Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

An Analysis of Unauthorized Wireless Network Usage in Western Australia

P. Szewczyk, D. Blackman and K. Sansurooah

ECU Security Research Institute, Edith Cowan University, Perth, Western Australia
e-mail: p.szewczyk@ecu.edu.au

Abstract

The use of unsecured wireless networks has increased to unprecedented levels within metropolitan areas, typically encompassing thousands of wireless networks within close proximity. Whilst the deployment of publicly accessible wireless networks provides end-users with a quick and efficient mechanism to access the Internet, limited research has been conducted into end-user's behaviour whilst connected to an unsecured wireless network. This paper assesses the behaviours through a series of empirical experiments. Wireless Raspberry Pi honeypots with high-gain antennas were deployed throughout the Perth, Western Australian metropolitan area. End-users connecting to the wireless network were asked to accept an absurd Terms of Use agreement. Once connected, any domains or services requested were captured for further analysis coupled with preferred network list data for subsequent device tracking. The research demonstrated that end-users neglect the need for personal privacy and may risk exposing their personal data by connecting to unknown networks. Key comparisons are made with previous research to better understand end-user behaviour.

Keywords

Public Wi-Fi, Wireless honeypots, Raspberry Pi, Mobile computing, Karma exploit

1. Introduction

Global mobile data traffic averaged 7.2 Exabytes per month in 2016, increasing by 63% from 2015 (Cisco, 2017). This unprecedented growth is driving consumers to utilise alternative mechanisms by which to access the Internet. Free and legally accessible wireless networks around metropolitan areas of the world are becoming a common occurrence (Shahin, 2017). New York is progressively transforming legacy pay phones into free hotspots to complement the number of devices that make use of Wi-Fi (Shahin, 2017). Subsequently, public Wi-Fi networks are theoretically enabling end-users to conform to "always-online" societal behaviours and thus reducing the financial burden of using purchased mobile data. Using public Wi-Fi networks does create a range cyber security challenges. For instance, consumers may have insufficient knowledge to make informed decisions regarding the state of security and their privacy when choosing and connecting to public Wi-Fi networks (Khoula et al. 2016).

In 2016, the fast uptake of the popular augmented reality smartphone game "Pokémon Go" grew significantly. The game resulted in many end-users using a significant quantity of their mobile data allocation, due to game's dependency on an

Internet connection. Many end-users experienced "bill-shock", where their mobile provider charged them for the excess data they had used (Chung, 2016). To prevent "bill-shock", many end-users of the game sought publicly accessible wireless networks, which provided "free data". In London in 2014, people unknowingly agreed to terms and conditions in exchange for accessing and using free Wi-Fi Internet in which they consented to a "Herod clause" which signed over their eldest child to the owner of the wireless access point (Fox-Brewster, 2016). In contrast, it is common practice for end-users to choose restaurants based on the quality of the free Wi-Fi service available rather than quality food (Cobanoglu et al. 2012).

The previously mentioned trends indicate that end-users may disregarded the importance of conforming to ideal cyber security behaviour, but rather focus on the benefits of free and immediate access to the Internet. Consumers may often lack sufficient expertise to make cyber security conscious decisions when configuring and connecting to Wi-Fi networks (Bada & Sasse, 2014). As a result, end-users may unknowingly place themselves in a situation, where their confidential information is accessed and misused by third parties thus making them a victim of cyber crime.

This research project (phase 2) extends previous research (phase 1) which was conducted in 2016 on the behaviour of end-users when connecting to public wireless networks (Sansurooah et al. 2016). The previous research was undertaken through a series of experiments using purposefully unsecured wireless honeypots. Wireless honeypots within this research are Wireless Access Points (WAPs) that are designed to entice inquisitive end-users into connecting to the network (Szewczyk, 2016). WAPs are typically used in home and business environments and broadcast their presence to allow wireless capable devices (such as smart phones, laptops and tablets) to access the Internet without the need for fixed cabling (Szewczyk, 2006).

In the previous research project (Sansurooah et al. 2016), a captive portal was used on each WAP to prompt end-users with a series of warnings; informing them that access to the wireless network was restricted to authorized individuals only. End-users were not directly connected to the Internet through the WAP but instead were continually informed of the cyber security risks associated with connecting to unknown wireless networks. The result of the previous research showed that 624 unique connection attempts were made to any one of the 26 deployed WAPs during the phase one test period. Of those individuals who did proceed to connect, 179 claimed they were an authorized end-user despite having no authority or knowledge of the wireless network.

2. Method and Project Design

This research project analysed the behaviour of end end-users who connected to a publicly open and accessible WAP. The research projected addressed the following two research questions:

- Should an end-user connect to the WAP, how many end-users will agree to an absurd "Terms of Use" agreement to access the Internet for free?

- Will end-users engage in confidential internet usage, when connected to an unknown wireless network?

In an attempt to answer the aforementioned research questions, the project utilised a series of experiments incorporating a number of customised WAPs. Each WAP comprised of a Raspberry Pi, a TP-Link WN722N antenna, a Telstra 4G mobile dongle and the Raspbian operating system. Telstra was selected as the mobile data provider due to its prominence as a telecommunications provider in Australia. Once configured the deployed WAPs did not require a password to access the Internet. Each deployed WAP would log all connection attempts. A captive portal was created and used to ensure end users' received a notification popup outlining the Terms of Use (ToU) agreement.

Should an end-user not agree to the ToU agreement, they were disconnected from the WAP, but were permitted to reconnect to the WAP the following day. If the end-user agreed to the ToU agreement, by clicking "I accept" they were then provided unrestricted Internet access for a period of 20 minutes. Any websites or services accessed were recorded and stored within a database. Account or personal information was not recorded during the research period. If an end-user's device sent a probe request asking to join a previously connected network, the WAP would respond and invite the end-user to connect.

This ethically approved research recorded each device's preferred network, the timestamps for any connection attempt, the end-user's responses to the Terms of Use agreement, the connecting device's name and Media Access Control (MAC) address. No other personal data or metadata was recorded. To track the ability to detect packets requesting access to a preferred network, a package based on Karma was compiled (Sharma et al. 2014). Once Karma was configured, this package provided the ability to capture specific preferred network data, log the packets and advertise the presence of the WAP for subsequent connections. The processes for initiating connections to the WAP was as follows;

- End-user connects to a WAP.
- The device's MAC address, device name, data/time of connection are recorded.
- A ToU page is displayed. If the user disagrees to the ToU the device is disconnected from the WAP and no further action is take. If the user agrees to the ToU the confirmation is recorded and subsequent connection attempts to websites and services is tracked. Once the time or data allowance is reached the user is disconnected.

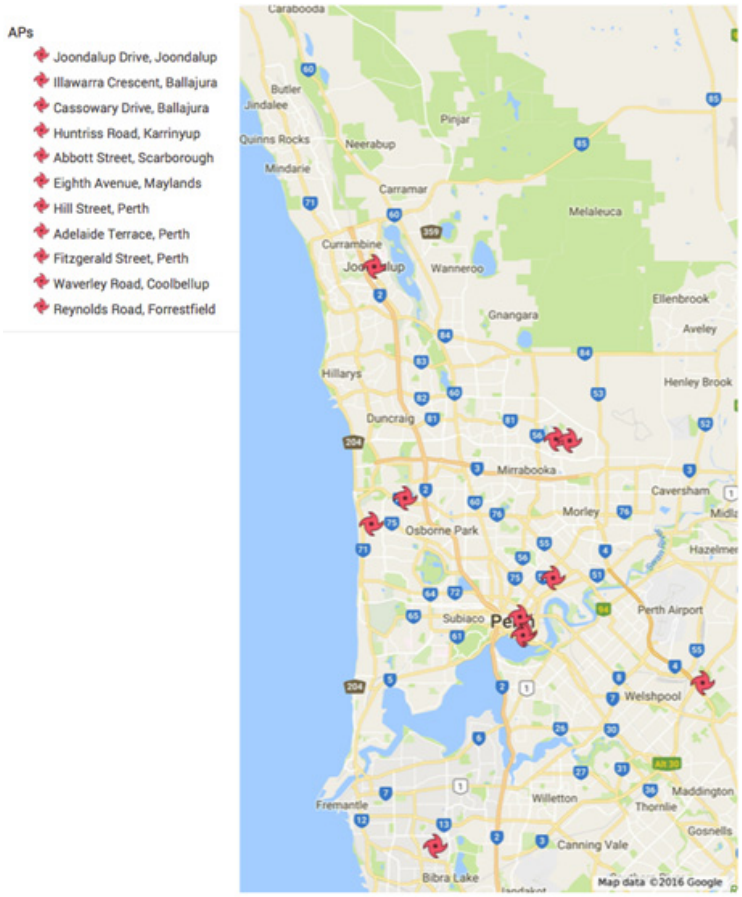

Figure 1: Deployed WAP locations throughout Perth, Western Australia

3. Results

3.1. Connecting Devices

The research project was undertaken between 15th September 2016 through to 12th November 2016. During this time period 919 connection attempts were made. 695 unique device names were recorded in-conjunction with 774 unique MAC addresses. Many devices identified themselves as a particular device or model as follows: 189 iPhone or iPad; 481 Android device; and 25 "MBP" (Macbook Pro) or "Air" (Macbook Air).

Of the 919 connections, 47 accepted the ToU agreement, 21 declined, and 851 did not respond. The majority of connection attempts originated from WAPs that were deployed within close proximity to an educational facility through a network named "Compromised Academic Network". The WAP with the second highest quantity of connections was in a residential location named "Your Neighbours Wi-Fi" followed by "Infected Corporate Network #2".

SSID Name (15)	Number of Connections (919)
Compromised Academic Network	267
Your neighbours Wi-Fi	178
Infected Corporate Network #2	160
Compromised Wi-Fi 2	78
Angels Beauty Wi-Fi	63
Infected Corporate Network	56
Private Wi-Fi	41
Very dodgy Wi-Fi	41
Compromised Wi-Fi	9
Dangerous Wi-Fi	8
Virus infected Wi-Fi	6
Unsafe Wi-Fi	5
Corrupt Wi-Fi	3
Untrusted internet	3
Malware Infected Wi-Fi	1

Table 2: Connections to each of the WAP Service Set Identifier (SSID)

Once a device connected to a WAP, a log was kept of the type of website or services that was being requested. As depicted through Table 2, social network related requests were the prominent category of connection attempts followed by email based services.

Site Requested	Prevalent Sites	Number of Connections
Social Networking	Facebook Twitter Flickr Bebo Instagram Pintrest	18059
Banking	Commonwealth Bank NAB Westpac ANZ Bankwest	349
Email	Gmail Outlook Live Gmx Yahoo Yandex Hushmail Zoho	3976

Table 3: Domain requests received by the Wireless Access Points

3.2. Reconnecting Devices

A relational "Postgresql" database was utilised to compare data from phase 1 and 2 of the research project. The database imported data from 683 devices from the phase 1 research and 919 devices from the phase 2 research. Analysis of the data

discovered 12 devices that were common across both phases of the research with the MAC address and device name being identical.

Device name	Device MAC Address
Joannas-iPad	70:e7:2c:74:--:--
ShavindasiPhone	68:db:ca:67:--:--
Hannahs-Air	7c:d1:c3:e5:--:--
android-5a280f133274f43f	7c:91:22:0a:--:--
android-bd6b61ae211f9515	c0:ee:fb:20:--:--
android-6018867e5b1fe37d	40:f3:08:f3:--:--
Hazels-iPad	f0:db:f8:15:--:--
MHD1500420	88:63:df:cf:--:--
android-78575c0b83975b5d	d0:22:be:d1:--:--
HafeezahsiPhone	6c:72:e7:e0:--:--
RedmiNote3-Redmi	64:cc:2e:11:--:--
Princess-em	40:e2:30:5b:--:--

Table 4: Identical devices discovered during both phases of research

Further analysis was conducted to locate devices with the same name but with different MAC addresses. This search found a total of twelve device names.

Device	Duplicate MACs located
iPhone	61
Windows-Phone	57
?	37
RedmiNote3-Redmi	7
iPad	6
HUAWEI_P9	5
iPhone-2	2
iPod-touch	2
iPhone-6s	2
Wendys-iPhone	2
Karens-iPhone	2
Chriss-iPhone	2
Sophies-iPhone	2

Table 5: Connected devices with different MAC addresses

Whilst Table 4 illustrates a number of generic device names, which cannot be assumed to be a single end-user, seven devices only had two MAC address changes. A further two devices featured names which appear to be non-generic. The device "RedmiNote3-Redmi" was already captured in Table 1. Therefore, it could be argued that eight further devices have connected in both research phases, despite having non-identical MAC addresses.

3.3. Device Identification and Preferred Network Lists

The second phase of the research included a mechanism to detect and log probe requests for Preferred Network Lists (PNLs) from devices in the area. Table 5 and 6 show that the deployed Raspberry Pi's logged 402,479 probe requests during the research period of which there were 3,619 networks with unique names identified.

Preferred Network Name	Probe Request Count
ECU	68749
Doh-Data	29575
TCS	24760
NTGR_ JjPCrAcIWADNhLI1vX6	24336
PTAPTH	18049
HEALTH-Data	14388
Josh Home	12899
eduroam	11385
ecu-access	11258
OPTUS_2E6E62	10178
.....	10105
Wirey	9503
ii1DA556primary	7895
belkin	6899
Vividwireless-7BFA	6436

Table 6: Top Preferred Network List (PNL) probes requested

One device "Hazels-iPad" transmitted 298 probe requests for a network named "Seventh Avenue" followed by 12 probe requests to a network named "Seventh Avenue 5GHz". Further investigation was conducted to account for the results depicted in Table 7 by examining the total number of probe requests for the two networks, which discovered an additional 898 requests from other devices. In order to verify and validate the results from the study, the Organizational Unique Identifier (OUI) values were compared and checked against online databases and then correlated with the phase 1 research data in order to determine the manufacturers and names of the devices. The outcomes of the PNL probes oscillating between the 2.4 GHz and the 5.0 GHz is shown in Table 8.

Device Name	MAC Address	Probe Requests	Preferred Network
Unknown	00:f4:b9:5d:68:d2	166	Seventh Avenue
Hazels-iPhone	54:9f:13:72:ec:6c	46	Seventh Avenue
Hazels-iPhone	54:9f:13:72:ec:6c	31	Seventh Avenue 5GHz
Unknown	58:82:a8:b2:e9:ef	308	Seventh Avenue
Unknown	58:82:a8:b2:e9:ef	274	Seventh Avenue 5GHz
Unknown	98:e0:d9:bf:94:63	63	Seventh Avenue
Hazels-iPad	f0:db:f8:15:6d:f8	298	Seventh Avenue
Hazels-iPad	f0:db:f8:15:6d:f8	12	Seventh Avenue 5GHz

Table 8: Preferred Network List (PNL) probes for Seventh Avenue

This research confirmed the discovery of two wireless networks through the capture of PNL data. The unique nature of the Service Set Identifier (SSID), along with an indication of the street on which the owner lived, were checked and compared against online websites to locate (Chernyshev et al. 2016), with precision, the location of two base stations (Figure 2).

Figure 2: Location of SSID "Seventh Avenue"

4. Discussion

In prior research, Chernyshev et al. (2016) discussed the challenges and opportunities in using passive wireless device fingerprinting for mobile computing location identification. The research concluded that the PNL of a wireless capable device provides a digital fingerprint and could therefore could be utilised in digital forensic investigations and GPS tracking. Leveraging the concepts as discussed by Chernyshev et al. (2016) and applying them to the second phase of the research as portrayed through this paper, it is evident that invading one's privacy and tracking the whereabouts of a mobile computing device is simple and efficient to deploy and potentially misuse. Although only one network was tracked and interrogated to a specific location, the same process could be utilised for any number of devices for the purposes of placing a device at a particular location or scene.

Unexpectedly, the research enabled the successful identification of the precise location of one end-user's device as well as the total number of devices that one would expect to typically associate itself with the home WAP coupled with the associated manufacturer of the devices. This type of information could be valuable in investigations relating to someone who has stolen another individual's digital devices or as a search warrant where law enforcement officers are attempting to

locate an otherwise unknown quantity of secreted devices (Vattapparamban et al., 2016; Watanabe et al., 2012).

Although this research project made use of an absurd and controversial ToU agreement, it didn't necessarily discourage all end-users from accepting the agreement. This trend mimics similar outcomes to research undertaken within London in 2014 which identified end-users also disregard controversial ToU agreement in favour of accessing a public WAP. This type of behaviour further demonstrates that further education and awareness raising must be supplied by government to further inform end-users when accessing public WAPs in the future.

A concerning facet of the research for end-users is the number of connections which were instigated towards a clearly compromised and/or vulnerable WAP. Furthermore, this issue is further extenuated since each deployed WAP was also within close proximity of a free accessibly safe wireless network – offered by a reputable company or local council. Many end-users may also be unaware of the background services that immediately attempt to access the Internet once a non-mobile related connection is made and the type of data that is transmitted through these services. Whilst social network related connections were expected, the fact that many devices were connecting to banking or email related services raises a number of security concerns.

5. Conclusion

This research has successfully established that end-users connecting to WAPs will often agree to a ToU Agreement, despite the terms being absurd or controversial. The naming of SSIDs has little effect on discouraging end-users from connecting to a WAP. Once connected to a wireless network, many end-users have little regard for their digital security and connect to websites which could potentially allow their personal data to be captured or compromised. Further research, education and analysis of end-user behaviour whilst connected a public wireless network is required.

6. References

Bada, M., Sasse, A. (2014). "Cyber Security Awareness Campaigns: Why do they fail to change behaviour" http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf (Accessed 10 October 2017)

Chernyshev, M., Valli, C., & Hannay, P. (2016). "Service Set Identifier Geolocation for Forensic Purposes: Opportunities and Challenges". Paper presented at the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA

Chung, F. (2016). "Pokemon Go players brace for bill shock", http://www.news.com.au/finance/money/costs/pokemon-go-players-brace-for-bill-shock/news- story/5cb0fc272174d03d1656fd8421e85ecd (Accessed 17 January 2017)

Cisco. (2017). “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper”, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html (Accessed 18 March 2017)

Cobanoglu; A, Bilgihan; K, K, Nusair & K, Berezina. (2012). “The Impact of Wi-Fi Service in Restaurants on Customers' Likelihood of Return to a Restaurant,” Journal of Foodservice Business Research, 15(3), 285-299

Fox-Brewster, T. (2016 10). “Londoners give up eldest children in public Wi-Fi security horror show”, https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod- clause (Accessed 18 March 2017)

Khoula, A., H., Shah, N., Shankarappa., A., N., S. (2016). "Smartphone's hotspot security issues and challenges", Paper presented at the 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain

Sansurooah, K., Szewczyk, P. & Blackman, D. (2016). “Unauthorised Wireless Network Access Attempts in Western Australia”. Paper presented at the 2016 International Conference on Computational Science and Computational Intelligence, Las Vegas, Nevada

Shahin, E. (2017). “Is WiFi Worth It: The Hidden Dangers of Public Wifi”, Catholic University Journal of Law and Technology, Vol. 25, No. 1, pp205-230.

Sharma, P., Chakraborty, D., Banerjee, N., Banerjee, D., Agarwal, S. K., & Mittal, S. (2014). KARMA: Improving WiFi-based indoor localization with dynamic causality calibration. Paper presented at the 2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Singapore, Singapore

Szewczyk, P. (2006). “Individuals’ Perceptions of Wireless Security in the Home Environment”. Paper presented at the 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia

Watanabe, K., Tanaka, H., & Otani, M. (2012). “Development of Geographical Location Estimation System for WiFi End-users in Campus”. Paper presented at the Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), Palermo, Italy