Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics, Istanbul, Turkey, May 27-29, 2006 (pp162-167)

WarDriving: Technical and Legal Context

HIRA SATHU
School of Computing and IT
Unitec
Private Bag 92025, Auckland
NEW ZEALAND

Abstract: - This paper, relates to computing practice where the inadequate deployment and configuration of Wireless Local Area Networks (WLANs) is considered. This inadequacy in deployment or configuration or both is open to attack by hackers and crackers. WarDriving is a term used for activities related to identifying and mapping of wireless access points/ router locations. At times these activities extend to include wireless clients viewing open WLANs, gaining access and viewing private data and even using available network resources. This study critically examines the current legal position in regard to WarDriving in countries like the UK, USA, and Australia. New Zealand could draw from the case law of these countries and put in place appropriate laws before major problems arise. The findings indicate that WarDriving activities fall within a wide range from legal to illegal activities. The illegality depends upon the intent and extent of the infringement by the wardriver. In view of the recency of WarDriving a large number of inconsistencies exist in the legal position across countries. The paper also provides a basic set of deployment and configuration recommendations for the small home office or the residential users and a more robust set of suggestions that could be adopted by the more security conscious.

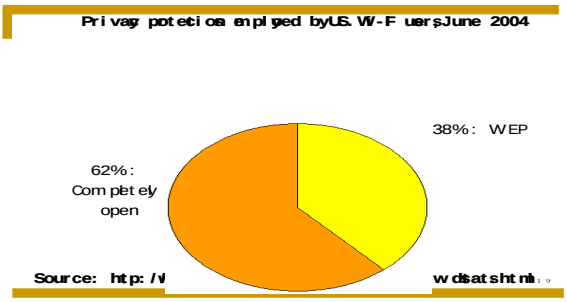
Key-Words: - WLANs, WarDriving, Legal, jurisdiction, MAC address, Filtering, WEP

1 Introduction

Proliferation of wireless local area networks (WLANs) is hard to avoid given the attractiveness of the ease, speed and flexibility of deployment. The overall cost when compared to alternative options is also lower. Whether it is a home user or a small to medium enterprise (SME) or at times even a large corporate user one is lulled into false sense of adequacy of the newly set up wireless network. This attitude of satisfaction stems from a common belief “if ain’t broke don’t mend it”. However, the network may seem to be operating properly till the company is made aware of security leaks or when complaints come in from users about poor performance of the internet connection. The losses due image, market position and legal damages etc. may be aspects least thought of while installing the WLAN. The WLANs discussed in this paper where not qualified refer to the popular IEEE802.11 based WLANs also termed as WiFi networks. An idea of the openness (unauthorised accessibility) of WLANs is evident from various Worldwide WarDriving (WWWD) results. The third WWWD exercise conducted in mid 2003 revealed that 67.7% had not even the basic wired equivalent privacy (WEP) enabled and WLANs using the default service set identifier (SSID) were 27.8%.
(Source: http://www.worldwidewardriving.org/).

A subsequent wardrive organised in mid 2004 revealed results that were only slightly improved as may be seen in Figure 1 below.

Figure 1 Wi-Fi Privacy: Observations



This paper begins by presenting the background to WarDriving and security issues of WLANs in Section 2. This is followed by some statistics of WLAN security in Section 3. Section 4 discusses a few cases of WarDriving and the legal position in regard to these activities in US, UK, Australia and New Zealand (NZ). Section 5 provides recommendations for WLAN deployment in the light of available WLAN features and future wireless LAN technologies. Section 6 concludes the findings for the study and delves on future implications for WarDriving

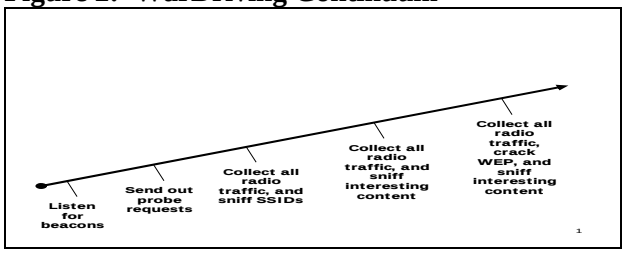
2 Background

The manufacturers of wireless LAN products, for ease of set up, enable networks to be ready for operation the moment power is turned on. However, these networks are enabled using their default settings. Due to the very nature of radio frequencies (RF) used in WLANs, devices that are capable of receiving the transmitted RF energy can easily get access to these WLANs. They are able to view, modify the data as well as use the resources that are available as a result of availability of such wireless connections. Where adequate steps are taken to deploy the access points (AP) or further secure the WLAN this connectivity can be minimised.

WarDriving in its simplest form is an exercise that involves a car equipped with a lap top computer having wireless capability driving in your neighbourhood with a view to pick up a wireless network connection. The laptops may be equipped with software utilities like NetStumbler (http://www.netstumbler.com/), or Cismet depending upon the operating system used being Windows or Linux (Anderson, 2004). Other utilities like "Kismet (http://www. Kismetwieless.net/) will also identify workstations that are talking to the AP / Wireless router and their MAC addresses" (Maiwald, 2003). There has been a large growth of WarDriving utilities. Some of these tools that are suitable for different activities or with different hardware and OSs include the MiniStumbler, Airsnort, WarLinux and MacStumbler. The computer used by the wardriver is looking for SSID that is being constantly transmitted by your AP as a beacon. The software used can also check for signal strength and encryption. Where the wardriver's computer is integrated with a GPS receiver card, the co-ordinates of the transmitted signal from the AP or a Wireless router can be located. Where the signal received is poor, one can return with a higher gain antenna for better reception.

Once a wardriver is connected, it can sniff the network traffic; can view private information such as login names, credit card numbers, passwords etc. The susceptible data on other computers on the network can be viewed and modified. Special attention where not given to files that are being shared are also open to the wardriver. The intention of this paper is to use WarDriving in a broader sense rather than the narrower sense which covers just sniffing and mapping for wireless APs / routers. Many would argue that such mapping without having current or future use would make little sense. Figure 2 below depicts the continuum of activities that could fall within the purview of WarDriving.

Figure 2: WarDriving Continuum



(Source: Josh Goldfoot, US department of Justice)

The activity undertaken from the above continuum of activities by the wardriver depends upon the wardriver's motivations. While some may just be interested in passive listening others may be involved in WEP cracking or using a free Internet service. The answer to wardriving being legal or otherwise depends upon the jurisdiction in place for the specific state/country. The next section discusses the status of these activities in a few cities.

3 WarDriving: Mapping and Statistics

The passive activity of listening to beacons, sending out probe requests, sniffing SSIDs and locating the radio signal (from the AP) would aid mapping hotspots. Once mapped these could be used either by the casual user or by a public (city council) or a private agency for planning of communication infrastructure. The actual status of mapping and the related statistics is far from clear since the position varies over time. This is on account of increase in the deployment of Wireless APs /routers as greater numbers of organisations find WLAN deployment and maintenance a more cost effective option as compared to the wired LAN option. The mapping and the statistics for WarDriving also varies from country to country. Some official data provided by the WWWD quoted in Section 1, above refers mainly to US. There have been other war drives in Australia and NZ the details for which are covered below.

3.1 Australian position

The data covered here relates to Canberra (Australia) central business district (CBD). A study of the Canberra CBD as of August 2004 revealed that 55% of the WLANs were open. The mapping covered 180 APs out of which 100 APs were found to be unsecured (without WEP) (Caslon, 2006).

3.2 New Zealand position

The data here relates to Auckland (NZ). WarDriving exercise of October 2003 in Auckland CBD revealed that 70% of the WLANs had either an identifiable or retained default SSID and 70% were unsecured (no WEP) (Lin, 2003). The war drive exercise of December 2003 in Auckland revealed that 60 % of the WLANs were unsecured. This mapping covered 700 APs out of which 420 APs were unsecured (Caslon, 2006).

4 WarDriving: Legal Position

There is no consistent clarity as to an industry wide code of practice. However, some suggestions by Duntemann with a view to avoid legal issues were covered for WarDriving exercises (Duntemann, 2003): Once an open AP was detected, the contents on the network should not be examined. No modification of any sort should be made including additions and deletions. The network resources like internet connection for email, web surfing, instant messaging etc should not be used. This entails that the system used for WarDriving needs to be configured in a way that even unintentional interactions with the scanned WLANs should not take place.

The considerations that arise are not just for the wardriver but also for the WLAN providers. Both these perspectives are covered below.

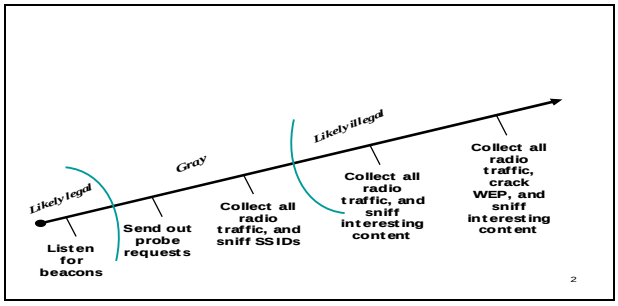
Wardrivers: The wardrivers (hacker/cracker) need to consider all their actions. These cover both intentional or unintentional that leads to any of the following activities by the wardriver:

- dishonestly steals data
- gains private information
- Uses unauthorised resources

WLAN providers- Where the providers do not secure their WLAN, a wardriver can seek defence when charged for criminal intent as the provider could automatically be seen to be abetting the criminal activity by providing an open WLAN

A common sense approach as to the possible legal, grey and likely illegal areas that form a part of WarDriving is demonstrated in Figure 6 below.

Figure 6: Is WarDriving Legal?



(Source: Josh Goldfoot, US department of Justice)

4.1 Legal Position in Other Countries

The legal position on WarDriving in most countries still falls in the grey area. Hence the legal position will be developed through recent charges bought against persons and sentences awarded in few of the countries. Some early discussions in New Hampshire (US) "proposed Bill No 495 would protect people who tap into insecure WLANs without the approval of the network owners" (Lin, 2003). This pointed towards the responsibility of the WLAN provider to secure its WLAN. Despite this, there have been cases that have been viewed differently. Last year (2005), in UK a man was prosecuted under the provisions of Sections 125 and 126 of the Communications ACT of 2003 (Ilett, 2005). The two sub sections of section 125 that relate to a person dishonestly obtaining an electronic service quoted below state: "A person who-

(a) dishonestly obtains an electronic communications service, and

(b) does so with intent to avoid payment of a charge applicable to the provision of that service"

It may be pointed out that the "and" conjunction that connects the two sub sections entails that both the sub sections of the Act need to be satisfied before a person is held guilty." In the UK depending upon the exact nature of the wardriving activity, these could be covered by at least two acts enacted earlier. Section 4 of the Theft Act 1968 which covers things that are stolen including "money and all other property, real or personal, including things in action and other intangible property" The second law is from the Computer Misuse Act 1990, that makes an unauthorised access to a computer system punishable, regardless whether the intention is malicious or not (Langley, 2003).

Another case of 2003 relates to a person in Michigan (USA), who was sentenced to a 9 year prison term for siphoning credit card numbers over a wireless network from the Lowes, hardware store (Poulsen, 2003). This case is a clear case of fraud since legal provisions already exist for credit card fraud even where committed without the use of the

wireless medium. Charges and prosecution could be got against persons downloading pornographic material or terabytes of video/audio even though they would attract different provision of case law in the US.

Another case in point is a person in Florida (USA) charged with felony for WarDriving (Arstechnica.com: 2006). The case involves the person accessing an unsecured WLAN from his SUV. Upon being spotted by the network owner, he closed his laptop but returned in the evening whereupon the network owner called the police who arrested and charged the person with felony. On the other hand is a case of acquittal in Houston Texas (USA) pertained to a security consultant penetrating a Texas County's WLAN to demonstrate its in-security to a newspaper reporter (Poulsen, 2003).

4.2 Legal Position in Australia and New Zealand

As per Calson Analytic (2006) Australia has no definitive case law of theft of network service by unauthorised means. The federal Cybercrime Act 2001 (CA) amended the earlier Act of 1995 to cover crimes related to computers and electronic communications. Quoting Calson Analytic (2006) the major computing related offences in Australia are covered under:

"1) Unauthorized access, modification or impairment with intent to commit a serious offence.
2) Unauthorized modification of data where the offender is reckless as to whether the modification will impair data, covering situations such as where a hacker unintentionally impairs data in the course of unauthorized access to a computer system.
3) Unauthorized impairment of electronic communications, including 'denial of service' attacks'.
……." (Caslon Analytics, 2006).

The above laws lay down different penalties for the offences varying from 2 years to 10 years in a prison. These laws have been quoted with a view to indicate that many of the activities as discussed above under WarDriving are not explicitly covered. However, where the WarDriving activity leads to denial of service, charges under the sub section 3) of the Australian Act above would be applicable.

NZ body of laws has its roots in the English Common law and legislated laws as well as the constitutional conventions. Moving from receiving legislation from the Parliament at Westminster NZ over time has been delegated to authorities in NZ to legislate and put in place new laws. Many times Courts in NZ consider authorities from other common law jurisdictions from countries like Australia, USA and Canada. Of late NZ lawyers look more to US and Canada than to UK (Greville, 2002). Some examples of this are like the NZ companies Act being based on the Canadian model while the Commerce Act and Fair Trading Act is based on the US anti- trust laws.

In NZ the first charge for hacking was laid some time in mid of 2003 (Wood, 2004). The charge was covered under the Amendment (No 6) of the Crimes Act 1961. Section 252 of this Act relates to "Accessing computer system without authorization". Sub section (1) of Section 252 states "Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorization, knowing that he or she is not authorized to access that computer system, or being reckless as to whether or not he or she is authorized to access that system." The sub section (2) and (3) cover exceptions to sub section (1). These relate to access by persons who are ordinarily given access to the system but for other purposes and access by law enforcement agencies. This Crimes Amendment (No 6) Act took about four years to be passed by the Parliament. Before passing of this act hackers could only be charged and prosecuted under general legislation (dealing with theft and criminal damage). The existing provisions in NZ law are similar to those in Australia, and there are a few grey areas that are dealt with in the next sub section along with a recommendation for NZ.

4.3 Grey areas and Suggestions for New Zealand

The business customers in NZ appear to be getting the message of security awareness, the same is not true for home users (Brislen, 2004). The general proliferation of wireless residential customers as the costs for wireless APs /Routers come down, as well as some home user clients using Intel's Centrino chipset that have inbuilt wireless connectivity, the chances for un intentional access will become more common. The grey areas with regard to the activity being legal or illegal arises where a person in-advertently accesses an unsecured WLAN and uses it to surf the net or view his emails as in the normal course of business. Greater debate is needed to establish the correct position as this situation could be argued either way. The earlier precedents of case law if applied with a broad brush could render many innocent people liable to criminal conviction. Another example in this regard could be a person equipped with a Wi-Fi enabled phone or a person using phones that automatically switch to the lowest cost connection, and thereby pick up an open WLAN

connection as the desirable connection being charged with a criminal offence. Most modern operating systems on laptops / PDAs with a wireless connection listen to beacons, send out probe requests, collect radio traffic, and even sniff SSIDs. A wireless client that gets an IP address after a request for an IP address from a DHCP service running on an AP/Router could be interpreted as an implied consent, so long as there is no other way to know that the consent is denied. While listening to beacons may be clearly outside the purview of a charge under the acts of most countries, the later issues of sniffing and sending out active probe requests fall in the grey area and need detailed deliberations.

NZ could draw from the case law of Australia and the other countries discussed above and put in place appropriate laws before major interpretational conflicts in the area of WarDriving and associated activities become rampant. In the meanwhile, suggestions for varying kind of users are covered in the next section. It is in the interest of the users to be safe than sorry. The level of protection that may be put in place could be in keeping with the level of security desired and the effort the organization is willing to make.

5 Protection against Wardrivers

This section has been considered under basic level protections and advance level protection. Basic level protection is a set of technical measures for the small home office or even casual residential users. The advance level protections are suggestions that could be adopted by the more security conscious SMEs or larger organisations.

5.1 Basic Level Protection

The measures recommended here are very simple to implement both in time and effort. Few of the suggestions here should be made obligatory for WLAN providers. This is to avoid unnecessary litigation where genuine community (free) hot spot clients accidentally access WLANs. Even the not so secure WEP is sufficient to disable accidental access of a WEP secured WLAN. For appropriate affect, the provisions below should be put in place immediately after a WLAN is established.

- The WLAN should be configured not to broadcast its SSID. This could however be guessed, where the default SSID is retained. Hence change the factory default SSID.
- The WEP encryption of the wireless AP/ router should be enabled.
- Change the default password of the wireless AP/ router. It is easy to use a browser and change the configuration of your AP/router.
- The MAC address filtering can be enabled on the wireless AP/ router after identifying the network card hardware addresses of the authorised clients.

The first two provisions above are recommended to be made obligatory for reasons as suggested above.

5.2 Advanced level Protection

The set of measure here are recommended for organisations that deal with sensitive or highly confidential data and have adequate resources to deploy, configure and maintain their WLANs.

- The APs should be deployed in a way that the authorised client base only should receive the RF signal. This may involve use and deployment of appropriate wireless AP/router critically. A simple example here would be use of say a Dick Smith low power AP for a small area coverage while a US Robotics with higher gain for a multilevel / larger house.
- Use of omni directional or a directional antenna with appropriate gain for the AP/router depending on the layout of the clients.
- Where file sharing exists, these should be password protected. Open shares could be construed as resources free for public domain.
- The wireless clients should be provided with multifactor authentication. Include biometric and smart card in addition to the standard login and password.
- Use of improved wireless standards like WPA (IEEE802.1X) or the IEEE 802.11i. The WPA is an interim standard that provides port based access control using EAP and temporary key integrity protocol (TKIP). The more recent 802.11i standard provides advanced encryption standard (AES) and the mutual authentication using PEAP. (Planet3 Wireless, 2003)
- Disable dynamic allocation of IP addresses and use static/manual allocation.

The radiation pattern may be verified using similar tools as used for WarDriving (NetStumbler, Kismet) to confirm adequate screening of RF radiation.

6 Conclusion

Summarising the findings for the NZ WLAN environment, indicates that over 60% of WLANs had no WEP enabled and at least 54% use identifiable SSIDs with Open WLANs as of end 2003. These figures are already a cause for concern. With greater numbers of WLAN users, chances of these percentages rising may not be unusual. A three fold strategy is recommended to be explored and put in place at the earliest.

The first strategy relates to legislating for appropriate law(s) that cover the diverse contingencies from passive and accidental wardriving activities to the clearly illegal activities. An example of laws reflecting the social structure of societies can be seen in the changes being brought in the US. The Digital Millennium Copyright Act criminalised things that used to be civil infractions before, the same is now being modified and toned down in view of new technologies(Mason, 2006).

The second strategy relates to educating the wireless client users and WLAN providers. This should cover the basic protection features in WLANs as well as the legal infringements in simple and a clear language through well advertised campaigns. Preservation of wireless AP/router log data and intrusion detection system logs to identify unauthorised network connections or access attempts.

The third strategy relates to educating law enforcement investigators and prosecuting officers about wireless technologies. These should include the use of lawful network monitoring to detect sources of criminal activities with a view to protect against future incidents.

It may be noted that on account of the fast rate of change of future wireless technologies a continued awareness of the vulnerabilities by the wireless device users, WLAN providers and law enforcement agencies is a must. While the technology savvy may have little problems but the common users may need to be educated about the associated risks to enable them to make an informed decision.

References:

[1] Anderson, Z., (2004): What Is WarDriving And How Can You Prevent It? Accessed March 07, 2006 (http://www.networknewz.com/).

[2] Arstechnica.com: accessed on March16, 2006 (http://arstechnica.com/newsars/post/)

[3] Brislen, P. (2004): Home users warned to secure networks, The New Zealand Herald-Business-Technology, July 20.

[4] Caslon Analytics: Caslon Analytics note WarChalking and WarDriving. Accessed March 07, 2006 (http://www.caslon.com.au/warchalknote.htm)

[5] Greville, M. (2002): LLRX.com, An Introduction to New Zealand Law & Legal Information 2002. Accessed March 18, 2006 (http://www.llrx.com/features/newzealand.htm)

[6] Ilett, D. (2005): Silicon.com: Wireless network hijacker found guilty. Accessed March 06, 2006 (http:// mangement.silicon.com/government/)

[7] Langley, N. (2003): The demise of the warchalkers, ComputerWeekly.com, 23 June 2003. Accessed March 28, 2006. (http://www.computerweekly.com/Articles/)

[8] Lin, C-T. (2003): *IEEE 802.11b-based Wireless Network Security*, Master of Computing Dissertation, Unitec, pp51-62 and p139

[9Maiwald, E. (2003): Network Security: A Beginner's Guide, Mc Graw Hill, Osborne, pp435-438

[10]Planet3 Wireless. (2003): Certified Wireless Network Administrator, Vendor-neutral wireless network training and certification, Mc Graw Hill, Osborne, pp404-409

[11]Poulsen, K. (2003): Wireless Hacking bust in Michigan, Security focus, The Register. Accessed on March 07, 2006. (http://www.theregister.co.uk/)

[12]Wood, R. (2004): NZ Police lay first charge for hacking, The dominion Post- IT Business, 15 March

[13]Worldwide WarDriving Results. Accessed March 06, 2006. (http://www.worldwidedrive.org/wwwstats.htm)