Configuration Manual

MSc in Cyber Security Evening

Andrzej Mackiewicz
Student ID: 18157815

School of Computing
National College of Ireland

Supervisor: Ben Fletcher

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Andrzej Mackiewicz

Student ID: 18157815

Programme: MSc in Cyber Security Evening Year: 2020

Module: Internship

Supervisor: Ben Fletcher

Submission Due Date: 17th August

Project Title: Configuration Manual

Word Count: ……………………………………… Page Count…………………………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:

Date: 17/08/2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Table of Contents

Case Study 1 setup

Description:

The first case study was regarding Mifare Classic a card by using RFID reader writer called ‘Mifiere RFID-RC522’ which I have bought on Alliexpress. It comes with a card and a tag.

Components:

- RFID-RC522 – two-way transmitter-receiver which can read and write to tag or card.
- Tag and card that allows to read and write cloned information (Note: that some of the cards may not work as expected it is better to buy a set of magic Chines cards from AliExpress to make sure that your blank card has changeable UID).
- Laptop with Windows OS.
- Arduino Uno – standard Arduino board, purchased online.
- Open-source Arduino app download from their page.
- Library called ‘rfid-master’ – available on GitHub or in 2.CT Solution.zip file.

How to connect all components and use the software?

1 The RFID-RC522 need to connect to Arduino as per below setup using Windows OS:
1.1 RC522 SDA pin connect to Uno 10 pin
1.2 RC522 SCK pin connect to Uno 13 pin
1.3 RC522 MOSI pin connect to Uno 11 pin
1.4 RC522 SDA pin connect to Uno 12 pin
1.5 RC522 IRQ not connect
1.6 RC522 GND pin connects to Uno GND pin
1.7 RC522 RST pin connect to Uno 9 pin
1.8 RC522 3.3V pin connect to Uno 3.3V pin
1.9 Please note:
1.9.1 Solder cable to RFID-RC522 before attaching to Arduino.
1.9.2 Please make sure that you power this device to 3.3V
2 Connect Arduino to laptop via USB cable and set it up using the following points:
2.1 Downloaded library ‘rfid-master’ (zipped if it is not with .zip format)
2.2 Open Arduino application
2.2.1 Go to Sketch > Include Library > Add Zip > Choose ‘rfid-master.zip’
2.2.2 Go to File > Example > MFRC522(the folder is on the bottom of the examples) > DumpInfo
2.2.3 Go to Tools > Board: > Arduino Uno
2.2.4 Go to Tools > Processor > ATmega328P(Old Bootloader)
2.2.5 Go to Tools > Port (COM #) # - it is port number that you have set up
2.2.5.1 To find # - Go to Device Manager and check Ports (COM & LPT)
2.2.6 Go to Tools > Serial Monitor - to view card information printed on the screen
3 Read card info and Clone card:
3.1 Scan MIFARE 1k card to view DumpInfo
3.2 Find card UID as per 5.1.3 Case Study 1 Hardware and software setup example in the report
3.3 In Arduino go to File > Example > MFRC522 > ChangeUID
3.4 Put a magic card with changeable id on the antenna
3.5 Go to line 35 in the code and change highlighted in red #define NEW_UID {0xDE, 0xAD, 0xBE, 0xEF} to ID’s that have been red from the card.
3.6 Example 5.1.5 Case Study 1 Results of the cloning RFID (MIFARE 1K Type) present this action and result by DumpInfo again to show that clone of the card was successful.
3.7 DONE!

Case Study 2 setup

Description:

The Proxmark3 Easy is a cheaper version of the Proxmark3 V2 tool. This tool uses open-source software and firmware that is available for download it can be used only on Windows operating system. The Proxmark3 is a dedicated for RFID analysis and providing: snooping, reading, emulation, demodulation, writing, analysis, replaying, modulation, decoding, encoding, decryption, encryption LF 125kHz – HF 13.56MHz tags. It has capabilities of reading and writing; it can analyse signals received over the air and can pretend the RFID.

Components:

- Proxmark3 Easy it is a transmitter and receiver which can read and write information.
- Tag and card that allows to read and write cloned information (Note: that some of the cards may not work as expected it is better to buy a set of magic Chines cards from AliExpress to make sure that your blank card has changeable UID).
- Laptop with Windows OS
- pm3-bin-2.4.0 software

How to connect all components and use the software?

1 Download pm3-bin-2.4.0 available on GitHub or in 2.CT Solution.zip file.
2 Please note that antivirus needs to be disabled for this test!
3 Connect Proxmark3 Easy to laptop via USB cable
3.1 On the task manager, the popup show message 'Device driver software was not successfully installed.'
3.2 Go to 'Device Manager' and find 'Unknown device' in 'Other devices' section
3.2.1 Right-click on the device, click 'Properties.'
3.2.1.1 Go to Drivers and select 'Browse my computer for driver software.'
3.2.1.2 Select folder 'Windows Driver' in pm3-bin-2.4.0 unzipped folder and confirm all
3.3 Go back to 'Device Manager' to check 'COM Port' that needed later on in this setup
3.3.1 Go to pm3-bin-2.4.0 > win32 (client + GUI) folder and find Go.bat filRight-clickck on the file and edit it
3.3.1.1 Set COMPORT – to a number which found 'Device Manager'
3.3.1.2 Save and close window
3.4 All should work fine; now please put the card on their antenna and type commands
3.4.1 For Mifare cards READ: 'hf 14a reader' to read the info
3.4.2 For other low frequency: 'lf search' to check if the low frequency
3.4.3 For other high frequency: 'hf search' to check if high frequency
3.4.4 Other found here: https://github.com/Proxmark/proxmark3/wiki/commands
4 Go to pm3-bin-2.4.0 > win32 (client + GUI) folder and find Proxmark Tool.exe file
4.1 GIU – it is an alternative to the command line option
4.1.1 When GUI Opens, need to set up COM Port on the top of the screen
4.1.1.1 The same like set up in Go.bat file.
4.1.2 On the top of the screen, allows to commands, the same from client
4.1.3 On the left of the screen, there is an expandable tree of options
4.1.3.1 Please find in LF ' Low-Frequency Search' it does the same job like 'lf search.'
4.1.3.2 Please find in HF ' High-Frequency Search' it does the same job like 'hf search.'
4.1.4 Allows to view commands in the output window which is on the bottom of the app
4.2 Please try other options for other cards
5 Done!

Case Study 3 setup

Description:

The RFID hacking tool developed by [29]bishopfox.com for penetration testing. It allows still badge information from the distances to get access to the secured building. This tool reads cards allow frequency cards 125KHz like HID Prox and Indala Prox. The aim is to of this testing is to show how easy it is still information and clone card. There is information on online n how to create and use this tool as a pentester.

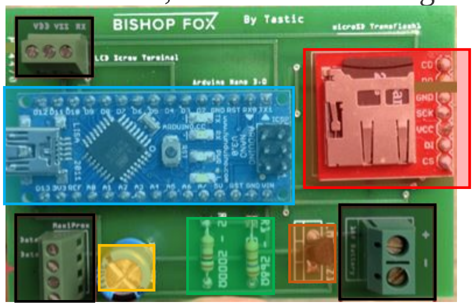
Components:

- Parts for antenna:
  - HID LONG RANGE READER MAXIPROX 5375 320(EUR)
  - Arduino Nano v3.0 (15EUR)
  - Breakout Board for microSD Transflash (9.16 GBP)
  - SanDisk 2GB MicroSD Card (6GBP)
  - Variable Voltage Regulator TO-92 (10GBP)
  - 2 resistors: 270 ohm and 2000 ohm 11(EUR)
  - 1 capacitor: 100uF 50V 13(EUR)
  - Serial LCD Module 20x4 Blue with White Backlight for Arduino 32(GBP)
  - Toggle Switch and Cover - Illuminated (Red) and ON/OFF button DC/AC 36V 2A 2(EUR)
  - Adafruit - Board Edge Mounting Kit - Pack of 4 - ID 1116 6(EUR)
  - 2/ 3 4 Pin 2.54mm PCB Universal Screw Terminal Block Connector 300V 6A GS019S 8(GBP)
  - AKKU Battery Box Holder Case 4 x AA with Leads Wire 6AA free shipping 7.50(GBP)
  - PCB (25EUR)
  - Soldering Station Hot
  - 12 AA Batteries 6 (GBP)
- Software required (All software provided in 2.CT Solution.zip file)
  - Arduino 1.0.1
  - Library with code sdfatlib (05Dec2011)
  - Arduino Sketch code

How to connect all components and use the software?

1 Download all software described in the above point

2 At first solder, the all hardware together starting from PCB custom board



2.1

2.2 Arduino Nano. – holds code from Arduino sketch

2.3 SD card reader. – holds data from cards

2.4 Two resistors – used to reduce current flow

2.5 Capacitor. – the component used to store energy electrostatically

2.6 2/3/4 Pins – allows connecting other components

2.7 TO-92 Regulator –used to regulate one or more AC or DC voltages

3 Connect screen to PCB board that just been solder with other parts.

3.1 Use 3 pins on the PCB

3.2 LCD must include RX pin other available for Arduino

3.3 LCD connected to first pins from the bottom

3.4 LCD RX pin connect to PCB board RX pin

3.5 LCD GND pin connect to PCB VSS pin

3.6 LCD VDD pin connect to PCB VDD pin

4 Connect batteries in series (+ to -)

4.1 Use 2 pins on the PCB

4.2 The positive (red) cable connect to button and another pin in button to positive pin on the board

4.3 The negative (black) connect directly to the board to the negative pin on the board

5 Connect HID MAXIPROX

5.1 Use 4 pins on the PCB

5.2 HID TB1-3 (Ground) pin connect to PCB negative(-) pin

5.3 HID TB1-1 (+DC) pin connect to PCB negative(+) pin

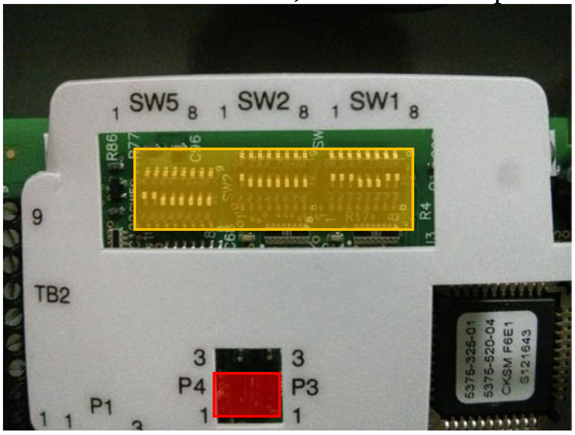
5.4 HID TB2-1 (Data0) pin connect to PCB Data 0 pin

5.5 HID TB2-3 (Data1) pin connect to PCB Data1 pin

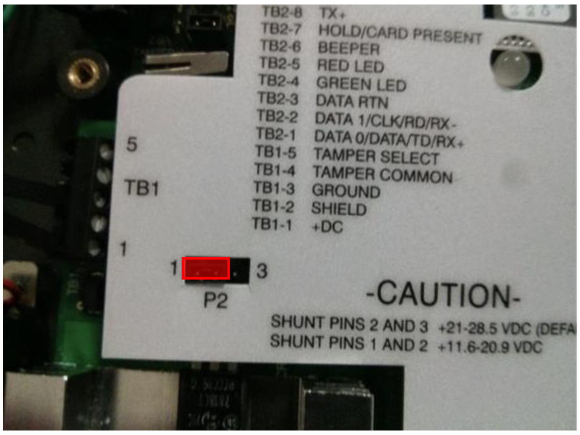
6 The last step is set up HID hardware as per below picture:

6.1 In yellow set up switches as per picture, in red P4 and 1 underP4 must be connected the same like P3 and 1 under P3, on the second picture 1 and P2

6.2



6.3



6.4

7 Power up, Done!

The issue during assembling components:

- LCD not compatible with hardware (standard Arduino screen)
- LCD burned during testing
- Arduino Nano burned during testing
- Components not solder
- End of cables that connect components not solder causing lack of connectivity