HACE Lab: An Online Hardware Security Attack and Countermeasure Evaluation Lab

PIs: Fareena Saqib, Dr. Mark Tehranipoor, Dr. Swarup Bhunia
Affiliations: Florida Institute of Technology and University of Florida
https://www.nsf.gov/awardsearch/showAward?AWD_ID=1623299&HistoricalAwards=false

Introduction

Educational activities lack in advanced state-of-the-art laboratory to help students to implement many of the learnt hardware security primitives, attacks, and countermeasures, obtain results, and analyze the results in a systematic manner.

Furthermore, given the very expensive set of instruments a hardware security lab may require to perform widely varying hardware security experiments (from Trojan attacks to reverse engineering), many of the colleges and universities cannot afford establishing them in their institutions. Multiple levels of electronic hardware (chips, circuit boards, and systems), which are subject to different attack modes and protection mechanisms, adds to the difficulty in creating such a lab that provides comprehensive coverage of hardware security.

The goal of this project is to establish a set of hardware security implementation and experimentation modules and enable adoption of this lab course at other institutions through the development of an On-Line Hardware Security Attack and Countermeasure Evaluation (HACE) Lab.

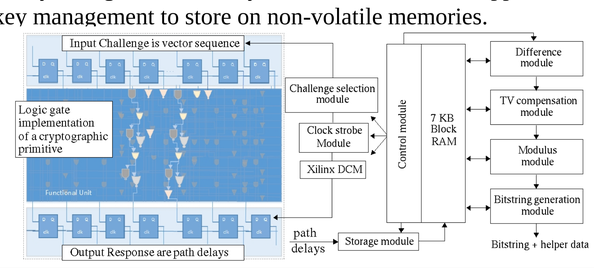
Approach

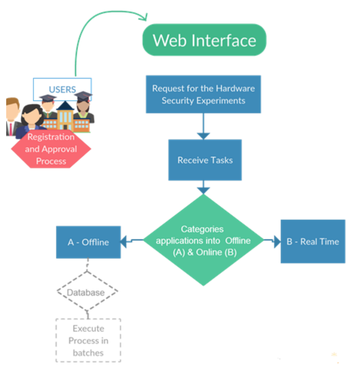
Focus of the project is to encourage adoption of a curriculum aimed at training students with skills in various aspects of hardware security and trust including trustable hardware, counterfeit detection, security primitives, side-channel attacks and countermeasures, reverse engineering, etc. This provides a solid base for interesting student projects with significant opportunities for innovation and plurality of project paths. Given the rapid growth of the hardware security community, lack of such lab is much felt and essentially needed.

Many of the projects can be done with an oscilloscope and a logic analyzer for hardware debugging and system level reverse engineering. Some other experiments can be done on low-cost FPGA boards. We expect that many educational institutions will be able to adopt this material in their own courses using existing lab equipment. However, advanced and complex labs requiring expensive instruments made available, through HACE to many institutions via low-cost fee based system, allows students to use these systems remotely to run their tests. An interface is setup by the HACE team to approve the requests to use the systems remotely.

Online Lab for Physical Unclonable Function PUF and True Random Number Generator TRNG

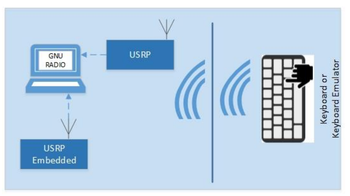
- Physical unclonable functions (PUFs) are embedded structures that utilize process variations such as wire and transistor variations to produce random but reproducible bit strings.
- PUF keys are generated on fly rather than traditional approach of key management to store on non-volatile memories.

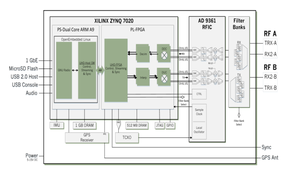


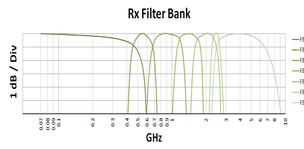


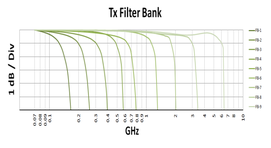
Keyboard Logging using USRP

- The electromagnetic waves generated by keyboard are being intercepted by USRP (Universal Software Radio Peripheral).
- This experiments uses E310 USRP model
- E310 has bandwidth of 56 Mhz and frequency range from 70 Mhz to 6 Ghz.
- GNU Radio is used to process the electromagnetic waveforms



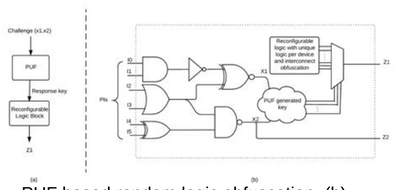






Logic Obfuscation – Springer Book Chapter

- Hardware obfuscation is a technique to conceal the design from malicious insiders and outsider adversaries.
- Chapter overviews the traditional design flow of integrated circuits, and assesses processes in terms of how much information is revealed to aid in reverse engineering the design.
- This chapter also investigates IP protection schemes that are designed to prevent illegal modifications and piracy for system-on-chip (SoC) IP-reuse-based design flows.



PUF based random logic obfuscation. (b) Integration in design Flow

Graduate course on Hardware Security and Outreach Engineering Camp to introduce Hardware security to graduate and High school Students – Summer

- A **course on Hardware security** was first time offered to graduate students at FIT.
- Several hands on labs were introduced in the course.
- Total enrollment was 10.
- Dissemination of results: curriculum slides, hands on labs and students presentations were posted on canvas.
- The **Engineering Camp** was an interactive 5-day experience into the life and studies of a student of Engineering.
- High school students were given an introduction to Hardware security, and importance of secure design flow.
- 2 hours hands on lab on FPGA design and security analysis.
- Dissemination of results: The results were disseminated form of tutorial, seminar and printouts to the high school students.

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

Florida Institute of Technology
High Tech with a Human Touch™