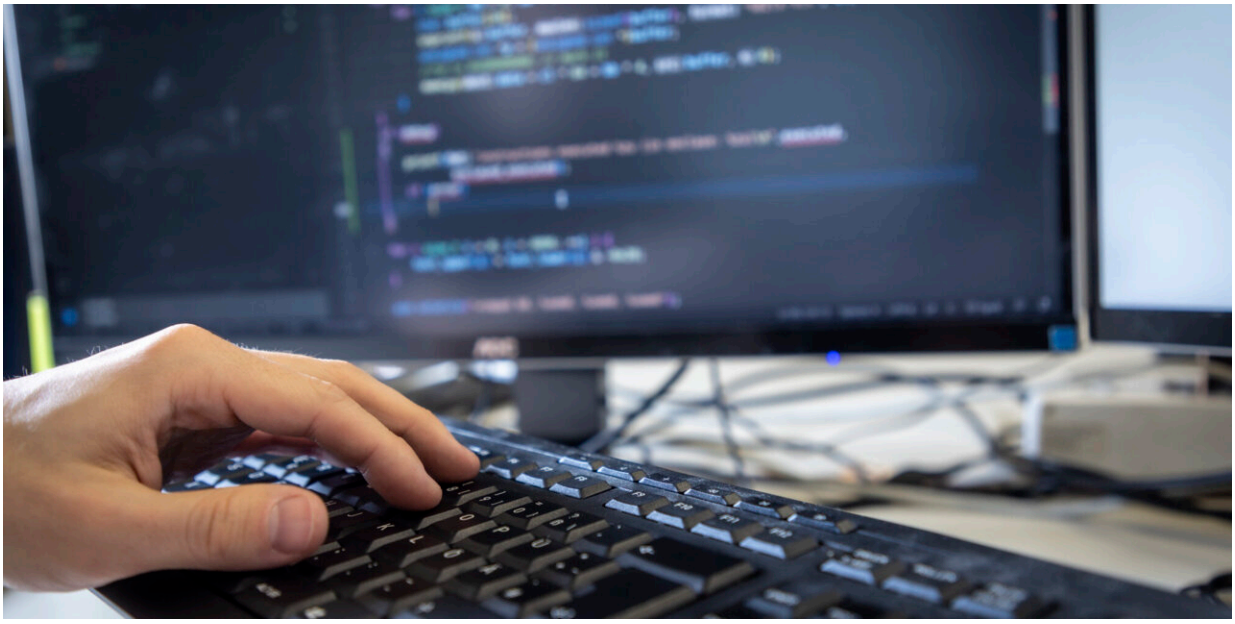
Security vulnerability in browser interface allows computer access via graphics card

April 15 2024



WebGPU opens the possibility for side channel attacks. Credit: Lunghammer - TU Graz

Modern websites place ever greater demands on the computing power of computers. For this reason, web browsers have also had access to the computing capacities of the graphics card (Graphics Processing Unit or GPU) in addition to the CPU of a computer for a number of years.

The scripting language JavaScript can utilize the resources of the GPU

via programming interfaces such as WebGL and the new WebGPU standard. However, this harbors risks. Using a website with malicious JavaScript, researchers from the Institute of Applied Information Processing and Communications at Graz University of Technology (TU Graz) were able to spy on information about data, keystrokes and encryption keys on other people's computers in three different attacks via WebGPU.

An appeal to the browser manufacturers

WebGPU is currently still under active development, but browsers such as Chrome, Chromium, Microsoft Edge and Firefox Nightly versions already support it. Thanks to its greater flexibility and modernized design compared to WebGL, the interface will be widely used in the coming years.

"Our attacks do not require users to interact with a website and they run in a time frame that allows them to be carried out during normal internet surfing. With our work, we want to clearly point out to browser manufacturers that they need to deal with access to the GPU in the same way as with other resources that affect security and privacy," says Lukas Giner from the Institute of Applied Information Processing and Communications at TU Graz.

The research team carried out its attacks on several systems in which different graphics cards from NVIDIA and AMD were installed—the NVIDIA cards used were from the GTX 1000 series and the RTX 2000, 3000 and 4000 series, while the AMD cards used were from the RX 6000 series. The research work and accompanying paper will be presented at the ACM Asia Conference on Computer and Communications Security from 1 to 5 July in Singapore.

For all three types of attack, the researchers used the access to the

computer's cache memory available via WebGPU, which is intended for particularly fast and short-term data access by the CPU and GPU. This side channel provided them with meta-information that allowed them to draw conclusions about security-relevant information.

Changes in the cache as an indicator

The team was able to track changes in the cache by filling it themselves using code in the JavaScript via WebGPU and monitoring when their own data was removed from the cache by input. This made it possible to analyze the keystrokes relatively quickly and accurately.

By segmenting the cache more finely, the researchers were also able to use a second attack to set up their own secret communication channel, in which filled and unfilled cache segments served as zeros and ones and thus as the basis for binary code. They used 1,024 of these cache segments and achieved transfer speeds of up to 10.9 kilobytes per second, which was fast enough to transfer simple information. Attackers can use this channel to extract data that they were able to attain using other attacks in areas of the computer that are disconnected from the internet.

The third attack targeted AES encryption, which is used to encrypt documents, connections and servers. Here, too, they filled up the cache, but with their own AES encryption. The reaction of the cache enabled them to identify the places in the system that are responsible for encryption and access the keys of the attacked system.

"Our AES attack would probably be somewhat more complicated under real-time conditions because many encryptions run in parallel on a GPU," says Roland Czerny from the Institute of Applied Information Processing and Communications at TU Graz.

"Nevertheless, we were able to demonstrate that we can also attack algorithms very precisely. We did of course communicate the findings of our work to the browser manufacturers in advance and we hope that they will take this issue into account in the further development of WebGPU."

More information: Lukas Giner et al, Generic and Automated Drive-by GPU Cache Attacks from the Browser (2024)

Provided by Graz University of Technology

Citation: Security vulnerability in browser interface allows computer access via graphics card (2024, April 15) retrieved 2 May 2024 from https://techxplore.com/news/2024-04-vulnerability-browser-interface-access-graphics.html