A Study of the Security Vulnerabilities in Consumer Grade GPUs.

Ayomide Owoade, Nathan Ketterlinus, Nick Arellano

Computer and Information Sciences Department

Fischer College of Science & Mathematics, Towson University

{aowoade1, nketter1, narella1} @ students.towson.edu

Project Scope

As the demand for graphical computing power has skyrocketed over time, the amount of consumer-grade electronics with discrete Graphics Processing Units (GPUs) has risen to match this demand. As GPUs become a more integral part of the average person’s devices, it becomes critical that they do not present themselves as a possible attack vector for malicious actors. This paper will examine various vulnerabilities and backdoors that exist in consumer-grade GPUs, and consider various solutions to these vulnerabilities, weighing the pros and cons in an ever-evolving cybersecurity landscape.

Abstract

In recent years, the soaring popularity of graphics processing units (GPUs) has highlighted the necessity to investigate the security challenges they bring. This paper goes into some emerging concerns such as where modern GPUs unintentionally send out sensitive information, enabling real-world attacks. It has been identified as a novel electromagnetic (EM) vulnerability in many GPUs from companies like NVIDIA and AMD. This vulnerability can be exploited in various ways, such as keystroke timing inference attacks and website fingerprinting. The reason for this vulnerability, featured in a lot of GPUs, is dynamic voltage and frequency scaling. In addition, the adoption of the General-Purpose Graphics Processing Unit (GPGPU) has revolutionized artificial intelligence and deep learning by leveraging GPUs’ powerful parallel computing capabilities. With the GPU’s potential computational power, it's important to address these risks and issues. Companies are looking for attacks that can potentially happen and get rid of known vulnerabilities.