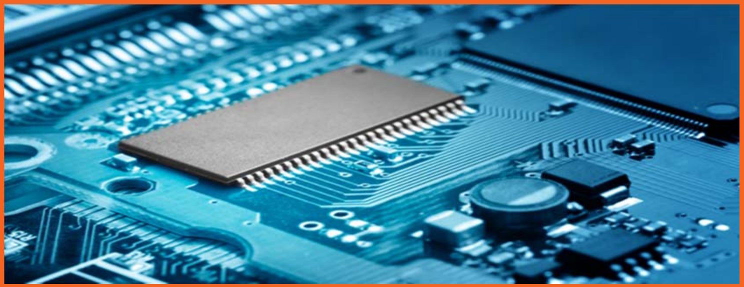
Hardware Trojan Detection



Team Intruder
Howard University
April 7, 2016

The Team

Taylor White Senior Computer Engineer
Darren Earle Senior Computer Engineer
Amanuel Getahun Senior Computer Engineer

Shrijanand Chintapatla Freshman Computer Science
Jah'lil Allen Freshman Computer Science
Sheriff Adewumi Freshman Electrical Engineer

(Not in picture)
Raza Shafiq Ajmi Graduate Student

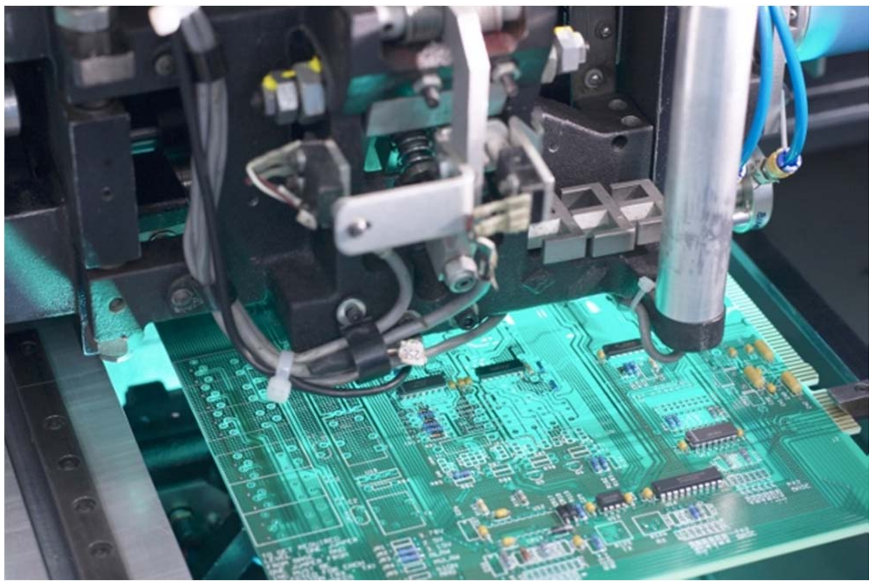
Advisor: DR. HASSAN SALMANI

AGENDA

- Project Overview
  - Background
  - Problem Statement
  - Design Requirements
- User Case
- Design Selection
- Implementation, Test and Evaluation
- Resources, Cost and Wrap up

Project Overview

BACKGROUND



Micro devices have ever increasing impact on our daily life and their horizontal design flow is widely practiced.

Trojans are a commonly known item that its total purpose is to attack a system

New age Trojans have now expanded into hardware as opposed to the traditional software based Trojans

Hardware trojans are generally harder to detect than software

PROBLEM STATEMENT

A Hardware Trojan is a malicious modification of the circuitry of an integrated circuit. These Trojans can be used to disable or destroy chips and its components as well as bypass or disable the security measures of a system.

DESIGN REQUIREMENTS

Ease of use
- ❖ Easily repeatable, systematic

Cost
- ❖ Affordable

Integrity of System
- ❖ Withhold system's functions

Accurate Detection
- ❖ Reliable

Ultimately, the Hardware Trojan detection method needs to be easily repeatable and systematic, affordable, and reliable all while withholding the system's functions.

Current Status of Art

- Research on detection methods are only beginning to emerge
- Department of Defense & Trusted Foundry Program

USER CASE

Scenario

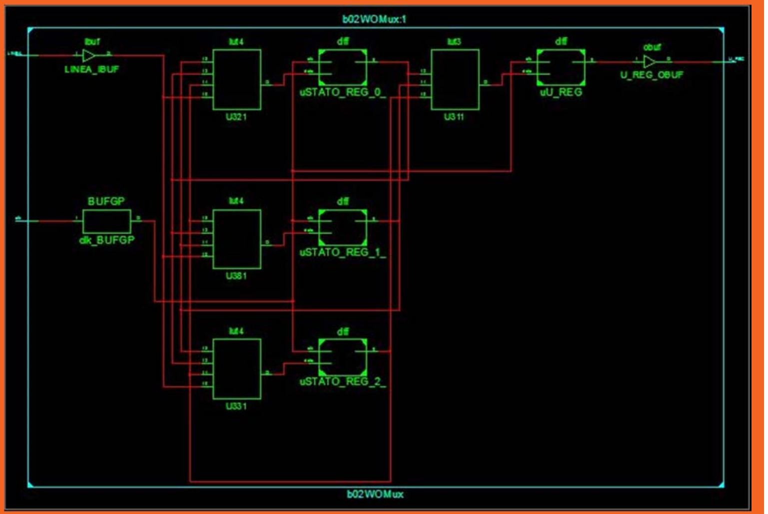
A small, "fabless" company wishes to fabricate their integrated circuit through outside foundry services.

- Concerned about any Hardware Trojans being integrated by the fabrication provider.
- Need to be able to check if their circuit has been compromised after manufacturing.

Circuit Specification

Name:

Schematic:

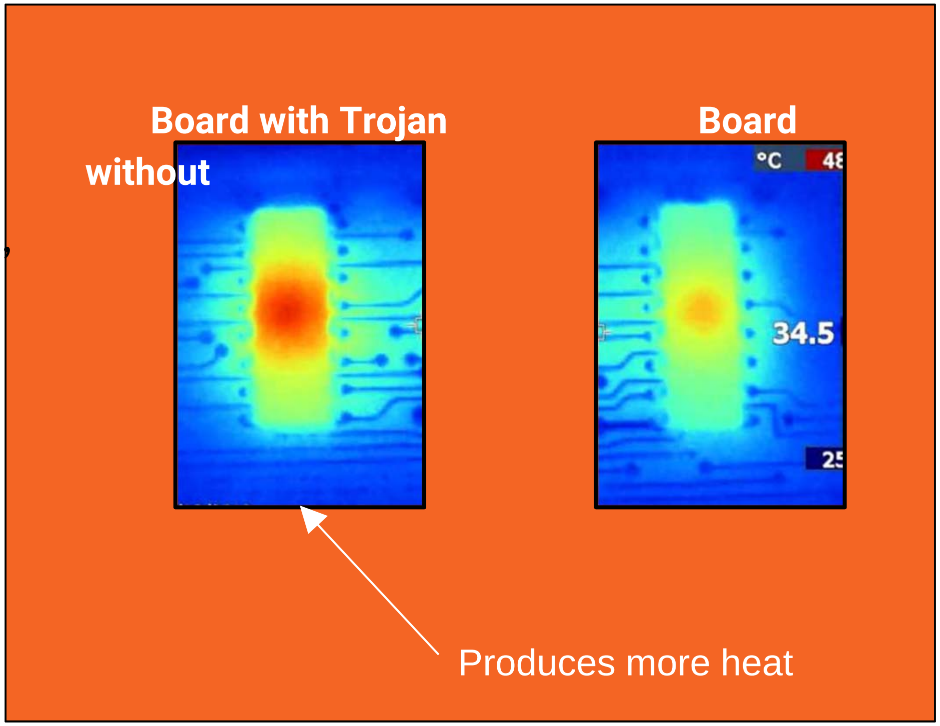


Design Selection

Solution Approach

Approach 1: Heat Dissipation Analysis

- Compares the heat maps of 2 FPGA boards using an IR (Infrared) camera
- Both boards will have identical circuits, with one also having a Trojan



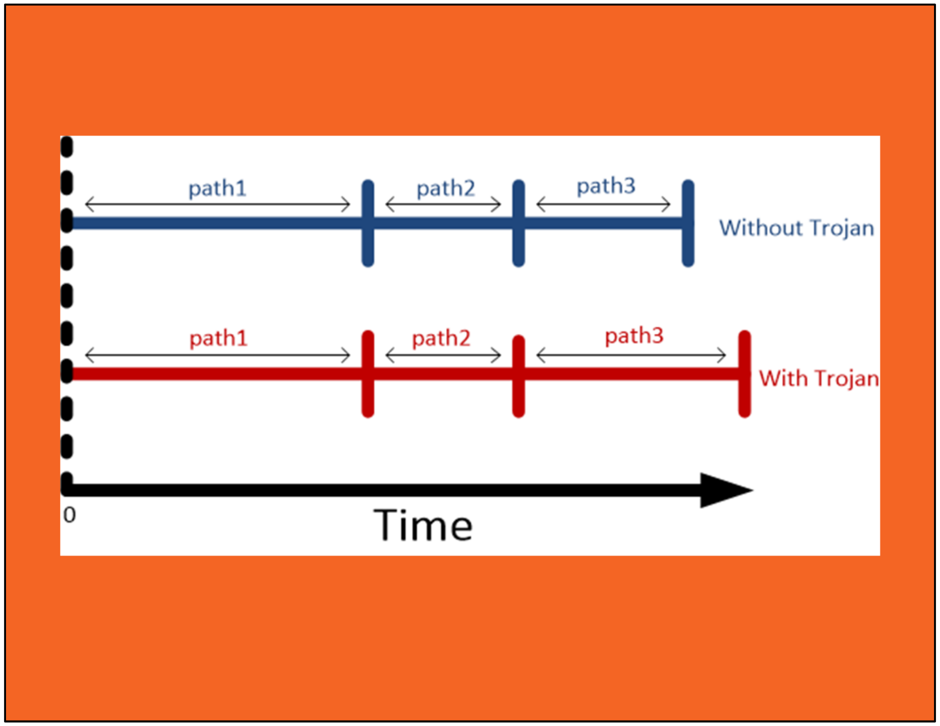
Solution Approach

Approach 2: Timing Analysis

Timing analysis will be ran on a circuit without a Hardware Trojan (A).

Timing analysis will be ran on an identical circuit with a Hardware Trojan (B).

The timing of the Trojan free circuit (A) will be compared with the timing of the circuit containing the Trojan (B).



Solution Approach

	Heat Dissipation Analysis	Timing Analysis
Ease of use		✓
Cost		✓
Integrity of system		✓
Accuracy		✓

Tools are provided and we have prior experience.

Tool are essentially free.

Systems functionality is maintained.

Heat Dissipation was more vulnerable to inaccuracy.

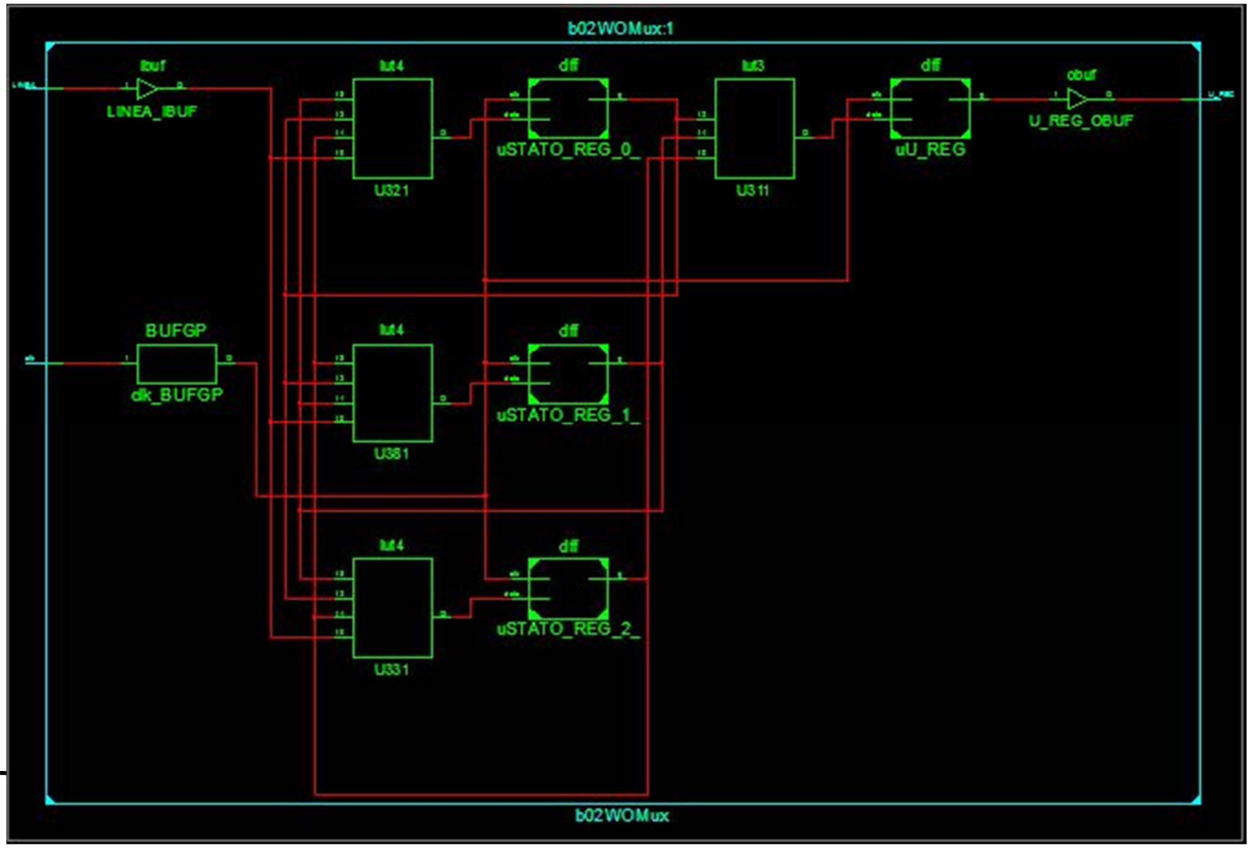
Room temperature

Unable to detect small trojans

IMPLEMENTATION, TEST AND EVALUATION

Schematic of Circuit

Highlighted are the vulnerable (short) paths



Multiplexer (MUX)

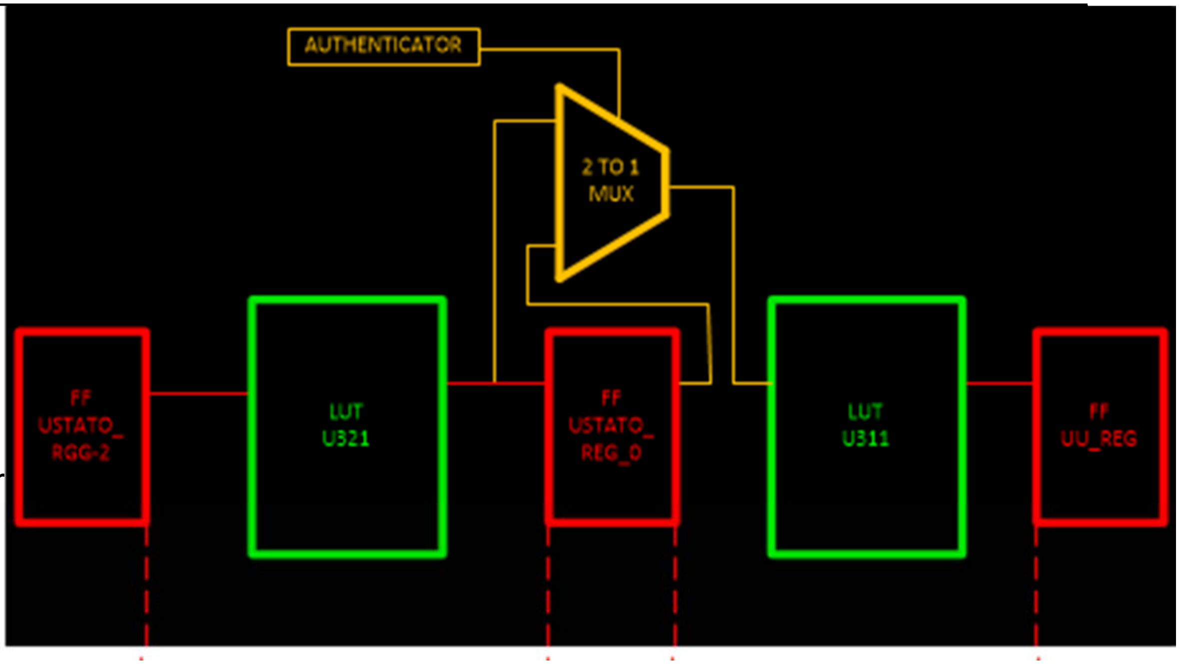
- Our MUX design will be implemented across the short paths' flip flops
  - This will allow us to concatenate them in order to realize their total time

Implementation of Multiplexer

Minimum clock period = 5.077 ns

Short Path ≤ 75% of minimum clock period

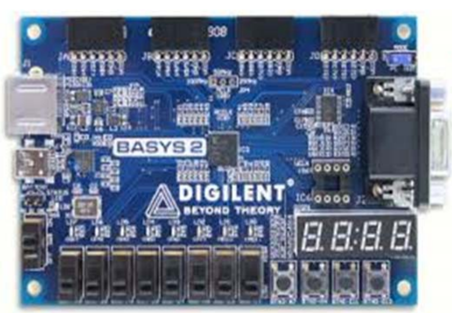
Short paths are considered to be 3.8077 or less



Resources, Cost and Wrap-up

Costs and Resources

- Xilinx ISE (FREE)
- Python 3.4 (FREE)
- 2 FPGA Board (Basys2) (Alternative) $65
- e) $400



Wrap up

- **Lessons Learned**
  - Work on tasks individually
    - Until one member has finished their task or needs help
  - Give ourselves room to make mistakes
    - Avoid pushing back deadlines
  - More team meetings
    - To stay on track

QUESTIONS?