Survey of Wireless Access Point Security

M. Voisin, B. Ghita and P.S. Dowland

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

The development of wireless networks has introduced a number of security issues inherent to the communication medium and to the different security approaches available. While WEP encryption is widely accepted as insecure, it remains one of the easiest to use and most widespread wireless security mechanisms – this is unsurprising as it is provided with most 802.11 wireless network equipment. In order to assess wireless access point security, a survey was conducted with a handheld device and wardriving software with the aim of covering a part of the city of Plymouth. While the results were insufficient to link wireless LAN security with demographic information, they provide a global picture of the spread of wireless technology mostly concentrated in the city centre and confirm the fact that many wireless access points are used 'out of the box' with default settings which are, or were until recently, not using any encryption.

Keywords

Wireless networks, Security survey

1. Introduction

With the increased availability of wireless equipment, numerous wireless local area networks (WLANs) have been set up, both for private and commercial use. While security issues on these networks have been well published (Farrow, 2001), activities like wardriving have spread and become a regular activity for hackers.

The study presented in this paper focuses on two different aspects related to wireless networking. The first part aims to analyse the spread of wireless networks, in order to evaluate the current usage of wireless technology, both for personal and business usage. The second part of the paper assesses the security of wireless networks as an exponent to the user's awareness of current network security threats. The results presented in this study reflect a set of surveys conducted in the city of Plymouth (United Kingdom) during 2004.

The paper is organised as follows. The next section will present different security mechanisms usually found in wireless networks. Section three will detail the survey methodology, including the hardware and software used, which aimed to evaluate WLAN security. Section four discusses the results of the survey, focusing on the use of encryption within wireless networks. The final section presents the conclusions of this study and outlines possible further work in the area.

2. Review of wireless security

In the context of the survey of wireless access point (AP) security, it is essential to describe the basics of existing security protection mechanisms. This section aims to give an introduction to some of the most common mechanisms, the level of security they provide as well as their limitations, in order to place this study in the context of wireless security.

2.1 Frame level mechanisms

To address security issues, two basic mechanisms act in the low level frames. The first one consists of muting APs so that they do not broadcast the Service Set Identifier, needed for any client to establish a connection to the network. Indeed, default settings are usually set to broadcast it regularly in plaintext to facilitate clients' connections. While default SSID can usually facilitate finding the administrator's password on the Internet for a device used "out of the box", setting this identifier to the name of the company it belongs indicates to potential hackers what categories of resources may be connected to this network. However, such measure implies the use of another process to supply the SSID to legitimate clients so that they can connect the network. The second mechanism relies on a filter based on a list of Medium Access Control (MAC) addresses of authorised devices. The level of security that this feature brings is also weak as MAC addresses are transmitted in plaintext in each 802.11 frame (whether the connection is encrypted or not) and can then be "spoofed" by almost any wireless card, using appropriate software.

2.2 Encryption

Due to the physical open-access nature of wireless networks, efforts were made to provide a higher level security mechanism, using encryption algorithms. Wire Equivalent Privacy (WEP) encryption is probably the most famous but also the most vulnerable security standard for wireless networks, aiming to restrict both network connectivity, as well as access to the data travelling over it, at a level comparable to the security provided by wired networks. Maybe due to the fact that it was the first wireless specific security method, the implementation of WEP suffers from several flaws. According to security experts, these include: lack of authentication key expiry, vulnerability to "disassociation request" injections, low security MAC level authentication and identification, lack of central security management and weakness of the cipher algorithm WEP due to the Initialisation Vector (IV) generation method used (Khan and Khwaja, 2003). Some of these flaws, such as the weakness in the key scheduling of Rivest Cipher 4 (RC4) encryption algorithm, led to the creation of a number of WEP cracking software applications, which are currently widely available on the Internet, an issue that will be covered in the next section.

Due to the flaws discovered in WEP-based wireless security, a security-driven IEEE workgroup (802.11i) was created in order to propose a standard on Robust Security Network (RSN) (IEEE, 2004). One of the aims of this workgroup was to provide separation between the user authentication process and the message protection, separation that prevents the possible decoding of data based on the observation of the authentication process. The resulting standard was WiFi Protected Access (WPA) (WiFi Alliance, 2002), strongly

supported by the Wireless Fidelity (WiFi) Alliance, which is the body that aims to provide interoperability between wireless products from all manufacturers. WPA was supported due to two main reasons: it did not require major hardware changes to current equipment and, more importantly, it provided improved security in comparison to WEP. WPA relies on the Temporal Key Integrity Protocol (TKIP) to address some of the WEP implementation weaknesses. TKIP adds various functionality to WPA, such as per-packet key mixing function, message integrity check (MIC), extended initialisation vector (IV) with sequencing rules, and re-keying mechanism. However, WPA is based on a Pre-Shared Key (PSK), usually generated from a passphrase, a fact that has recently been proven to be prone to different kinds of attacks (Moskowitz, 2003). WPA2, an evolution of WPA based on the Advanced Encryption Standard (AES), together with a new MIC implementation, may replace the first version in the future.

2.6 Authentication Server

The 802.1x standard (IEEE, 2004), based on interactions between a supplicant, an authenticator and an authentication server, can bring another security level to wireless networks. The service requested by the supplicant to the authenticator will be granted after the verification of its authorised services to the authentication server (usually a Remote Authentication Dial-In User Service – RADIUS server). In spite of the strength of this method, allowing regular and automated key changing within a connection, it presents weaknesses and has already been cracked (Mishra and Arbaugh, 2002).

3. The survey methodology

The previous section provided clear indication that even the latest encryption protocol used within the wireless networking environment have certain design or implementation flaws which make them vulnerable to attacks. In spite of this situation, it is also widely admitted that they all provide some level of security for the transiting data in comparison to the non-encrypted case. The purpose of the survey performed was not to evaluate the level of protection provided by existing encryption schemes, but to observe the percentage of the networks which have not implemented or enabled even the most basic of the techniques listed (i.e. WEP) rendering them vulnerable to a wide range of attacks, from unauthorised network access to privacy breaching.

3.1 Hardware and software configuration used

In order to conduct a survey of wireless security, both software and hardware tools are needed. Most of the wardriving software applications have common features like channel hopping and detection of network parameters: SSID, BSSID (MAC address format identifier of the network), received signal strength and noise, maximum data rate, channel used, type of network and whether encryption is enabled or not. The major difference between them is the platform they run on and the wireless cards supported. Other special wardriving software applications exist and take advantage of special hardware drivers (on Linux and some BSD operating systems) to passively monitor WLAN. Unlike promiscuous mode, which needs the wireless device to establish a link with the AP for sniffing each frame, monitor mode (RFMon mode) enables a device to monitor any wireless packet (even frames with bad CRC) without

emitting any signal. Examples of these include Kismet (Kershaw, 2004) and AirSnort (The Shmoo Group, 2004) which find cloaked APs when legitimate clients are connected. In addition, they can also give access to a WEP protected network, by computing WEP keys using information from the acquired frames. The last step, in order to accurately assess AP security, would require a connection to be established with the network, using the above tools to defeat cloaked APs, MAC filters and to compute WEP keys. At this stage, a connection would reveal the use of further security mechanisms such as 802.1x, giving a full assessment of the AP security.

As the use of appropriate software is crucial for the accuracy of results, the choice of hardware devices, each of which having its own inherent advantages and limitations, is also an important factor in this survey. A number of different hardware solutions were considered:

- A laptop computer equipped with a wireless interface (PCMCIA wireless cards, USB WiFi dongles or built-in wireless equipment like Centrino processor-based laptops).
- A Personal Data Assistant (PDA) with built-in wireless or with an expansion slot in which a Compact Flash wireless card can then be plugged in.
- WiFi detector devices like Kensington WiFi Finder or Smart ID WiFi Detector which are compact devices that indicate the strength of any received wireless signal, or the newer WiFisense wearable WiFi detector that can identify the signal strength together with the encryption method (WEP or WPA) used.
- WLAN stand-alone chips (Dallas 2004).

As for locating the AP, a Global Positioning System (GPS) device was considered the best solution. These devices usually use a serial communication protocol as stand alone, Compact Flash cards or BlueTooth devices.

While the development of a new device is time consuming and the new WiFi detectors seem to lack accuracy, the PDA approach has been chosen for its flexibility and discretion. The equipment used in this survey was a PDA Toshiba e740 with integrated WiFi (Prism2 based card) and a Pretec Compact Flash GPS device. The software chosen was Kismet (Kershaw, 2004) for its passive monitoring mode allowing the detection of cloaked APs together with its GPS compatibility.

Due to legal issues, any survey can not list precisely the protection used in a particular network (implying illegal data eavesdropping to compute WEP key and illegitimate connection to the network so as to test the presence of authentication request). Therefore, the results presented are based on characteristics that could be observed without any connection to the network (e.g. encryption).

3.2 Preliminary work

After testing the different devices supplied in order to determine their limitations (range, battery lifetime, sensitivity to interferences) attempts were made to run Linux on the PDA to use passive monitoring software. Unfortunately, the results of this were not reliable which led to the choice of Microsoft Pocket PC and MiniStumbler (Milner, 2003), reducing the

logging of security characteristic of each AP to the presence or absence of the use of encryption (i.e. no distinction between WEP and WPA).

3.3 Data collection

The survey in the city of Plymouth was conducted during 2004. The first areas covered were those with high student populations, according to 2001 census data (National Statistics, 2001), in order to observe student wireless activity during term time. Following this the city centre and neighbouring areas were covered, walking/driving through streets to gather wireless data and locate APs.

During the survey, various problems were encountered, a number of which could not be solved. The poor reception of the GPS antenna (worse during cloudy weather) led to unusable data, the limited lifetime of the PDA battery and a number of bugs in the software also contributed to the problems and limited the number of APs that were subsequently discovered.

4. Results

In order to work with all the collected data, a database approach was adopted, with the creation of scripts to adapt data formats, to populate the different tables and finally to process the maps and statistics on which the conclusions of the survey were based. The results were then compared with the findings of a similar survey, conducted in 2003 (Wilks and Ghita, 2004).

4.1 Increase in wireless usage

Table 1 shows the initial results from the three separate surveys conducted. It should be noted that while there is a clear trend indicating an increase in the usage of wireless LAN APs, it is the proportions of protected/unprotected networks that are more relevant. These figures show a consistent level of unprotected WLAN APs across all three sampling periods.

	Winter 2003	**Summer 2004**	**Winter 2004**
Wireless AP found:	96	228	265
Protected networks:	34 (35.42%)	86 (37.72%)	96 (36.23%)
Unprotected networks:	62 (64.58%)	142 (62.28%)	169 (63.77%)

Table 1: Comparison of surveys results

As for the increase in the number of WLANs in the areas covered by the surveys, all of the previous APs discovered in the 2003 survey were found with the same configuration parameters. However, a third more wireless networks appeared between winter 2003 and summer 2004. Among these new APs, about 33% were protected, again in-line with the results presented in Table 1.

4.2 Spread of wireless technology

If the first goal of the survey was to profile wireless security, a study of the use of wireless technology is necessary to give sense to further results. The graph illustrated in Figure 1 presents the distribution of the detected APs as a function of their distance from the city centre. It can be observed that nearly half the detected APs were no more than 500 meters away from the centre with the graph revealing that this number decreases linearly up to 2km and seems to approach zero as the test area was expanded.

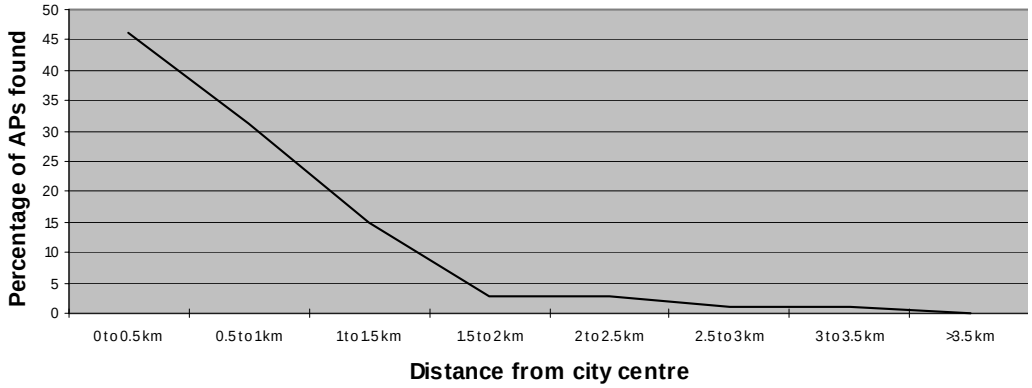

Figure 1: Distribution of wireless LANs in Plymouth

4.3 Profiling wireless security

In order to correlate the results from this survey with demographic data from the 2001 census, a distribution of the APs by areas was determined. While any correlation is hard to observe, most of the covered areas seem to follow the percentages given in Table 1 (about 1/3 of WLAN use WEP based encryption). If the number of APs is not proportional to the population (103 APs found in Drake whose population is 8,831 compared to 18 APs found in Stoke with a population of 12,146), Figure 2 reveals a strong correlation between the number of APs found per area and the percentage of students in the population, with only one unexplained exception.

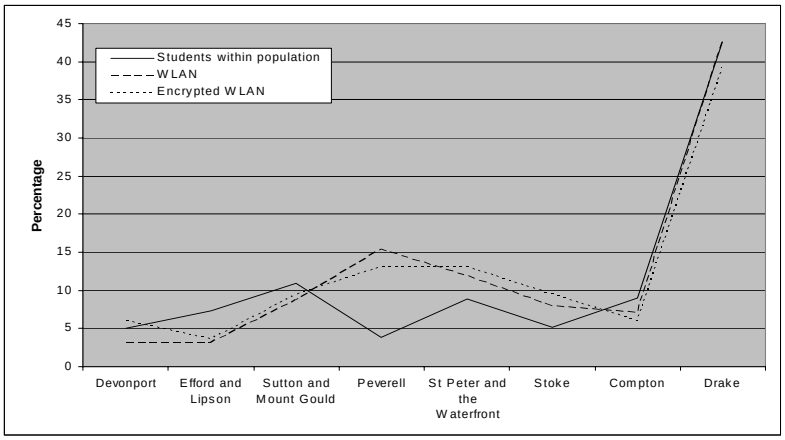

Figure 2: Number of WLANs as a function of student population

The representation of the percentage of encrypted WLANs by area indicates that the proportion of secure networks does not follow the same law: while there appears to be more encrypted networks in areas with few students and fewer overall APs, this result can not be generalised to every area.

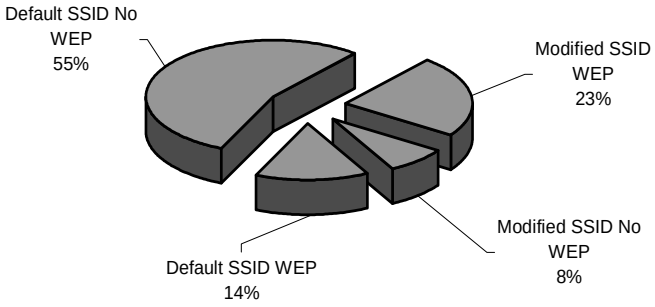

Figure 3: Encryption and SSID

An approximation of the number of APs used with default settings is possible through the observation of the SSID (though by no means definitive). Figure 3 shows clearly the predominance of these networks, with 69% of the APs found retaining the default SSID. These numbers represent only a lower bound estimate ratio, due to the non exhaustive list of default SSIDs used.

This survey also confirms that wireless equipment can still be qualified as emergent technology for commercial use as the number of networks with multiple APs is limited (only 7 were found). It could therefore be concluded that only a few networks allow their users to roam in the organisation while keeping connected to at least one AP. Among the data collected during the survey, only one large network was found using more than ten APs: the University of Plymouth network, which spreads over about a kilometre, relayed by wireless APs in most of the university buildings.

5. Discussion

Profiling wireless security with demographic data did not lead to consistent results. One of the causes of this inconsistency may be the fact that this survey is based only on WEP (and WPA) protection hence does not take into account any other security method mentioned in section 2.

As no mathematical model was found to describe the distribution of protected and unprotected APs, other parameters collected during the survey may help to produce a model. Among the different information observed, some parameters may be more likely to be found in unprotected WLANs, leading to the conclusion of the conditional probability of protection which is illustrated by the difference between the last two columns of Table 2 (with $\mathbf{P_A}$: the probability of parameter **A**, $\mathbf{P_{WEP}}$ the probability of the network being protected and $\mathbf{P_{[A \cap WEP]}}$ the probability of a network having both the parameter **A** and the WEP protection).

A	$P_A * P_{WEP}$	$P_{[A \cap WEP]}$
Data rate: 54Mbps	0.0366	0.0284
Data rate: 22 Mbps	0.0427	0.0397
Vendor: Askey	0.0305	0.0114
Vendor: Belkin	0.0284	0.0056
Default SSID	0.2095	0.1079

Table 2: Examples of unconditional and conditional probabilities

From these observations, the use of a Bayes probability approach (e.g. Bayesian networks) may help to identify unprotected networks. Using an initialisation dataset and feeding it with the data collected for a particular AP, a Bayesian network would then be able to compute the overall probability of any AP using encryption. This probability is based on the observation of the number of protected and unprotected AP in which each parameter appears; each new probability computed brings a new sample and refines the network. The advantage of such "learning" Bayesian network based algorithm is the automated process of evolution for the different parameters which are subject to change: the more APs with a particular SSID and the same settings will be found, the higher will be the probability for any AP with the same SSID to have also the same encryption setting; allowing more accurate conclusions as they do not rely anymore on a static, non-exhaustive, list of default SSIDs.

However, due to a matter of time, no implementation could be produced to confirm or invalidate these results.

6. Conclusion

This survey confirms that, while wireless networks seem to be used more for private than commercial use, they spread widely across the city yet remain concentrated around the city centre. This geographical distribution is most likely influenced by the interest within the student population for 'mobile' technologies. In spite of the recognition of the lack of security in these technologies and the efforts from manufacturers to facilitate the use of basic security methods, a large number of wireless LANs do not seem to be protected by any visible

security mechanism, offering hackers a potentially easy way to access personal data or to use the network's resources. A possible explanation for this could be a lack of awareness from wireless LAN users about security. In order to solve this issue, it is necessary to identify the knowledge and needs of inexperienced users. This first stage (a census of existing wireless networks and their security) should be followed by an investigation into the awareness of security from the end-user perspective to determine if users are simply unaware or (more worryingly) uninterested in securing their networks.

7. References

Dallas Semiconductors (2004), "802.11b WLAN transceiver shrinks circuit board and bill of materials", *Maxim Engineering Journal* Vol 50, pp12-15.

Farrow, R. (2001), *Wireless Security: A Contradiction in terms?*, [Online]. http://www.networkmagazine.com/article/NMG20011203S0008 [Accessed 11 Feb 2004].

IEEE (2004), *802.11 standards* [Online.] http://grouper.ieee.org/groups/802/11/ [Accessed 27 Nov 2003]

Kershaw, M. (2004), *Kismet*, [Online]. http://www.kismetwireless.net [Accessed 23 Nov 2003].

Khan, J. and Khwaja, A. (2003), *Building secure wireless networks with 802.11*, Wiley, Indianapolis.

Milner, M. (2003), *NetStumbler.com The New World of WiFi* [Online]. http://www.netstumbler.com [Accessed 23 Nov 2003].

Mishra, A. and Arbaugh, W.A. (2002), *An Initial Security Analysis of the 802.1X Standard*, [Online] http://www.cs.umd.edu/~waa/1x.pdf [Accessed 27 Nov 2003].

Moskowitz, R. (2003), "Weakness in Passphrase Choice in WPA Interface", *Wi-Fi Networking News*, [Online.]. http://wifinetnews.com/archives/002452.html [Accessed 23 Jan 2004].

National Statistics (2001), *Census 2001: The most comprehensive survey of the UK population*, [Online.]. http://www.statistics.gov.uk/census2001 [Accessed 5 Apr 2004]

The Shmoo Group (2004), *Airsnort*, [Online]. http://airsnort.shmoo.com [Accessed 23 Nov 2003].

WiFi Alliance (2002), *Wi-Fi Alliance Announces Standards-Based Security Solution to Replace WEP*, [Online.]. http://www.wi-fi.org/OpenSection [Accessed 12 Feb 2004]

Wilks, A. and Ghita, B. (2004), "An analysis of wireless security implementations", poster presentation, *4th International Networking Conference*, July 2004, Plymouth, UK