horizontal line

**Bi0s Hardware**

Amritapuri, Vallikavu

Kerala

690546

CompatrIoT

**8th March 2022**

# OVERVIEW

The CompartIoT Security learning kit is a great way to get started with IoT device security and exploitation using the DIVA (Damn Insecure and Vulnerable Application) board and other targets. This kit includes everything that you need in your arsenal to perform UART, I2C, SPI, JTAG, WiFi, BLE analysis. These labs provide guidance and step by step process of performing each lab. It will teach you everything from finding the communication ports, sniffing, manipulating communication to exploiting IoT devices.

# GOALS

1. PCB Redesign
2. Firmware Development
   1. Labs
      1. UART
         1. Lab 1 – UART Identification Method 1
         2. Lab 2 – UART Identification Method 2
         3. Lab 3 – UART Communication With Target
      2. JTAG
         1. Lab 1 – JTAG Identification Method 1
         2. Lab 2 – JTAG Identification Method 2
         3. Lab 3 - Microcontroller firmware extraction over JTAG
         4. Lab 4 - Microcontroller firmware patching over JTAG
         5. Lab 5 - Microcontroller peripheral access over JTAG
      3. I2C
         1. Lab 1 – I2C chip recon naissance
         2. Lab 2 – I2C communication sniffing to bypass authentication
         3. Lab 3 – I2C chip memory dumping
      4. SPI
         1. Lab 1 – SPI chip recon
         2. Lab 2 – SPI communication sniffing to bypass authentication
         3. Lab 3 – SPI chip memory dumping and firmware extraction
      5. BLE
         1. Lab 1 – Recon
         2. Lab 2 – GATT Services and Characteristics enumeration
         3. Lab 3 – Sniffing GATT protocol communication (Android)
         4. Lab 4 – Analyze GATT Protocol communication
         5. Lab 5 – Controlling the Device
         6. Lab 6 – Crack BLE LTK

# Objective

* Labs
  + UART
    - Lab 1 – UART Identification Method 1
      * UART Identification Method 1 using micro-controller pins and DMM (Digital Multimeter) conductivity test. The objective is to identify UART pinouts on the PCB board provided we have the knowledge of microcontroller UART pins, which can be found in the datasheet of the microcontroller.
    - Lab 2 – UART Identification Method 2
      * UART Identification Method 2 using DMM Voltage tests on the board pinouts. The objective is to identify UART pinouts on the PCB board when we do not have the knowledge of the microcontroller UART pins and the datasheet of the microcontroller.
    - Lab 3 – UART Communication With Target
      * Once the UART port is identified, communicate with the target device to further analyze read/write access to the device. The objective is to understand the process of interfacing with the target device, identifying the correct baud rate that it uses to communicate and analyze the read/write access.
  + JTAG
    - Lab 1 – JTAG Identification Method 1
      * JTAG Debug port identification method 1 using micro-controller pins and DMM (Digital Multimeter) conductivity test. The objective is to identify JTAG pinouts on the PCB board provided we have the knowledge of microcontroller JTAG pins, which can be found in the datasheet of the microcontroller.
    - Lab 2 – JTAG Identification Method 2
      * Automated JTAG Pin scanning and Identification using JtagEnum on Arduino. The objective is to understand the process and perform automated JTAG scanning using JtagEnum running on Arduino.
    - Lab 3 - Microcontroller firmware extraction over JTAG
      * Use the JTAG Debug port to access the microcontroller and extract the firmware. The objective is to understand how to connect over JTAG with the target board and how to extract data from the internal memory of the microcontroller.
    - Lab 4 - Microcontroller firmware patching over JTAG
      * Find out the hardcoded password from the extracted firmware, modify it, write it back, and log in. The objective is to familiarize yourself with firmware extraction, analyze hardcoded data, and patch the firmware on the fly.
    - Lab 5 - Microcontroller peripheral access over JTAG
      * Use JTAG Debug port to manipulate GPIOs of microcontrollers and generate LED patterns with onboard LEDs. The objective is to understand how to control the GPIOs of the micro-controller over JTAG to change the behavior of the target as per your needs.
  + I2C
    - Lab 1 – I2C chip recon naissance
      * To perform reconnaissance on EEPROM using the datasheet. The objective is to understand what information to obtain from the memory chip datasheet, which will help in further analysis.
    - Lab 2 – I2C communication sniffing to bypass authentication
      * I2C communication sniffing using the Logic analyzer and bypass authentication. The objective is to get experience in interfacing with a Logic analyzer and reverse engineer the communication between the microcontroller and the I2C chip to identify any issues or vulnerabilities.
    - Lab 3 – I2C chip memory dumping
      * I2C EEPROM memory dumping using Bus Pirate. The objective is to get familiar with the process of dumping I2C memory chip data.
  + SPI
    - Lab 1 – SPI chip recon
      * To perform reconnaissance on EEPROM using the datasheet. The objective is to understand what information to obtain from the memory chip datasheet, which will help in further analysis.
    - Lab 2 – SPI communication sniffing to bypass authentication
      * SPI communication sniffing Using Logic analyzer and bypass authentication. The objective is to get experience in interfacing with a Logic analyzer and reverse engineer the communication between the micro-controller and the SPI chip to identify any issues or vulnerabilities.
    - Lab 3 – SPI chip memory dumping and firmware extraction
      * SPI Flash memory dumping using Bus Pirate. The objective is to get familiar with the process of dumping SPI memory chip data and extracting Linux-based firmware.
  + BLE
    - Lab 1 – Recon
      * The objective is to perform scanning for BLE devices in proximity.
    - Lab 2 – GATT Services and Characteristics enumeration
      * To enumerate the GATT services and characteristics of the BLE device. The objective is to understand what characteristics and services are and how do you get that information from a BLE device.
    - Lab 3 – Sniffing GATT protocol communication (Android)
      * Sniff the GATT protocol communication on Android. The objective is to understand how to sniff the GATT protocol communication, on an Android phone, with a BLE peripheral.
    - Lab 4 – Analyze GATT Protocol communication
      * To identify write characteristic commands, their handles, and written values when you trigger an action on the BLE device. The objective is to understand how to identify and analyze which characteristics correspond to which commands/operations you perform on the device via the Android app.
    - Lab 5 – Controlling the Device
      * Control the behavior of the device by writing characteristic commands on the GATT protocol. The objective is to understand how to communicate with the device using tools instead of the actual app, send it specific values and analyze the behavior or control it remotely.
    - Lab 6 – Crack BLE LTK
      * Crack the LTK (Long Term Key) and decrypt the communication. The objective is to understand the process of cracking the LTK and what data is required for cracking.