**Researchers have developed a new fingerprinting approach that uses your GPU to track you.**

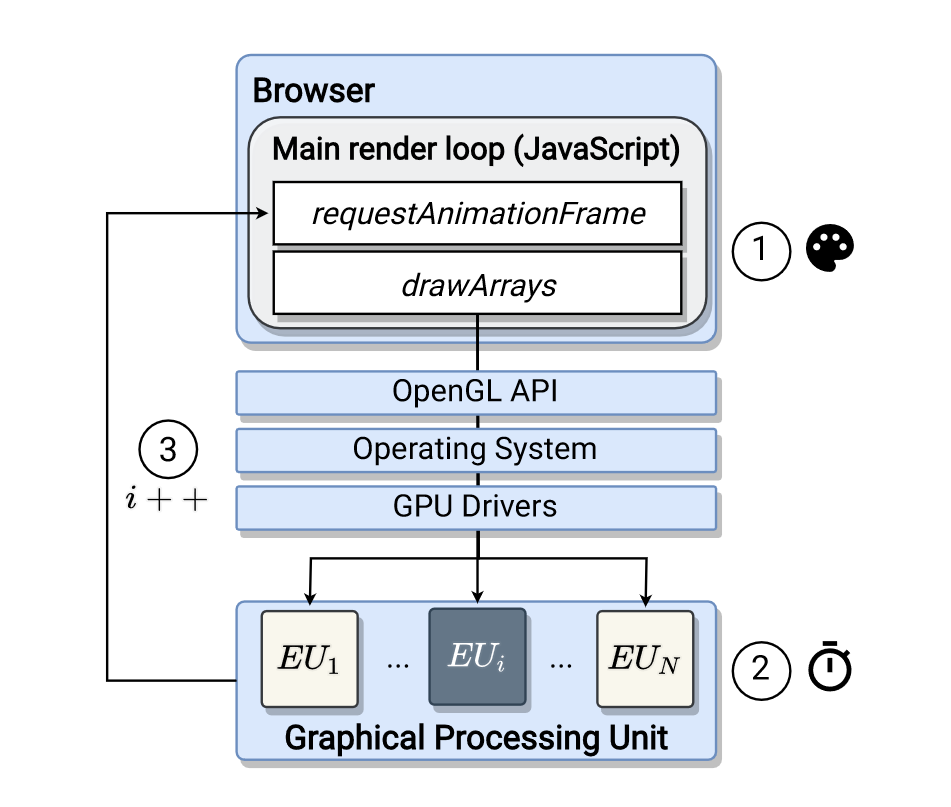
Each GPU generates a distinct trace.



Lack of privacy: Although privacy seems to be a rarity these days, with enough care and work, you can largely disguise your digital imprint from both large internet corporations and international governments. That is, at least, what has happened thus far. Researchers from France, Israel, and Australia have collaborated to demonstrate that even the most stringent privacy safeguards may not be sufficient to cover all monitoring gaps. Your own computer hardware, it turns out, may be working against you.

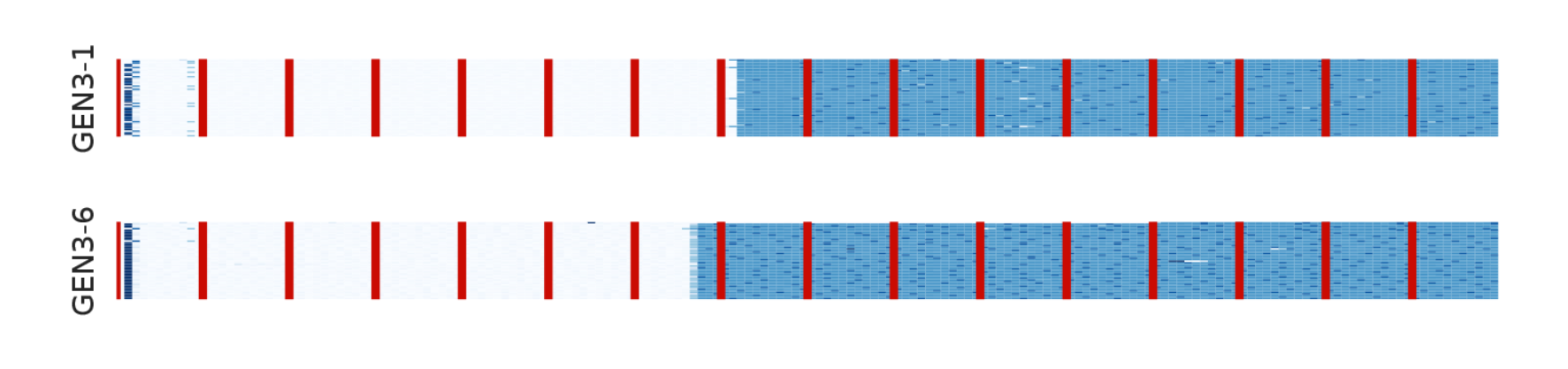
The researchers in question have created "DrawnApart," a method of device identification. This technique improves on existing browser fingerprinting technology by identifying a user's device based on the "unique features" of its GPU stack, which tends to become obsolete the longer a fingerprint is in use.

Browser fingerprints are typically confused over time as people with similar devices and hardware access the same page. GPU fingerprinting looks for "slight variances" caused by the manufacturing process of each video card; differences that aren't easily concealed or obfuscated.



So, on a more technical level, how does DrawnApart work? It starts by generating a "series of rendering tasks," each of which targets distinct "Execution Units" on a user's GPU, according to researchers. These tasks provide a fingerprint trail, which is then fed into a machine learning network, which converts it into a "embedding vector." This vector describes the fingerprint and can be used to direct an adversary (the person or entity who uses this approach) to the device that created it.

WebGL, the graphics framework responsible for rendering across innumerable websites, is used to create DrawnApart's workloads. The workloads in question are intended to detect even the tiniest discrepancies in GPU power usage and processing power. Even if their make and model are identical, each card will render WebGL points (single-vertex objects) differently and handle stall functions differently. The trace image below, which compares two GPUs that appear to be similar, shows an example of these minor variances.



Researchers collected 50 traces from both devices using DrawnApart, with each trace consisting of "176 measurements of 16 points." After that, the measurements are divided into 16 groups of 11, each of which "stalls" at a different location. The time it takes the GPU to produce each point is represented by a colour gradient spanning from pure white to deep blue, with the former indicating a faster render (nearly 0ms) and the latter indicating a slower render (almost 100ms) (up top 90ms). The red bars in the figure above are simply used to distinguish the groups, which is why they are the same on both traces.

These two traces, as you can see, have significant variances. Some of these differences are to be expected, according to the researchers, because even the same equipment does not always work equally. Despite this, the team believes that the traces indicate significant patterns that allow them to distinguish between two similar cards. Naturally, this granularity enables for highly precise fingerprinting that can follow people for far longer periods of time than older methods. Drawn Apart, when paired with a "state-of-the-art" tracking algorithm, improves the length of time a target may be tracked by up to 67 percent, according to Bleeping Computer (28 days versus the normal average of 17.5 days).

So, why are you conducting this study in the first place? If these researchers are so worried about user privacy, as they say, why do they hand over the keys to the kingdom to advertising and other nefarious actors? The team believes that by exposing these possible privacy flaws, the creators of graphics libraries like WebGL and the future WebGPU API will think about the privacy implications of their technology and implement safeguards sooner rather than later.

In any case, this study is intriguing and raises major concerns about the future of digital privacy. For better or worse, we're excited to see what comes of it in the future.