Wi-Pi: a study of WLAN security in Auckland City

Ar Kar Kyaw1[1, 2], Zhuang Tian [2], Brian Cusack [2]

Faculty of Business and IT, Whitireia Community Polytechnic, Auckland, New Zealand[1]
Digital Forensic Research Labs, Auckland University of Technology, Auckland, New Zealand[2]

Abstract
The inherent nature of wireless networks exposes them to cyber threats. To keep this critical technology from attacks, advancements in security standards demand simultaneous outspread of their awareness among people. Periodic evaluation of Wireless Local Area Network (WLAN) security status in any given region recognizes the awareness trends and sets directions for concerned authorities. This research studies the prevailing security practices of WLANs in Auckland city, to describe the course of their alertness with respect to similar studies done in 2007 and 2013. Raspberry Pi 2 Model B is used for research to provide a basis for comparison and reference for future relevant studies. The results are significant from commercial perspective.
Keywords:
Warwalking; Wi-Pi; Raspberry Pi; wireless security.

1. Introduction

Wireless networking is a boon to mankind. Ever since its evolution, this technology has been experiencing considerable improvements for over a decade [1], but the past few years have witnessed its emergence as a way of life [2]. The concern for securing it against threats, which have continuously been parasitic to it [3], rises as it gets associated with the lifestyles of the people. Although to answer these concerns, enhancements at technical scale have accompanied its progression [4], securing a wireless network is a critical component of public awareness. Advance standards of wireless security mechanisms will only be of assistance if they are put in to practice. Information about Wireless Local Area Network (WLAN) practices in an area, in order to determine its security status, can be collected by capturing and analysing as many wireless signals, while driving around in a vehicle. Wardriving is "the gathering of statistics about wireless networks in a given area by listening for their publicly available broadcast beacons" [2]. When this activity is done by walking, it is called warwalking.
Information about WLANs in an area to understand their adoption practices is desirable to local technical and administrative authorities [5]. It helps to identify growth hurdles of the technology and thus set path to overcome them. It also helps the authorities to compare results of such studies overtime and analyse outcomes of their previous campaigns done in similar direction.
Wireless networking is designed to welcome all users without resorting to any physical connections and manual configurations [4]. The absence of a physical barrier and medium for its transmission makes this technology highly vulnerable to attacks [6]. This vulnerability poses a major hurdle for its growth, to an extent that it had almost brought its commercialization to a standstill when a major flaw in its security mechanism was discovered in 2002 [1]. Despite its endurance up to that time, until new acceptable methods were launched, security of wireless networks has always been questionable [4]. This research thus takes a deeper look into the WLAN security practices and reports the findings to assist with improving security. It also presents the transmission channels used by the detected networks. Misconfigured and rogue networks can be located using this information and can be useful for security standard authorities like the Payment Card Industry (PCI) for reconfiguring or removing them. The report also presents the list of Access Point (AP) manufacturers for all detected WLANs which can be useful for new users as well as business competitors. The major contributions of this research are as follows:

- For the section of society involved in improving public awareness about the significance of wireless security, this research provides the current security status for planning their campaigns.
- The results of this research can assist users looking for new wireless installations to refrain from security malpractices and in selecting amongst the prevalent wireless routers.
- A channel frequency distribution graph helps identify rogue and misconfigured wireless networks.

Our research explains the technology trends and updates in its standards over time. This paper has been organized into six sections to classify closely related matter under the same hierarchies. After highlighting the importance of this study and briefing about its execution methodology in the "Introduction (Section 1)", the report presents a "Literature Review (Section 2)" of similar published works to gain contextual knowledge and work towards the fulfilment of any gaps in the existing information. The study of previous

Manuscript received August 5, 2016
Manuscript revised August 20, 2016

literature is also used for data comparison in later sections. The "Research Methodology (Section 3)" describes the research overview as well as the adopted sequence of its execution. The "Research Findings (Section 4)" presents any variations found during the field trial and the results obtained using the practiced methodology. The "Discussion (Section 5)", explains a significant part of this study including the comparison of our findings with previous studies and critically analysing the reasons for the obtained results. The "Conclusion (Section 6)" provides the opinion of the authors based on the study and makes recommendations for future studies.

2. Literature Review

Imparting awareness is a never ending struggle [7]. Consequently, warwalking and the likes become a part of never ending research. Over the period of time new technologies are discovered and so are the loopholes associated to them [3]. To keep updating the security deployment statistics is thus a periodic activity which has been done by many researchers in the past and will continue in the future. To carry it out effectively, reports from previous researches were studied and their suggestions were noticed. This section reviews similar published works in the field of warwalking, conducted in different parts of the world. It includes research related to warwalking, WLAN standards and their security mechanisms. However, the analysis of WLAN signal propagation and other wireless technologies are not part of the literature review.

Halim [8] conducted his field trials by walking for an hour with a Windows laptop, having Netstumbler installed for WLAN sniffing. His route was limited to Queen Street in Auckland CBD. Similarly, Sarkar and Abdullah [9] conducted a warwalking field trial in Auckland CBD area to compare security updates in 2010 with respect to 2004 and 2007; while Nisbet [1] drove around all surrounding areas of Auckland City for more than four hours to cover as many APs as possible. Kalbasi, Alomar, Hajipour and Aloul [10] conducted similar drive in the United Arab Emirates (UAE) with two laptops and with a GPS to locate detected APs. Tsang, Kwok, Kwan, White and Fox [11] also did their wardriving using a Windows laptop as well as a Linux one to have a better comparison. They also covered the central area of Hong Kong by flying in a helicopter to capture signals at vertical heights. Most of the studies were limited to Central Business Districts of respective locations, but Nisbet [1] took the additional step of collecting data from suburbs too. His results presented more awareness in suburban parts than in business districts. Halim [8] also considered running the same scan at night to collect statistics of residential areas. Tsang, Kwok, Kwan, White and Fox [11] went an extra mile by listing the physical layer types of the detected APs. Along with unique characteristics, most of the researchers have matching aspects too. Halim [8], Sarkar and Abdullah [9], Tsang, Kwok, Kwan, White and Fox [11] as well as Nisbet [1] all compared their study results with past studies to investigate changes in security status over the past few years. Moreover, Netstumbler on Windows and Kismet on Linux were the most used software in all the studies.

As part of wireless security, Singh, Mishra and Barwal [4] describe the history of wireless encryption standards. WEP was introduced with 802.11b standards and was found to be weak in terms of protection. Kalbasi, Alomar, Hajipour and Aloul [10] suggest WPA-PSK instead of WEP. They also consider Media Access Control (MAC) address filtering as a security mechanism which Halim [8] also suggests to deploy as an additional security layer, in conjunction with a robust one. Singh, Mishra and Barwal [4] however advocate in favour of MAC binding with IP addresses. Nisbet [1] considers WEP as even worse than an unencrypted channel as it gives the users a false sense of security. WPA2 is the suggested mechanism of all studies as, unlike WEP, it keeps updating the encryption keys periodically. SSID broadcast hiding is also recommended by most, however, Tsang, Kwok, Kwan, White and Fox [11] do not consider this feature noteworthy. If SSID is to be broadcasted, Halim [8] advises to at least change the default settings. Other than regular encryptions, Singh, Mishra and Barwal [4] endorse practical methods like virtual private network (VPN) and placement of AP outside the firewall. They also explain 802.11i which is specifically introduced for wireless security. Halim [8] adds an intrusion detection system (IDS) in the practical solution list to enhance security. Sarkar and Abdullah [9] found a considerable increase, not only in adoption of encrypted wireless networks, but also in other practices in Auckland CBD, and provided four specific recommendations for securing wireless communications over WLAN. These recommendations include better encryption technology should be chosen for WALNs, the default SSID should not be used to improve security, WLAN access should be controlled by minimising MAC addresses and VPN should be used to improve security. Similarly, a continuous monitoring of security status of these wireless networks in Auckland City is also recommended [9]. Nisbet [1] describes the existence of 11 channels in 2.4GHz band but mandates configuring the APs to communicate in 1st, 6th or 11th channel only. He explains how the channels may overlap if not kept distant. His study also listed the channel configurations of all the detected APs. Tsang, Kwok, Kwan, White and Fox [11] state that the 2.4GHz band interferes with microwave and Bluetooth devices. They collected channel data for both 2.4GHz and 5GHz bands. Kalbasi, Alomar, Hajipour and Aloul [10] explained how SSID provides the channel information. Their study found more than 70% APs using channel 11, which can slow down all the APs in the vicinity of each other. Halim's [8] study though, did not captured

this information. Christie [5], on the other hand, takes this to next level. Kismet running on Raspberry Pi can identify Rogue Access Points (RAP). He encourages notifying these misconfigured or malicious RAPs to authorities like PCI for appropriate actions.

Similarities among different studies do highlight the importance of this field. Majority of the warwalking studies were limited to WLAN sniffing and done in business districts only. Their aim was to recognize security patterns primarily at commercial level, as their necessity was considered to be more crucial in such areas. Netstumbler and Kismet were the mostly used software for sniffing and collecting data. The collected data mostly specified the encryption standards and the communication channels of the APs. Apart from similarities, each research also had its unique findings. But a research which combines all these unique characteristics into one is missing. Since each researcher has compared individual data with previous studies, a combination of their exclusive parameters can be a platform for comparison of unusual datasets for future studies. This inspires the selection of Raspberry Pi 2 Model B for the study. Although Raspberry Pi is not widely used, it is cost effective and portable, and the listing of physical layer types and manufactures is also not a usual attribute. Likewise, comparisons of day and night results as well as a comparison of data from different sources constitute the qualities of this research which makes it distinct from its counterparts.

3. Research Methodology

Planning plays a vital role in the delivery of quality researches [12]. This research was planned to be carried out in six different phases with a mixed research approach to employ both qualitative as well as quantitative methods of study. The review of warwalking related studies in Section 2 provided a fair understanding for building up the experimental system, devising a route to carry out the warwalking in the field for passive sniffing and covering the planned distance within predefined time duration. This section further outlines the analysis and presentation methods of collected data. The aim of this research was to answer the following research question:

What is the current security status of WLANs in Auckland city?

In order to answer it effectively the question was divided into following sub questions:

How many WLANs are there in the Auckland city (especially in CBD, Mt Albert and Parnell)?

How many, with respect to the total number of WLANs, are encrypted?

What is the ratio of cloaked networks?

What is the difference in the percentages of encrypted WLANs between present and previous studies in Auckland CBD?

The total number of WLANs detected in the Auckland city areas was the first set of data. Among them the number of networks which use encrypted methods for data communications portrays the WLAN security state of the area. A comparison of this proportion to the one obtained in previous studies indicates the awareness trend among people and sets a direction for its improvement.

To effectively answer questions, research was carried out in six phases (Figure 1). These phases include literature review, system setup, pilot testing, data collection, data analysis and its comparison with results of previous research.

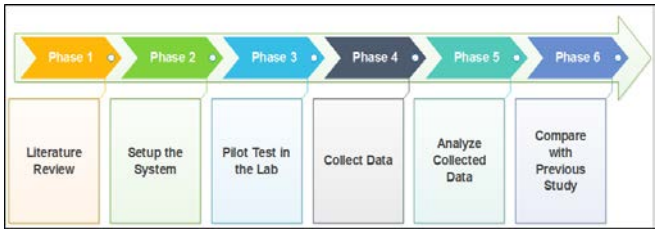

Fig. 1 Research phases.

Different research phases employ different research methods. The literature review section, for example, was done to understand the work of different authors and their future recommendations. This phase constitutes the qualitative part of the study. The data collection, on the other hand, includes an experiment conducted by warwalking in the field on a designated route and for a fixed duration. This was preceded by the system setup phase to prepare the equipment for the field trials. These rational phases constitute the quantitative part of the study. The final phase compares the results obtained from both parts of the study. With both the parts being significant, related and compared to reach a conclusion, the study takes a concurrent triangulation mixed research approach [13].

After understanding the requirements from the study of previous literature in first step, the system was setup for the experiment. This included the required hardware, software and related configurations, explained in the System Design (Section 3.1). With the Wi-Pi (Figure 2) setup, a trial run would be made to test the basic functionality of the system. The obtained pilot results would help to improve the system before the final run. With the updated system, the final data would be collected for analysis and compared with the results obtained earlier in literature review.

3.1 System Design

To attain configurability as good as that of a laptop and portability of a smartphone, a card sized mini-computer

called Raspberry Pi 2 (Model B) was used. A wireless adapter and a Global Position System (GPS) were attached to it, with a 5V battery for powering the equipment.
The Raspbian operating system (OS) was installed on the Pi by formatting the 2015-05-05-wheezy-raspbian.img image [14] on the Micro Secure Digital (SD) card using the free utility Win32DiskImager.exe (www.sourceforge.net) on Windows laptop. After booting the device with the installed OS, it was connected to a network switch with internet connection using network cable. The laptop was also connected to the same network to remotely log into the system with a secure shell (SSH) session by using free utility putty.exe (www.putty.org). Using the guidelines described by Christie [5], the device was configured to expand its filesystem, update default OS packages and change default password and host settings. A GPS and Wi-Fi adapter were then connected to the Pi and using apt-get utility of the OS, gpsd and gpsd-client packages were installed. These packages were configured to communicate with the GPS on the ttyUSB0 device, created automatically by the OS after connecting the GPS. The device name was found using dmesg command.

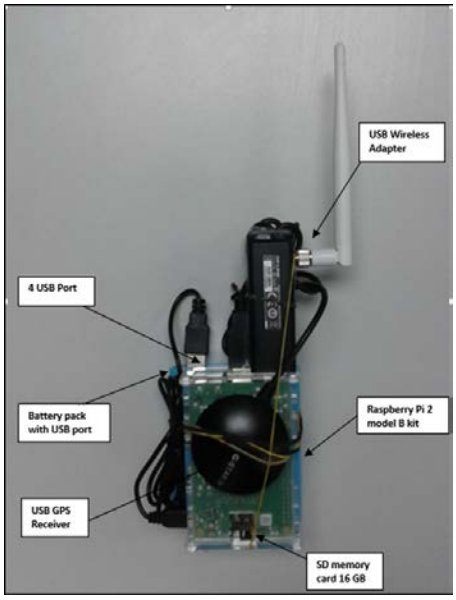

Fig. 2 Wi-Pi device.

Kismet is a free utility for logging Wi-Fi signal data. The source code for this software was downloaded and compiled on the Pi for compatible installation. The latest software release 2013-03-R1b at the time of the project execution was used along with the required ncurses-dev, libpcap-dev, tcpdump and libnl-dev dependencies. Network identifier 'wlan0' created by the OS for Wi-Fi adapter was determined using the command ifconfig and configured in the kismet.conf file for passing wireless signal information to kismet. Similarly, data from GPS was also tied to this information by configuring gpsd and ttyUSB0 port in the kismet configuration file. The services required for GPS and Kismet were configured to start automatically at runtime and log data at predefined locations. The resulting Wi-Pi device is shown in Figure 2.

3.2 Pilot Test

After setting up the Wi-Pi system, a pilot run was planned to be run for functional testing of the device. The test would be done by walking with the equipment in the nearby area of the laboratory for a few minutes and then copying the resulting Kismet log files from Wi-Pi to a workstation. The log analysis would be the same as an actual run to test the system.

3.3 Data Collection

Final data collection was planned to be done by walking around Auckland CBD and suburbs (namely Mt Albert and Parnell) which covers main areas of Auckland city in our research. For result accuracy, it would be done twice during daytime between 1500 to 1600 hours (referred to as "Day Scan" in later sections), and after hours between 1900 and 2000 hours (referred to as "Night Scan"). To compare results with previous study, it was planned to follow the same route as used by Halim in his research [8]. Although the slower the movement, the more networks may get detected [5], the speed of walking would also be maintained just enough to cover the route in an hour in order to make the duration of the run the same as Halim's [8] research.

3.4 Data Processing and Analysis

Kismet creates five log files with extensions .alert, .nettxt, .netxml, .gpsxml and .pcapdump [15]. The netxml file carries all the required information for warwalking studies [5]. The created files would be copied using WinSCP (www.winscp.net) to Windows from Wi-Pi and then from Windows to virtual Linux to run the python script, netxml2xml.py [15] to generate the .kml file. The kml file would be uploaded to Google Maps (http://mymaps.google.com) to view the location of the APs. Kismet logs are a large set of parameters for each wireless network. These logs include the basic service set identification (BSSID), manufacturer of the AP, operating frequency, channel, network type and GPS information, among others. These would be mapped to Microsoft Excel for readability and to easily classify the networks based on their encryption status, encryption standard, AP manufacturer, frequency channel and SSID broadcast status. The ratio of each of the above categories with respect to the total network count would provide answers to the research sub questions and thus the main question.

3.5 Data Presentation

In order to provide a clear understanding of the status of WLANs, the processed data will be presented in tables and pie-charts. A comparison table will show the total number of APs found in both the scans and the total number of secure APs. The geographical location of the APs will be presented using Google Map. The comparison with previous studies will be made on the basis of encryption status by evaluating the proportion of encrypted APs to total APs. The transmission channel also plays a significant role in wireless networks as APs in neighbourhoods bleed into bands of other APs if configured for similar channels [1]. The frequency channels of APs would also be presented in tabular form.

3.6 Limitations

The Raspberry Pi, though portable and configurable, lags behind the resourceful laptops with efficient battery backups for better wireless signal detection. Moreover, the speed of walking was required to be slow but fast enough to cover the 3-kilometre distance in an hour. This, to some extent, could miss out off-road APs along the way. The APs in buildings next to the road but vertically high were also likely to be missed from detection. Also, the real time calculations done by GPS on a mini computer would not be truly accurate to generate exact AP locations. Similarly, the laptop scan was only conducted in Auckland CBD due to the time constraint.

4. Research Findings

A field trail was done as per the methodology adopted in the previous section, which identified a few issues. These issues were resolved before the actual run. The discovery of functional errors in the initial phase, helped maintain the schedule in later phases of the research. The data collection with the updated Wi-Pi device also faced challenges and had to be repeated with a laptop and an advanced Wi-Fi adapter, as described in Section 4.1.2. Readings with both sources, Wi-Pi and laptop, were analysed and presented in each result subsection of this section.

4.1 Variations Encountered

Despite adherence to the planned sequence, the field study observed slight variations from its track. This section explains them with respect to each phase.

4.1.1 Pilot Test

After the pilot run, GPS data for most of the APs was not logged and geographical locations of most of the logged ones, after mapping on Google Maps, were incorrect. Moreover, the time displayed in the readings was not accurate. Also, some of the log files were found to be corrupted.

4.1.2 Data Collection

After updating the system for issues in the previous section, as explained in Section 5.1, the final run was done. The results found that all the APs were listed to have 802.11b+ standard. As explained later in Section 5.1, the study resorted to using a Windows laptop with Acrylic WiFi (www.acrylicwifi.com) installed for sniffing wireless signals.

4.1.3 Data Processing and Analysis

The Kismet log files were copied after stopping its running service to avoid any file corruptions (Section 5.1). The collected log was mapped to excel for analysis to generate a kml file using new script (see Section 5.1). The kml file was uploaded to Google Maps to view the location of the wireless APs as shown in Section 4.2.8.

4.2 Findings

Tabular representation of total networks found in different scans and their classifications based on encryption, manufacturer, SSID cloaking and other criteria are presented here. The “Day Scan” was conducted at 1500 hours while the “Night Scan” was done at 1900 hours. The scans were conducted using the Wi-Pi, and the “Pi Scan” represents a day and night combination excluding any duplications (Section 5.2). The “Laptop Scan” was done at 1500 hours in Auckland CBD only. All the field runs were done on weekdays.

4.2.1 Wireless Network

Among the different types of wireless networks found, the report considers only the actual WLANs for which the information was complete and valid. The Probes are generated by the clients attempting to connect to APs and hence are ruled out as they are not a wireless network themselves. The data networks represent incomplete or vague information and not considered for analysis. The effective WLANs are therefore reduced in count as shown in Table 1. During the combination of “Day and Night Scan” results, a few networks reported as data in one scan were found with complete information in the other scan results and vice versa. This adds to the significance of Wi-Pi scan results.

Table 1: Classification of total wireless networks detected in Auckland CBD

Scan	Detected Wireless Networks	Client Probes	Vague Data	Effective WLANs
Day Scan	1010	183	249	578
Night Scan	1010	136	209	665
Wi-Pi Scan (Day + Night)	1482	313	310	859
Laptop Scan	3495	1	0	3494

Table 2: Classification of total wireless networks detected in Mt Albert

Scan	Detected Wireless Networks	Percentage
Day Scan	956	75.5
Night Scan	311	24.5
Wi-Pi Scan (Day + Night)	1267	100

Table 3: Classification of total wireless networks detected in Parnell

Scan	Detected Wireless Networks	Percentage
Day Scan	446	57.8
Night Scan	326	42.2
Wi-Pi Scan (Day + Night)	772	100

4.2.2 Encryption Status

Illustrated in Table 4, 5 and 6 are all the WLANs categorized according to their encryption standards along with the one without any encryption in the "None" row. Among all the standards, WPA2, scores the highest number of occurrences. The "Other" column is for WLANs with incomplete information preventing them qualifying as one of the known standards. The percentage of open networks in Section 5 is calculated considering the "Other" as encrypted networks.

Table 4: Auckland CBD encryption status in WLANs

Encryption Standard	Day Scan	Night Scan	Wi-Pi Scan (Day + Night)	Laptop Scan
WPA2	391	453	584	2672
WPA	14	16	19	122
WEP	3	8	8	25
None	125	142	173	675
Other	45	46	75	0
Total	578	665	859	3494

Table 5: Mt Albert encryption status in WLANs

Encryption Standard	Day Scan	Night Scan	Wi-Pi Scan (Day + Night)	Laptop Scan
WPA2	391	453	584	2672
WPA	14	16	19	122
WEP	3	8	8	25
None	125	142	173	675
Other	45	46	75	0
Total	578	665	859	3494

Table 6: Parnell encryption status in WLANs

Encryption Standard	Day Scan	Night Scan
WPA2	232	173
WPA	97	72
WEP	1	2
None	47	41
Other	69	38
Wi-Pi Scan	446	326

4.2.3 Channel Distribution

Other than security, one of the contributions of this research is to find the misconfigured APs (see Section 1). This can help to correct their configurations. There are many channels where an AP can be configured to communicate, but only a few are advisable [3]. The misconfigured ones can be found using the channel distribution in the following sub sections.

4.2.3.1 2.4GHz Channels:

The results for 2.4 GHz with Wi-Pi were concentrated in the first channel while those from the laptop, illustrated in Figure 3, show a predictable behaviour. In addition, Table 7 demonstrates that channels of 1, 6 and 11 are used by over 75% APs. This adherence to the recommended channels is pleasing. However, with almost of fourth of the networks using other channels cause significant network inefficiency. This also follows the trend of private networks being more securely configured than commercial network.

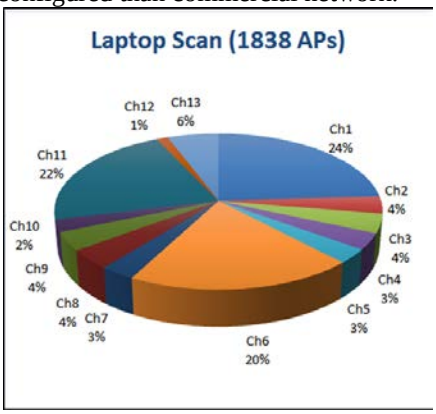

Fig. 3 Wi-Pi device.

However, the Wi-Fi adapter used with Wi-Pi device supported only the 2.4GHz band when we conducted warwalking in Mt Albert and Parnell.

Table 7: Channel distribution of 2.4 GHz band in Mt Albert & Parnell

Channel	Mt Albert	Parnell
1	43	68
2	9	11
3	8	17
4	6	17
5	3	11
6	40	71
7	5	14
8	2	19
9	12	13
10	3	18
11	53	98
12	0	5
13	9	19
Total	193	380

4.2.3.2 5GHz Channels:

As shown in Table 8, almost half of the networks were found in this band and signify the purpose of laptop scanning.

Table 8: Channel distribution of 5 GHz band in Auckland CBD

Channel	Laptop Scan
36	270
40	47
44	120
48	58
52	106
56	17
60	59
64	55
100	110
104	12
108	63
112	19
116	13
120	0
124	4
128	4
132	60
136	6
140	13
149	186
153	32
157	119
161	57
165	37
Dual Channel (40MHz wide)	189
Total	1656

4.2.4 Network Types

The ad hoc and Infrastructural network types found in Auckland CBD are shown in Table 9. Laptop scan shows only four ad hoc networks while the results from Wi-Pi are considerably higher.

Table 9: Network types in Auckland CBD

WLAN Type	Day Scan	Night Scan	Wi-Pi Scan	Laptop Scan
Ad hoc	19	17	24	4
Infrastructural	559	648	835	3490

4.2.5 Manufacturers

The list of manufacturers of effective WLANs (Section 4.2.1) presented in Table 10 is not exhaustive, however, comprehensive enough to identify market leaders in the selected region. The rows with few networks are categorized into the "Others" category. The manufacturers of "Unknown" items are not recognized by sniffing software. As apparent from the list, proportions for Ruckus and Huawei are remarkably different for laptop and Wi-Pi. Proportions for other list items, though, are similar. On the other hand, Table 11 and 12 show the WLAN device manufactures detected using "Day Scan" and "Night Scan" in Mt Albert and Parnell. These results confirm that users from Auckland CBD are composed of residential and business users who have different demands in choosing WLAN devices compared to users in Auckland suburbs.

Table 10: Auckland CBD AP manufacturers of effective WLANs

Manufacturer	Day Scan	Night Scan	Wi-Pi Scan	Laptop Scan
Aerohive Networks	22	28	29	285
Altai Technologies	15	20	20	33
Apple	3	3	4	64
Aruba Networks	59	41	70	300
Asustek Computer	6	5	7	60
Cisco	27	30	40	683
Cisco-Linksys	8	11	12	27
D-Link	3	5	5	54
Hewlett Packard	1	2	1	96
Huawei Technologies	2	1	2	238
Netcomm Ltd	11	16	19	61
Netgear Inc	3	7	9	56
Routerboard.com	28	23	30	46
Ruckus Wireless	10	13	15	347
Sercomm Corporation	24	32	39	92
Technicolor	15	15	21	34
TP-Link Technologies	10	14	17	116
Ubiquiti Networks	38	47	59	214
Unknown	233	274	359	415
Others	60	78	101	273
Total	578	665	859	3494

Table 11: Mt Albert AP manufacturers of effective WLANs

Manufacturer	Day Scan	Night Scan
Aerohive Networks	81	36
Apple	53	14
Asustek Computer	0	6
Intel Corporation	13	0
Netcomm Wireless	7	8
Samsung	12	0
Sercomm Corporation	16	11
Technicolor	17	17
Thomson Telecom Belgium	20	16
TP-Link Technologies	14	0
Others	723	203
Total	956	311

Table 12: Parnell AP manufacturers of effective WLANs

Manufacturer	*Day Scan*	*Night Scan*
Cisco	11	12
Netcomm Wireless	18	13
Routerboard.com	16	0
Ruckus Wireless	29	0
Sercomm Corporation	29	39
Technicolor	19	15
TP-Link Technologies	12	12
Ubiquiti Networks	33	29
Others	280	206
Total	446	326

4.2.6 PHY Type

Table 13 shows the distribution of physical layer standard types of results obtained from the Laptop scan along with their percentage with respect to total WLANs found.

Table 13: PHY types from laptop scan

PHY Type	*Laptop Scan*	
	Count	*%*
802.11a	89	2.5
802.11b	12	0.3
802.11g	219	6.2
802.11n (2.4GHz)	1604	46
802.11n (5GHz)	945	27.1
802.11n (2.4GHz + 5GHz)	2549	73.1
802.11ac	625	17.9
Total	3494	100

4.2.7 SSID Broadcast

The networks discovered in Auckland city with blank SSID values have been tabulated in Table 14. The percentages of cloaked networks in the Wi-Pi and the Laptop scans are not matching.

Table 14: Auckland CBD hidden SSID broadcast WLANs

SSID Broadcast	*Day Scan*	*Night Scan*	*Wi-Pi Scan*	*Laptop Scan*
Hidden (or Cloaked)	134	138	202	302
Cloaked %	23.18	20.75	23.51	8.64

Similarly, the total percentages of cloaked networks in Mt Albert and Pernell can be found in the following table.

Table 15: Total hidden SSID broadcast WLANs in Mt Albert and Parnell

SSID Broadcast	*Mt Albert*	*Parnell*
Hidden (or Cloaked)	146	301
Cloaked %	75.64	79

4.2.8 Geolocation of APs

As explained in Section 3.5, the data presentation includes locating the APs on Google Maps. Figure 4, 5 and 6 show geographical mapping of APs found on the route covered in Auckland CBD, Mt Albert and Parnell during warwalking.

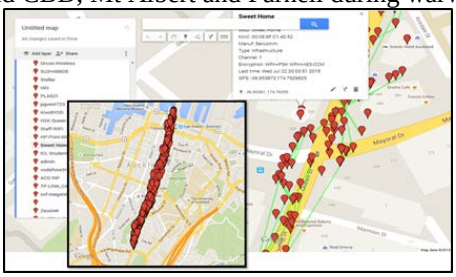

Fig. 4 Location of APs in Auckland CBD from laptop scan on Google Maps.

Fig. 5 Wi-Pi device.

Fig. 6 Wi-Pi device.

5. Result Discussion

A comprehensive result set was provided in the previous section. Results were recorded at different times of a day and on different days to confirm their accuracy. Based on these results, this section discusses their implications and reasons and then answers the research questions.

5.1 Discussion on Variations

The reasons for errors found in the pilot run in Section 4.1.1 were identified and corrected by detailed analysis. The missing geolocations of APs was most likely because of the considerable delay required by GPS for satellite communications to locate its initial position. Beginning the field run, without waiting for GPS to set its initial location, misses out the initial APs. Secondly, the time displayed in the readings was taken from the system time set on Wi-Pi. To resolve this issue, the system time on Wi-Pi needs to be updated. Kismet keeps writing to the log files continuously, which can corrupt them if copied abruptly. To avoid this, stopping the Kismet server before copying is advisable. Finally, the calculation of the average GPS coordinates was believed to be affected due to real time processing done by Kismet [15]. A workaround was done by manipulating the .kml conversion python script, netxml2xml.py (Section 3.4), to calculate the average from maximum and minimum longitude and latitude values.

After data collection, all APs were listed under the 802.11b+ category. This error could not be identified with pilot readings as they were numbered. Kismet detects the PHY type based on its communications with the Wi-Fi adapter driver [15]. To overcome the error, an advanced adapter with dual band support was required. However, most of the latest adapters are not supported by Raspbian [14] or Kismet [15], giving way for the use of a Windows laptop instead.

5.2 Discussion on Findings

The experiment was conducted many times, as explained in Section 4.1.2. Other than the pilot run, the Wi-Pi was used twice for "Day and Night Scans" and once with the laptop during the day (only in Auckland CBD). This section discusses the results obtained from each run.

5.2.1 Discussion on Wireless Network Results

The total number of networks found was different in every scan (Section 4.2.1). The Wi-Pi scan was obtained by combining the results from both scans and ruling out the rows with duplicate BSSIDs. It showed a relatively higher number of networks (Table 1, 2 and 3), indicating that majority of the APs found in each scan were exclusive. It could be because the ones used for official purposes during daytime were shut down at night, with the personal APs being turned on. This justifies the purpose of running the test twice during selected hours. The total number of networks obtained from the laptop, however, varies considerably with Wi-Pi results. In fact, the Wi-Fi adapters used were different (Section 5.1). The one used with the laptop was a dual band adapter that can sniff 2.4GHz as well as 5GHz channels while the one supported by Raspbian sniffs only 2.4GHz.

5.2.2 Discussion on Encryption Status Results

Results of the encryption status in Auckland CBD show a similar majority of 68% in day and night scan results for WPA2 standard (see Section 4.2.2). This is the latest security standard in practice since 2004. Over all these years it has proved secure enough to safeguard wireless networks [1]. This justifies the adoption of WPA2 standard by a majority of wireless networks, which is also apparent from the laptop results that show 77% of WPA2 encrypted networks (Section 4.2.2). The WPA2 proportion from laptop, however, is higher than that from Wi-Pi results, but same as its sum of "Other" and WPA2 standards which are 9% and 68%, respectively. The "Other" networks, which are a result of incomplete information, could actually have been WPA2, refrained from getting detected during the walk due to real time processing on a minicomputer like Raspberry Pi.

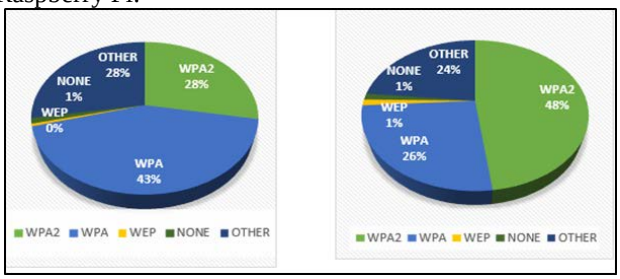

Fig. 7 Day and Night Scan Results of Encryption Status in Mt Albert.

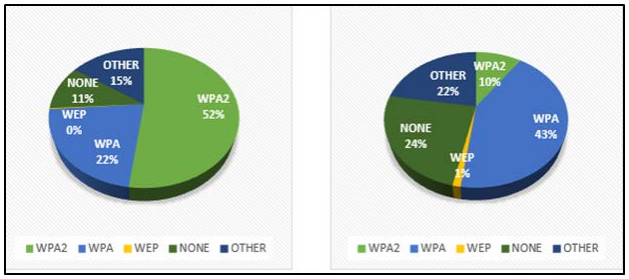

Fig. 8 Day and Night Scan Results of Encryption Status in Parnell.

On the other hand, results of encryption status in Mt Albert (Figure 7) show different in percentage of day (28%) and night scan (48%) results for WPA2 standard. However, there is not much different in percentage of day (52%) and

night scan (43%) results for WPA2 standard in Parnell (Figure 8).

The proportion for "Open" networks in Auckland CBD remains the same, roughly 21% for all the scans (see Table 4). This, although less with respect to encrypted networks, is a substantial percentage for this category. However, the proportion for "Open" networks in Mt Albert and Parnell are very minimal, just over 1% and 11% respectively (see Tables 5 and 6). With an increasing number of cybercrimes, especially in the wireless domain, advanced security measures are being put in place to counter them. The existence of 21% of open networks in Auckland CBD shows a clear demand for increasing security awareness in the region. This demand appears justified at first glance of the results but keeping the networks open, however, could be deliberate. The Auckland CBD area has many shops and public attractions. For their promotion and public welfare, they can provide wireless networks. These networks could primarily be for the sake of entertainment and online social updates, instead of critical applications like banking and e-commerce. To share this message across all the users of their networks, the administrators could have deliberately disabled its encryption, avoiding any false sense of security. Other reasons could be to allow users to easily connect to the network without any compatibility issues arising due to the security standards. Furthermore, instead of enabling encryption, some of the networks rather use captive portals where users maybe authenticated on the browser after connecting to the Wi-Fi network.

In spite of rational justifications, these arguments, however, do not defend all the open networks. Some of these connections can be for home or office users, having improper installations, or even could be malicious networks, kept open to attract as many users, allowing the network owner to easily analyse any financial or other critical usage over the unencrypted channel.

5.2.3 Discussion on Channel Distributions

The distribution of APs among all the channels in 2.4Hz band for Pi and laptop is drastically different. For the Wi-Pi results, almost all the networks are either using channel 1 or their channel was undiscovered and set to 0. The results from the laptop are more noteworthy and even. This variation could be because of differences in the capabilities of the Wi-Fi adapters or due to real time processing by Wi-Pi, as explained previously (Section 5.2.2). The figure and the table showing laptop (Figure 3) and Wi-Pi scan (Table 7) results state larger proportions of networks lying under the 1, 6 and 11 channels but there are APs communicating on non-recommended channels as well. Collectively, they form an average of 33.7% of the total networks in the 2.4GHz band (34% in CBD, 29.5% in Mt Albert and 37.6% in Parnell). These APs bleed into the frequency bands of the neighbouring ones, not only decreasing their own speed of operation but also of neighbouring APs, even of those which use the recommended channel bands [1]. On the other hand, the 5GHz band (conducted only in Auckland CBD due to limitation, Section 3.6) has enough channels to avoid any limitations and all of the 24 channels divided into 4 channels are usable [16]. As Table 8 shows, there is an even distribution of APs in this band. This justifies a shift of the latest 802.11 standards such as 802.11n supporting both bands instead of only 2.4GHz and 802.11ac is only used in the frequency band of 5GHz.

5.2.4 Discussion on Network Type Results

Almost all of the APs were infrastructural except a minor percentage of ad hocs (Table 9). These could be one used for internal testing purposes in offices, as names in a few SSIDs suggested, or connecting different electronic equipment in homes or hotels. Differences between Wi-Pi and laptop results could be due to incomplete information collected by Wi-Pi.

5.2.5 Discussion on Manufacturers Results

In the list of manufacturers, Aruba and Cisco are the leaders in the Auckland CBD region, evident from all the scans in Tables 10 whereas Aerohive, Apple and Ubiquiti are front-runners according to scan results as shown in Tables 11 and 12 (see Section 4.2.5). Few manufacturers like Ruckus and Huawei, have considerable differences in Wi-Pi and laptop results. Latest devices of these manufacturers might not be updated in Kismet. This could have caused their APs getting listed in the "Other" networks category of the Wi-Pi results. However, according to previous research [9], the top three AP manufacturers are Cisco, Thomson and D-Link (Table 16) although D-Link was the most favourite one in 2007. Hence, our results confirm that Cisco AP are popular and still dominating the market in Auckland CBD.

Table 16: List of manufactures in Auckland CBD

Vendor	*Count*	*Percentage*
Cisco Systems	218	18.3
Thomson Telecom Belgium	184	15.4
D-Link Corporation	144	12.1
Netgear Inc	143	12.0
Askey Computer Corporation	86	7.2
…	…	…
Total	1194	100

5.2.6 Discussion on PHY Type Results

It is more than four years since launch of 802.11ac standard, which is not a long time span looking at its percentage, 17.9%, especially when its predecessor 802.11n had successful hold in WLAN domain [4]. A drift for latest technology trends is evident from these statistics.

5.2.7 Discussion on SSID Broadcast Results

Hiding the SSID broadcast, may not completely secure the networks, but does add to security [1]. Exposing the identity like address, manufacturer, name or other personal information, if does not help to crack the network traffic, can always guide the attackers towards selecting desired networks. Only 8.4% and 23.51% of the networks in laptop and Wi-Pi scans (respectively) were found to have hidden SSIDs in Auckland CBD, which shows a poor concern for hiding identity (see Table 14). On the other hand, 75.64% and 79% of the networks were found in Mt Albert and Parnell areas by Wi-Pi scans. The Wi-Fi routers by default do not hide the SSIDs. Most home users, either out of laziness, fear of accidental misconfigurations or due to lack of technical know-how do not change the default settings. The lesser number of cloaking percentages found in Auckland CBD could also be due to the shop and hotel owners keeping the SSIDs open for their users to easily identify and connect. Likewise, the offices could have kept them open to allow their employees to continue connectivity even when away from their workstations. The difference in the readings between Wi-Pi and laptop could be due to the total AP count. Nevertheless, our results confirm that the security of WLANs in Auckland suburbs is higher than those in CBD area.

5.2.8 Comparison of Findings

Table 17 contrasts the results of this research with studies conducted by Nisbet [1], Halim [8], Sarkar and Abdullah [9]. Comparing against 40% encrypted signals in 2004, which raised to 74% in 2007, Sarkar and Abdullah [9] found 88% signals, out of total 1194 detected, to be encrypted. This count includes 31 ad-hoc networks. The remaining infrastructural networks, showed an increase from 75.7% SSID broadcasting encrypted networks in 2007 to 87.5% in 2011. Among the detected encrypted networks, 71% usage of better encryption protocol, WPA2 was found suggesting an awareness improvement. Citing the importance of wireless security, the authors recommend updated encryption technologies, changing default SSID, MAC address filtering and VPN as practical solutions to further enhance security. Understanding an appreciable wireless security increase of 48% since 2004, they still find room for further improvement and recommend additional wireless security practices.

Table 17: Result comparison with previous literature (adapted from: [1], [8], and [9])

Criteria	*Halim (2007)*	*Sarkar and Abdullah (2011)*	*Nisbet (2013)*	*Pi Scan (2015)*	*Laptop Scan (2015)*
Total Networks	506	1194	3255	859	3494
Encrypted %	74.31	88	77.6	79.86	80.68
Cloaked %	4.94	0.58	0.3	23.51	17.56
Ad Hoc %	4.54	2.6	1.16	2.79	0.06
Infrastructural %	95.46	97.4	98.84	97.21	99.94

Comparing Wi-Pi with Nisbet [1], the total number of WLANs shows a decrease. His study was run for a longer duration using a laptop. Comparison between the ratios of encrypted networks, although not significantly, has increased from 74.31% in 2007 to 77.6% in 2013 to 79.86% with Pi and 80.68% with laptop. The SSID broadcast hiding shows an increase when compared to 4.94% cloaking in 2007 and 0.3% in 2013. The ratio of ad hoc networks when compared with Wi-Pi results shows an increase while that with the laptop shows a decrease. This could be because the readings were taken on different days.

5.3 Answers to Research Questions

Equipped with the current and comparison statistics, this section answers the main research question after discussing answers of its sub questions, mentioned in Section 3. Table 18 presents this discussion in a tabular form.

Table 18: Research answers

Questions	*Answers*	*Discussion*
How many WLANs are there in the Auckland city (especially in CBD, Mt Albert and Parnell)?	In Auckland CBD Wi-Pi = 859 Laptop = 3494 In Mt Albert Wi-Pi = 1267 In Parnell Wi-Pi = 772	The count is not exhaustive, as during each run the number of WLANs found was different. These results only indicate the detected WLAN count (Section 4.2.1)
How many, with respect to total WLANs, are encrypted?	In Auckland CBD Wi-Pi = 79.86% Laptop = 80.68% In Mt Albert Wi-Pi = 95.86% In Parnell Wi-Pi = 78.68%	Section 5.2.2 discusses reasons, other than the accidental ones, for the networks to be deliberately kept open. Encryption percentage of WLANs in Mt Albert area is much higher than Auckland CBD and Parnell.

What is the ratio of cloaked networks?	In Auckland CBD Wi-Pi = 23.51% Laptop = 8.64% In Mt Albert Wi-Pi = 75.64% In Parnell Wi-Pi = 79%	Although not completely in practice, SSID hiding has considerably increased over past years (Tables 14 and 15). Section 5.2.7 discusses this result.
What is the difference in the percentages of encrypted WLANs between present and previous studies in Auckland CBD?	For 2013 Wi-Pi = 2.26% Laptop = 3.08% For 2011 Wi-Pi = (-8.14) % Laptop = (-10.26) % For 2007 Wi-Pi = 5.55% Laptop = 6.37%	Percentage increased in 2011 then decreased in 2013 and almost similar in 2015 (see Table 17 for details).
Main: What is the current security status of WLANs in Auckland city?	Insignificantly increasing but appreciable	Although not significant, the current security status has minor improvements. An increase in technical awareness among people can be seen based on the increase in cloaking percentage. Discussion on deliberate deployment of unencrypted WLANs (Section 5.2.2) justifies slow growth in security trends.

Conducting the field run three times might not be exhaustive in terms of the total number of networks, but getting similar proportions is indicative of the correct ratio of selected categories. This is confirmed by comparing the results from the Wi-Pi and laptop for encryption standards, SSID broadcast and to some extent for the manufacturers (Section 4.2). With this confirmation, it can be safely concluded that such warwalking trials to evaluate security status are worth conducting.

Apart from encryption methods, other practical security mechanisms are also recommended. They include changing the default SSID to ensure that the identity of the user such as name, address, phone number or AP manufacturer is not disclosed. MAC address filtering is another method which allows only the registered devices to be able to connect to the AP by filtering the unregistered MACs. VPN is another successful security mechanism [4]. Deployment statistics of these methods were not evaluated.

6. Conclusion

Our research is to comprehend the extent of public awareness in an area, and the significance of WLAN security. It was accomplished by identifying the WLAN security practices in Auckland city including Auckland CBD, Mt Albert and Parnell – three locations, and comparing them against results from previous studies in similar locations. Wireless networking is a significant technology but highly exposed to attacks. Thus securing communications over a WLAN is a matter of concern as well as a major challenge. This was highlighted in Section 1 to explain the objective of this study and its significance. It also discussed the methodology used to carry out this research and the contributions it would make to different sections of society. Section 2 emphasizes reviewing similar published works done by other authors. Other than complying with best practices for wireless sniffing and precautions to avoid likely errors, Section 2 also identifies the information gaps which exist between the referred literatures. Objectives, descriptions and justifications of the methodology adopted for this research was stated in Section 3. It also explained the components used for the experiment, design of the equipment and procedures to capture data, analyse and present it. Section 4 tabulates the collected findings along with any variations encountered during field runs. The findings discussed in Section 5 answer the research questions. Finally, this (conclusion) section, interprets all the findings to conclude this study.

With respect to the status of Auckland city in 2007, an increased number of WLANs accompanied with an increased percentage of encrypted ones, which was also observed from 2013 statistics, emphasize the orientation of public attention towards securing wireless networks. Drastic increments in SSID cloaking and statements supporting deliberate deployment of open WLANs also nullify the substantial percentage of unencrypted channels, thus favouring the conclusion that a psychological inclination does exists among people to safeguard their wireless communications. Other than security, concentration of physical layer types in 802.11n and 802.11ac category and even distribution of WLANs across channels of both frequency bands also demonstrate a shift towards newer technology standards with proper configurations. Either for economical or awareness factors, the pace of technology advancement is always faster than its practice at the social level. Therefore, albeit with considerably slower pace, people are getting aware of the need for wireless security.

During its course, the research came across many other areas of knowledge, closely coupled to the key research focus. The list of manufacturers, for example, can be shared with advertising agencies to guide users during fresh installation of WLANs. The list of APs with misconfigured channels can be shared with concerned authorities like PCI for necessary actions. Due to technical and time constraints, the research could not completely analyse the WLANs compliant to the latest IEEE standard 802.11ac. As specified by IEEE, the data rates for this standard can be configured for much higher throughput than its previous counterparts. Considering this privilege, further statistics

related to security and deployment of this standard, especially in a central business district, is extremely prospective and worth exploring. This report recommends a continuation of similar evaluations for upcoming technology upgrades working towards the advancement of secure wireless networking.

Acknowledgments

We would like to thank Pulin Agrawal, Dinesh Rai and Anoop Wadhawan for conducting warwalking at Auckland CBD, Mt Albert and Parnell in Auckland City, New Zealand.

References

[1] Nisbet A. A 2013 study of wireless network security in New Zealand: Are we there yet?. In: Proceedings of the 11th Australian Information Security Management Conference, Edith Cowan University, 75-82; 2013 Dec 2; Perth, Australia.
[2] Priya CS, Umar S, Sirisha T. The impact of war driving on wireless networks. International Journal of Computer Science and Engineering Technology. 2014; 3: 230-235.
[3] Gopalakrishnan S. A survey of wireless network security. International Journal of Computer Science and Mobile Computing. 2014; 3: 53-68.
[4] Singh P, Mishra M, Barwal PN. Analysis of security issues and their solutions in wireless LAN. In: Proceedings of Information Communication and Embedded Systems, IEEE, 1-6; 2014 Feb 27; Chennai, India.
[5] Christie S. War Pi. Bethesda, Maryland (United States of America): SANS Institute; 2013.
[6] Kyaw AK, Cusack B. Security challenges in pervasive wireless medical systems and devices. In: High-capacity Optical Networks and Emerging/Enabling Technologies, IEEE, 178-185; 2014 Dec 15; Charlotte, North Carolina, United States of America.
[7] Lin CI. Raising security awareness among higher education recipients [Doctoral Thesis]. Cheney (WA): Eastern Washington University; 2009.
[8] Halim SA. Exploring wireless network security in Auckland City through warwalking [Master's Thesis]. Auckland (New Zealand): Auckland University of Technology; 2007.
[9] Sarkar N, Abdullah AH. Exploring wireless network security in Auckland City through warwalking field trials. In: Proceeding of the 13th International Conference on Advanced Communication Technology, IEEE, 685-689; 2011 Feb 13; Gangwon-Do, South Korea.
[10] Kalbasi A, Alomar O, Hajipour M, Aloul, F. Wireless security in UAE: A survey paper. In: Proceedings of the 4th IEEE-GCC Conference; IEEE, 2007 Nov 12; Manama, Bahrain.
[11] Tsang P, Kwok P, Kwan R, White B, Fox R. Innovation in ICT teaching: A longitudinal case study of Wi-Fi in Hong Kong. International Journal of Innovation and Learning. 2011; 10: 85-101.
[12] Bryman A. Social research methods. Oxford, United Kingdom: Oxford University Press; 2012.
[13] Bryman A, Bell E. Business research methods. Oxford, United Kingdom: Oxford University Press; 2015.
[14] RaspberryPi.org [Internet]. Raspberry Pi - teach, learn, and make with Raspberry Pi: 2015. Available from: https://www.raspberrypi.org.
[15] Kismetwireless.net [Internet]. Kismet: 2013. Available from: http://www.kismetwireless.net/index.shtml.
[16] Gast MS. 802.11ac: A survival guide. Sebastopol, California (United States of America): O'Reilly Media Inc.; 2013.