

A Sample of Consumer Wi-Fi Use & Security in the UK

Stuart Cunningham & Vic Grout
 Centre for Applied Internet Research (CAIR)
 Glyndŵr University, UK
 {s.cunningham | v.grout}@glyndwr.ac.uk

Bogdan V Ghita
 Information Security & Network Research Group (ISNRG)
 University of Plymouth, UK
 bghita@cisnr.org

Abstract—Wireless networking technologies permit a great deal of convenience for mobile users. However, as is often the case, increased levels of technological freedom means there is more potential for abuse and misuse of these services. In this work we find the uptake of wireless networking technology has risen rapidly in recent years and the perceived awareness of security issues has also been heightened. We undertake a number of practical investigations in various communities to determine exactly how many and how accessible Access Points (APs) are in the metropolitan environment. This paper presents comparisons between previous and new independent studies carried out by two research teams in different areas of England and Wales, in the United Kingdom (UK).

Index Terms— Internet, Networks, Security, Wireless LAN

I. INTRODUCTION

WIRELESS (Wi-Fi) Internet access is now commonplace among Internet users. Access Points (APs) provide wireless Internet coverage in the areas surrounding their installation. The lack of a physical link between a client and AP means that anyone within transmission range of an AP has the potential to access the network that the AP services. Such activities, undertaken to misuse wireless access points, are commonly referred to as war driving.

This work presents independent investigations into Wi-Fi use within communities in the UK. The ISNRG research group is based in the University of Plymouth and the CAIR research group are based in the North East Wales Institute of Higher Education, part of the University of Wales. Each research group undertook their investigations in areas within their own regions of the UK. After detailing the findings of each of the research groups, we then compare and contrast the findings of the two groups and discuss prominent issues which need to be addressed in future investigations and research activity.

II. CAIR STUDY

A. Overview

In these investigations, we focused on two distinct

community areas. In order to realistically and practically assess the accessibility of APs within these communities we did not opt to employ any special equipment in our studies (aside from the inclusion of a Global Positioning System (GPS) which is not directly involved in the *detection* of APs). Our main intention in employing non-specialist equipment was to emulate the kind of equipment and conditions which could be easily acquired; to simulate closely the materials and environment of the casual war driver. To this end we did not use any external, extended range antennae or amplifiers to boost the signal in any way. We also made the assumption that only the most determined of war drivers would leave the confines of a vehicle as this provides an element of urban camouflage, power for equipment and shelter. This meant covering each designated investigation area in a car. Arbaugh *et al.* (2002) notionally refer to such intrusion attempts, under the constraints we described, as the “*parking lot attack*” [1]. When undertaking such actions for the purposes of academic research and to raise awareness of the issues related to wireless Internet use, we name our activities peace driving.

We followed the road network across the designated areas and employed a Toshiba laptop computer with an integrated wireless adapter and a Global Positioning System (GPS) to ensure that we were able to make an accurate mapping of the APs, and most crucially, the relative density of APs within this limited area. This allows for the detection of available wireless networks, both secure and insecure (and the ability to discriminate between them), and an associated GPS location for the point where the AP was discovered. The NetStumbler software package was used for the detection of APs. In all of our studies we followed the road network in each area over several days during the hours of 09:30 to 12:00 and 13:30 to 17:00.

The first investigation took place across a 16km² area which, from our own prior observations, we knew to contain residential, commercial and industrial zones. The total population within the area surveyed is approximately 60,000. This first study was undertaken in April of 2007. Further detail of this study can be found in a previous work [2].

The second study was undertaken some time after the first in order to strengthen the findings of the original study and to draw comparisons with the results of the first investigation.

Though only eight months separated the two studies, and a different region would be surveyed, it is interesting to look at the number of APs encountered and how many of these are considered to be secure. The second investigation was carried out over a similar area constituted of the same type of zones. The main difference in this second survey was that the area was approximately 4km². The population of the area in this second investigation is approximately 15,600. This second investigation was carried out on two separate days, the first in December 2007 and the second in January 2008.

B. Mapping and Features of Access Points

The mapping of APs discovered in both searches is shown in Figures 1 and 2 and detailed in Table 1. These figures show two classes of APs which have been detected; those which employ WEP (Wired Equivalent Privacy) encryption and those which do not.

It should be noted that, for the purposes of anonymity, the orientation, exact scale, and identifiable parameters are removed from all information presented in this section. Where appropriate, we indicate broad areas and classifications from actual knowledge of the area surveyed and data retrieved, but we feel it is not appropriate to detail particulars.

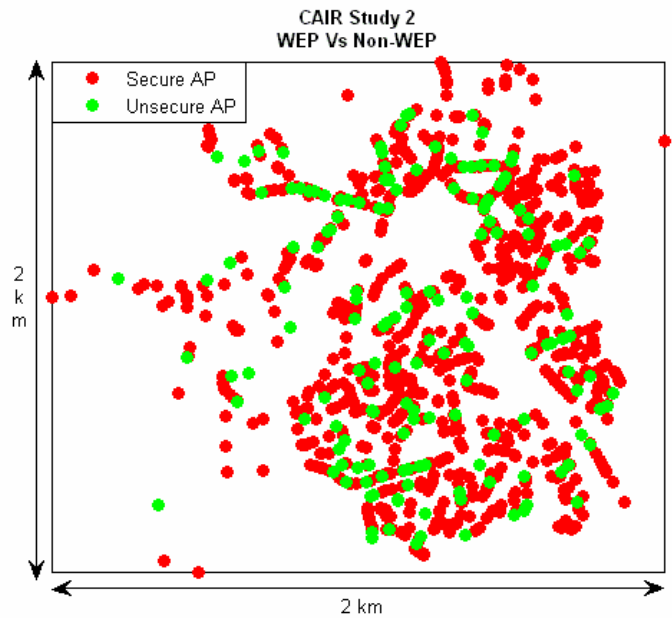


Fig. 2 Mapping of WEP and non-WEP APs in Study 2

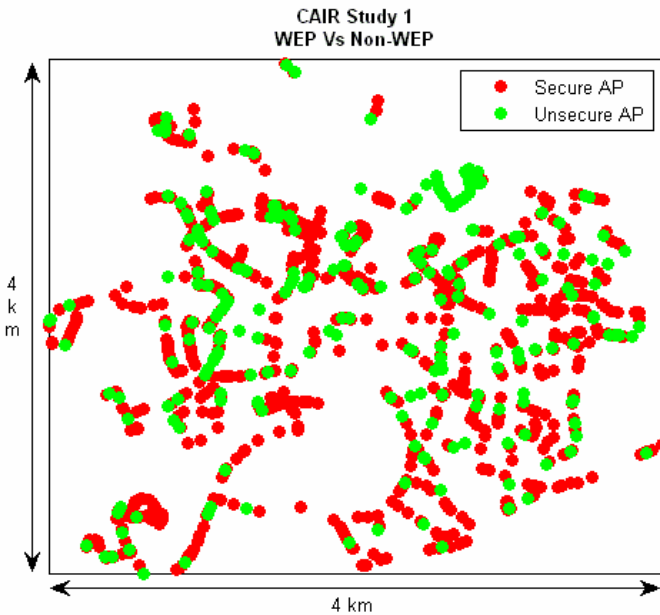


Fig. 1 Mapping of WEP and non-WEP APs in Study 1

TABLE I
AP DETAILS FROM CAIR WI-FI STUDIES

Study	Area	APs	Mean APs / km ²	Non-WEP APs	WEP APs
1	16 km ²	1153	72.06	262 (23%)	891 (77%)
2	4 km ²	1113	278.25	159 (14%)	954 (86%)

The mapping results from the first study provide interesting contrast to that of the second study. If we initially consider the distribution of APs across each square area, the first study shows APs which are sparser and more evenly spread than those in the second study. We must remember the differences in size and approximate population between the two areas, however, this is also an interesting point to note when we take into account the fairly similar number of APs despite the size of the second study being smaller. Of course, the mappings do have an underlying structure to them, which is most clearly seen in Figures 1 and 2, because of the road network followed to allow discovery of APs.

It is of particular interest to note that the majority of APs are encountered within residential zones. This was supported by noting the occurrence of default SSID (Service Set Identifier) names on many of the access points. In the second study, many more APs were encountered with the default names associated with Internet Service Providers and equipment manufacturers. For example, SSIDs such as “BTHomeHub”, “BT Fusion”, “NETGEAR”, “BTVoyager”, “DLINK_WIRELESS”, “linksys”, and “Wanadoo” frequently appeared. In the second study in particular, there was a marked increase in other providers which had recently launched broadband Internet services such as “LiveBox”, “SpeedTouch”, “TalkTalk”, and “Sky”.

Given the size differences in the areas covered we can assume that on average, there has been growth in the uptake of wireless networking within the community. The number of users aware of the need for security, even if that might only be

by using WEP, has also increased, although this is not entirely conclusive for reasons mentioned elsewhere in this paper. However, in the areas covered during the second study it was noted that there was a much larger amount of residential and suburban zones encountered, along with smaller commercial and industrial areas, than in the first study. The zones also differed in terms of the surroundings which were not covered as part of the study (to incorporate these outlying zones in the original study would have considerably increased the size and time required to methodically inspect the additional areas). Beyond the square area in the first study there remained some other residential and industrial areas whereas in the second study almost all of the entire community was concentrated within the square area, which has the effect of making the results of this study somewhat more reliable and representative of the *community* under investigation rather than purely the sampled area.

In a previous work, where we concentrated on the results present from the first study, we suggested that it was useful to be able to define zones or areas within a set of AP point mappings. As we state in our previous work, once a number of zones have been identified it then becomes much easier to correlate particular characteristics discovered during the peace driving with other information about the region such as population, financial and social trends, for example. In particular, having an automated method of defining zones would be highly beneficial, as this eliminates the immediate need for any local knowledge of the area [2]. One method we found reasonably successful in being able to separate out larger known areas from the AP survey data was the k -means algorithm [3].

The best results in the first study were achieved where $k=4$, and this is visually shown in Figure 3.

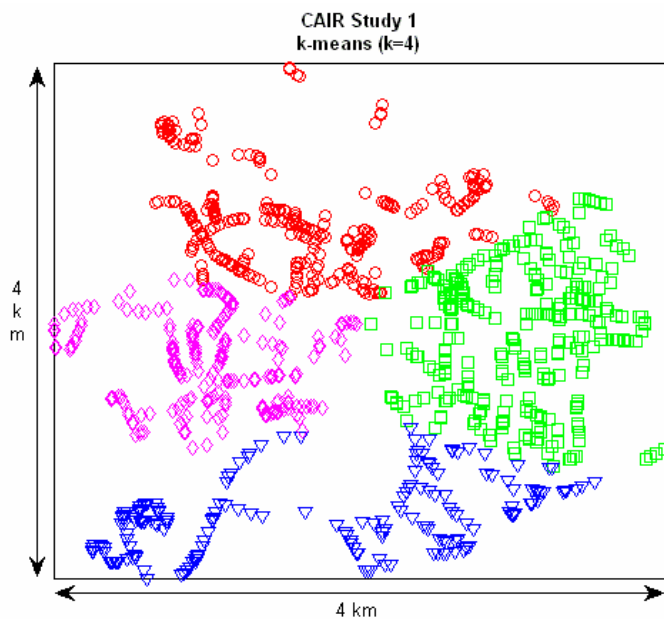


Fig. 3 k -means 4 cluster distribution for the first CAIR study

Again, in our second study we had some local knowledge

of the area and found that again the k -means algorithm, with a value of $k=4$, was most successful in providing some dividing-up of the surveyed area. The result of dividing the results using the k -means algorithm is shown in Figure 4.

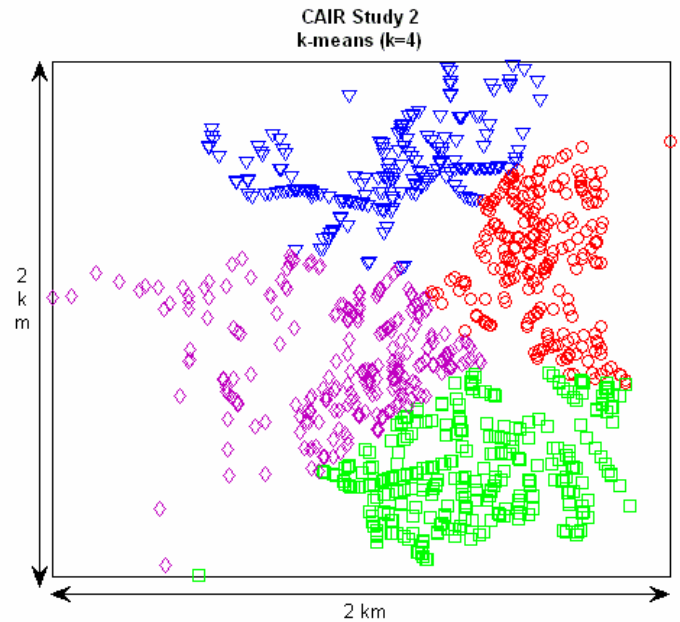


Fig. 4 k -means 4 cluster distribution for the second CAIR study

C. Community Survey

A small scale survey was undertaken of the communities examined in the earlier AP mapping exercise to seek further knowledge of the awareness and uptake of security measures and the main reasons for users having Wi-Fi access. A brief profile of AP use and configuration is shown in Table II.

TABLE II
SURVEY DETAILS

Wi-Fi Internet Usage		
Personal (68.2%)	Mix of Personal & Work (31.8%)	
Have you changed the SSID?		
Yes (68.2%)	No (22.7%)	Don't Know (9.1%)

Figure 5 illustrates the distribution of the range of security measures available to protect Wi-Fi APs, based upon the survey responses received. These range from implementing the encryption processes WEP and WPA, access control filtering using either MAC addresses or IP addresses, hiding the SSID of the AP, and changing the default administration password of the router configuration tool.

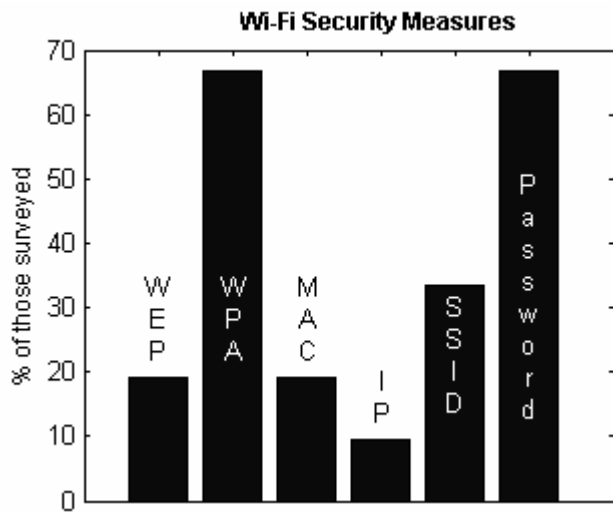


Fig. 5 Security Measures Implemented

The survey results are encouraging from the perspective of assuring that a reasonable and contemporary range of security measures are being applied. The majority of encryption employed by users is the more robust WPA rather than WEP and the bulk of users have also taken the fundamental step of changing the default passwords on their routers / APs. Nevertheless, whilst the surveyed majority of users may be employing these measures there are still at least 30% of users who are not. Additionally, only a low percentage of those surveyed employ access control filtering, which, particularly when combined with WPA, offers much more robust protection.

III. ISNRG STUDY – WIRELESS SECURITY TRENDS

A. Overview

A series of four surveys was conducted between winter 2003 and winter 2006 in the city of Plymouth. The surveys mainly focused on the city centre and neighboring wards as well as the areas with higher student population, with slight variations between the studies. The equipment used also varied – the 2003 and 2005 surveys used a laptop either with a PCMCIA dongle and an external antenna or with integrated WiFi, while the 2004 study used a PDA with integrated WiFi and Compact Flash GPS device. In terms of software, the initial 2003 study used a software developed as a final year project (AirWalk), while the other studies used NetStumbler. A more detailed description of the study from summer 2004 can be found in [4].

While all efforts were made to fully cover the surveyed area, the occasional poor reception of the GPS antenna led to unusable data, with some access points being recorded with zero coordinates. Similarly, due to the variations in hardware, it is possible that some of the access points might have been missed in successive studies.

B. Results

While several parameters were recorded for each collection, the main aim of surveys was to monitor the evolution of the

security features for wireless networks. As in the CAIR study, for each access point, amongst other information, the collection recorded the SSID and whether the WEP is enabled or not. The results of the study are summarised below in Table III.

TABLE III
SUMMARY OF RESULTS FROM THE PLYMOUTH SERIES OF STUDIES

Study	AP found	Default name*	No WEP	Default name and no WEP
Winter 2003	105	39.04%	60%	32.38%
Summer 2004	296	41%	60.96%	31.75%
Winter 2005	343	47.53%	51.03%	32.94%
Winter 2006	751	42.61%	30.76%	17.04%

* The default name values, as described in the initial studies, were reviewed with more comprehensive lists of default SSIDs, such as the one from <http://www.wardriving.ch/hpneu/info/doku/ssiddefaults.txt>

The table indicates an encouraging trend between the studies, as the number of non-WEP networks, while comparable between the first two studies, decreased by 10% in the 2005 survey and, by 2006, less than a third of the access points were not using WEP. This is reflected also in Figure 6, shown below, which presents the distance mapping of the access points, based on the GPS coordinates.

A generic comment, as discussed in section 2 is that WPA or any other additional encryption technique cannot be identified using the non-intrusive techniques employed by Netstumbler. As a result, the number of unsecured access points is likely to be smaller. For example, the University of Plymouth wireless access points allow unencrypted access, but require logging on a VPN server in order to allow any further network connectivity – the surveys include between 7 and 25 such access points (identified through their location and SSID). Another observation, this time on the positive side, is that access points with the SSID in the form of 2WIRExxx (where xxx is a combination of digits) were all identified to use WEP encryption. This is correct, as these devices are likely to be 2Wire wireless routers, which come with WEP enabled as standard and allow the user to disable it only by interacting with the device and saving the changes; the 2004 study found 8 such devices, all using WEP encryption.

The 2006 study revealed a different worrying trend: 26 access points were named by their location (house number and street name). This provides potential attackers with address information – should they be able to eavesdrop or misuse the network, they would also be able to correlate the information they send with personal information about the owner of the network. Luckily, only 8 (eight) access points were both named using their address and had no WEP encryption enabled.

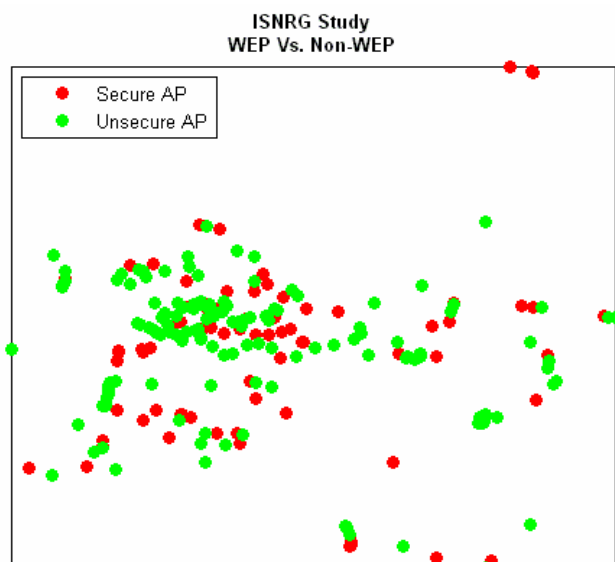


Fig. 6 Distribution of the Plymouth wireless access points (2004 study)

IV. COMPARISON OF STUDIES & FUTURE WORK

A. Netstumbler Limitations

One particular point for consideration is that the NetStumbler software is currently only able to detect secure access points as those which are enable with WEP encryption. This means that APs which use other techniques such as MAC address filtering or WPA (Wi-Fi Protected Access) are detected, within the realms of this study, as being insecure. This, in fact, can be extended to identifying even those APs using WEP as also being insecure. WEP is widely acknowledged as having many shortcomings [1, 5, 6]. It is also possible that those APs using WEP might also have further underlying protection mechanisms in place; however, we believe this to be less likely for two reasons. First, WEP is often the default security measure implemented during initial set-up for an access point. Secondly we would assume a user sufficiently informed about wireless security would be aware of the problems with WEP and opt for another set of security measures. The authors acknowledge that data collection should not impact on the user privacy, but it is felt that, in its current form, the lack of interaction required by the law is severely limiting the scope of the study.

B. Study Comparison

The two studies indicated that the level of security on wireless network is improving over time. Starting with a worrying 60% of networks not employing any security¹ back in Plymouth 2003, the most recent studies indicated similar levels of non-WEP networks, around 30%. The increasing usage of WEP as the encryption protocol of choice for wireless networks was presented throughout this study as a

¹ Although the software cannot differentiate between WPA and no encryption, based on the time of the survey (and the early stages of WPA adoption), it is likely that the endpoints identified as “non-WEP” were in fact not employing any encryption, rather than using WPA.

positive outcome. However, in the wider context, this is not necessarily a good trend. As demonstrated by prior studies, WEP is a rather weak encryption by current standards and cracking it is only a matter of time. From this perspective, it is actually the non-WEP wireless access points, which include alternative encryption methods that are more likely to provide appropriate security.

C. Further Work

The two parallel studies provide an initial overview of comparative statistics between wireless securities in remote geographical locations. Due to the differences in hardware and collection methods, it is difficult to infer whether the collected information is a good estimate for the actual number of networks in the two locations. In future, for better consistency, the parallel studies should be using the same methodology

One aspect that was not pursued due to insufficient data was the persistency of access points over time. The lifespan of access points can be tracked over time by using their MAC addresses in order to determine possible network/infrastructure upgrades, as well as determine any changes in the configuration (e.g. enabling encryption or renaming the access point).

Due to the limited scope of the study, the series of surveys was not followed by a series of interviews with the owners of the network in order to determine their awareness of wireless security issues or the reasons behind implementing / not implementing any authentication/encryption solutions for their access points.

REFERENCES

- [1] Arbaugh, W.A., Shankar, N. and Wan, Y.C.J. (2002), “Your 802.11 Wireless Network has No Clothes”, *IEEE Wireless Communications*, Vol. 9, 2002, pp. 44-51.
- [2] Cunningham, S & Grout, V. (2007), “War & Peace: A Practical Study of Wi-Fi Related Issues”, *Proceedings of the International Conference on E-Activity and Leading Technologies (E-ALT 07)*, Porto, Portugal, December 2007, pp. 393-399.
- [3] Bishop, C.M. (2006), *Pattern Recognition and Machine Learning*, Springer-Verlag, New York, 2006.
- [4] Voisin M., Ghita B.V., and Dowland P.S. (2005), “Survey of Wireless Access Point Security”, *Proceedings of the Fourth Security Conference 2005*, Las Vegas, USA, 30-31 March 2005
- [5] Fluhrer, S., Martin, I. and Shamir, A., (2001), “Weaknesses in the key scheduling algorithm of RC4.” *Eighth Annual Workshop on Selected Areas in Cryptography*, August 2001.
- [6] Walker, J. (2000), “Unsafe at any key size: an analysis of the WEP encapsulation,” Tech. Rep. 00/362, *IEEE 802.11 Committee*, March 2000.