Hardware Trojan Detection System for Medical Devices

Jonnetta Bratcher, C.E.
Naja Green, E.E.
Candace Ross, C.E.
Jonathan Lopera, E.E.
Justin Powell, E.E.

Howard University | Senior Design | December 3, 2014

Agenda

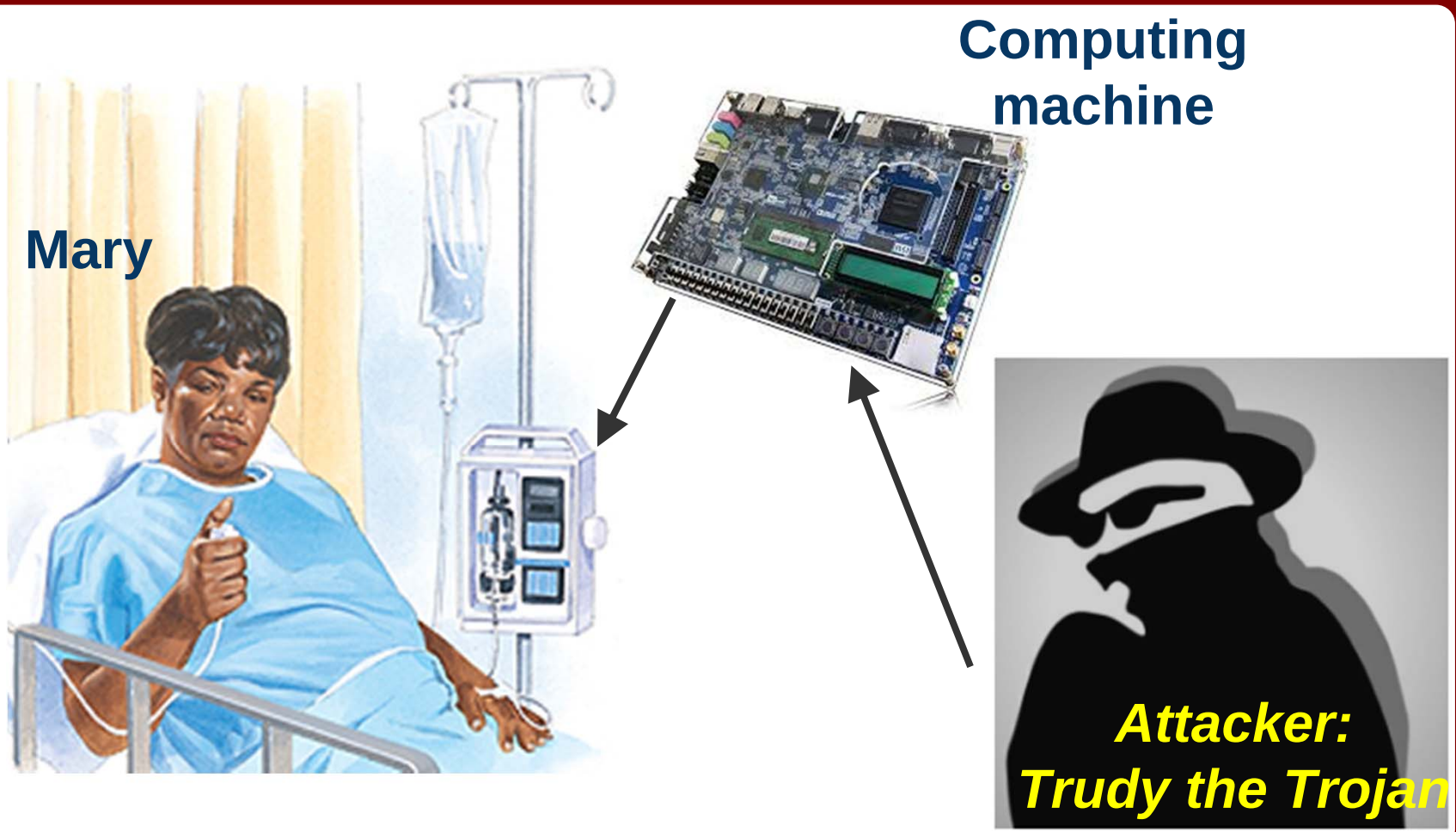
- Project Relevance & Background
- Problem Formulation
- Current Status of Art
- Implementation Plan
- Cost & Resources
- Deliverables
- Conclusion / Recap

Key Terms

- Field-Programmable Gate Array (FPGA)
- Verilog Hardware Description Language (VHDL)
- Cryptosystem
- Hardware Trojan

Background

- Hardware security is important
  - Medical devices, cellular phones, laptops, etc.
  - **FPGAs** (field programmable gate arrays)
- Cryptosystems protect data
- Who is trying to access the data? How are they accessing data?
  - Hardware Trojans, ticking time bombs, back-doors


Computing machine
Mary
Attacker:
Trudy the Trojan

Problem Formulation

How can we develop a system to detect hardware Trojans?

Problem Formulation

The detection system should be:

- Size efficient
  - Appropriate for hospital
- Response time
- User interface / ease of use
- Encryption should meet HIPAA (Health Insurance Portability and Accountability Act) standards

Current Status of Art

- Smart Cards
  - Unique ability to store large amounts of data
  - Carry out their own on-card functions (e.g., encryption and mutual authentication)
  - Interact intelligently with a smart card reader

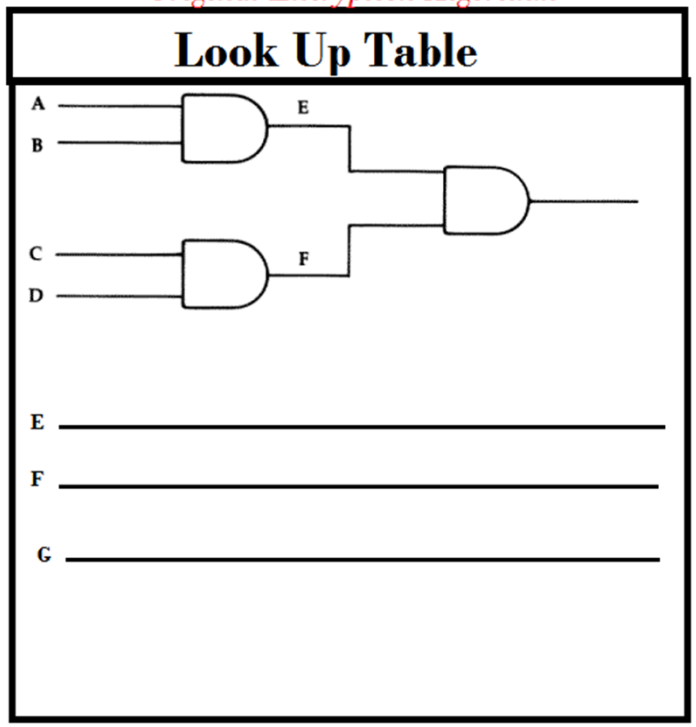
Current Status of Art

ZigBee Chip

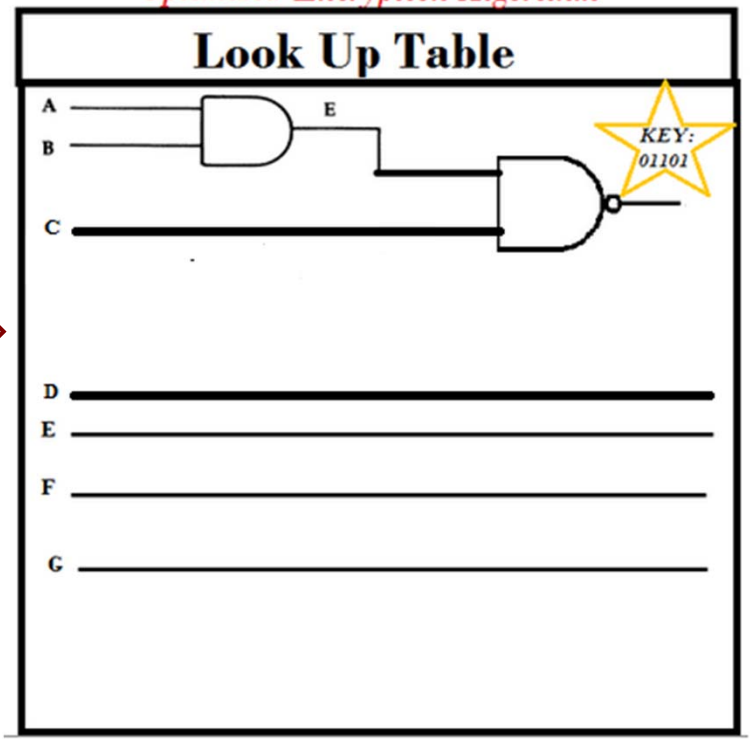
- Embedded system used in medical devices
- Cryptosystem design for long-distance data transmission

Solution Approach

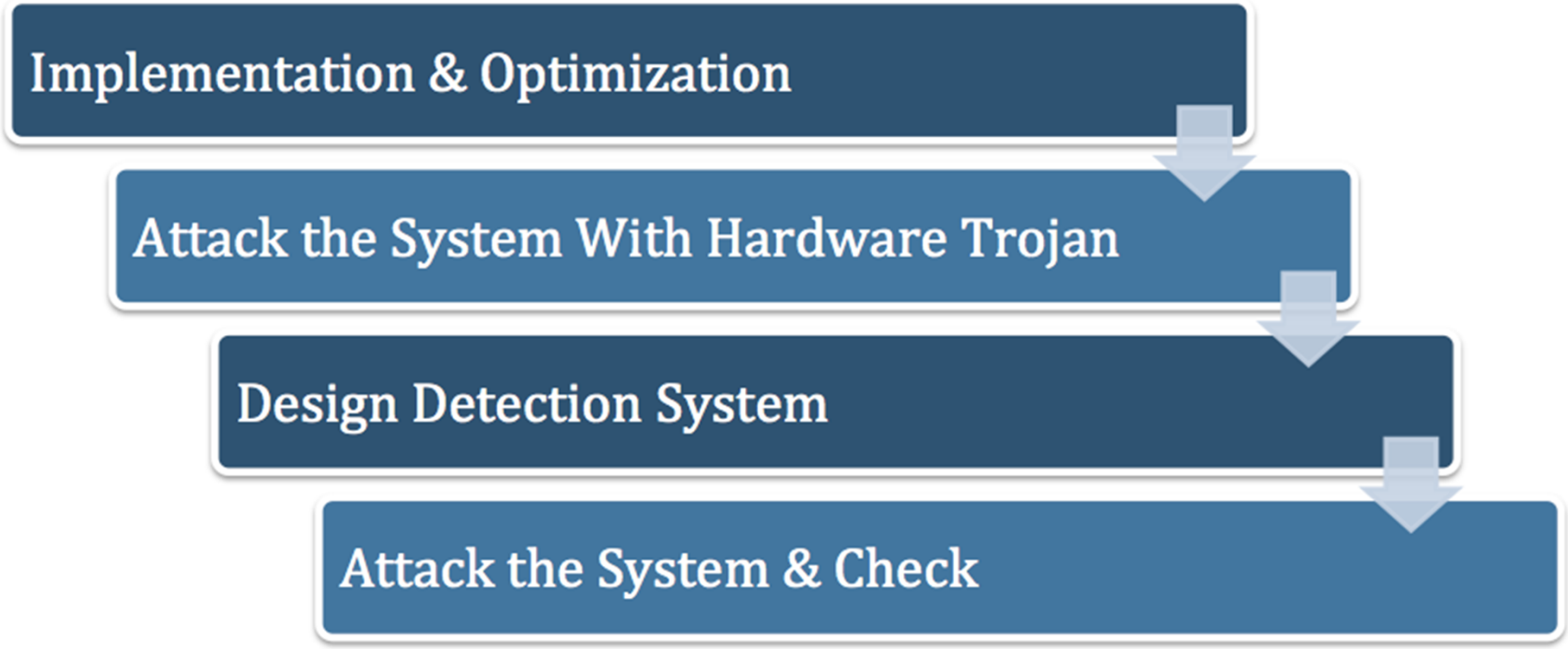
Original Encryption Algorithm



Optimized Encryption Algorithm



Solution Approach



Solution Approaches- Initial Plan

- Side-channel Analysis
  - Device emits certain signals
    - electrical field, magnetic field, etc.
  - Correlates to “device signature”
  - Exploit device signature for detection

Alternative Solutions

- Heat Dissipation Analysis
  - sensor, thermometer
- System Speed Analysis
  - on-screen time
- Physical Inspection Analysis
  - Visual inspection
  - SEM (scan electron microscopy)

Solution Approaches-
Top Design Selection Process

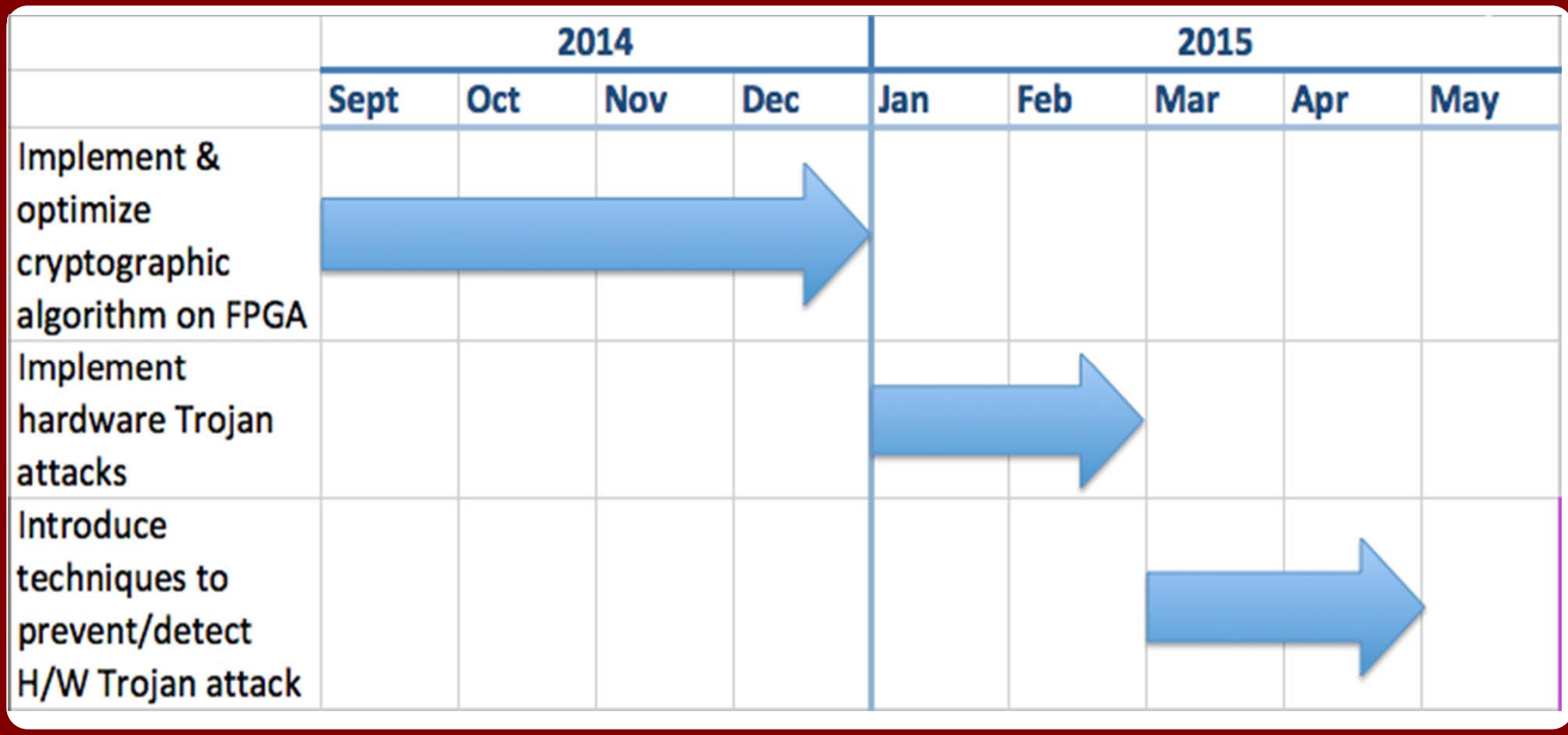
	Side-channel Analysis	Heat Dissipation Analysis	System Speed Analysis	Physical Inspection
Time (5)	5*(8)=40	5*(8)=40	5*(7)=35	5*(6)=30
Cost (3)	3*(7)=21	3*(6)=18	3*(9)=27	3*(5)=15
Resources (4)	4*(7)=28	4*(6)=24	4*(7)=28	4*(5)=20
Longevity (3)	3*(9)=27	3*(9)=27	3*(8)=24	3*(2)=6
Total	116	109	114	71

Highest Possible Score: 150
Weight: Scale 1-5 (1 least important, 5 most important)
Score: Scale 1-10 (1 least feasible, 10 most feasible)

Implementation & Verification Plan

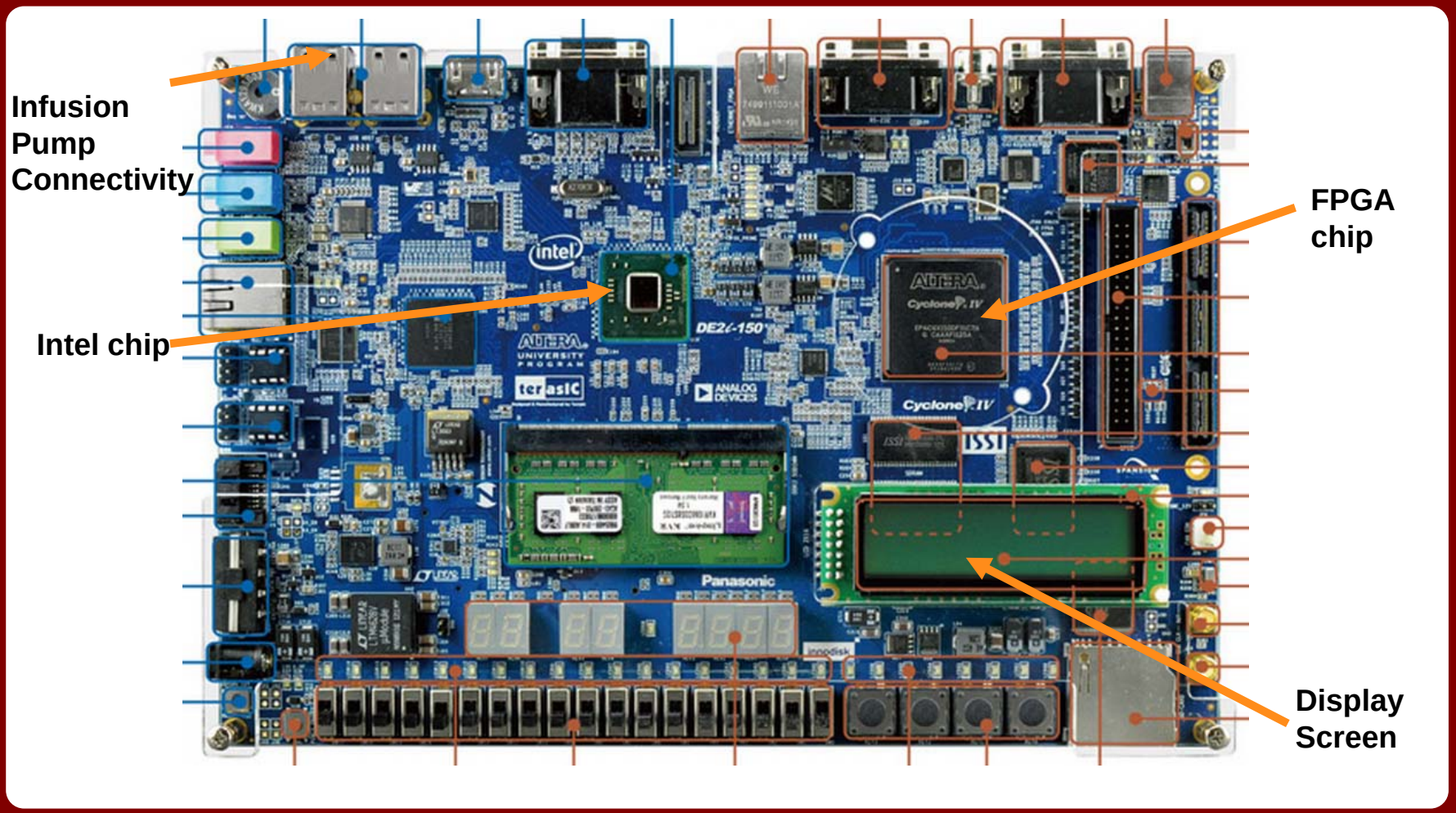
- Implement cryptographic algorithms in VHDL
- Optimize algorithms
  - Parameters include area overhead, size, speed
- Attack system with Trojan
- Analyze for methods of detection
- Create detection system
- Attack and check

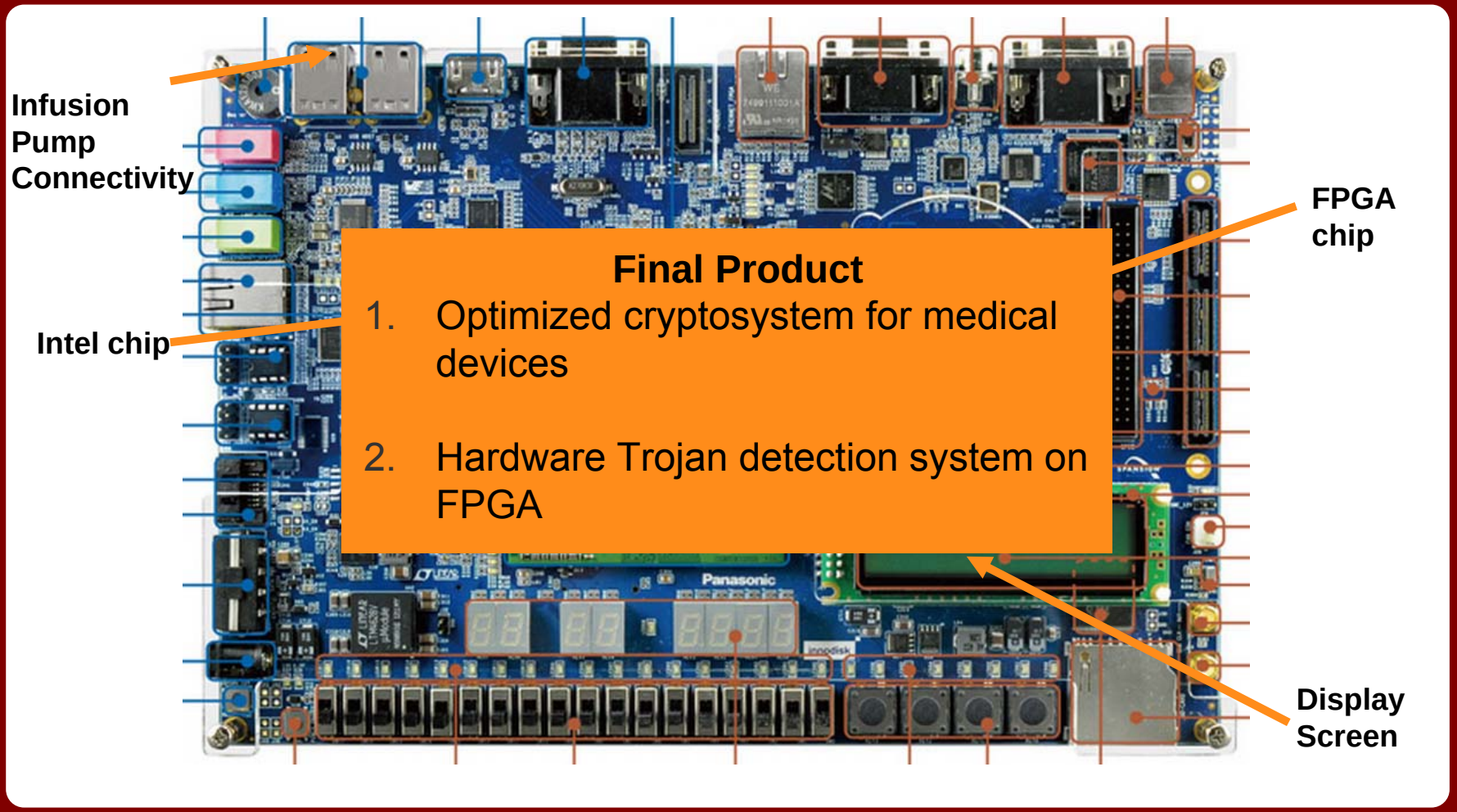
Project Timeline



Cost & Resources

- DE2i-150 board
  - Howard University EECE Department (Dr. Kim)
  - ~$1500
- Xilinx- ISE Design Suite
- Infusion Pump
  - Amazon- $100


Infusion Pump Connectivity
Intel chip
FPGA chip
Display Screen
intel
ALTERA
Cyclone IV
DE2i-150
ALTERA UNIVERSITY PROGRAM
terasIC
ANALOG DEVICES
ISSI
Panasonic



Final Product

1. Optimized cryptosystem for medical devices
2. Hardware Trojan detection system on FPGA

Conclusion/ Recap

- Implement and optimize cryptographic algorithm on FPGA
- Study and attack algorithm with hardware Trojan
- Develop techniques to detect hardware Trojan

Questions?