Fault Injection & Side Channel Analysis

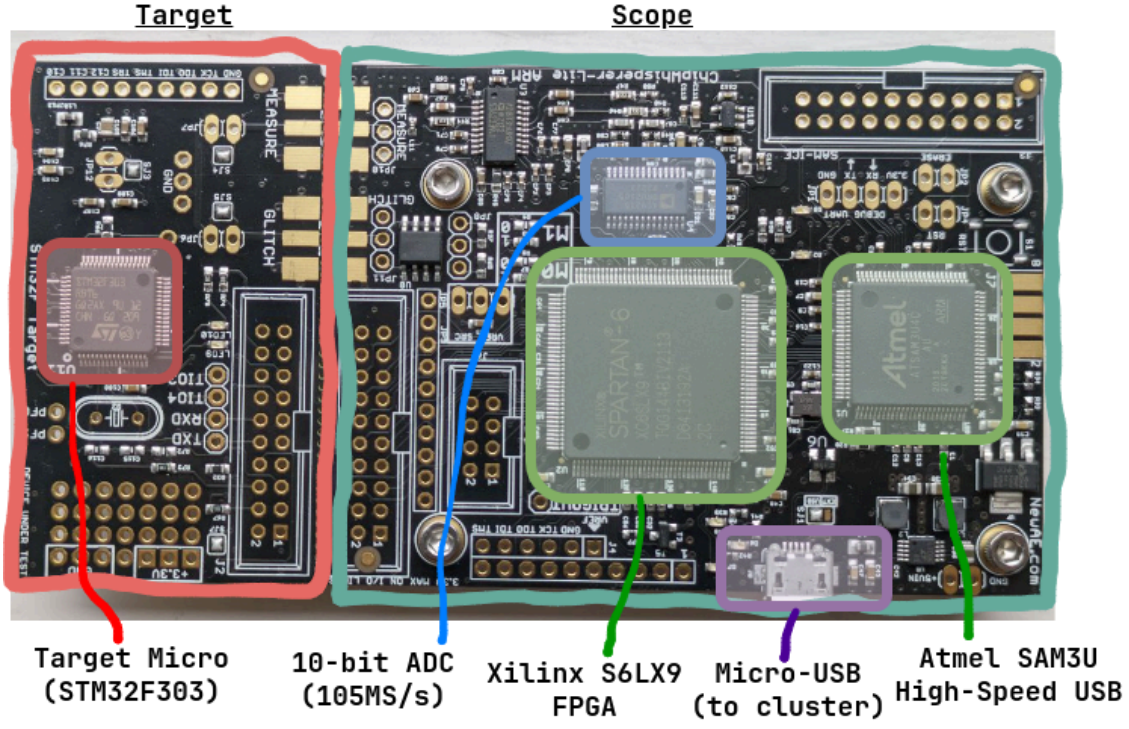
Hardware Security 2025

Overall Goal

In this project you will get practical hands-on experience on power side channel analysis and fault injection attacks. Your main goal is to learn our precious cryptographic secret, stored in some special firmware created for this course! In the first week, you will try to extract this (protected) cryptography key via a power side channel, i.e. just by observing the power consumption of the victim device. In the second and third week, you will use a fault injection primitive to bypass the ReaDout Protection (RDP) to obtain arbitrary code execution and leak the secret key with a memory dump.

Background: ChipWhisperer

"ChipWhisperer is an open source toolchain dedicated to hardware security research." – https://github.com/newaetech/chipwhisperer



For this project, each group will be assigned a **ChipWhisperer-Lite board**, reachable from the cluster. These boards contain:

- A **target** part (right), which in our case includes an STM32F303 microcontroller (ARM Cortex-M4 core) – schematic (end of page)
- A **scope** part (left)that contains circuitry to perform power SCA, voltage FI and clock glitching, among others - schematic (end of page)

Logistics

The ChipWhisperer (CW) boards are available for you on node hwsec-cw in the HS cluster. Each group (max. 2 people) will get their own ChipWhisperer. After we confirm the allocation of a group to this project, please send an email with both members in CC containing:

- The name of the group
- The name and student ID of each member

Once all the users are added to the cluster, you will receive the SSH configuration to access hwsec-cw and the serial number of your assigned CW. Differently from the other hwsec nodes, **you do not need** to reserve this machine via the nodeman application: you can use it as much as you need. The toolchain is already installed.

> Even if you are co-located with other users on the same machine, we expect you to work on your own assignment and not exhaust the resources of the machine. In case any student is actively interfering with other students' work, we will apply penalties and kick them out of the server.

Attack Scenario

The Company LameCorp© has just released their new authentication dongle LameDongle™ claiming that it is unhackable. It uses military grade encryption[1] (DES) with **ReaDout Protection (RDP)** making the firmware unreadable, and thus the stored secret key. On top of this, LameDevices© claims that the DES implementation is time-constant so any timing side channel attack cannot work.

Since you took HWSec you know that all these claims are garbage and you want to prove it! Your view of the system is completely black-box and you just know

[1] DES is definitely no more “military grade encryption”. We decided to use DES to make your life a bit harder, but this attack works perfectly fine on AES.

that it is implementing DES encryption in software with a constant time implementation.
By reading the product manual you notice that the authentication protocol is defined as follow:

1. The authenticator system sends a random 8 byte challenge to the LameDongle™ via UART.
2. The LameDongle™ will encrypt the challenge using the secret key stored in the device.
3. The ciphertext is then sent back to the authenticator system via UART. If the system confirms that the ciphertext is the expected one, authentication will be granted.

After reading this you noticed that this a perfect attack scenario for Power Side-Channel Analysis attacks! You can grab your oscilloscope and measure the power consumption of the LameDongle™ performing multiple encryptions to extract the key!

On top of this you know that protecting secret data in the firmware just with ReaDout Protection may be not sufficient when you can do Fault Injection! In week 2 and 3 you'll obtain the secret DES key by means of FI, which skips completely the annoying math behind SCA.