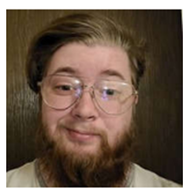
Hermes – Locating a Target Chip Using Digital Controls 2022 - 2023

Automated framework for iterative electromagnetic fault injection attacks (?)

Team Members

Melanie Griffith
Senior Majoring in
Computer Engineering

Caylie Charlton
Senior Majoring in
Computer Engineering



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

Problem Statement

- The purpose of this project is to modify the ChipWhisperer to make the system more efficient and safer by adding a set of digital controls for the XYZ-bed and to add a wireless aspect to that control system.

- Currently the controls are not user friendly and have the possibility to break the target device. Creating an easy-to-use control system that has software locks to prevent the CNC router from running through the board or causing other damage.

Methods

In order to create the set of digital controls the following steps must be completed.

- User inputs the X and Y-dimensions.
- Send user data to XYZ-bed.
- Check to see if the dimensions will cause harm to the board. If not, then ask user for new dimensions.
- Execute the movement sequence.
- Verify that the target board has been found.
- Initiate connection between RaspberryPi and PyWhisperer and trigger and EMFI attack using the ChipSHOUTER

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.

Figure 1: EMFI attack on a STM32 Discovery Board

Current Setup

For this project, a XYZ-bed, ChipSHOUTER, and ChipWhisperer are currently being used to do the EMFI attack. The ChipSHOUTER provides the electromagnetic pulse while the ChipWhisperer measures and analyzes the power output from the pulse. The current setup uses manual controls for the XYZ-bed and the researcher must line up the injection tip to the board using only their eyes.

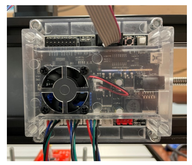


Figure 2: ChipWhisperer

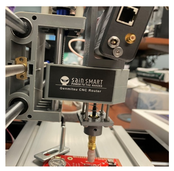


Figure 3:CNC router

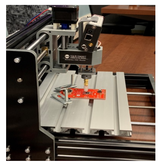


Figure 4: XYZ Bed

Future Work

Future Work for this project includes:

- Selecting a microprocessor to interface with the ChipWhisperer (currently leaning towards the Raspberry Pi).
- Research needed hardware materials (camera, distance sensors, control platform).
- Research software for digital controls of XYZ-bed.
- Manufacture a substitute EMFI component for testing (3D print a holder for laser pointer).
- Design a testing validation process.

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

Group Members:
- Melanie Griffith (mgriff25@uwyo.edu)
- Caylie Charlton (ccharlt1@uwyo.edu)

Figure 1: https://eprint.iacr.org/2022/301.pdf
Figure 2: Courtesy of Melanie Griffith
Figure 3: Courtesy of Melanie Griffith
Figure 4: Courtesy of Melanie Griffith