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. The first piece of hardware consists of a pair of stepper-motor–driven linear actuators configured for x–y motion to raster scan a focused laser over the target area, approximately 1 mm^2–25 mm^2 depending on whether the target is an ESD protection diode or LED.

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 circuit boards. C++ source code for the Arduino microcontroller that controls the stepper motors—measuring the SDA bus voltage (0–3.3 volt) with the Arduino's analog-to-digital converter (ADC) at each point in the raster scan, and writing it to a file—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`.

Figure 1: M5 CPU

2 M5 CPU

M5, shown in Figure 1, 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 unique 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 of the paper. 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 pro-

cess 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.

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. Verilog source code for the CPU is available at https://github.com/jloughry/basilisk_artifacts/blob/main/experiments/M5/code/Verilog and C++ source code for the attacker is available at https://github.com/jloughry/basilisk_artifacts/tree/main/experiments/M5/code/Arduino.

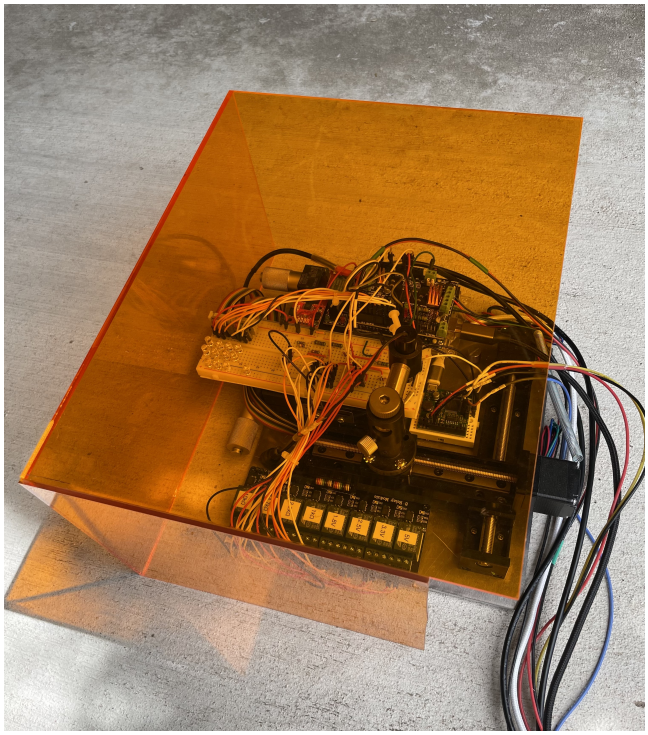

Figure 2: Raster scan apparatus used in experiments. This photo will replace the one in the final paper, as it shows the safety shield. A schematic of this device is Figure 5 of the paper.

2.1 Lasers

The lasers used in this experiment were 405 nm near-UV diode laser modules of unknown power rating that were extracted from "cat toys" sold on Amazon.com at https://www.amazon.com/gp/product/B09Y4D7NFB/. In operation, they draw approximately 150 mA each from a 3.3 V supply, so their optical power must be < 500 mW and is probably considerably less, as they get warm in continuous operation. *These are absolutely not eye-safe and should never have been sold as cat toys.*

For safety when using 405 nm lasers, we recommend an enclosure made from #2422 transparent orange polycarbonate sheet 3 mm thick, as shown in Figure 2.

The lasers are modulated by switching their power supply on and off with a MOSFET. Two important considerations apply to these lasers; firstly, they need 3.3 V and will burn out quickly at 5 V, but the MOSFETs won't switch a load less than their gate (control) voltage. So to make the MOSFETs work and avoid burning out the lasers, always switch 5 V through the MOSFET, and drop it down to 3.3 V with an LM317 voltage regulator between the MOSFET and the laser. The MOSFET modules used are available from Amazon.com: https://www.amazon.com/dp/B07F5JPXYS and the voltage regulators at https://www.amazon.com/gp/product/B08CDMZMDN/.

These lasers were chosen for use because they exhibit quick response when modulated in this way, typically $< 100\,\mu$s turn-on and turn-off latency. Many other laser modules from other sources, when measured, had a turn-on latency of more than 4000 µs, limiting modulation to < 0.25 kHz.

3 I^{2}C experimental apparatus

The apparatus shown in Figures 3 and 4 below is an improved version of the one shown in Figure 16 of the paper, and will replace that photo in the final paper. It was designed for attacking a live I^{2}C bus and comprises several devices on the bus—addressable alphanumeric displays and a nonvolatile memory chip—together with a microcontroller and ESD protection for the bus.

The target of the attack is a pair of 1N34A glass-enclosed small signal diodes commonly used for electrostatic discharge (ESD) protection for an I^{2}C bus.[1]

These are mounted—for accessibility—on a mezzanine board plugged into the top of an Arduino Uno microcontroller (actually, a SparkFun clone with USB-C) in the center of the baseplate. The same mezzanine board holds the 10 kΩ pull-up resistors for the I^{2}C bus, and an isolated photodiode amplifier circuit used separately for speed tests on the lasers. The Arduino here is really only used for two minor purposes: it sends out commands on the I^{2}C bus every few minutes to display the words 'NORMAL OPERATION', and it also measures the voltage on the bus with its internal ADC, drawing a bargraph on some off-board LEDs (connected to GPIO pins) for help with aiming. There is also a tiny pushbutton on the bargraph board (at the end of the rainbow ribbon cable) to reset the target so it refreshes the display.

[1] Actually, these are modern Schottky equivalents of the original germanium component, but they work the same.

Other devices on the I^{2}C bus, available for attacking, include an array of quad alphanumeric displays at address 0x70–0x73, and a nonvolatile memory chip at address 0x50.

The baseplate is 6 mm aluminum plate, drilled and tapped for mounting holes. The attacker is another Arduino Uno in the lower left corner of the baseplate; atop the attacker is another mezzanine board holding the MOSFETs used to modulate the lasers, and a red/green LED to indicate when the attacker is ready, and whenever the lasers are firing.

Below the attacker there is a pushbutton to start the attack, and a pair of BNC jacks for convenient access to connect and oscilloscope for measuring the I^{2}C bus, although these are not connected to the attacker in any way, except mechanically.

When the button on the attacker is pressed, it fires the lasers as fast as it can to impress a signal on the I^{2}C bus, attempting to write the words 'PROOF OF CONCEPT' on the display. The lasers, in this case, are 780 nm near-infrared, because that is a good wavelength for ESD protection diodes. It has to do this blindly, as it has no feedback from the I^{2}C bus, so for example it can't detect a collision, nor can it read data back from the memory chip. But the time needed to write a complete message to the alphanumeric display is around 10 ms, so there is a very small time window for collisions to occur.

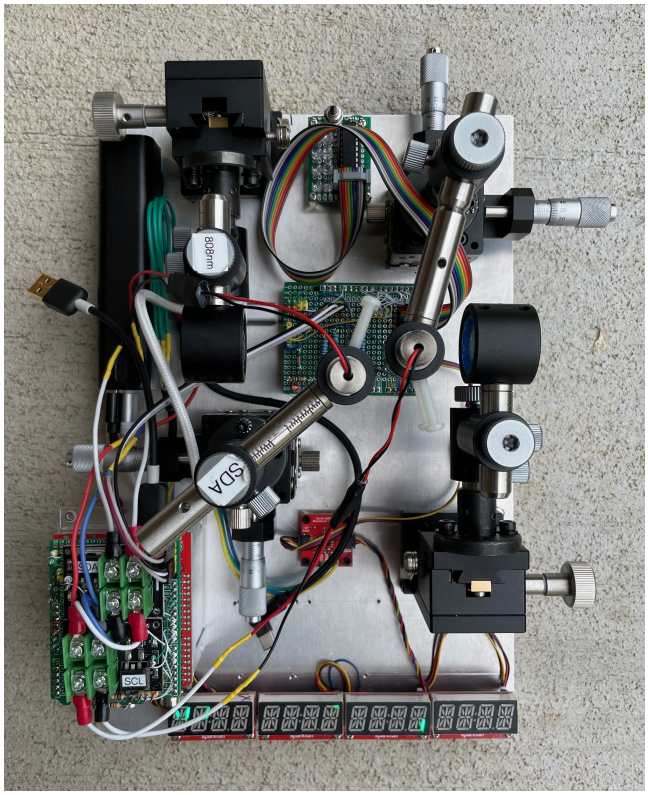

Figure 3: Experimental apparatus used to demonstrate I^{2}C bus attack.

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/.

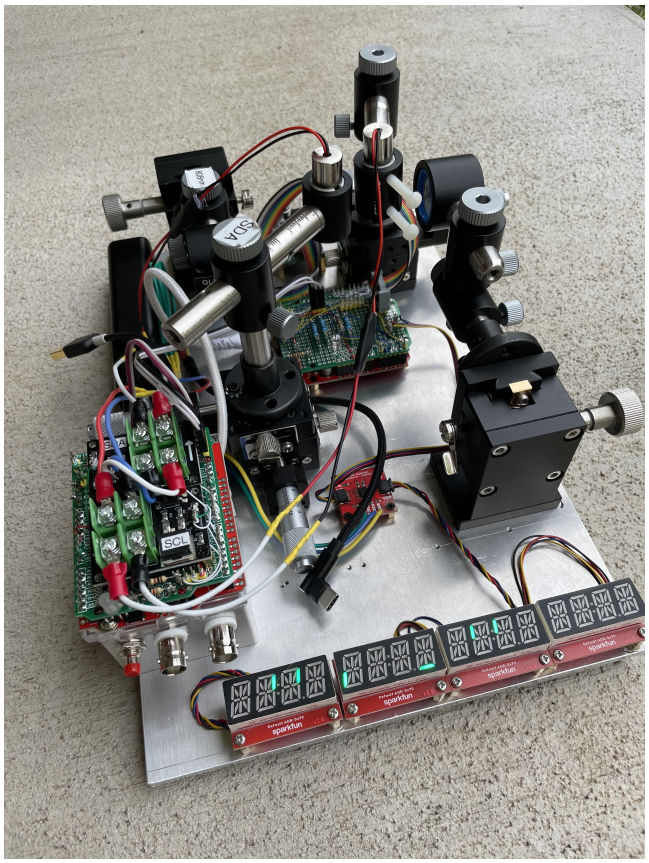

Figure 4: Oblique view.

3.1 Mechanical

Vernier adjustments are provided for aiming the lasers. Each vernier comprises a 40×40 mm x–y linear actuator (ThorLabs LX-20 or equivalent) bolted to the baseplate, onto which is bolted a Quarton model QLM-1125 polar laser mount. The polar axis of the mount provides easy coarse positioning for aiming, with the linear actuator providing fine positioning.

For precise focus, a second Quarton model QLM-1125 laser mount is paired with pieces of a Quarton model QLM-1225 to make a double-jointed polar axis mount, bolted atop a z-axis linear actuator (rack-and-pinion). The polar mount holds a 20 mm doublet converging lens with a focal length of around 25 mm. This arrangement allows the laser modules' internal lenses to be fixed at infinity.

3.2 Portability

The apparatus is 250×350 mm and about 3 kg. It runs on internal USB batteries.