WarDriving

António Franco / Pedro Camacho
Universidade da Madeira

UNIVERSIDADE da MADEIRA
www.uma.pt

Abstract

The use of wireless networks is the technology most commonly used nowadays. Every home, professional environment or university has it, sharing information through cables is becoming part of the past. The use of wifi technologies can be unsecure because of the lack of physical security and with this new methodologies like wardriving were invented. This methodology gives the ability to find wireless networks. Although not legal, many people use it because of the benefits, a good database of access points can save you a lot of money since you do not need to pay to access the internet. Over time it became increasingly easy to do it, many applications are available for all kind of Operating Systems.

WarDriving

Definition

The name of "wardriving" is often misunderstood. "Wardriving" is the act of searching for Wi-Fi networks. This term derives from the term "wardialing", when modems were used to connect networks a long time ago. Basically this technique consists of collecting information from Wi-Fi networks like the security type, location and network name, and then this information can be used for statistics of Wi-Fi network security and usability. This collection can be done in various ways either by car or by foot, through a portable phone, Sony PSP, Nintendo DS, in short, any hardware that supports Wi-Fi. Despite the importance of using a GPS to collect the exact location of each network, there is the possibility of using a map to mark the locations if you do not have a GPS. There is a great variety of available software for this purpose. The best known are NetStumbler [1], Kismet [2] and inSSIDer [3] (for Windows), KisMAC [4] and iStumbler [5] (for Mac OS) and WiGLE [6], WarDrive [7] and G-Mon [8] (for Android).

The use of such applications although not completely legal, can be very useful if we think that people around the world have the possibility to use such applications of wardriving. The use of a website (database) to share the gathered information through the internet gives the ability to anyone to see and connect to the internet free of charge. But like everything else, there is always a bad side. This technology when used by people with bad intentions could create ethic and safety problems. Although there are very different security algorithms, there is always someone that figures out how to break them. Often the security problems are more due to the lack of information from people or weak password access. There are no laws that forbid the wardriving if done passively (no connections), just listening to the network broadcasts. But the use of these network services is illegal without permission from the network provider (individual or company).

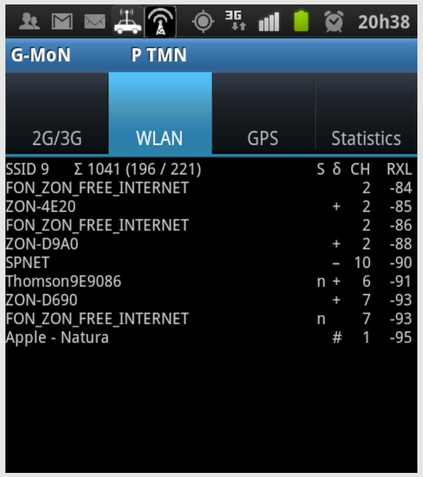
Investigation Area

Initially we thought we would get better results near the Funchal city center. However, after the first WarDrive analysis, we decided that the Forum Madeira area would best correspond to our expectations. We chose Forum Madeira surrounding area because it is a very popular area for offices (enterprises), housing, coffee shops, restaurants and shopping centers.

Methods

Methodology

The first step was to search for applications that could do this kind of work, we found some good applications, but they needed external GPS support. We started to test KisMac and NetStumbler, both gave us a good feedback on Wi-Fi networks like the SSID (Service Set Identifier), channel, gain and security but unfortunately GPS functionality did not work. Since the collected information did not have GPS support it became difficult to organize it. Then we tried the WarDrive application for Android, but like the other applications, we started to have problems and the collected data was incomplete, due to many problems with the GPS on this application. We did not give up, many other testing were done, since the results were not what we expect, we tried another application named G-Mon. After analyzing the following applications, NetStumbler, KisMac, WarDrive, WiGLE and G-Mon we concluded that the one with better results was G-Mon 2.x.
G-Mon is a powerful WarDriving scanner and GSM/UMTS net monitor and dive test tool which can be used on Android platform. It scans for all Wi-Fi networks in range and saves the data with GPS coordinates into a file on a SD card. A kml file for Google Earth can be also created. It shows the encryption, channel and signal strength.
G-Mon gives the ability to collect and map all detected Wi-Fi access points. It is also a 2G/3G net monitor and field test drive tool for radio planning engineers. Needs enabled GPS for correct position in map.



Surveys

1st Survey

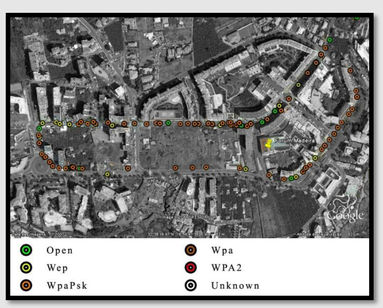
On April 10th, 2011, we made our first approach to the "Forum Madeira's area" in order to gather information about the access points available in that area. For that, we used two mobile phones, Samsung Galaxy S I9000 and HTC Magic, and at the end joined the two kml files in order to see the "Google Earth access points map". The car we used while wardriving has been driven at an average speed of 40 km per h.

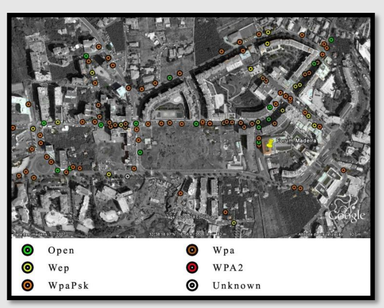
2nd Survey

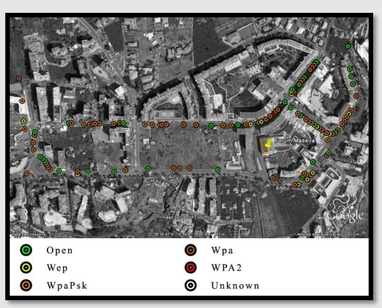
On May 10th, 2011 we made our second approach on the same area. For that we used again two mobile phones, a Samsung Galaxy S I9000 and an HTC Desire HD, and at the end we joined the kml files exported. Unfortunately, a small area has not record any data, maybe the application crashed out. This time, the car we used while wardriving has been driven at an average speed of 50 km per h.

3rd Survey

On 19th June, 2011, we made our final approach to the area of study, and this time, we got more access points near the Forum Madeira Commercial Center. We used for that only one mobile phone, Samsung Galaxy S I9000. The car we used while wardriving has been driven at an average speed of 40 km per h.







Applications Comparison

In this section we will make a brief comparison between the four wardriving application tested, NetStumbler, KisMac, WarDrive and G-Mon.
NetStumbler is an active wireless network detection application that does not passively listen for or receive packets. Its interface also provides filtering and analysis tools.
KisMAC is a passive network detector on supported cards (e.g. Apple's AirPort), packet sniffer and an intrusion detector system.
After using WarDrive service we've noticed that the GPS locator showed up for two seconds and disappeared again. Location gets fixed if we start another GPS location fixing application (i.e. GPS status) that records WarDrive locations properly. After exporting the kml file, only two locations were mapped.
WiGLE (Wireless Geographic Logging Engine) is a website for collecting information about the different wireless hotspots around the world. Anyone can use it, and share a local on WiGLE's website, so anyone can see a global map with all the access points available.
Finally, G-Mon application was the one that gave us better results. It is an easy to use application because we just need a mobile phone with embedded GPS and wireless internet. After wardriving, a kml file with the daily export is saved on SD card. That kml file can be opened in Google Earth, and lets us see all the access points scanned. Note that we made three approaches, within approximately one month each, and different samples were collected.

Conclusion

WarDriving is a technique that can be very valuable to the technology community, assuming that it is used with the intent that it was planned on.
WarDriving can be both fun and informative and can be done by anyone, it does not have to be done only by computer professionals.
The easy use of this technology has made that people take care about their wireless network configurations.
Wardrivers can help anyone to set their networks more secure. Many of the insecure networks can illegally be exploited by crackers and attackers.
We have to adapt to new technologies, wardriving is not going away, we have to learn and improve security. After reviewing several applications we found that wardriving is very easy to do. With this project we acquire knowledge in security and wifi networks. The security of networks can be improved, many alternatives can be done to make a wifi network secure.

References

1. NetStumbler (2011) - http://www.netstumbler.com/
2. Kismet (2011) - http://www.kismetwireless.net/
3. InSSIDer (2011) - http://www.metageek.net/products/inssider/
4. KisMac (2011) - http://kismac-ng.org/
5. iStumbler (2011) - http://www.istumbler.net/
6. WiGLE (2011) - http://wigle.net/
7. WarDrive (2011) - http://code.google.com/p/WarDrive-android/
8. G-Mon (2011) - http://www.wardriving-forum.de/wiki/G-Mon
9. Minkyong Kim, Jeffrey J. Fielding, and David Kotz (2006), Risks of Using AP Locations Discovered Through War Driving, Department of Computer Science (Dartmouth College)
10. Chris Hurley, Russ Rogers, Frank Thornton, Daniel Connelly, Brian Baker (2006), WarDriving & Wireless Penetration Testing
11. H Berghel (2004), Wireless Infidelity I: War Driving