Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux

Eiman Al Neyadi, Shaima Al Shehhi, Ameera Al Shehhi, Noora Al Hashimi, Mohammad Qbea'H, and Saed Alrabaee
United Arab Emirates University, Collage of IT, Department of Information Systems and Security
{201306078,2014020048,201401662,201501355,mqbeah,salrabaee}@uaeu.ac.ae

***Abstract*—Free wireless Internet is getting so common that we're starting to expect it pretty much everywhere we go from coffee shops to airports, which is great in a lot of ways but it also means there are more opportunities for hackers to fool People because anyone can sit down somewhere set up a mobile hotspot or wireless network of their own and give it a believable name like an airport name, and if someone use their network they can watch and record all the network traffic including any usernames password an credit card details. This report introduces testing public Wi-Fi security using Rasbperry pi and Kali Linux, by performing attacks including DNS Spoofing, Wi-Fi password Cracking, Man in the Middle and Evil Twin, it also discusses Public Wi-Fi vulnerabilities and how to prevent or avoid such attacks.**

I. INTRODUCTION

In today's modern world, public Wi-Fi is available widely in majority of public places, such as: Airports, restaurants, hotel rooms, coffee shops, etc. Most of us jump on a public Wi-Fi network because it's free and a convenient way to check emails and catch up on work while on the go. However, most individuals donot re-alize that network traffic sent through public Wi-Fi can be captured or intercepted easily[1-3].

Wi-Fi is a technology that helps you access the Internet on your handheld device it does it over the air or wirelessly IEEE or the Institute of electrical and electronics engineers defines the Wi-Fi standard under the family of 802 networking specifi-cations where 802.3 defines the Ethernet, 802.15 defines the Bluetooth and 802.11 defines the Wi-Fi networking standards. Wi-Fi network is filled with the help of several hardware components like wireless access points or routers and us-er devices like mobile phones, tablets, laptops, etc. Which are equipped with Wi-Fi adapter. On the other hand the wireless router is connected to the Internet via a physical connection there is with the fiber, the Wi-Fi router then connects to the end devices via radio waves to establish an end to end Internet connection, where the wireless router receives the data from the Internet translates it into the radio signals and send it over the wireless network to the connected devices the same process also happens in reverse with the astounding increase in the Internet traffic we have seen an amazing growth in the bandwidth and speed available to the end user from 1995 till the end of 2016 the Internet users have grown from 16,000,000 to more than 3000 million[4].

According to Norton Report, they found that 68% of public Wi-Fi users are vic-tims to cybercrimes, "It can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos and so on." Vanhoef's report said, this was in 2013. Nowadays, the technology has developed rapidly, new cyber-attacks, viruses and exploits are constantly being created and found [5].

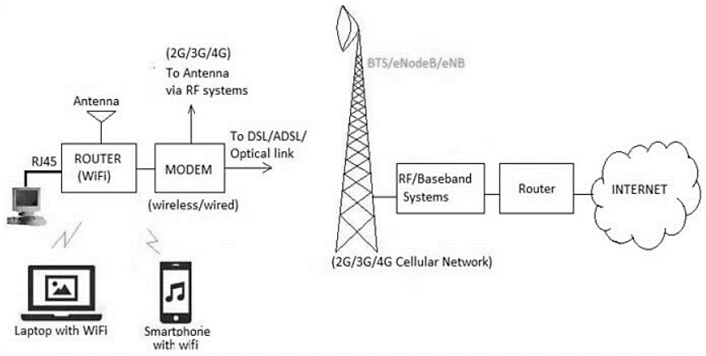

Fig. 1. Wi-Fi network topology (Source: softwaretestinghelp.com)

Another Survey was done on U.S. titled with (Do you ever use unsecured public Wi-Fi networks?) The results found as shown in (Fig.2). It states that majority of them, 81% will still connect to public Wi-Fi, even though it has many security risks, which is an alarming percentage, through this report we hope to shed a light on this why it's vital to avoid Public Wi-Fi networks or protect the connection in case it can't be avoided, through demonstrating some attacks that hackers can perform to intercept and monitor network traffic to ultimately steal valuable in-formation [6-7].

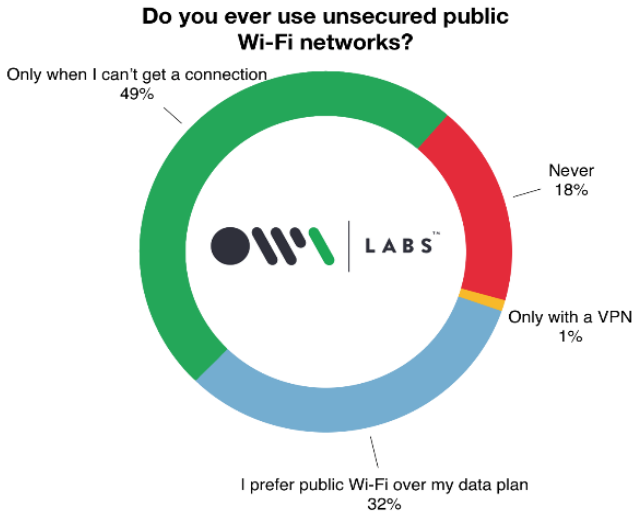

Fig. 2. Survey results (Source: Norton.com)

978-1-7281-9789-0/20/$31.00 ©2020 IEEE

II. Background Information

Before we get into testing, we'll discuss our main components which are Raspberry pi, Kali Linux respectively.

Raspberry pi is essentially an affordable credit card sized computer that can easily be plugged into a monitor and uses standard keyboard and mouse. It capable of performing all task you'd expect a normal desktop computer to do from Internet browsing, to running software like Word documents to programing with languages like Python and Scratch. It's designed and made by the Raspberry pi foundation to make computer programing easy and accessible by kids and adults alike. It can Run Raspbian which is a Linux based OS, Windows 10 IoT core, Linux, Ubuntu core and others.

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing, computer forensics, security research and auditing and reverse engineering, it was released on 13th March,2013 as a rebuild to its predecessor BackTrack Linux. It has more than 600 penetration testing tools, It's free and open source Git tree meaning anyone can access the ulter packages to their specific needs, supports wide-ranging wireless devices, Kali adheres to the Filesystem Hierarchy Standard, allowing Linux users to easily locate binaries, support files, libraries, etc. It's developed in a secure environment, funded and maintained by Offensive Security

III. Methodology

We choose Raspbery pi 3 b+ model to build our independt hacking machine.

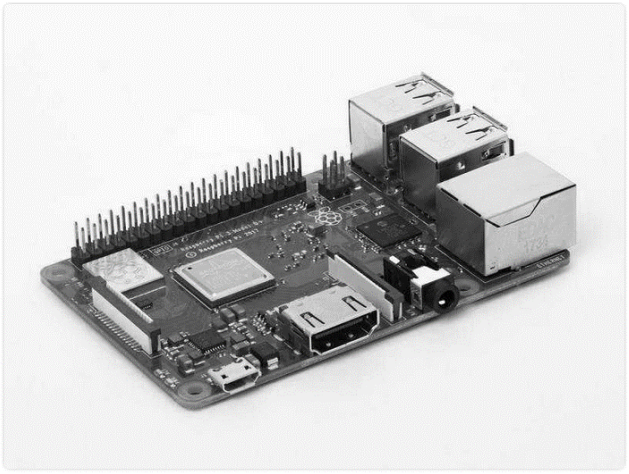

Fig. 3. Raspberry Pi 3 B+ model (Source: raspberrypi.org)

Technical Specification Include: 1.4GHz 64-bit quad-core processor, dual-band wireless LAN, Bluetooth 4.2/BLE, faster Ethernet, and Power-over-Ethernet support (with separate PoE HAT).

We downloaded and stored Kali Linux ARM Image version 2019.4 for Raspberry Pi 3 on a 32GB SanDisk extreme micro SD card. We attached a TFT LCD screen to the Raspberry Pi. Then we inserted the micro SD card into the Raspberry Pi plugged the Pi to a monitor via HDMI cable and powered it up using an external 30000mAh power bank. Once the OS booted up, we plugged in our mini keyboard that has a touchpad for screen control. From here we proceeded to fix some issues including displaying the output to the attached screen, installing missing tools for our test attacks and installing a Wi-Fi adapter.

Fig. 4. Our Implementation.

Main components to note here are (Kali Linux OS, display screen, keyboard and touchpad for controls, independent power supply and Wi-Fi adapter to capture Wi-Fi network traffic)

Reasons why we choose this set-up is because it's affordable all hardware costs were approximately 400Dhs, it's less conspicuous in public settings, but most im-portantly it's a portable independent hacking machine.

IV. Testing

In this section, we'll discuss what some of the attacks that are possible on a public Wi-Fi network with a step by step guide on how we per-formed them and how ultimately, they lead to compromising confiden-tial information.

Man in the Middle attack, is an attack where the attacker come in between two victims who are communicating with each other, attacker may alter or do some changes on the communication while the victims think that they are talking di-rectly to each other.

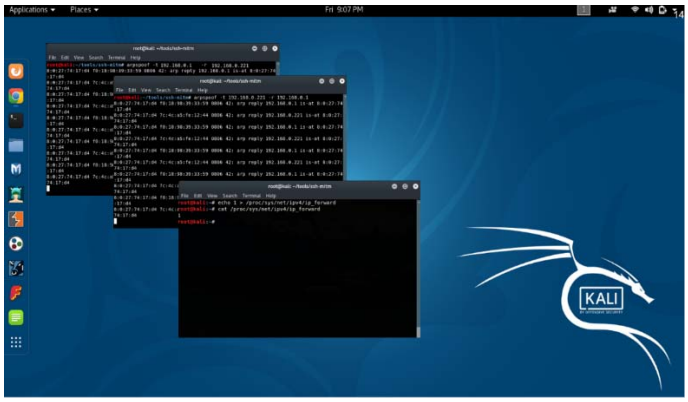

Fig. 5 Man in the Middle attack demo

Steps:

1. **Enter Monitor Mode:** enable monitor mode on the Wi-Fi adapter to capture ALL Wireless traffic.

   By inputting this code into a terminal:
   ifconfig
   To see the network interfaces. You should be choosing the wireless one.
   airmon-ng check kill
   To kill the processes that could interfere with the airmon-ng suite.
   airmon-ng start wlan0
   where wlan0 is the wireless interface.

2. **Switches & Spoofing:** Modern switched keep a CAM table (Content Addressable Memory) that basically maps IP addresses to MAC addresses. In order to capture traffic, we need to intercept the connection which is done by corrupting CAM table of both client and server using ARP Spoofing.
3. **ARP Spoofing:** Our goal to get client to believe we are the server & vice versa.

   - Open Three Terminals.
   - 1st terminal window: Arpspoof Client to Server
     Using this code:
     arpspoof -t 192.168.1.116 192.168.1.118
     where:
     arpspoof -t *client IP Address* *server IP address*
   - 2nd terminal window: Arpspoof Server to Client.
     By swapping IP addresses in the above code.
   - 3rd terminal window: Pass Packets with IPforward.
     Using this code:
   - Sniff the Traffic with wireShark.

Evil twin attack, an attack that relay on the fact that devices can see the SSID only of wireless network. Essentially duplicate a wireless network by spoofing the network name and its MAC address in the hope that clients will connect to your access point.

Steps:

1. **Connect to Wireless Network.:** to gain Internet access.
   In a terminal type …. Where wlan0 is your interface name.
2. **Start Airmon-Ng wlan0:** to Enter Monitor Mode.
3. **Start Airdump-Ng wlan0:** to gather information from network traffic.
4. **Identify target, Create a New AP with Same SSID & MAC Address.**

Using this code:

airbase-ng -a <BSSID here> --essid <ESSID here> -c <channel here> <interface name>

5. **Force target to disconnect from actual network so they'd connect back to the fake AP we created.**
   Using this code:

aireplay-ng --deauth 0 -a <BSSID> mon0 --ignore-negative-one

6. They'll recconnect to the fake network, where multiple further attacks can be done like DNS Spoofing.

V. Solution

Now, just because a password is required to log in, doesn't mean that online activities are encrypted. There are few precautions should be taken to keep this sensitive information safe, such as:

1- Use Virtual Private Network (VPN): because data will be strongly encrypted.
2- Use Secure Sockets Layer connection: it adds a layer of encryption to your communication.
3- Make sure to turn off sharing: because most of the time when people do connect to public Wi-Fi do not share anything, so it is preferred to turn the sharing off.
4- Turn off the Wi-Fi (when not needed): the Wi-Fi hardware in your device will still transmit data between network withing range, even if you are not actively connected to a network.
5- Protect your device: by installing anti-virus and keeping it up to date, by doing the previous points, and be careful with what type of data you are sharing or accessing or entering when connecting to public Wi-Fi.

These are some possible public Wi-Fi security precautions, it doesn't eliminate the issues, but it could reduce them, even individuals who take all the precautions are going to face some issues from time to time.

VI. Summary

We introduced Raspberry pi, Kali Linux and we had some statistics. and we discussed why public Wi-Fi is vulnerable and the possible attacks that are made possible due to such lack of security. We have done some implementation and listed some results not to mention that we included some solutions to prevent some of the attacks. However, the best way to protect your information is to avoid accessing sensitive information or performing sensitive transactions when connected to public Wi-Fi.

Disclaimer: Gaining unauthorized access to computer systems or privileged Information is illegal and can lead to extreme consequences, people have been sentenced to years of imprisonment because of hacking, but it can be legal if done with permission now.

REFERENCES

[1] . Ftp1.digi.com. (n.d.). *An Introduction to Wi-Fi*. [online] Available at: http://ftp1.digi.com/support/documentation/0190170_b.pdf [Accessed 2 Dec. 2019].

[2] 2. Halfacree, G. (n.d.). *THE OFFICIAL Raspberry Pi Beginner's Guide How to use your new computer*. [online] Raspberrypi.org. Available at: https://www.raspberrypi.org/magpi-issues/Beginners_Guide_v1.pdf [Accessed 2 Dec. 2019].

[3] 3. Buchanan, C. and Ramachandran, V. (n.d.). *Kali Linux Wireless Penetration Testing*. [online] Illshiz.com. Available at: http://www.illshiz.com/ethical_hacking/Kali%20Linux%20Wireless%20Penetration%20Testing%20Beginners%20Guide%20Third%20Edition.pdf [Accessed 2 Dec. 2019].

[4] 4. Hu, H., Myers, S., Colizza, V. and Vespignani, A. (2007). *WiFi networks and malware epidemiology*. [online] Pnas.org. Available at: https://www.pnas.org/content/pnas/106/5/1318.full.pdf [Accessed 2 Dec. 2019].

[5] 5. Caneill, M. and Gilis, J. (2010). *Attacks against the WiFi protocols WEP and WPA*. [online] Pdfs.semanticscholar.org. Available at: https://pdfs.semanticscholar.org/ebf5/defff09c27fd77421c32a176ecc05cd73983.pdf [Accessed 3 Dec. 2019].

[6] 6. Sidiropoulos, N. and Mioduszewski, M. (2012). *Open Wifi SSID Broadcast vulnerability*. [online] Os3.nl. Available at: https://www.os3.nl/_media/2012-2013/courses/ssn/open_wifi_ssid_broadcast_vulnerability.pdf [Accessed 3 Dec. 2019].

[7] 7. Cheng, N., Wang, X., Cheng, W., Mohapatra, P. and Seneviratne, A. (2013). *Characterizing privacy leakage of public WiFi networks for users on travel*. [online] Available at: https://www.researchgate.net/profile/Aruna_Seneviratne/publication/261060472_Characterizing_privacy_leakage_of_public_WiFi_networks_for_users_on_travel/links/560e32d008ae2aa0be4a8265/Characterizing-privacy-leakage-of-public-WiFi-networks-for-users-on-travel.pdf [Accessed 3 Dec. 2019].