ISSN:2231-0711

Ch.Sai Priya et al | IJCSET |June 2013 | Vol 3, Issue 6, 230-235

The Impact of War Driving On Wireless Networks

Ch.Sai Priya, Syed Umar, T Sirisha

Department of ECM,
KL University, A.P., INDIA.

***Abstract* — Wardriving is searching for Wi-Fi wireless networks by moving vehicle. It involves using a car or truck and a Wi-Fi-equipped computer, such as a laptop or a PDA, to detect the networks. It was also known as 'WiLDing' (Wireless LAN Driving).Many wardrivers use GPS devices to measure the location of the network find and log it on a website. For better range, antennas are built or bought, and vary from Omni directional to highly directional. Software for wardriving is freely available on the Internet, notably, Nets tumbler for Windows, Kismet for Linux, and KisMac for Macintosh.**

Keywords — **Wardriving, hacking, wireless, wifi cracking.**

1. INTRODUCTION

Wardriving is searching for Wi-Fi wireless networks by moving vehicle. Wardriving was first developed by Pete Shipley in April 2001. It involves using a car or truck and a Wi-Fi equipped computer, such as a laptop or a PDA, to detect the networks. Many wardrivers use GPS devices to measure the location of the network find and log it on a website. For better range, antennas are built or bought, and vary from Omni directional to highly directional. Software for wardriving is freely available on the Internet, notably, NetStumbler for Windows, Kismet for Linux, and KisMac for Macintosh. The gathering of statistics about wireless networks in a given area by listening for their publicly available broadcast beacons is War Driving. Wireless access points (APs) announce their presence at set intervals (usually every 100 milliseconds) by road casting a packet containing their service set identifier (SSID; basically, the user-defined name of the access point) and several other data items. A stumbling utility running on a portable computer of some sort (a laptop or PDA) listens for these broadcasts and records the data that the AP makes publicly available. Wireless networks have become a way of life in the past two years. As more wireless
Networks are deployed; the need to secure them increases. The activity of driving around discovering wireless access points is called WarDriving. In order to successfully WarDrive, there are some tools, both hardware and software. Wardriving is a fun hobby that has the potential to make a difference in the overall security posture of wireless networking.

1.1 THE ORIGIN OF WARDRIVING

WarDriving is an activity that is misunderstood by many people. This applies to both the general public, and to the news media that has reported on WarDriving. Because the name "WarDriving'* has an ominous sound to it, many people associate WarDriving with a criminal activity WarDriving originated from wardialing, a technique popularized by a character played by Matthew Broderick in the film WarGames, and named after that film. Wardialing in this context refers to the practice of using a computer to dial many phone numbers in the hopes of finding an active modem.
A WarDriver drives around an area, often after mapping a route out first, to determine all of the wireless access points in that area. Once these access points are discovered, a WarDriver uses a software program or Web site to map the results of his efforts. Based on these results, a
statistical analysis is performed. This statistical analysis can be of one drive, one area, or a general overview of all wireless networks During the fall of 2000,Shipley conducted an 18-month survey of wireless networks in Berkeley, California and reported his results at the annual DefCon hacker conference in July of 2001.This presentation, designed to raise awareness of the insecurity of wireless networks that were deployed at that time, laid the groundwork for the "true" WarDriver.

1.2 WARDRIVING MISCONCEPTIONS

These days, you might hear people confuse the terminology WarDriver and Hacker. As you probably know, the term hacker was originally used to describe a person that was able to modify a computer (often in a way unintended by its manufacturer) to suit his or her own purposes. However, over time, owing to the confusion of the masses and consistent media abuse, the term hacker is now commonly used to describe a criminal; someone that accesses a computer or network without the authorization of the owner. The same situation can be applied to the term WarDriver. WarDriver has been misused to describe someone that accesses wireless networks without authorization from the owner. An individual that accesses a computer system, wired or wireless, without authorization is a criminal. Criminality has nothing to do with either hacking or WarDriving. The news media, in an effort to generate ratings and increase viewership, has sensationalized WarDriving. Almost every local television news outlet has done a story on "wireless hackers armed with laptops" or "drive-by hackers" that are reading your e-mail or using your wireless network to surf the Web. These
Wardriving Division Of Computer Science, SOE, CUSAT
3 stories are geared to propagate Fear, Uncertainty, and Doubt (FUD). FUD stories usually take a small risk, and attempt to elevate the seriousness of the situation in the minds of their audience. Stories that prey on fear are good for ratings, but don't always depict an activity accurately. An unfortunate side effect of these stories has been that the

reporters invariably ask the "WarDriver" to gather information that is being transmitted across a wireless network so that the "victim" can be shown their personal information that was collected. Again, this has nothing to do with WarDriving and while a case can be made that this activity (known as sniffing) in and of itself is not illegal, it is at a minimum unethical and is not a practice that WarDrivers engage in. These stories also tend to focus on gimmicky aspects of WarDriving such as the directional antenna that can be made using a Pringles can. While a functional antenna can be made from Pringles cans, coffee cans, soup cans, or pretty much anything cylindrical and hollow, the reality is that very few (if any) WarDrivers actually use these for WarDriving. Many of them have made these antennas in an attempt to both verify the original concept and improve upon it in some instances from the Underground.

1.3. THE TRUTH ABOUT WARDRIVING

The reality of WarDriving is simple. Computer security professionals, hobbyists, and others are generally interested in providing information to the public about security vulnerabilities that are present with "out of the box" configurations of wireless access points. Wireless access points that can be purchased at a local electronics or computer store are not geared toward security. They are designed so that a person with little or no understanding of networking can purchase a wireless access point, and with little or no outside help, set it up and begin using it. Computers have become a staple of everyday life. Technology that makes using computers easier and more fun needs to be available to everyone. Companies such as Linksys and DLink have been very successful at making these new technologies easy for end users to set up Wardriving Division Of Computer Science, SOE, CUSAT 4 and begin using. To do otherwise would alienate a large part of their target market. According to the FBI, it is not illegal to scan access points, but once a theft of service, denial of service, or theft of information occurs, then it becomes a federal violation. While this is good, general information, any questions about the legality of a specific act in the United States should be posed directly to either the local FBI field office, a cyber crime attorney, or the U.S. Attorney's office. This information only applies to the United States. WarDrivers are encouraged to investigate the local laws where they live to ensure that they aren't inadvertently violating the law. Understanding the distinction between "scanning" or identifying wireless access points and actually using the access point is understanding the difference between WarDriving, a legal activity, and theft, an obviously illegal activity.

2. HOW CAN WE GO WARDRIVING?

This section will introduce you to all of the tools that are required in order to successfully WarDrive and how we can do WarDriving. There are several different configurations that can be effectively used for WarDriving, including:

1. Getting the hardware
2. Choosing a wireless network card.
3. Deciding on an external antenna
4. Connecting your antenna to your wireless NIC
5. Mapping the access points.

2.1 Getting the hardware:

The following sections discuss potential equipment acquisitions and common configurations for each. Getting the Hardware You will need some form of hardware to use with your WarDriving equipment. There are two primary setups that WarDrivers utilize:

> The Laptop Setup
> The PDA Setup

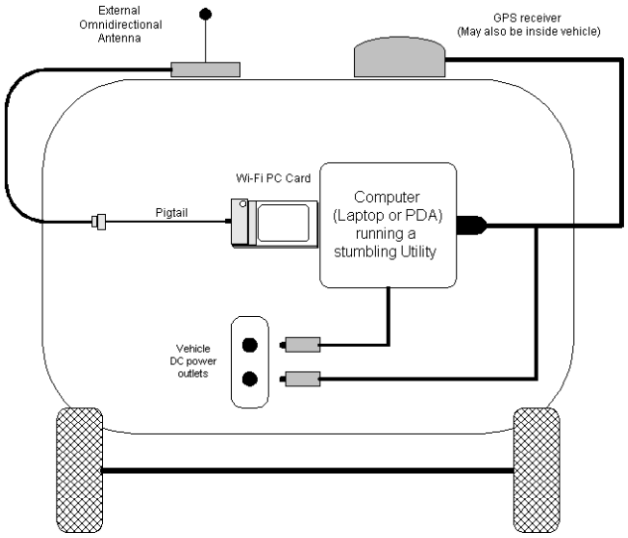

Figure 1: WarDrving Kit

The Laptop Setup:

The most commonly used WarDriving setup utilizes a laptop computer. To WarDrive with a laptop, you need several pieces of hardware and at least one WarDriving software program. A successful laptop WarDriving setup includes:

- A laptop computer
- A wireless NIC Card
- An external antenna
  - A pigtail to connect the external antenna to the wireless NIC
- A handheld global positioning system (GPS) unit
- A GPS data cable
- A WarDriving software program
- A cigarette lighter or AC adapter power inverter

Figure 2. The Laptop Setup

The Personal Digital Assistant (PDA) Setup:
PDAs are the perfect accessory for the WarDriver because they are highly portable. The Compaq iPAQ (see Figure 2), or any number of other PDAs that utilize the ARM, MIPS, or
SH3 processor can be utilized with common WarDriving software packages. As with the laptop setup, the PDA setup requires additional equipment in order to be successful:

- A PDA with a data cable
- A wireless NIC Card
- An external antenna
- A pigtail to connect the external antenna to the wireless NIC
- A handheld global positioning system (GPS) unit
- A GPS data cable
- A null modem connector
- A WarDriving software program

Similar to the laptop configuration, the software package you choose will affect your choice of PDA. MiniStumbler, the PDA version of NetStumbler, works on PDAs that utilize the
Microsoft Pocket PC operating system .The HP/Compaq iPAQ is one of the more popular PDAs among WarDrivers that prefer MiniStumbler. WarDrivers that prefer to use a PDA port of Kismet are likely to choose the Sharp Zaurus since it runs a PDA version of Linux. There are also Kismet packages that have specifically been designed for use on the Zaurus.

Figure 3. The PDA Setup

2.2 Choosing a Wireless Network Interface Card:
Most of the wireless networks that are currently deployed are 802.11b networks. You will find more access points if you use an 802.1 lb NIC. 802.1 lg access points, which transfer data at nearly five times the speed of 802.11b (54 MBps as opposed to 11 MBps) are gaining popularity and it is likely that an 802.1 lg card will soon supplant an 802.1 lb card as the favorite of WarDrivers. In addition to increased speed, the 802.1 lg standard supports WiFi Protected Access (WPA) encryption. Once effectively deployed, WPA will help to improve the overall security posture of wireless networks. Some 802.1 la cards are currently supported by WarDriving software under certain conditions. As a general rule, 802.1 la (or any 802.1 la/b/g combo) cards are not recommended for WarDriving. When Kismet and NetStumbler were first introduced, there were two primary chipsets available on wireless NICs: the Hermes chipset and the Prism2 chipset. Although there are many other chipsets available now, most WarDriving software is designed for use with one of these two chipsets. As a general rule NetStumbler works with cards based on the Hermes chipset. Kismet, on the other hand, is designed for use with cards based on the Prism2 chipset. This is not a hard and fast rule since some Prism2 cards will work under NetStumbler in certain configurations. Also, with appropriate Linux kernel modifications, Hermes cards can be used with Kismet.

2.3 Deciding on an external antenna:
In order to maximize the results of a WarDrive, an external antenna should be used. An antenna is a device for radiating or receiving radio waves. Most wireless network cards have a low power antenna built in to them. An external antenna will increase the range of the radio signal detected by the wireless network card. Many different types of antennas can be used with wireless NICs: parabolic antennas, directional antennas, and Omni-directional antennas are just a few. Because of their size, parabolic antennas (see Figure 5.) are not overly practical antennas for WarDriving. Many WarDrivers use either an external Omni-directional antenna or an external directional antenna in conjunction with their wireless network card. Both of these are available in many different sizes and signal strengths. There are many factors that need to be considered when determining what type of antenna to use. There are some basic terms you should understand when determining what type of antenna should be used while WarDriving: *Decibel (dB):* A decibel is the unit of measure for power ratios describing loss or gain, normally expressed in watts. A decibel is not an absolute value it is the measurement of power gained or lost between two communicating devices. These units are usually given in terms of the logarithm to Base 10 of a ratio.
dBi value: This is the ratio of the gain of an antenna as compared to an isotropic antenna. The greater the dBi value, the higher the gain. If the gain is high, the angle of coverage will be more acute.
Isotropic antenna: An isotropic antenna is a theoretical construct that describes an antenna that will radiate its signal 360 degrees to cover the area in a perfect sphere. It is used as a basis by which to describe the gain of a real antenna.
Line of sight: Line of sight is an unobstructed straight line between two transmitting devices. You will most often see the need for a line of sight path for long-range directional radio transmissions. Due to the curvature of the earth, the maximum line of sight for devices not mounted on towers is six miles (9.65 km).
Omni-directional Antennas:
As the name indicates, Omni-directional antennas "see" in all directions at once. An Omni directional antenna is best used when driving alone, and can be purchased for $50.00 and up depending on the gain and mounting mechanism.

One common misconception is that the stronger the gains of the antenna, the better your WarDriving results will be. This is not entirely true, however. The important thing to understand from the preceding definition of dBi value is the last sentence: "If the gain is high, the angle of coverage will be more acute."

Because the signal of an Omni-directional antenna is shaped roughly like a donut, the higher the gain, the "shorter" the donut Another advantage of the 5 dBi gain antenna is that many are available with a magnetic base. This means that you can simply put it on the roof of your car and the magnet will hold it in place while driving; no additional mounting brackets are required. An 8 dB gain or higher, antenna is excellent for use on longer drives in open areas with few obstructions such as interstate highways. These antennas are very effective when businesses or residences are farther away from your vehicle and there is a large field or roadway between you and any potential access points. It is more difficult to find magnetic mounted antennas that are stronger than 5 dBi gain .These antennas usually require some form of external mounting bracket.

Directional Antennas:

Directional antennas also rely on line of sight to transmit; however, unlike Omni-directional antennas, they can only "see" in the direction they are pointed. Directional antennas are excellent for use in areas with tall buildings. From a stationary position near the base of the building, you can sweep the antenna up and down the length of the building and detect access points that would have been missed with an Omni-directional antenna. Additionally, directional antennas can have a much stronger dBi gain in a shorter package There are several types of directional antennas such as yagis, parabolic grids, and so forth. However, the most commonly used antenna is the yagi antenna since these can be purchased relatively inexpensively and provides a large dBi gain.

2.4 Connecting Your Antenna to wireless NIC

In order to connect your antenna to the external antenna connector on your wireless NIC you will need the appropriate pigtail cable. Most antennas have an N-Type connector but the wireless NIC usually has a proprietary connector. When you purchase your card you should verify with either the retailer or the card manufacturer what type of external antenna connector is built into the card.

Once you have identified the type of external connector your card has, you will need to purchase a pigtail that has both the correct connection for your card as well as the correct NType connector.. This will allow you to successfully connect your antenna to your wireless NICs external antenna connector. Since you may have multiple antennas with both male and female N-Type connectors, it might also be a good idea to purchase barrel connectors that will allow you to attach your pigtail to either a male or female N-Type Connector.

2.5 Mapping the access points.:

Most WarDrivers want to map the results of their drives. To do this, a portable GPS capable of National Marine Electronics Output (NMEA) is required. Some WarDriving software supports other proprietary formats (such as Garmin).For instance, NetStumbler supports the Garmin format. The Gannin format "reports" the current location to your software every second, whereas NMEA only reports the location once every two seconds. Using the Garmin format increases the accuracy of the access-point locations. Unfortunately, Kismet only supports NMEA output. By purchasing a GPS capable of NMEA output, there will be flexibility to switch between WarDriving software without requiring additional hardware

Figure 4. Garmin GPS

When choosing a GPS, several factors should be considered. As mentioned earlier, making sure it is capable of NMEA output is a must. It is also important to find out which accessories come with the GPS unit. For instance, there are several models in the Garmin eTrex line of handheld GPSs. The base model, simply called the eTrex retails for about $120.This unit has all of the functionality required for a WarDriver and is capable of NMEA output. When comparing this to the eTrex Venture, which retails for $150, the initial indication would be to go with the cheaper model. However, once the accessories included with these two are looked into, you will notice that the Venture comes with the PC Interface cable, whereas the base model doesn't. Because this cable costs about $50, the Venture is a better purchase. In addition to the PC Interface cable, you get additional functionality with the Venture that, while not required for WarDriving, can be fun to play with, all for $20 less. Determine if your laptop computer has a serial port. Most PC Interface cables have a serial interface. If laptop doesn't have a serial interface, purchase a serial to Universal Serial Bus (USB) cable for use with GPS. In order to use GPS with a PDA, you will need a null modem connector and the proper connection cables for PDA. The proper configuration for this setup is PDA | Proprietary connector/serial conversion cable | Null Modem Connector | GPS PC Interface cable. This will open the Properties for your wireless network card. Next, simply remove the check from the Internet Protocol (TCP/IP) checkbox and then choose OK .Your TCP/IP stack is now disabled and your wireless network card will not be able to connect to any network. Your WarDriving software will function perfectly even with TCP/IP disabled but you will not expose yourself to possible legal action by inadvertently connecting to a network that you discover while WarDriving. When you are ready to resume normal operations with your wireless network card, simply repeat steps one and two and then replace the checkmark in the Internet Protocol (TCP/IP) checkbox and click OK. And after setting up all the hardware now you can drive around spotting access points and you can map it in your GPS.

3. LEGAL AND ETHICAL ISSUES

The act of wardriving itself is not illegal, but it does bring into some ethical issues. The legality of wardriving has not been tested, but people think that wardriving itself is illegal. Wardriving itself is a computer security professionals, hobbyist, and others interest, which they provide information to the public about the security vulnerabilities that are present with "out of the box" configurations of wireless access points. The main issue here is what is legal and the ethical dilemmas of tracking wireless vulnerabilities. The problem that comes up is that sometimes network crackers use wardriving tools to locate networks and then crack into them, which is illegal. Ways to keep wardriving legal is to make sure to obey the law as it exists today, and to encourage journalists to draw distinction between wardriving tools and their abuse by crackers and attackers. The problem here as that when the press picks these technology stories, they have a tendency to no always use the correct terminology, which hurts all users. This is the idea of that one bad user is the same as all the other users, which is not the case. There are many people out there using wardriving for it intended purpose. The problem occurs when a few crackers use the same techniques for their own benefits and gains. So it is each users responsibility to make sure that they stay on the right side of the law and avoid committing illegal acts The main ways to stay on the right side of the law is to make sure that each wardriver follows a strict code of ethics that can come down to something as simple as, do not look, do not touch, and do not play through. This breaks down to mainly do not examine the contents of the network, do not add, delete, or change anything on the network, and do not even use the network's internet connection for Web surfing or other online activities, this is referred to as piggybacking. [2] The idea behind this is to just find the network and see that it exist, but don't connect to it in any way. This will prevent you from breaking the law, because connecting to it is stealing and is illegal by today's laws. Just because as a wardriving you don't mean to connect doesn't mean that it is illegal. This can be a problem with some client adapters that auto connect to the a network whenever it comes into range. This is still illegal to connect to any of there non-public access points without permission. The keys on this part is a wardriver is responsible for the hardware that they choose, so make sure that it is running as expected and don't get caught in a situation where something illegal could be taking place. The main thing with the legal issues here is that wardriving is legal and can be beneficial, but this does not mean that everything a wardriver does can be ethical. Wardrivers should take the knowledge they gain from doing such task and help notify people of their vulnerabilities. Having all this information on networks in a given area brings into some ethical issues that a wardriver must make sure they follow, because a wardriver has a database of all these vulnerable networks, it makes it easy for them to get caught into ethical dilemmas. This information can be both used for good and for bad. The good notifying people of their vulnerabilities and the bad taking advantage of these networks or selling information about them to others who might take advantage of this information. This is each users responsibility to ask themselves, is what I'm doing ethical. If the answer is no or even shady it is time to stop doing it and think about the purpose of wardriving and the effects each wardriver has on the technology community.

4. CONCLUSION AND FUTURE WORK

Wardriving is a technique that can be very valuable to the technology community as a whole assuming that it is used with the intent that it was planned on. Wardriving can be both fun and informative and does not just have to be done by the computer professionals, and with online support growing task such as wardriving can be accomplished by just about anyone these days.

In an attempt to change negative public opinion about War Driving and educate consumers about the need to institute wireless security methods on their networks, the University of Advancing Technology funded the Phoenix War Driving research project, which focused on gathering data concerning wireless access points in the Phoenix metropolitan region and the level of security that is utilized in these areas.

During the data collection phase of the war driving project, 60% of the access points discovered had none of the built-in security settings turned on, demonstrating the need for a grassroots consumer education program to inform users of wireless networks about the importance of utilizing these security settings. As the War Driving research project continues, our focus will shift to the development of educational programs that inform the average consumer of the methods for securing wireless networks

REFERENCES

1. ^ Ekahau Heat Mapper
2. ^ WlanPollution
3. ^ http://www.spamlaws.com/war-driving-attack.html
4. ^ Tsow, Alex. "Warkitting: the Drive-by Subversion of Wireless Home Routers".
5. ^ Myers, Steven. "Practice and Prevention of Home-Router Mid-Stream Injection Attacks".
6. ^ Rose, Frank (2006-06). "Lost and Found in Manhattan". *Wired* (14.06). Retrieved 1 September 2007.
7. ^ Blackwell, Gerry (19 December 2005). "Using Wi-Fi/Cellular in P2P Positioning". *Wi-Fi Planet*. Retrieved 1 September 2007.
8. ^ Marwick, Alice (15 February 2005). "Seattle WiFi Map Project". *Students of COM300, Fall 2004 - Basic Concepts of New Media*. Retrieved 1 September 2007.
9. ^ Heim, Kristi (18 February 2005). "Seattle's packed with Wi-Fi spots". *The Seattle Times*. Retrieved 1 September 2007.
10. ^ WiFi user charged for not buying coffee
11. ^ Wardriver arrested for snagging coffee shop signal
12. ^ Worldwide WarDrive Aftermath
13. ^ "Google-Debatte: Datenschützer kritisieren W-Lan-Kartografie - SPIEGEL ONLINE". Spiegel.de. Retrieved 2012-11-08.
14. ^ "mapping MAC addresses - samy kamkar". Samy.pl. Retrieved 2012-11-08.
15. ^ Wei-Meng Lee (27 May 2004). "Wireless Surveying on the Pocket PC". *O'Reilly Network*. Retrieved 1 September 2007.
16. ^ Brenner, Susan (12 February 2006). "Access". *CYB3RCRIM3*. Retrieved 2 September 2007.

17. ^ Bierlein, Matthew (2006). "Policing the Wireless World: Access Liability in the Open Wi-Fi Era". *Ohio State Law Journal* **67** (5). Retrieved 1 September 2007.
18. ^ Ryan, Patrick S. (2004). "War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics".*Virginia Journal of Law & Technology* **9** (7). SSRN 585867. - Article on the ethics and legality of wardriving
19. ^ Kern, Benjamin D. (2005-12). "Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law". *CIPerati* **2** (4). Retrieved 1 September 2007.