DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING  
COLLEGE OF ENGINEERING AND APPLIED SCIENCE  

RESEARCH OPPORTUNITIES FOR UNDERGRADUATE students  
APPLICATION DEADLINE: 10/01/2023  

PROJECT TITLE: Secure Coding against Hardware Attacks  

Physical Requirement: No physical requirement  
Project's Technical Skills Requirement: cybersecurity, binary analysis, assembly, reverse engineering  
Project's Available Positions: 1  

Boyang Wang  
Department of Electrical and Computer Engineering  
Rhodes 806A  
boyang.wang@uc.edu  
https://homepages.uc.edu/~wang2ba/index.html  

Project Description  

A fault injection attack (also referred to as glitch attack) is a physical attack on data and behavior of an embedded device by changing the voltage, temperature or electromagnetic radiation. For example, it takes one fault to change a Boolean value from 0 to 1 (or 1 to 0) to bypass secure boot, extract a secret key, or extract firmware from an embedded device. To mitigate fault injection attacks, one effective way at the software layer is to write secure code that is more robust against the attacks. For instance, Boolean values in an if statement (e.g., if (flag == 0)) can be easily modified by fault injection attacks while using non-trivial numerical values (e.g., if (flag == 0x3CA5)) can make the attacks more difficult.  

The goal of this project is to develop an automatic method to detect lines in C, assembly, or even binary, that are vulnerable under fault injection attacks. The students will (1) study secure code patterns; (2) leverage and extend existing tools that our research group has developed to automatically identify vulnerabilities at different levels. Students with background in binary analysis and reverse engineering are strongly encouraged to apply.