# Hermes – Side-Channel Attacks on Hardware Wallets

**Summer 2022**

## Can we craft new exploits against known hardware wallet implementations?

## Team Members

Clay Carper
3rd year PHD student in Computer Science. Studies side-channel attacks.

Melanie Griffith
Senior Majoring in Computer Engineering

## Problem Statement

In order to explore vulnerabilities using EMFI attacks certain hardware aspects must be integrated into the target board. The main problem to be solved was how to drive a seven segmented display and two buttons using the target board. Once that step was completed, the question became how to add a pin checking functionality using the buttons and segmented display.

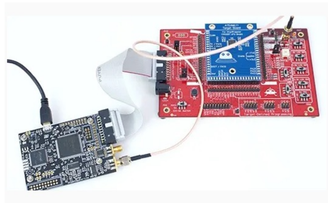

Figure 1: Target board and ChipWhisperer

## Results

Over the course of the summer most of the desired goals were reached. A program to drive and control two buttons and a seven segmented display was written. The program was then successfully transferred to the target board using a JTAG device. The pin checking functionality is currently struggling with having two buttons pressed at the same time. This action is being used as an enter pin button.

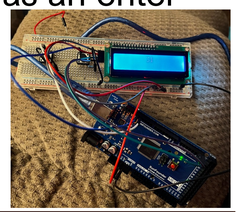

Figure 5: Pin Check set up using the SunFounder Mega board

## Background

Hardware wallets that are based on the STM32F3 architecture are known to be susceptible to electromagnetic fault injection (EMFI) attacks. Since cryptographic recovery phrases are dumped directly from flash, understanding known vulnerabilities is becoming increasingly important. This project uses a STM32F303 target board and a ChipWhisperer Lite to explore these exploits. The ChipWhisperer is a device that performs high-speed power measurements to explore side channel analysis.

## Methods

Due to the poor documentation of the target board, it became easier to try to integrate the hardware aspects on other microcontrollers first. Then, use the same logic to drive the hardware to the target board using a JTAG device. The other microcontrollers used for testing include the Arduino Mega and the STM32F3Discovery boards.

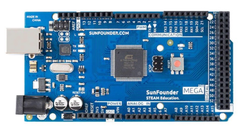

Figure 2: Arduino Mega

Figure 3: STM32F3Discovery

Figure 4: ST-LINK/V2-ISOL (JTAG)

## Challenges & Future Work

Short term challenges and future work for this project include:

- Figuring out how to read a simultaneous button push on the Arduino Mega board
- Transferring that logic and building the same program on the STM32F3Discovery Board.
- Debugging how the seven segmented display is interacting with the STM32F3 architecture.


**Advisor**: Dr. Mike Borowczak (mike.borowczak@uwyo.edu)
**Grad Mentors:**
- Clay Carper (ccarper2@uwyo.edu)

**Group Members**:
- Melanie Griffith (mgriff25@uwyo.edu)



**Figure 1: https://www.newae.com/chipwhisperer**
**Figure 2: https://www.sunfounder.com/products/arduino-mega2560-board**
**Figure 3: https://www.waveshare.com/stm32f3discovery.htm**
**Figure 4: https://www.win-source.net/products/detail/stmicroelectronics/st-link-v2-isol.html**
**Figure 5: Courtesy of Melanie Griffith**


University of Wyoming

CEDAR
Cybersecurity Education And Research Center