Snooping IoT Devices with Raspberry Pi

SAMUEL GODWIN ABU

Thesis presented in fulfilment
of the requirements for the degree of
Bachelor of Science Honours
at the University of the Western Cape

Supervisor: **Dr Michael Norman**
Co-supervisor: **Mr Muyowa Mutemwa**
Co-supervisor: **Mr Francois Mouton**
version date: April 17, 2018

Declaration

I, Samuel Godwin Abu, declare that this thesis *"Snooping IOT Devices with Raspberry Pi"*, is my own work, it has not been submitted before for any degree or assessment at any other university, and that all the sources I have used or quoted have been indicated and acknowledged by means of complete references.

Signature:...................... Date:......................

Acknowledgement

This thesis was done with the support of Dr Norman. The weekly meetings and updates were of immense help. Thank you for your patience and awesome communication skills. I will also like to thank the CSIR team of Muyowa Mutemwa and Francois Mouton. Grateful for the updates and support.

Abstract

This paper is written to highlight the process of Snooping IoT devices using a Raspberry Pi. The purpose of the project is to create Cyber Security Awareness and to demonstrate how easy it is to identify IoT devices over a WiFi network. The aim of this project is to build an IoT snooping tool on a Raspberry Pi and track how many IoT devices the snooping tool detects in the process. The hardware and software tools necessary to carry out this project will be documented. The process flow of the project will also be clearly outlined. The scope of the project is restricted to devices connected to a WiFi network like the WiFi-Support(Limited-Period) or the UWC-Campus.

Contents

List of Figures

1 User Requirements Document

1.1 Introduction

The world today is a world filled with countless connecting devices. Every other adult and teenager has a phone with internet connecting capabilities. A lot of people quickly connect without a second thought to WiFi networks that a not password protected not knowing the security risks they expose their devices to. According to Anthony Spadafora [1] writing for 'IT Pro Portal', Electronics manufacturers, Samsung is working on integrating the company's offerings under one application that will allow for seamless connection experience at home, at the office and even in cars. Such announcements make it easier to believe that there will most likely be more connecting devices all around us in the future. This project will showcase some security risks people with devices can face over a WiFi network.

1.2 User's view of the project

This project is done in conjunction with CSIR (Council for Scientific and Industrial Research). Below is a direct quote from the CSIR team.
"The aim of this project is to have the candidate build an IoT snooping tool on a Raspberry Pi and track how many IoT devices the candidate comes into contact with as they walk around campus.

- *Step1: Build an IoT snooping tool on a Raspberry Pi. Build a Command and Control machine which will communicate with the Raspberry Pi and keep track of information that is found.*
- *Step 2: Power the Raspberry Pi using a Power Bank.*
- *Step 3: Test and confirm that the snooping tool functions as designed.*
- *Step 4: The candidate should walk around campus especially in busy areas such as the Student Centre during lunch or lecture halls. The snooping tool should get the name of the device and send the information back to the Command and Control machine. The Command and Control machine should keep track of how many distinct devices of a certain type were found. If possible remove duplicates.*
- *Step 5: Document findings and educate students around campus."*

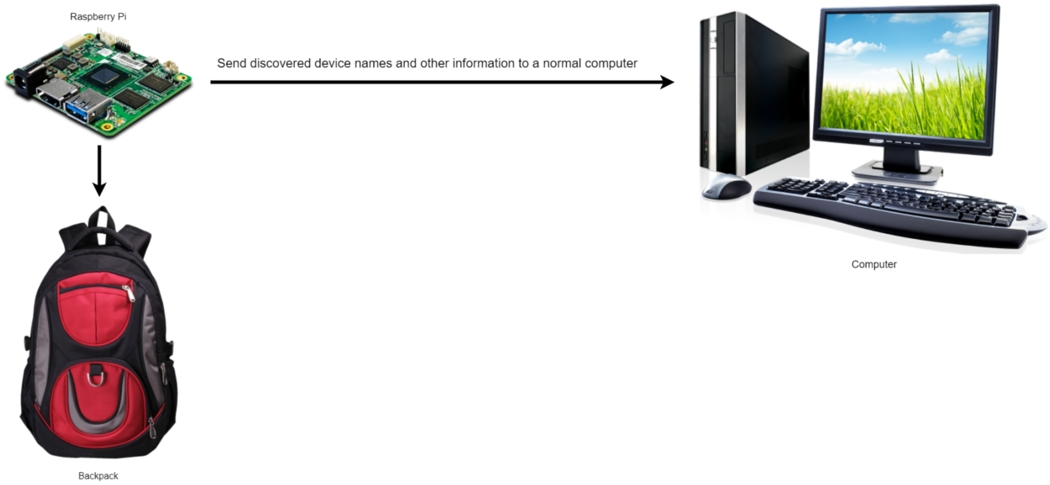
Raspberry Pi
Send discovered device names and other information to a normal computer
Computer
Backpack

Figure 1: A simple illustration of the snooping tool

1.3 Description of project

The stakeholders (CSIR) require that an IoT snooping tool should be built on a Raspberry Pi. This Raspberry Pi will be used as a penetrating device to obtain safe information from penetrated devices over a WiFi network. This safe information will then be transmitted to a Command and Control center which is another computer. The stakeholder wants a list of encountered devices during the snooping. Figure 1 illustrates an overview of the task.

1.4 Limitations

The hardware required to move around campus and conduct the snooping experiment may not be available but it does not necessarily stop the process of completing the project. The snooping tool thus comprises of the Raspberry Pi and a desktop monitor. These hardware tools require a power connection and thus limits the experiment to be conducted in one room, provided there are connected devices in the room. Another limitation might be setting up the Command and Control center but there might be a way around this hurdle.

2 Requirements Analysis Document

2.1 Purpose of project

The purpose of this project is to raise awareness about cyber security. It also gives me a chance to gain some valuable practical learning experience. Cyber security is not something users of devices often think about although some do. Functionality is what most users are more concerned about. The occurrence of data breaches has forced security to be a merging priority. This project will show a scenario of how safe information can be obtained from IoT devices connected over a WiFi network with the intention of alerting users to issues of cyber security. This project will also show that a small device like the Raspberry Pi that can fit in a small backpack can be used as a penetration tool on connected devices over a WiFi network.

2.2 Scope of the system

The project will only cater for IoT devices connected over a WiFi network. The snooping tool will be implemented to function over a WiFi network. Snooping over a Vodacom or Telkom network should be considered outside the scope of this project. The snooping tool is not intended to perform in a malicious manner.

2.3 Objectives and Success criteria of project

The project will be deemed successful if the Raspberry Pi is successfully programmed to snoop connected devices over a WiFi network and keep track of some safe information about the devices encountered during the process. Another objective would be to set up the Raspberry Pi to send this collected and compiled safe information to another computer that will act as a Command and Control center.

The extent of snooping and the safe information currently is the type of discover-able IoT devices found over a network.

2.4 Designer's interpretation of user requirements

The stakeholders(CSIR team) listed a number of steps with which to proceed with the project. They are listed in the "User's view of the project" section of this document above in page 1. Some of the hardware needed for a more accurate execution of the project are not currently available(such as Power Bank for USB Portable Power Supply). Hardware currently available are:
1. Raspberry Pi (see Figure 2)
2. 16GD micro SD Card (see Figure 3)
3. Desktop Computer at the Honours lab.

The Raspberry Pi does not have a display of its own. It is currently connected to a desktop monitor at the Honours lab. This means that the Command and Control center (Desktop Computer) and Raspberry Pi have to share the same monitor. So work cannot be carried out on both Raspberry Pi and Desktop computer (Command and Control center) at the same time. Internet access is also a necessity for the project and this is readily available at the Honours lab.

Figure 2: the Raspberry Pi

Software is also needed to execute this project. After meeting with the stakeholders, it was decided the Kali Linux operating system would serve best. Further research showed that the initial basic installation of Kali Linux OS on a 16GB micro SD card may not have all the functions required to commence with the experiment.

The 16GB micro SD card provided by the Department already had an operating system on it but the OS was not Kali Linux. The first task was to find a way to format the 16GB micro SD card and then install the basic Kali Linux OS which amounted to 4GB in size on that SD Card. See Figure 3 for a visual depiction of a micro SD card

Figure 3: the micro SD card: the hard drive of the Raspberry Pi

2.5 Current System

Formatting the SD card was a success. Installation of Kali Linux and update to the full version was completed. The only drawback now is, the 16GB micro SD card is almost full. The full Kali Linux installation occupies 14GB of the 16GB micro SD card. This may not necessarily be a big issue but it is worth noting that the initial SD card is almost full and only installations have been done so far(see Figure 4). The Raspberry Pi currently accesses the internet via the Ethernet cable at the lab.

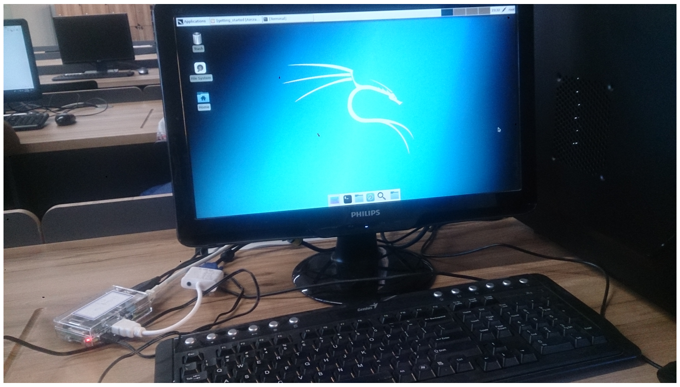

Figure 4: current state of snooping tool

2.6 Proposed System

The snooping tool should be able to detect access points in a network. It should also detect connected devices on a network. The snooping tool should also be able to communicate with the Command and Control center (a desktop machine).

3 Conclusion

Current requirements gathered are for a simple implementation of the project. This simple implementation would be a snooping tool without a power bank. Chances are if the tool can snoop while plugged to power(electricity), snooping on battery power can become a possibility.

References

[1] A. Spadafora. (2018, Jan.) Samsung lays out its vision for the future of iot. https://www.itproportal.com/news/samsung-lays-out-vision-for-future-of-iot//. Accessed: 2018-04-15.

[2] S. S. A. N. N. F. Noah Apthorpe, Dillon Reisman, “Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic,” https://arxiv.org/pdf/1708.05044.pdf/, Aug. 2017, accessed: 2018-04-15.

[3] S. Shenker, “Fundamental design issues for the future internet,” *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 13, pp. 1176–1188, 1995.

[4] M. Jurečka, “Raspberry pi based traffic counting system.”

[5] M. Niket, D. Jaiswal, and P. Y. B. Mane, “Design and implementation of raspberry pi based remote home security and appliance control system.”