Artifact Evaluation (AE) abstracts

Joe Loughry
Netoir
joe@netoir.com

Kasper Rasmussen
University of Oxford
kasper.rasmussen@cs.ox.ac.uk

1 Git repository

This is a `git` repository of source code used to collect and analyze data from experiments in the paper. It works with the hardware shown in Figures 5–6 and 13–14 of the paper. Figure 5 is a schematic of the hardware, consisting of a pair of stepper-motor–driven linear positioners configured for *x*–*y* motion to raster scan a focused laser over the target area, approximately 1–25 mm^2.

Two runs of experiments were done on LEDs and ESD protection diodes at 405, 532, 650, 780, 808, and 980 nm on a variety of 5 mm visible LEDs and glass enclosed small signal diodes of the type used for ESD protection of I^2C bus connections on printed boards. C++ source code for the Arduino microcontroller that controls stepper motors and ADC is in https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/LEDs/code/Arduino for LEDs and https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/diodes/code/Arduino for ESD protection devices.

Transcripts of the output of these programs are in https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/LEDs/data/raw_data and https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/diodes/data/raw_data, respectively.

Gnuplot scripts to extract and plot the data are in https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/LEDs/code/gnuplot and https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/diodes/code/gnuplot, respectively; in addition, R code for statistical analysis of the effect of elliptical beam axis rotation is in https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/diodes/code/R/beam_rotation.r. C++ source files are intended to be used with the Arduino IDE, available from https://www.arduino.cc/en/software. Gnuplot scripts are provided with a `plot_all_data.sh` shell script in lieu of a `Makefile`.

2 M5 CPU

M5, shown in Figures 13–14 of the paper, is a minimalist CPU intended not so much to show the practicality of the attack against real hardware (Lattice Semiconductor iCE40-HX8K FPGA evaluation board) but rather to highlight certain difficulties of the attack, beyond the obvious ones like aiming and focusing. Note: a schematic of M5 will be included in the final paper, an oversight noted by the reviewers.

This is a 4-bit computer with an accumulator that is visible on the front panel. (Visibility is key to establishing a phase lock on the internal state of the CPU.)

It has a very simple instruction set to make feasible the reachability analysis in Figure 15. The particular FPGA chosen is not significant except that most FPGA development tools are proprietary, closed source, and expensive; in contrast, a completely open source toolchain—Project IceStorm—exists for the Lattice iCE40. Every step in the process is visible, down to a plain text file containing an array of ones and zeros that is what is actually uploaded into the interconnection fabric of the FPGA. This is an unprecedented level of transparency, and is sorely lacking for other FPGA vendors.

> Project IceStorm: https://clifford.at/icestorm.

`Makefile`s are provided to build and install the software. Project IceStorm was successfully run on both macOS 14.4.1 and Ubuntu 20.04.

Physically the unit is a 1U rackmount enclosure that can sit on a table. The attacker is a separate 1U height rackmount box. Both devices are USB powered.

3 Experimental apparatus

The apparatus shown below (Figures 1–2) is an improved version of the one shown in Figure 16 of the paper. It was designed for attacking a live I^2C bus and comprises several

devices on the bus (addressable alphanumeric displays and a nonvolatile memory chip) with a microcontroller and ESD protection for the bus.

The display scrolls “NORMAL OPERATION” every few seconds. The attacker is in one corner of the apparatus; when a button on the attacker is pressed, the display changes to read “PROOF OF CONCEPT”.

Vernier adjustments are for aiming the lasers. The apparatus is 250×350 mm and about 3 kg. It runs on internal batteries. Snapshots of the C++ source code for the attacker and the target are available at https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/I2C/.

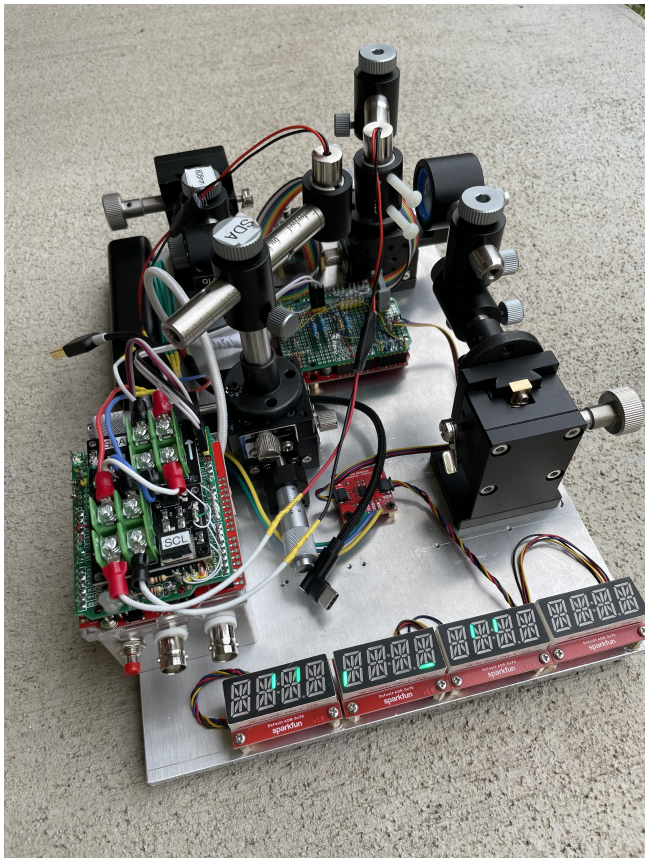

Figure 1: Experimental apparatus used in I^2C bus attack.

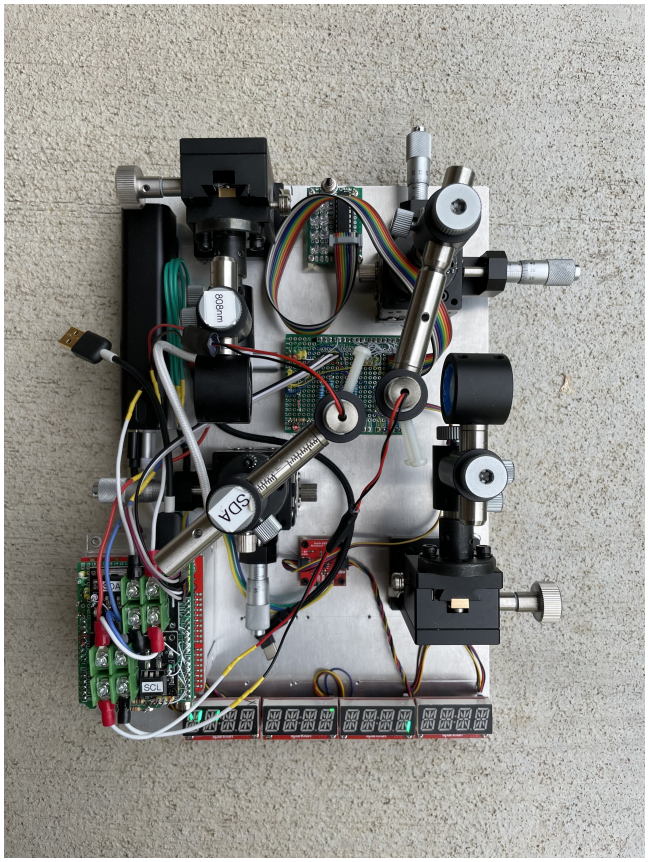

Figure 2: Top view.