INSE 6120: Security Evaluation Methodologies
Project: Free Wifi / DRAFT

Lino Antonio Nava Romero
Concordia University
Student ID: 27655975

IMPORTANT:

- All information related to this project is located in: https://github.com/ptkrm/INSE6120/ , this public repository contain, code samples (work in progress), evidence (work in progress) and report.

- Part that use terminal font: `terminal.`Means information just explanatory for progress report, not include in final report or expanded.

Abstract - This paper concern about the possible problems involved in using free wifi hotspots, are we sure this free connection are secure? Or in what kind of danger user could be involved?. In this paper We describe possible problems related to Free Public Wifi Hotspots and perform passive test against of them. Additionally We encourage to users to start to use a VPN solution when they required to use this hotspots.

1. INTRODUCTION

In recents years, business are offering free wireless internet access as a way to attract customer also We can found theses hotspots in public spaces like airports and parks, even now it is common to hear from customer is there is available free internet access and in some cases business that do not provide these services, customers leave the place. But nobody stop to think, Are these services are really free? Or more worrying Are these connections secure?.

`{-Pending: Expand introduction-}`

2. BACKGROUND

In this sections, We are going to define some basic concepts required to understand our research.

A. Wifi Hotspot

A generally public space like business, parks, restaurants, hotels, Where user can access to internet via Wireless (WiFi). Usually they are free and user just required to login through a Captive Portal to start using the service.

B. Captive Portal

It is usually the first website after user connect to the Wifi Hotspots where user is required to authenticate before access to the network is allowed. Often We observe here user have to accept the Terms of Services (ToS) but in some cases they required to give personal information like Name, Phone Number, Email or Postal Code to start using the service.

Generally after user accept condition, the MAC Address of the users device is save it into the Wifi Hotspot and allow it to use Internet, to avoid unauthorised users to access to the services, they just redirect the traffic to this portal or to Walled Garden.

C. Walled Garden

Also know as Closed Ecosystem are allowed sites without identification in the Captive Portal where users can access, is called closed ecosystem because Hotspot providers control what sites users can access, usually these are company information or services provider information.

`{-Pending: definitions, why are we concerned-}`

3. SECURITY CONCERNS

A. DNS HIJACKING

Is refers to the practice of alter a legit Domain resolutions queries, usually when is made it by a malicious users can use to do a phishing attack (steal information) or by companies to block or lead the user to another website with advertisement, here we can found two cases.

A.1 DNS Redirection: Here we refers just went a valid and active domain is redirected to another one, for example: from http://google.com to http://yahoo.com. Security concerns happen because It is possible to redirect the traffic to a very similar fake site that original user want to access and user security and privacy can be compromised.

A.2 NXDOMAIN: Also know as Non-Existent Internet Domain Names, this condition occur when is unable to resolve a specific domain, usually because it was misspelled or nonexistent. The problem occur when services providers or malicious users redirect the traffic to another server to all the NXDOMAIN responses, in some cases the redirection just lead to a website full of advertising but think about a user who want to access to his personal email account, for example **http://gmail.com** and misspelled a put **http://gmaill.com** (not real domain), this can be a very serious trouble.

B. INFORMATION GATHERING

Some Wifi Hotspots required to ingress any kind of personal information to start using their services, usually this information could be our Name, Phone Number, Email Address or Postal Code. But users should know what they do with our data, this sometimes is explained into their Terms of Services but most of the user do not read them.

Additionally they can retrieve and store information about the equipment We use to access to their network or even spy our browser history.

C. TERMS OF SERVICES

Generally We just require to agree with them to start using the internet services, but not so many people stop to read them before accept, the problem here is because maybe We are accepting some clauses than allow these company to share our personal information (very related to Information Gathering concern) or they keep our browser history record during that session and sell it to another companies. Projects like Terms of Service Didn’t Read (***https://tosdr.org/***) encourage users to read them, this project focus on Web Services but similar clauses could happen on Wifi Hotspots.

D. *CONTENT INJECTION*

E. ROGUE ACCESS POINTS

4. METHODOLOGIES

This project not focus on how to perform attack against this Wifi Hotspots, We just want to know what of previously mentioned security concerns happen with more or less frequency.

There are some specific rules that We must apply in our project:

1) Just perform test against business wireless hotspots (restaurants, coffee shop, shopping malls, etc) and not against home private connections or public connection misconfigured.

2) Wireless hotspots without password requirement (or with a captive portal that require a username and password) this is trying to mimic the behaviour of final user who require free internet. But hotspot that require personal information to give you access are ok.

3) We are not going to execute any attack agains the AP (Access Point) or STA (Stations), that means Death authentication, Man in the Middle or crack password. But networks scanner, change my adapter setting is allow.

{-Pending: Next to small explanation about our tool, explained better for final report-}

Information gathering about hotspots is going to perform in two steps, one is manual where we capture (copy) information related to ToS or fields required to access to these hotspots (if apply).

Second step is using the collecting information tool, this tool consist in two application, server.js and client.py:

1) server.js: a node.js code that run in a external server that receive information from the hotspots and send some instruction to the client, for example one test to detect DNS HIJACKING is to compare how Server and Client resolve domains and NXDOMAIN just trying to access fake domain by client.

2) client.py: a python code that is in charge to perform test using hotspots configuration and collect information to storage into server,js for further analysis later.

Both tools are in this moment into development phase and are tested using a lab environment.

The lab environment consist in:

- A Mikrotik Routerboard RB2011UiAS-2HnD-IN: cheap router that provide hotspot functionality which include tool that allow us to create captive portal, walled gardens, DNS redirection and try different security configuration.

- A Raspberry PI running OpenWRT (https://openwrt.org/) and WifiDog (http://dev.wifidog.org/), this configuration is commonly found into “Île Sans Fil” hotspots, inclusive WifiDog a captive portal tool is develop for the “Île Sans Fil” technical team.

This use to help me to improve the tool at home, source code from the tool can be founded into “Code” folder in github repository, very experimental in this moment.

Configuration file used in Labs will be uploaded in future.

5. FIELD STUDIES RESULTS

{-Pending: Result analysis, next to small explanation **-}**

A. WARDRIVING

Here we are going to summarize how many hotspots are open, using wardriving techniques to collect information, into information collected are: SSID, BSSID, Security Type (for project we just focus on OPEN), Latitude and Longitude.

This information is going to use it, to calculate how is the ratio between open and secure networks, theses files are going to be released on final report but for preserve residential user privacy, all information that contains for example router that contains default ISP providers name (BELLXXX, VIDEOTRONXXX) are going to be deleted.

This step is performed using Kismet (Wireless Network Sniffer)

In this moment some “Evidence” are located into project repository.

B. TESTING

Here is just the analysis the information collected by the tools and manually, just selected a sample of hotspot a describe it (Case of studies).

6. RECOMMENDATIONS

One solution to reduce risk of using free wifi hotspots is to start using a VPN solution, We can define VPN (Virtual Private Network) as an intermediary server between the user and the destination, that means every traffic coming from the user is routed by the VPN server to the destination that makes the traffics appears coming from the VPN server and not by the user (user IP is masked). One interesting fact is the traffic between the user and the VPN server is encrypted, thats mitigate eavesdropping attacks and prevent DNS request alterations.

Some VPN providers like ExpressVPN (https://www.expressvpn.com/) or Private Internet Access (https://www.privateinternetaccess.com/), allow to access to this service paying an affordable monthly rate and their application (including configuration part) is very easy and straightforward to start using as soon as possible but it is required We trust in these company that they do not alter, spy or collect our traffic.

Additionally more skilled user can deploy their own VPN Server (common using OpenVPN), a VPS (Virtual Private Server) popular ones are Digital Ocean (https://www.digitalocean.com/) or Amazon EC2 (https://aws.amazon.com/).

We encourage users that become more concern about their security using theses free hotspots, changes of their habits like avoid visiting website that require your credentials like banks and email accounts. Always verify sites authenticity (usually in the browser bar, it is possible to observer a small lock who provide all the important information for the website) or much better start using HTTPS Everywhere extension (https://www.eff.org/https-everywhere).

7. CONCLUSION

{-Pending-}

8. REFERENCES

- Tunneling for Transparency: A Large-Scale Analysis of End-to-End Violations in the Internet. David Choffnes, Alan Misove, Taejoong Chung

- Website-Targeted False Content Injection by Network Operators, Gabi Nakibly, Jaime Schcolnik, Yossi Rubin

- Wireless Hotspots: Current Challenges and Future Directions, Anand Balachandran, Geoffrey M. Voelker, Paramvir Bahl

- Authenticating Ubiquitous Services: A Study of Wireless Hotspot Access, Tim Kindberg, Chris Bevan, Eamonn O'Neill, James Mitchell, Jim Grimmett, Dawn Woodgate

- Wireless hotspots: petri dish of wireless security, Bruce Potter

- Measuring Trust in Wi-Fi Hotspots, Tim Kindberg, Eamonn O'Neill, Chris Bevan, Vassilis Kostakos, Danaë Stanton Fraser, Tim Jay

- Security Analysis on Public Wireless Internet Service Models, Kenji Ohira, Ying Huang, Yasuo Okabe, Kenji Fujikawa, Motonori Nakamura

- "Free" Wi-Fi from Xfinity and AT&T also frees you to be hacked, http://arstechnica.com/security/2014/06/free-wi-fi-from-xfinity-and-att-also-frees-you-to-be-hacked/

- Why I don't use Airplane WiFi, https://blog.joemanna.com/dont-use-airplane-wifi-security/

- Terms of Service Didn't Read - https://tosdr.org

- Comcast Wi-Fi serving self-promotional ads via JavaScript injection, http://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/

- Public Wi-Fi hotspots - know the risks, http://www.welivesecurity.com/2014/11/14/public-wi-fi-hotspots-know-risks/

- If You Are Using Hola VPN, You Need To Know This (Hint: Botnet And Bandwidth), http://www.techtimes.com/articles/56706/20150530/if-you-are-using-hola-vpn-you-need-to-know-this-hint-botnet-and-bandwidth.htm

- How to stay safe at a public Wi-Fi hotspot, http://arstechnica.com/security/2011/01/stay-safe-at-a-public-wi-fi-hotspot/

- GOP delegates suckered into connecting to insecure Wi-Fi hotspots, http://www.theregister.co.uk/2016/07/21/gop_wifi_privacy_fail/

- How long does it take to get kicked out of a coffee shop for mooching free Wi-Fi?, http://o.canada.com/business/how-long-does-it-take-to-get-kicked-out-of-a-coffee-shop-for-mooching-off-its-free-wi-fi