# Wi-Fi Hacking with a raspberry pi

**Project analysis – Term1**

Zukisa Dyantyi

3567302@myuwc.ac.za

Faculty of Natural Science

Department of Computer Science

Project adviser

Dr M.Norman

Faculty of Natural Science

Department of Computer Science

mnorman@myuwc.ac.za

## ABSTRACT

The objective of this project is to create Cyber Security awareness and show people how easily their devices can be attacked using small a device like a Raspberry Pi. The prototype that will be built for demonstration on the Raspberry Pi will automatically scan the 2.4 and 5.0 Gigahertz (GHz) Radio Frequencies (RF) used by Wi-Fi devices for communications in order to determine the hardware and software information of these devices. In some cases, where possible the prototype will attempt to connect to Wi-Fi networks that have weak encryption algorithms or authentication mechanisms in order to further elicit more hardware and software information. Once an attacker has obtained the hardware and software information of a device, the attack can then craft specialized attacks towards that device in order to achieve the attacker's desired goal. This report will provide more information about the hardware and software's necessary to carry out the project.

## 1 INTRODUCTION

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These digital attacks are aimed at accessing, changing, or destroying sensitive information; extorting money from user [1]. The objective of this project is to build a hacking tool on a raspberry pi that automatically scans the 2.4 and 5.0 Gigahertz (GHz) Radio Frequencies (RF) used by Wi-Fi devices for communications in order to determine the hardware and software information of these devices. In some cases, where possible the prototype will attempt to connect to Wi-Fi networks that have weak encryption algorithms or authentication mechanisms. The prototype built can attempt to connect to the network either using a brute force or other techniques of choice such as rainbow table.

### 1.1 Problem identification and justification

The number of IoT devices is increasing, that means the connection between these devices has increased. By design IoT devices are not built with security in mind, that the inherent capability to protect the information the IoT device processes or stores. Having many devices connected, there are high chances of digital attacks or cyber-attacks that can be launched against them. These devices connect, interact and exchange data. When there is breach between these devices there will be leaked of information and other personal stuff. The project objective is to educate peers around campus about the importance of strong password encryption.

## 2 LITERATURE REVIEW

After reading the paper on security of the Internet of Things (IoT) which came to the conclusion that outside attackers can gain access to the network through many different ways especially if the network is vulnerable for some reasons for example the network vulnerability is weak encryption [2]. The paper focused more on Wi-Fi networks secured with WPA2 which was considered to be secured network until October 2017 when Key Reinstallation Attack (KRACK) was announced. The paper state that WPA2 passwords are still vulnerable to attacks if weak passwords are used and it also shows that any device with outdated software are vulnerable to attacks [2]. IoT device users should avoid connecting to

suspicious Wi-Fi network and leave their devices unattended. To summarize the paper, it showed how multiple devices on the same network can be attacked because of one device venerability and variety of activities can be accomplished using raspberry pi for example controlling lights, turning any TV to smart TV etc., especially if the Raspberry Pi connected to the Wi-Fi network.

The book [3], the focus of this book is to turn a raspberry into hacking arsenal and it also focused to those who have low budget, small form hacking tool that is remotely accessible. Implementation of this was done by running kali Linux on a raspberry pi. They placed the middle attack; middle attack is when attacker is adversary places herself in the middle of the communication. Methods to exploit targets using attack tools are provided. Testing was done by running kali Linux OS on a raspberry pi and they used low power process that can run about one or two days on external battery. The testing was done from remote location and since they created a portable device security testing was done in different location.

# 3 USER REQUIREMENTS DOCUMENT

## 3.1 Introduction

As mentioned in the introduction of the project proposal the number of devices connected to the network has increased and so the chances of cyber-attacks are also high. Users of these devices use Wi-Fi networks to accomplish their tasks or to share information with their colleagues or peers. Some of Wi-Fi networks these users use have weak encryption which result the risk of being attack. This project will educate IoT device users the importance of strong password encryption either on their application such as E-mails or social media account, the project will focus more on Wi-Fi networks.

## 3.2 User's view of the project

This project is proposed by the Council for Scientific and Industrial Research (CSIR) and technical guidance will be provided by the CSIR team. Their view of the project. "The aim of the project is to building a tool on a raspberry pi that can automatically scan and attempt to connect to Wi-Fi networks with weak encryption.
Step 1: the candidate should build a tool on Raspberry Pi capable of connecting to Wi-Fi networks with basic Wi-Fi encryption key enabled on them.

Step 2: Using a phone, the candidate should setup dummy Wi-Fi hotpots using different encryption options and test that the hacking tool works as designed in step 1.

Step 3: Walk around campus with raspberry pi. The raspberry pi should attempt to connect to the network either using brute force or rainbow table or other techniques of choice.

Step 4: Document the findings and notify the owners of the Wi-Fi networks that were found to have weak encryption key."

## 3.3 Description of the project

Stakeholders (CSIR) require Wi-Fi hacking tool to be built on a Raspberry Pi. The objective of this project is to detect how many networks are available either around campus or within the building, which of these networks have weak and strong encryptions algorithms, which type of network protocol (WPA2, WEP or EAP) and what RF signal Wi-Fi network is broadcasting on either 2.0 or 5.0 Ghz. To extend the project, the hacking tool on the Raspberry pi should be able to extract information such as Wi-Fi network name, the Wi-Fi connected device MAC address, make of the device, software or operating system on the device. This raspberry should send all information to a computer that will store all the results.

## 3.4 Expectations from the project

The tool will be built on a Raspberry Pi should automatically scan and where possible attempt to connect to any Wi-Fi network detected either using a brute force or rainbow table or any technique of choice. The tool should work on any environment either around campus or within the building. This tool must retrieve as much as information about the Wi-Fi network as possible and the devices on that network, which Wi-Fi networks are available, type of encryption, Wi-Fi network authentication type, broadcasting RF and all the information should be displayed on command prompt. Figure 1 shows some expectations from the project and they are also functional requirements

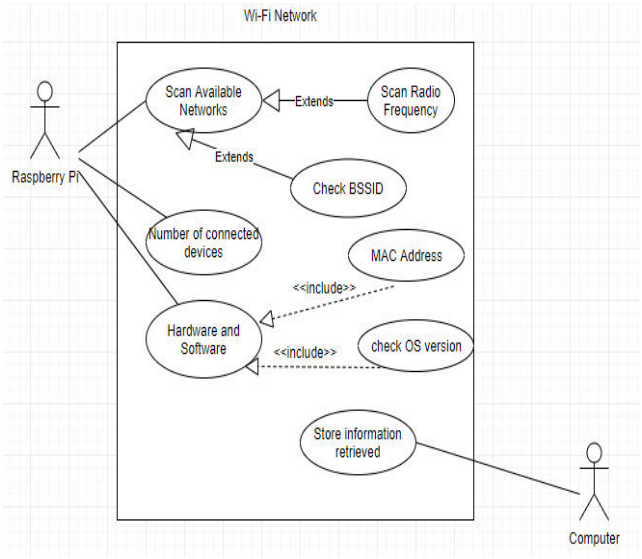


**Figure 1: Use Case, show functional requirements of the project.**

# 4 REQUIREMENTS ANALYSIS DOCUMENT

## 4.1 Purpose of project

Purpose of this project is to educate campus community about Cyber Security. Educate means users must understand and comply with basic data security principles like choosing strong passwords and backing up data. The number of IoT devices has increased to point

where security has to be an emerging priority. The project will determine the Wi-Fi network information and the type of devices connected to the network (hardware & software information of the devices). The project will be useful to teach Wi-Fi network owners and those who connect in it the importance of strong password encryption.

## 4.2 Scope of the system

The hacking tool will automatically scan and where possible attempt to connect to Wi-Fi networks with weak encryption. This tool will connect to the network using brute force. The tool built should retrieve information about network (such as what type of encryption used and type of network protocol), which networks are available, channel Wi-Fi broadcasting on and devices connected to the network. The hacking tool will not access the devices it will only give information such as the MAC address and Operating System of the device. The information about the network found weak by the tool will not be shared without the permission of network owner.

## 4.3 Objectives and criteria of the project

The project will be successful when these following set of objectives are met.

1. When Raspberry Pi is programmed to connect to Wi-Fi networks with weak encryption.
2. Raspberry Pi should manage to retrieve some information about the network and devices connect in it.
3. When the hacking tool can send all the information retrieved from the network to the external computer that will act as data center.
4. When the findings are documented and Wi-Fi network owners with weak encryption are notified.

## 4.4 Current system

The installation of Kali Linux and the update to the full version has been completed. Current state of the system is shown in figure 2.

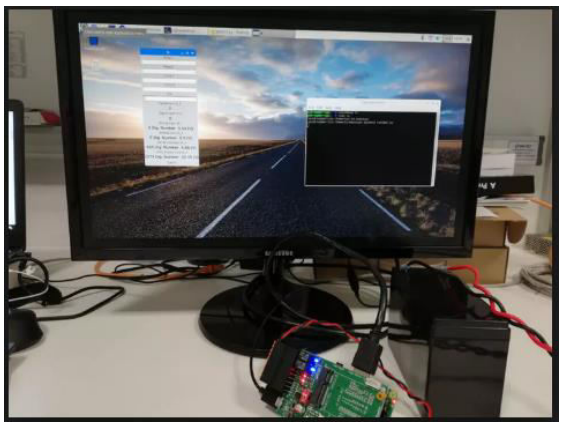

**Figure 2: Current system of hacking tool.**

## 4.5 Proposed system

The hacking tool should be able to detect which networks are available and check either the encryption used is strong or weak. The hacking tool should determine which security protocol used (e.g. WPA2, WEP etc.) and it should be able show channel Wi-Fi is broadcasting on. Figure 3 shows the sequence tool will be able to accomplish all expectations.

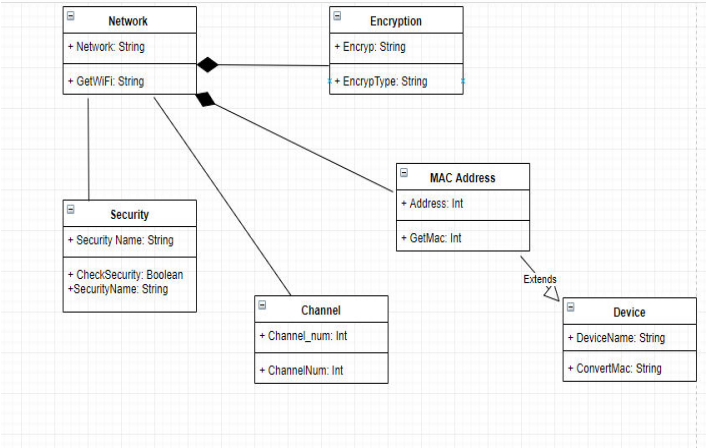


**Figure 3: UML Class Diagram, shows the objects, their attributes, their operation and the relationship among them.**

# 5 NON-FUNCTIONAL REQUIREMENTS

## 5.1 Response time

The hacking tool built should not take more 45 seconds to display available networks, type of security network is using and it should take less than 1 minutes to determine whether the network used weak or strong encryption and channel network broadcasting on.

## 5.2 Reliability

Equipment and tools that will be used to carry out this project will be tested separable before integrated together. The project will be tested by using dummy Wi-Fi hotpots that will be set using mobile phone.

# 6 USER INTERFACE SPECIFICATIONS

According to stakeholders and some research I have done the user interface should be on command prompt, it should be a simple terminal-based application. The interface of this project will be the terminal display. The terminal should display all the information required by the project (e.g. available networks, type of security protocol network use etc.). Figure 4 shows how the user interface will be like.

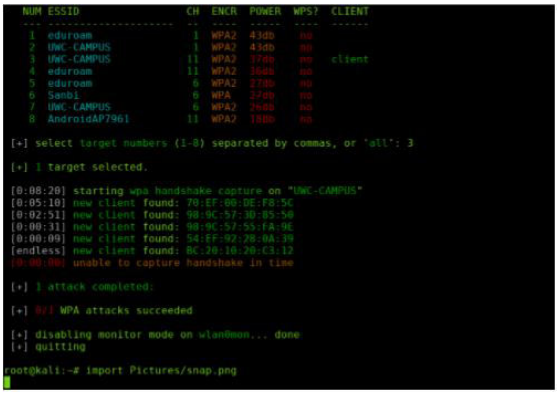


**Figure 4: Expected User Interface.**

# A Appendix

## A.1 Project plan

Figure 5 shows the plan for the project throughout the year, the project plan includes March.


**Figure 5: Project plan for 2019.**

# References

[1] CISCO, "CISCO/SECURITY," CISCO, 2018. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html. [Accessed 14 February 2019].

[2] J. F. a. S. A. Tyler Williams, "Digitalcommons.murraystate.edu," 2017. [Online]. Available: https://www.google.com/search?rlz=1C1AVFC_enZA833ZA833&ei=myOCXMrnCeGU1fAPkqOooAI&q=security+of+the+internet+of+things%28iot%29+murray+state+university&oq=%22security+of+the+internet+of+things%28IoT%29%22+murray+state+&gs_l=psy-ab.1.0.33i160.6166.12427..1. [Accessed 03 March 2019].

[3] A. L. a. J. Muniz, Penetration Testing with Raspberry Pi, Birmingham,UK: Packt Publishing Ltd., 2015.