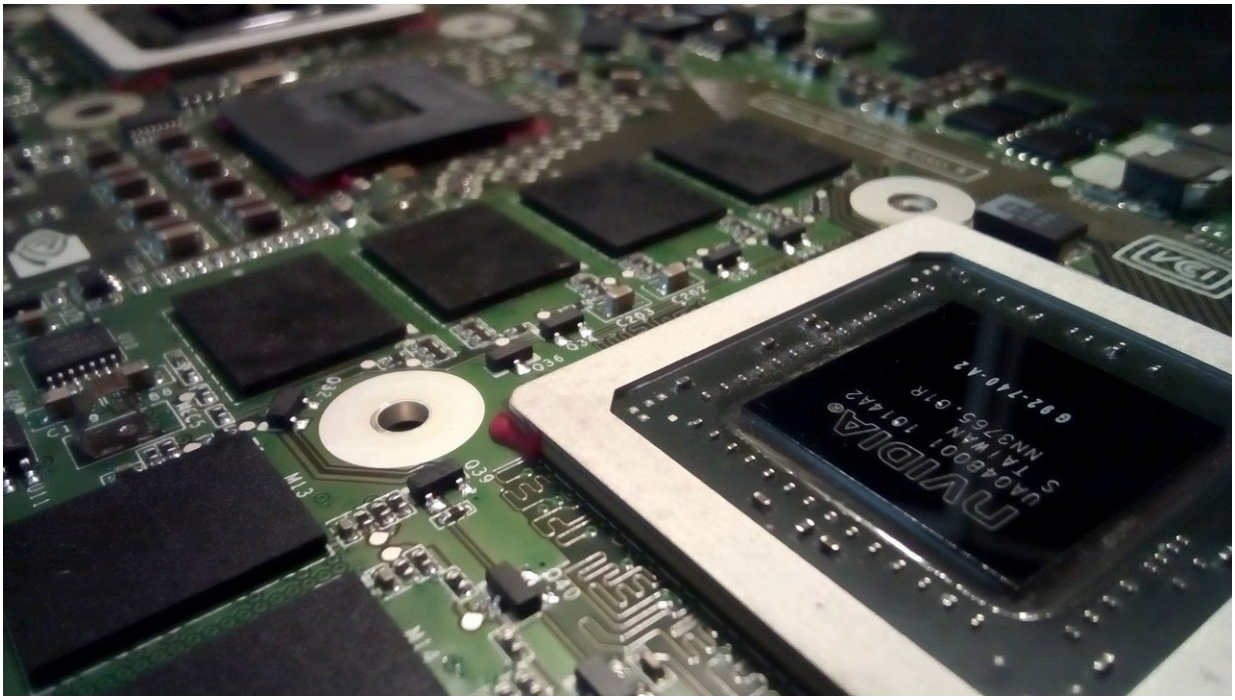
New attacks on graphics processors endanger user privacy

November 5 2018, by Holly Ober



Credit: CC0 Public Domain

Computer scientists at the University of California, Riverside have revealed for the first time how easily attackers can use a computer's graphics processing unit, or GPU, to spy on web activity, steal passwords, and break into cloud-based applications.

Marlan and Rosemary Bourns College of Engineering computer science

doctoral student Hoda Naghibijouybari and post-doctoral researcher Ajaya Neupane, along with Associate Professor Zhiyun Qian and Professor Nael Abu-Ghazaleh, reverse engineered a Nvidia GPU to demonstrate three attacks on both graphics and computational stacks, as well as across them. The group believes these are the first reported general side channel attacks on GPUs.

All three attacks require the victim to first acquire a malicious program embedded in a downloaded app. The program is designed to spy on the victim's computer.

Web browsers use GPUs to render graphics on desktops, laptops, and smart phones. GPUs are also used to accelerate applications on the cloud and data centers. Web graphics can expose user information and activity. Computational workloads enhanced by the GPU include applications with sensitive data or algorithms that might be exposed by the new attacks.

GPUs are usually programmed using application programming interfaces, or APIs, such as OpenGL. OpenGL is accessible by any application on a desktop with user-level privileges, making all attacks practical on a desktop. Since desktop or laptop machines by default come with the graphics libraries and drivers installed, the attack can be implemented easily using graphics APIs.

The first attack tracks user activity on the web. When the victim opens the malicious app, it uses OpenGL to create a spy to infer the behavior of the browser as it uses the GPU. Every website has a unique trace in terms of GPU memory utilization due to the different number of objects and different sizes of objects being rendered. This signal is consistent across loading the same website several times and is unaffected by caching.

The researchers monitored either GPU memory allocations over time or GPU performance counters and fed these features to a machine learning based classifier, achieving website fingerprinting with high accuracy. The spy can reliably obtain all allocation events to see what the user has been doing on the web.

In the second attack, the authors extracted user passwords. Each time the user types a character, the whole password textbox is uploaded to GPU as a texture to be rendered. Monitoring the interval time of consecutive memory allocation events leaked the number of password characters and inter-keystroke timing, well-established techniques for learning passwords.

The third attack targets a computational application in the cloud. The attacker launches a malicious computational workload on the GPU which operates alongside the victim's application. Depending on neural network parameters, the intensity and pattern of contention on the cache, memory and functional units differ over time, creating measurable leakage. The attacker uses machine learning-based classification on performance counter traces to extract the victim's secret neural network structure, such as number of neurons in a specific layer of a deep neural network.

The researchers reported their findings to Nvidia, who responded that they intend to publish a patch that offers system administrators the option to disable access to performance counters from user-level processes. They also shared a draft of the paper with the AMD and Intel security teams to enable them to evaluate their GPUs with respect to such vulnerabilities.

In the future the group plans to test the feasibility of GPU side channel attacks on Android phones.

The paper,"Rendered Insecure: GPU Side Channel Attacks are Practical," was presented at the ACM SIGSAC Conference on Computer and Communications Security October 15-19, 2018, in Toronto, Canada.

Provided by University of California - Riverside