NIST LWC Side-Channel Security Evaluation Lab

Laboratory for Safe and Secure Systems, OTH Regensburg, Germany

February 25, 2022

1 Introduction

We would like to commit to hosting a basic side-channel security evaluation lab for NIST LWC ciphers. In the past, we already engaged in the NIST LWC project regarding benchmarking and evaluating software implementations on various mircocontroller plattforms (see https://lwc.las3.de). Therefore we will focus on the side-channel leakage assessment of protected software implementations on a subset of our evalualtion boards (details below). We can enable developers to submit protected implementations via our web interface, which will then be directly fed to the evaluation framework. We plan to provide a similar workflow as with our performance benchmarking setup. Moreover, we would like to make our captured traces available to the public in order to support result validation and further analysis by other researchers.

2 Equipment

1. Oscilloscope
   - (a) PicoScope 6403E: 4 channels, 300MHz bandwidth, 5GS/s max. sampling rate, 8 bit resolution
   - (b) TA436 P2036 300MHz 10:1 passive probes
2. Software
   - (a) Python scripts for controlling the Hardware (triggering) and data collection
   - (b) Jlsca for advanced side-channel analysis (https://github.com/Riscure/Jlsca)
3. Evaluation Platforms

   We list the five platforms here, that we also use in the standard benchmarking setup. We will be able to support **two** of them due to hardware limitations of the oscilloscope. While we believe the AVR and Cortex-M3 chips are the most relevant for software LWC, we can also shift e.g. to the RISC-V MCU in order to avoid offering the exact same platforms as other evaluation teams.
   - (a) Microchip AVR ATmega328P, 8 bit, 16MHz clock frequency, 32KB flash memory
   - (b) ARM Cortex-M3, 32 bit, 72MHz clock frequency, 64KB flash memory
   - (c) RISC-V GD32VF103CBT6, 32 bit, 108MHz clock frequency, 32KB flash memory
   - (d) ARM Cortex-M7, 32 bit, 216MHz clock frequency, 1MB flash memory
   - (e) Tensilica Xtensa LX6 (dual-core), 32 bit, 240MHz clock frequency, 4MB flash memory

3 Services and Tests

1. TVLA (Test Vector Leakage Assessment), Welch's t-test (fixed vs. random)
2. Automated submission system for new implementations
3. Result feedback for developers/submitters
4. Publication of raw trace data once measuring is completed
5. Generation of TVLA graphs for result illustration

4 Team

The project will be technically led by Sebastian Renner and Enrico Pozzobon. Both have experience in setting up evaluation frameworks for embedded systems. This includes measuring setups on evaluation boards, as well as (automated) side-channel and fault injection test benches for electronic control units. Besides their interest in applied cryptograhy, Sebastian and Enrico focus on penetration testing and the design of embedded systems in critical infrastructures. The scientific lead of the project will be taken by Jürgen Mottok, professor for safe and secure systems of systems at the Laboratory for Safe and Secure Systems at the OTH Regensburg.

5 Period of Lab Operation

We intend to operate the lab until the end of 2022.

6 Contact Information

Sebastian Renner and Enrico Pozzobon
Laboratory for Safe and Secure Systems
OTH Regensburg
https://lwc.las3.de
lwc@las3.de