NTNU | Norwegian University of Science and Technology

LAB INTRODUCTION

TTM4205

Caroline Sandsbråten

26.09.2025

Contents

Contents

What's ChipWhisperer

- Open source platform for learning about side channel attacks on embedded devices and hardware security research.
- Makes validating side channel resistance easier.
- Designed specifically for side channel analysis (SCA) and fault injection (FI).

Why ChipWhisperer

- Affordable.
- SCA and FI in one platform.
- Accessible for beginners and experts alike.
- No need for an advanced research lab with expensive equipment

Main Features

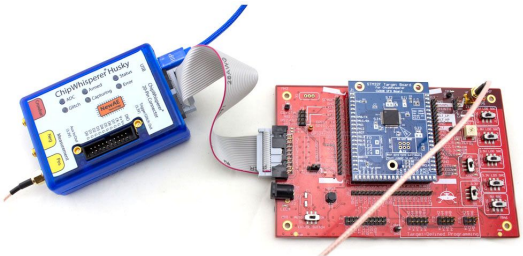
- Captures power consumption or EM traces from microcontrollers.
- Performs differential power analysis (DPA) and correlation power analysis (CPA).
- Supports clock/voltage glitching to induce faults.
- Integrates with Python and Jupyter notebooks for experiments.

How is it Used?

1. Load cryptographic firmware onto a target device.
2. Capture side channel signals during cryptographic operations.
3. Analyze traces to extract secret keys or detect vulnerabilities.
4. Test countermeasures against SCA and FI attacks.

ChipWhisperer Hardware

- **Two main parts:**
- Scope board - Used to mount side channel attacks.
- Target board - Used as the device under test.



Firmware

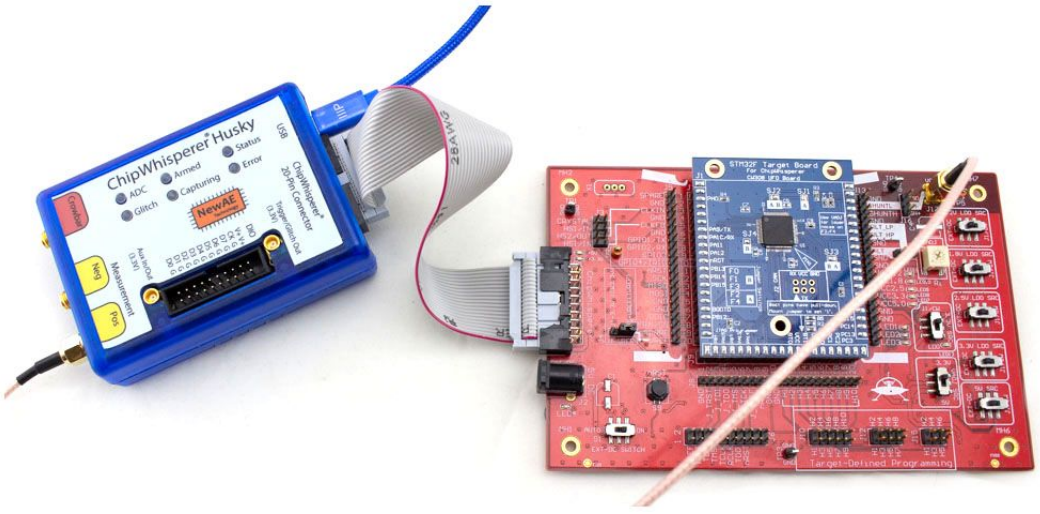
- Scope board firmware is not something we will look at in this course, but the FPGA board and USB microcontroller Verilog and C code can be found on Github for those that are interested.
- Target board firmware written in C will be analysed and potentially modified by you. This is the code that controlls what the target board does and what you measure when mounting side channel attacks.

Software

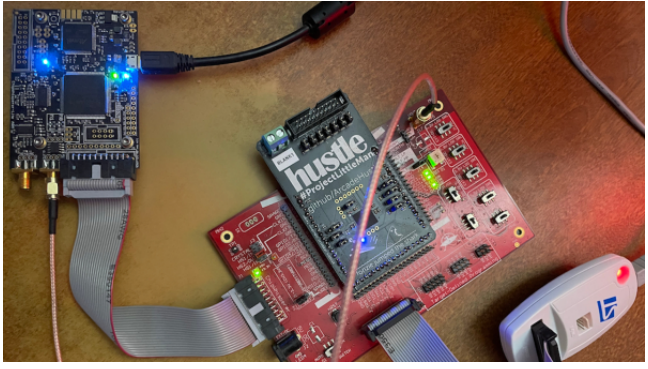
- Newae have made an open source python library for controlling capture hardware and communicating with the target board. This is the main bulk of the code we will be interacting with.

Contents

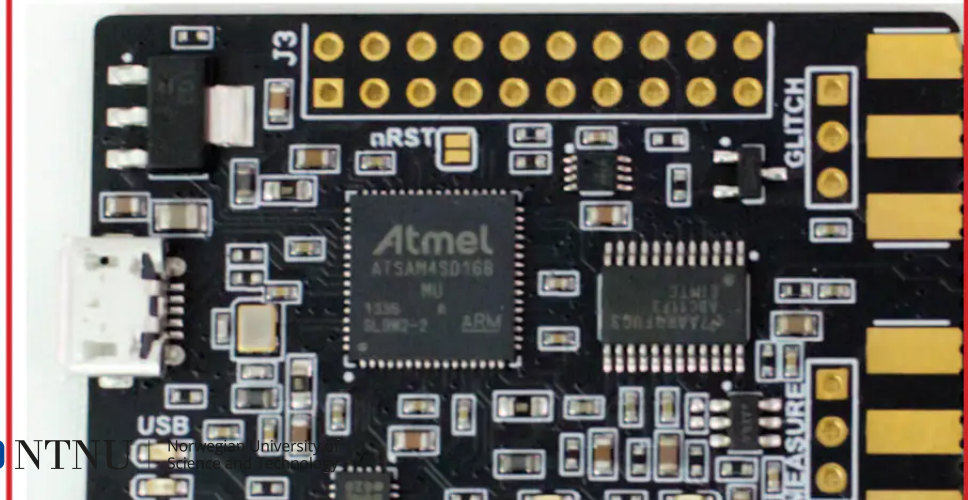
CW Husky


ChipWhisperer Husky
USB
Status
Armed
Error
ADC
Capturing
Glitch
NewAE
ChipWhisperer 20-Pin Connector
Trigger/Glitch Out (3.3V)
Aux/Out (3.3V)
Meas
Measurement
Vpin
STM32F Target Board
For ChipWhisperer
CW308 UFO Board
Target-Defined Programming

CW Lite



CW Nano



Contents

Introduction

- There are 3 different ways to install the required software to run ChipWHisperer on your computer.
- “Vanilla” installation downloading everything manually and optionally running a python virtual environment.
- Using the ChipWhisperer installer (Windows only).
- Virtual machine installation (Recommended).

Prerequisites

- Nice to have: Python version manager (pyenv OR anaconda).
- Compilers and other packages
- Git

Newae Installation Guide

The newae installation guides can be found here:

- Windows
- Linux
- MacOS

If following these guides, make sure to use the course repository for the lab instead of the newae ChipWhisperer repository. This repository contains all the required files to run the lab, including target board firmware.

Vagrant Virtual Image Config

The repository for our vagrant config can be found here:
git.ntnu.no/ie-iik/chipwhisperer-v6-vagrant

Questions?

Let’s install ChipWisperer together!