }
18 }

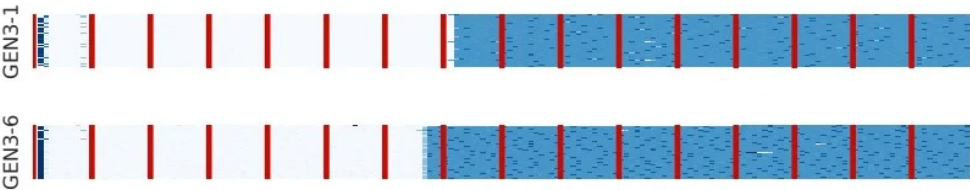
```

Render loop used for the on-screen test

Source: Arxiv.org

This process generates traces consisting of 176 measurements taken from 16 points that are used to create a fingerprint. Even when evaluating the individual raw traces visually, one can notice differences and distinct timing variations between devices.





The resulting raw traces from two identical GPUs

Source: Arxiv.org

The researchers also tried swapping other hardware parts on the machines to see if the traces would remain distinguishable and found that the fingerprints solely depended on the GPU.

Even if a set of integrated circuits is created through an identical manufacturing process, has the same nominal computational power, the number of processing units, and the exact same cores and architecture, each circuit is slightly different due to normal manufacturing variability.

These differences are indistinguishable in normal day-to-day operations, but they can become useful in the context of a sophisticated tracking system like DrawnApart, which is specifically designed to trigger functional aspects that highlight them.

TABLE I. ACCURACY GAINS ACHIEVED UNDER LAB CONDITIONS

Device Type	GPU	Device Count	Timer	Base Rate (%)	Accuracy (%)	Gain
Intel i5-3470 (GEN 3 Ivy Bridge)	Intel HD Graphics 2500	10	Onscreen	10.0	93.0±0.3	9.3
			Offscreen	10.0	36.3±1.6	3.6
Intel i5-4590 (GEN 4 Haswell)	Intel HD Graphics 4600	23	Onscreen	4.3	32.7±0.3	7.6
			Offscreen	4.3	63.7±0.6	14.7
			GPU	4.3	15.2±0.5	3.5
Intel i5-8500 (GEN 8 Coffee Lake)	Intel UHD Graphics 630	15	Onscreen	6.7	42.2±0.7	6.3
			Offscreen	6.7	55.5±0.8	8.3
			GPU	6.7	53.5±0.8	8.0
Intel i5-10500 (GEN 10 Comet Lake)	Nvidia GTX1650	10	Offscreen	10.0	70.0±0.5	7.0
			GPU	10.0	95.8±0.9	9.6
Apple Mac mini M1	Apple M1	4	Offscreen	25.0	46.9±0.4	1.9
			GPU	25.0	73.1±0.7	2.9
Samsung Galaxy S8/S8+	Mali-G71 MP20	6	Onscreen	16.7	36.7±2.7	2.2
Samsung Galaxy S9/S9+	Mali-G72 MP18	6	Onscreen	16.7	54.3±5.5	3.3
Samsung Galaxy S10e/S10/S10+	Mali-G76 MP12	8	Onscreen	12.5	54.1±1.5	4.3
Samsung Galaxy S20/S20 Ultra	Mali-G77 MP11	6	Onscreen	16.7	92.7±1.8	5.6

Tested devices and classification accuracy

Source: Arxiv.org

Implications and considerations

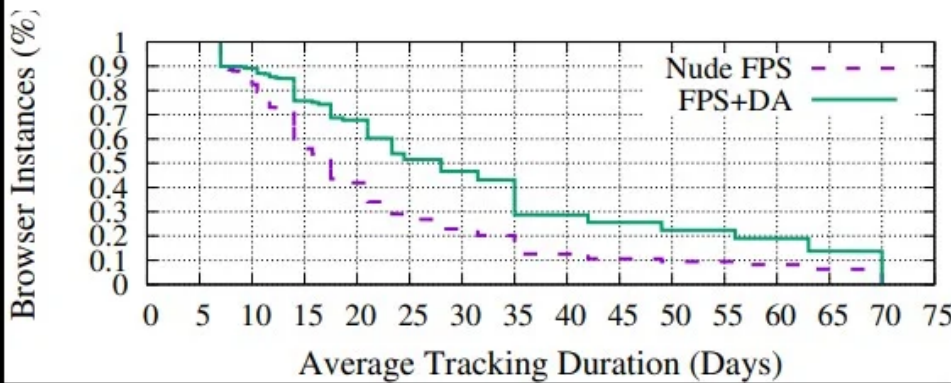
When DrawnApart is used in conjunction with state-of-the-art tracking algorithms, the median tracking duration of a targeted user increases by 67%.



As illustrated in the following diagram, the standalone tracking algorithm can achieve an average tracking time of 17.5 days, but with the help of GPU fingerprinting, this is extended to 28 days.

TABLE III. AVERAGE TRACKING TIME BY COLLECTION PERIOD

Collection Period	Tracking duration in days		Improvement
	Nude FPS	FPS+DA	
2 days	17	26	+52.94%
3 days	17.25	25.5	+47.82%
4 days	17	28	+64.70%
5 days	17.5	27.5	+57.14%
6 days	18	30	+66.66%
7 days	17.5	28	+60.00%



Tracking duration diagram

Source: Arxiv.org

This evaluation was based on the testing conditions that the GPU operational temperature range is between 26.4 °C and 37 °C, with no voltage variations.

Apart from these conditions, workload variations, GPU payloads from other web browser tabs, system restarts, and other runtime changes don't affect DrawnApart.

The next-gen GPU APIs currently in development, most notably WebGPU, features compute shaders which come in addition to the existing graphics pipeline.

As such, the upcoming API may introduce even more ways to fingerprint internet users, and quite likely faster and far more accurate too.

When the researchers tested compute shaders in the now-abandoned WebGL 2.0, they found that DrawnApart delivered 98% classification accuracy in just 150 milliseconds, much faster than the 8 seconds used to collect fingerprinting data through the WebGL API.

"We believe that a similar method can also be found for the WebGPU API once it becomes generally available. The effects of accelerated compute APIs on user privacy should be considered before they are enabled globally," concludes the research paper (<https://arxiv.org/pdf/2201.09956.pdf>).



Potential countermeasures to this fingerprinting method include attribute value changes, parallel execution prevention, script blocking, API blocking, and time measurement prevention.

The developer of the WebGL API, Khronos group, has received the researchers' disclosure on the above and formed a technical study group to discuss potential solutions with browser vendors and other stakeholders.

Related Articles:

ProtonMail introduces a new email tracker blocking system
(<https://www.bleepingcomputer.com/news/security/protonmail-introduces-a-new-email-tracker-blocking-system/>)

Beijing 2022 Winter Olympics app bursting with privacy risks
(<https://www.bleepingcomputer.com/news/security/beijing-2022-winter-olympics-app-bursting-with-privacy-risks/>)

Android users can now disable 2G to block Stingray attacks
(<https://www.bleepingcomputer.com/news/security/android-users-can-now-disable-2g-to-block-stingray-attacks/>)

Firefox Focus now blocks cross-site tracking on Android devices
(<https://www.bleepingcomputer.com/news/security/firefox-focus-now-blocks-cross-site-tracking-on-android-devices/>)

Europol ordered to erase data on those not linked to crime
(<https://www.bleepingcomputer.com/news/security/europol-ordered-to-erase-data-on-those-not-linked-to-crime/>)

