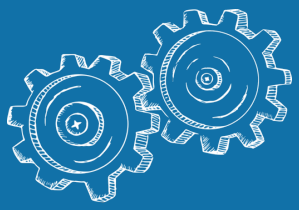

System Security Mechanisms for the Vortex Open-Source GPU

Advisor: **Paul Gollob**

Motivation

GPUs process highly sensitive data such as machine-learning models and user inputs, and are shared between many applications. Still, their hardware security mechanisms are far less studied than those of CPUs. Attacks have shown that GPUs leak data between applications, e.g., through shared on-chip memory, caches, or side channels. As commercial GPUs are closed, such problems are hard to study and fix.

Vortex is an open-source, RISC-V based GPU written in SystemVerilog that runs OpenCL programs in simulation and on FPGAs. This makes it an ideal platform for GPU security research at the **RTL level**.

In this master project or thesis, you will analyze Vortex for security weaknesses and develop hardware security mechanisms, e.g., isolation of memory and on-chip resources between kernels, clearing of state on context switches, or memory-safety checks.

Goals and Tasks

- Get familiar with GPU architecture, the SIMT execution model, and the Vortex RTL and toolchain.
- Analyze Vortex for isolation and leakage issues (e.g., shared memory, caches, scheduling).
- Implement selected security mechanisms in the Vortex RTL and the software stack.
- Evaluate your design in simulation and on FPGA in terms of security, performance, and area.

Literature

- B. Tine et al.
  Vortex: Open-Source RISC-V GPU
  MICRO 2021
  https://github.com/vortexgpgpu/vortex
- H. Naghibijouybari et al.
  Rendered Insecure: GPU Side Channel Attacks are Practical
  CCS 2018
  https : / / doi . org / 10 . 1145 / 3243734 . 3243831

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Computer architecture, SystemVerilog
- C/C++, ideally OpenCL/CUDA

Advisor Contact

paul.gollob@tugraz.at