Senior Design
Electrical and Computer Engineering
Howard University
Instructor: Dr. Charles Kim
Website: www.mwftr.com/SD1415.html

Hardware Trojan Detection & Prevention for Health-care Computer Systems

Howard University
April 9, 2015

Jonnetta Bratcher, Naja Green, Jonathan Lopera, Justin Powell, Candace Ross
Skander Charouchi (Grad)
Dr. Hassan Salmani (Advisor)

Agenda

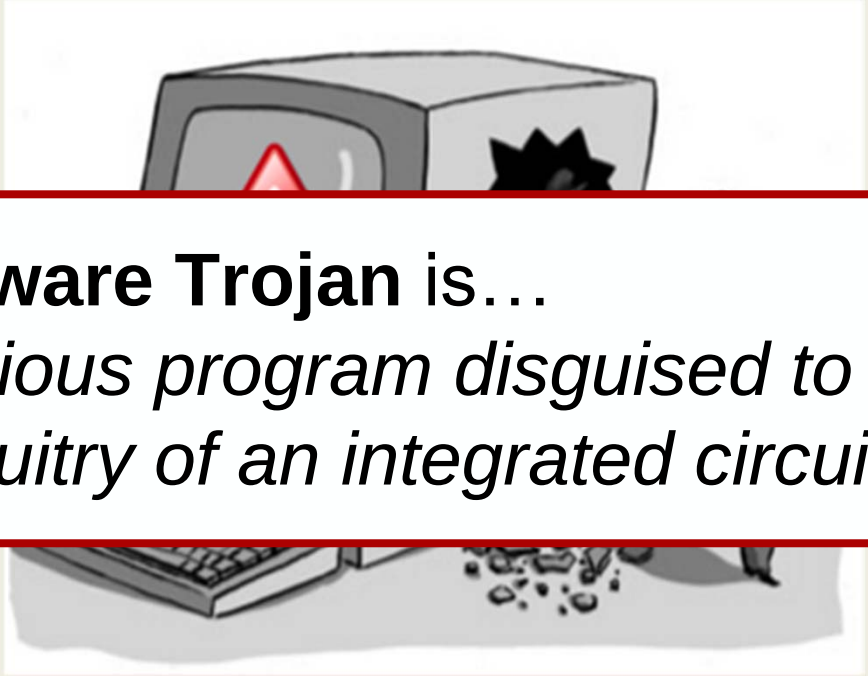
- Project Overview
- User Case
- Design Selection
- Implementation, Test and Evaluation
- Resources, Cost and Wrap up

Project Overview

Background

- Medical security is important
  - Computers increasingly being used in security
- Begin with **security primitives**
  - Confidentiality
  - Integrity
  - Authentication

Problem Statement



A **hardware Trojan** is…

A malicious program disguised to modify the circuitry of an integrated circuit.

Design Requirements (1)

- Size efficient
  - Appropriate for hospital environment
- Quick response time
- User-friendly interface / Ease of use
- Security primitives

Design Requirements (2)

Two Prong Detection & Prevention System

Intel Galileo
Authenticates user
Sends authentication bit

+

FPGA
Decrypts command
Receives authentication bit

=

Command is sent to medical device

Current Status of Art

Personal Health Records (PHR) Systems contain highly sensitive health information that discloses the patient's identity.

Tethered	Untethered
Organization based	Web or Cloud based
Care Provider friendly • Kiaser Permante	Patient friendly • WebMD

User Case

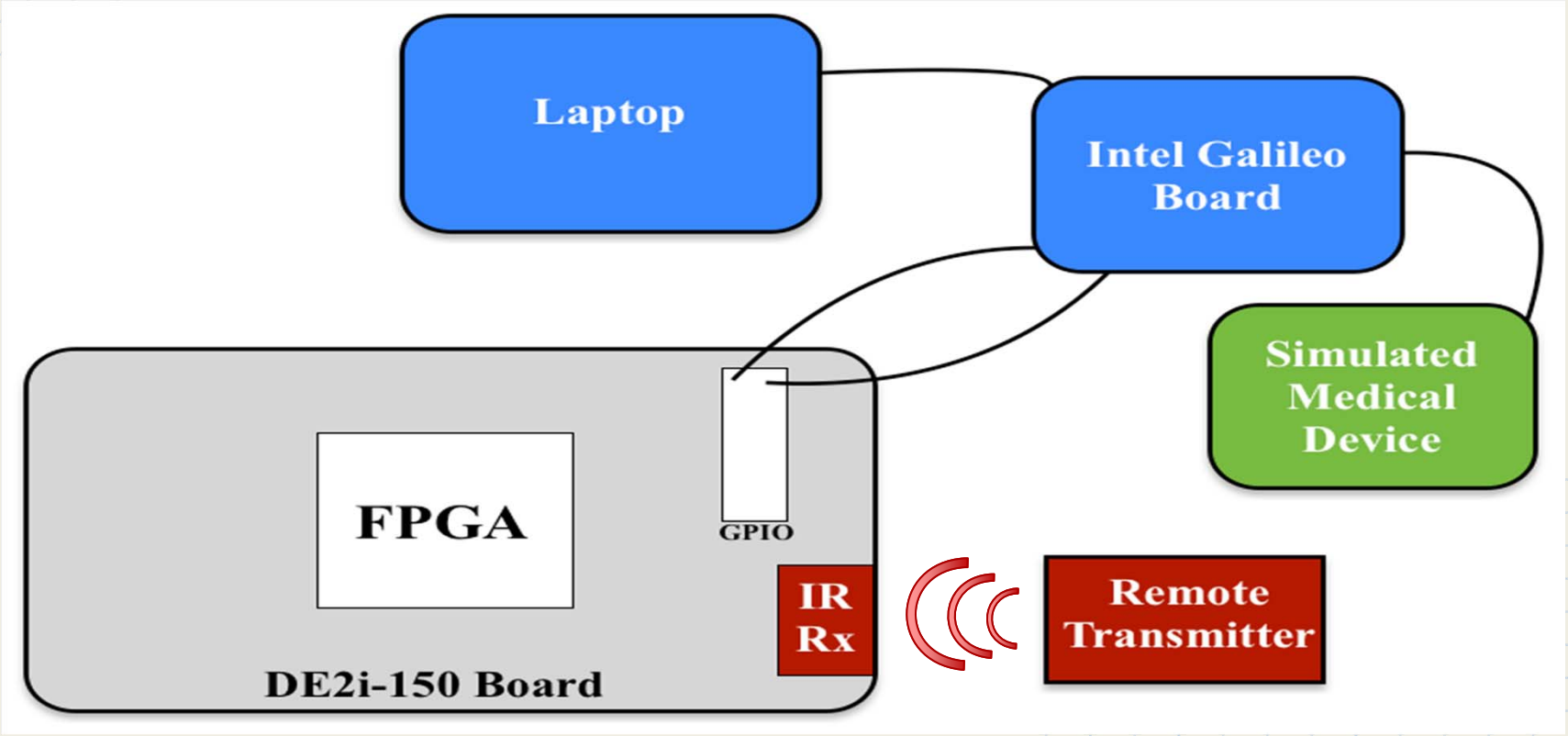
Consider…

- Busy hospital
- Both doctors and patients have physical access to health care computer system
- Someone attempts to gather information about a patient and maliciously alter their medicine dosage

Assumptions

- No protective security measures in place
- Medical device controlled using keyboard and monitor
- Open user environment in hospital setting
  - Allows for both authorized and unauthorized physical access

Final Schematic



Design Selection

Conceptual Design

- *Physical Transmitter* :
  Remote vs. Smartphone
- *Means of Communication*:
  Bluetooth vs. IR
- *Cryptographic Algorithm*:
  RSA vs. RC4

Conceptual Design: Physical Transmitter

		
Time	✓	
Cost	✓	
Resources	✓	
Longevity	✓	

Winner:

Remote

Conceptual Design: Means of Communication

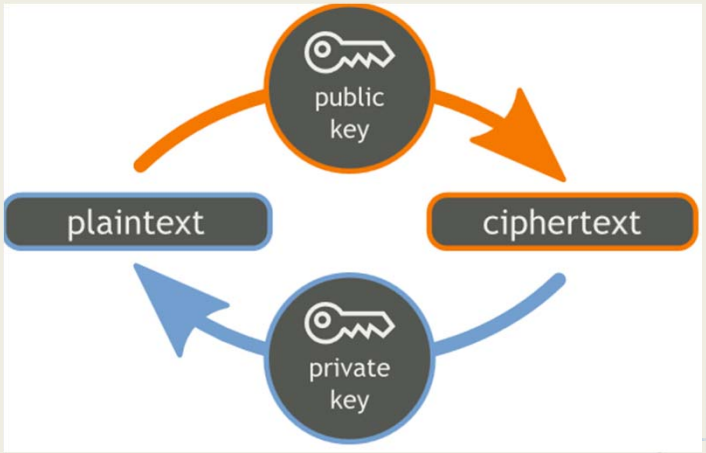
		
Time		✓
Cost		✓
Resources	✓	
Longevity	✓	✓

Winner:

Infrared

Conceptual Design: Cryptographic Algorithm

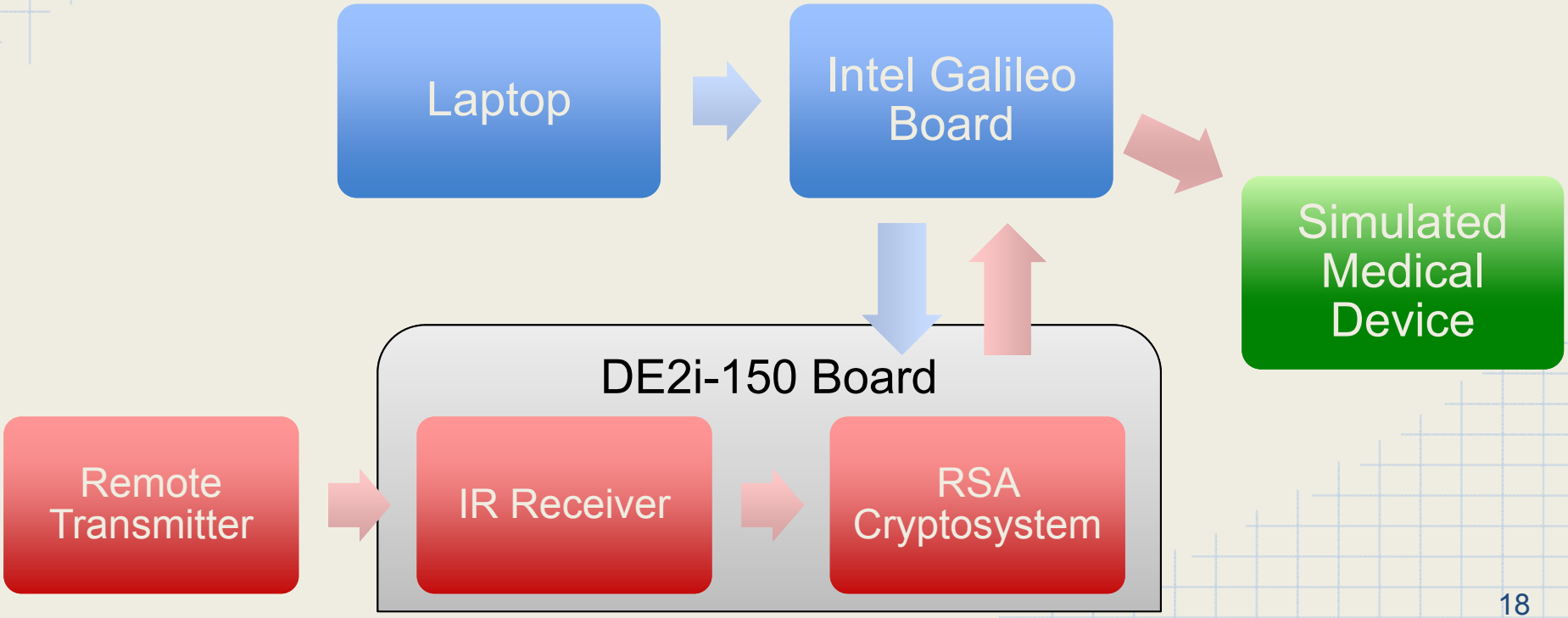
	RSA	RC4
Time		✓
Cost	✓	✓
Resources	✓	
Longevity	✓	



Winner:

RSA

Final Top Design



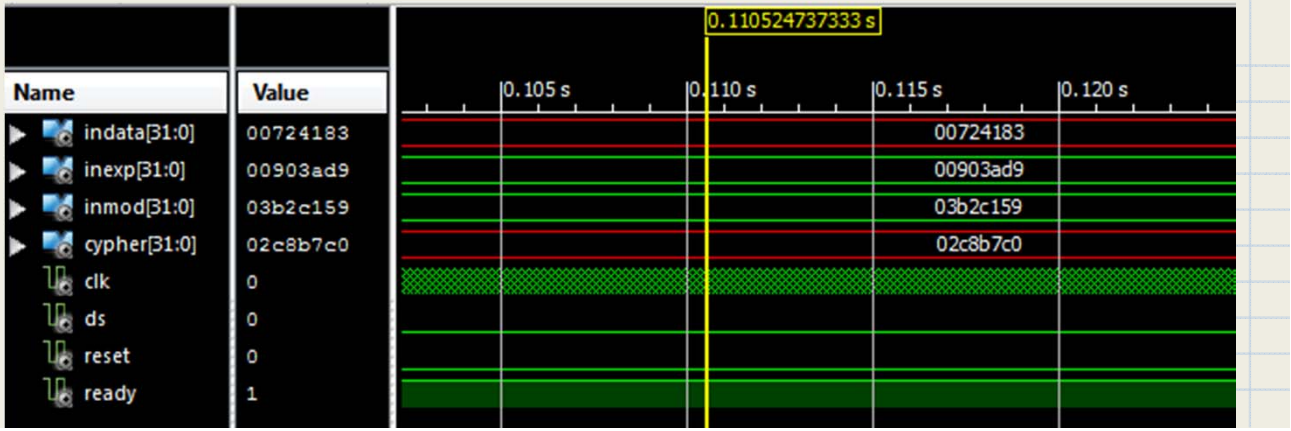
Implementation, Test and Evaluation

The IR Transmitter & Receiver

- Language: VHDL
- Pass output of receiver module to 7-segment display
- Verify transmitter command is correct

The RSA Algorithm

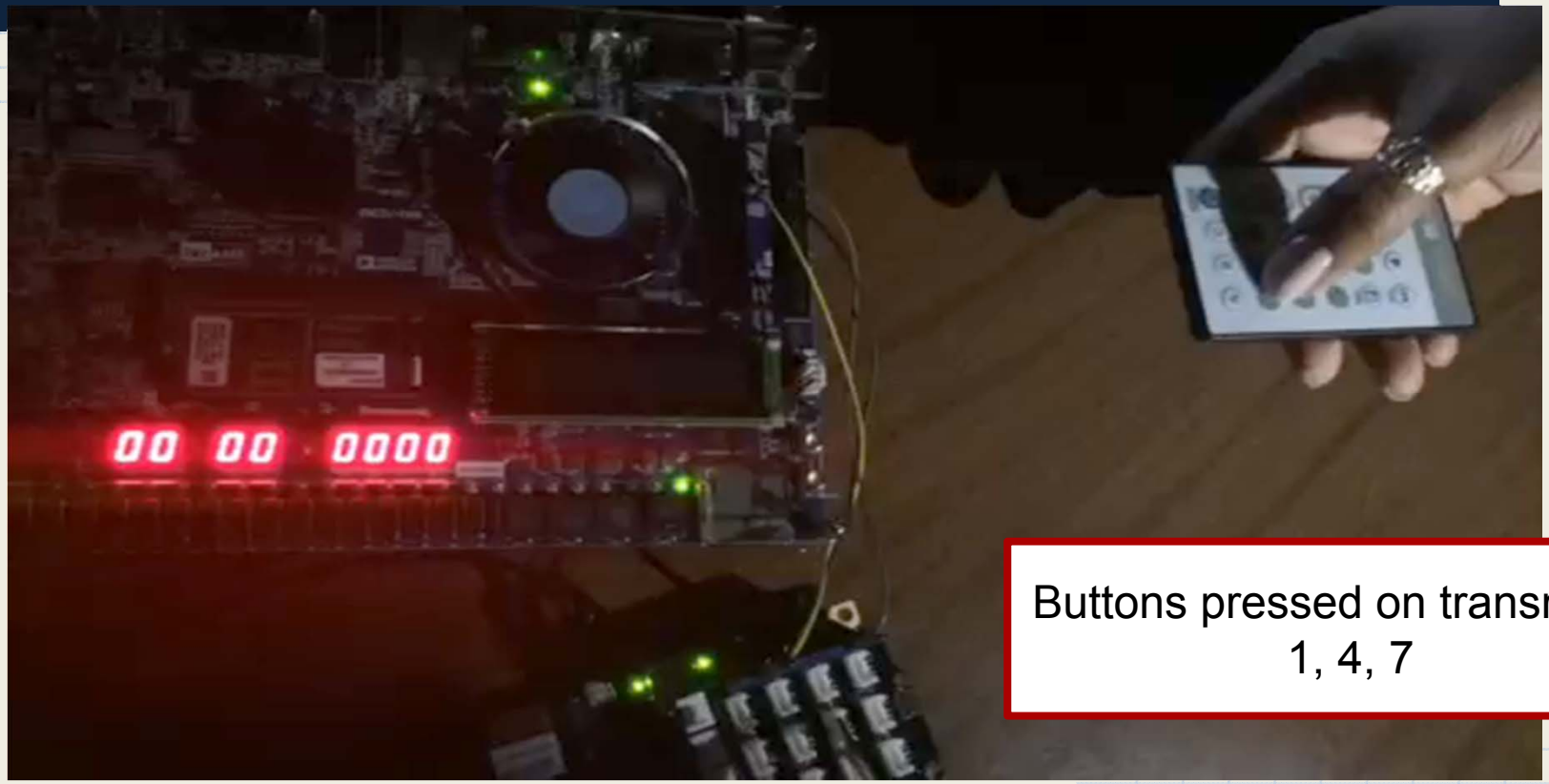
- Language: VHDL
- Adjust source code to fit project scope
- Simulate in Xilinx
- Send various registers & outputs to LEDs to make sure data is correct



Connecting IR and RSA

- Language: Verilog
- Connect modules in Quartus II
- Send various registers & outputs to LEDs and 7-segment display to make sure data is correct

Connecting IR and RSA



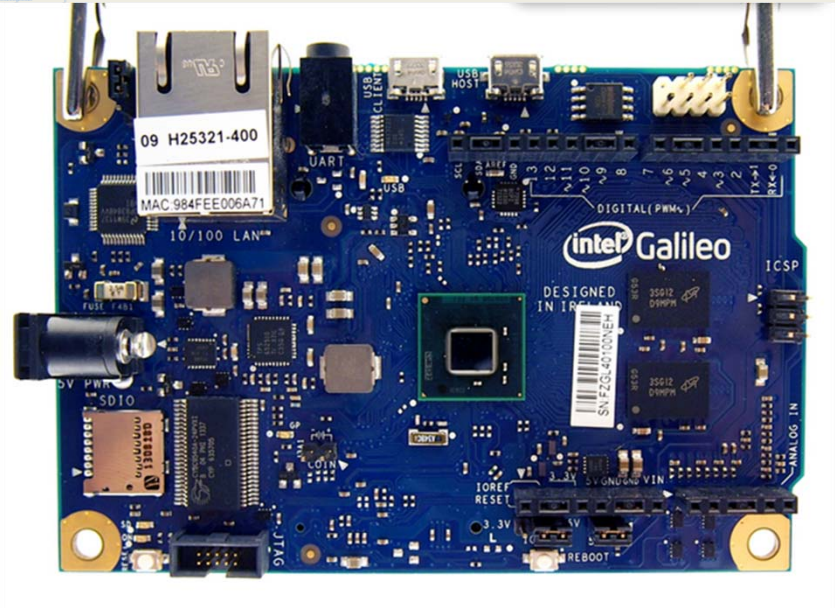
Buttons pressed on transmitter:
1, 4, 7

The Patient Database & Interface

- Language: C
- Arduino
- Input accurate information & confirm access
- Input inaccurate information & confirm denied access

```
const int numPeople = 3;
const int lengthFirstName = 5;
const int lengthLastName = 5;

int firstNames[numPeople][lengthFirstName] = {{65, 108, 105, 99, 101}, //Alice
                                              {66, 111, 98, 98, 121}, //Bobby
                                              {84, 114, 117, 100, 121}}; //Trudy

int lastNames[numPeople][lengthLastName] = {{83, 109, 105, 116, 104}, //Smith
                                            {76, 111, 112, 101, 114}, //Loper
                                            {66, 97, 116, 101, 115}}; //Bate

void setup() {
        pinMode(isMatch, OUTPUT);
        Serial.begin(9600);     // opens serial port, sets data rate to 9600 bps
}

void loop() {
        int getFirstName[5];
        // send data only when you receive data:
        int getLastName[5];
        if (Serial.available() > 0) {
                // read the incoming byte:
                for (int i=0; i < 6; i++)
                {
                  getFirstName[i] = Serial.read();
                }
```

Communication to FPGA via Galileo

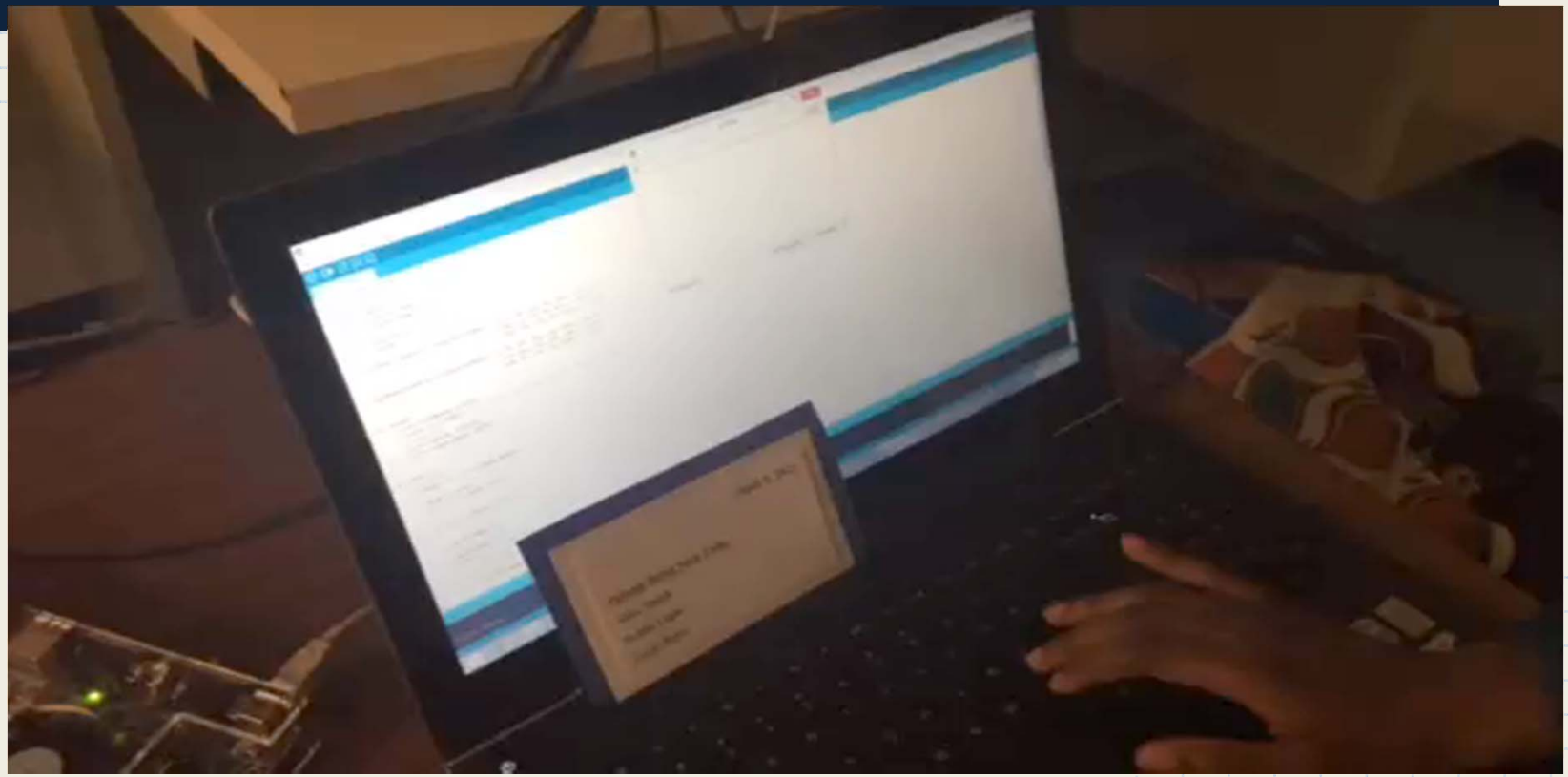


- Arduino used to code database
  - Interface: Serial Monitor
- General Purpose Input Output (GPIO) pin connections
- Connect modules in Quartus II

The Medical Device

- Dosing pump
- Controlled via Galileo
- Connect to board to receive commands
- Update accurately according to commands

Full Demo



Resources, Cost & Wrap-Up

Resources & B

- Resources
  - DE2i-150, Intel Galile
  - Quartus II 13.1
  - Xilinx ISE Design Stu
  - Arduino software
  - Dosing Pump (Abdul
  - Power supply (12V)
- Budget?

Conclusions

1. **Secured communication** in a simulated hospital environment to ensure the following **security primitives**:
   - Confidentiality
   - Integrity
   - Authentication
2. Prevention
   - RSA Cryptosystem
   - Authentication via interface
3. Secured Personal Health Record System
   - Tethered

Future Works

Continuing the VIP (Vertically Integrated Project) approach:

- Attack system with hardware Trojan
- Use smartphone to transmit commands
- Use of Bluetooth
- Medical device compatibility (For real time simulation)
- Internet connectivity for instant updates to patient database

Questions