Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Guide to Wardriving and Detecting Wardrivers

Computer users have been deploying 802.11b wireless access points in homes, offices, and schools without any regard to the security of these devices. The overall coolness and convenience of wirelessly accessing the Internet from the office cafeteria or from the next bedroom in the house has distracted most users from taking measures to protect themselves against potential digital threats. Meanwhile, a new activity has taken form: Wardriving. Participants of this activity assemble their rigs of hardware and software wit...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn
More

A Guide to Wardriving and Detecting Wardrivers

Name: Andrew Etter
Certification: GSEC
Version: 1.4b
Option: 1

Table of Contents:

I. Abstract
II. The Rig
III. Scanning Software
IV. Hitting the Road
V. Mapping
VI. Two Methods of Detecting Wardrivers
VII. Conclusion
VIII. References

I. Abstract

Computer users have been deploying 802.11b wireless access points in homes, offices, and schools without any regard to the security of these devices. The overall coolness and convenience of wirelessly accessing the Internet from the office cafeteria or from the next bedroom in the house has distracted most users from taking measures to protect themselves against potential digital threats.

Meanwhile, a new activity has taken form: Wardriving. Participants of this activity assemble their rigs of hardware and software with the intent of cruising streets to find your wireless access point. They share their results and plot the location of your wireless access point on a map – it's probably listed on a web site right now. This paper will discuss the components needed to construct a wardriving rig and suggest methods for detecting wardrivers as they drive past your wireless network.

II. The Rig

A "rig" refers to all of the hardware and software components used while wardriving. A forum on Netstumbler.com is dedicated to sharing details of your rig with others: http://forums.netstumbler.com/forumdisplay.php?s=&forumid=10. The forum is a valuable resource, especially to new wardrivers, because they may learn what components are effective and not effective for wardriving. This forum also allows security professionals to observe how the activity is progressing over time and may even assist in recognizing a wardriver on the road.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Computer System

The foundation of every wardriving rig is a computer system. Most wardrivers choose to use either a laptop or PDA since these devices are relatively light and portable and they may function on batteries if necessary. A simple power inverter may be used with the cigarette lighter adaptor found in most vehicles to provide power for the entire rig.

The selection of a laptop or PDA will affect your available scanning software options. An x86-based laptop may utilize software on several Linux and Windows operating systems. A PowerPC-based laptop will be able to utilize software on Mac OS X or Yellow Dog Linux. With a Pocket PC PDA, one would be restricted to software that runs on Familiar Linux or Microsoft Pocket PC, while Palm OS devices do not have any relevant software available for wardriving at the moment.

Wireless Card

The next necessary component of a wardriving rig is a wireless LAN card. The most important specification of a wireless LAN card is the chipset that the wireless card contains. Three major chipsets are used in 802.11b wireless LAN cards that support wardriving (Johanson, p.2):

Chipset	Vendors
Hermes	Lucent, Dell, IBM, Sony
Prism	Intel, Linksys, NetGear, Proxim, SMC, UsRobtics, Zoom
Aironet	Cisco

NOTE: This table may not represent a complete list of vendors.

When obtaining a wireless LAN card, you must note what chipset it contains because some software programs will only function with one type of 802.11b chipset.

Another characteristic to note about wireless LAN cards is whether or not they have an external antenna connector. According to the Seattle Wireless web page, “the external antenna connection is great for if/when you finally breakdown and admit you need/want one” (Johanson, p.11). Most Hermes based wireless LAN cards have an external antenna connector and most of the time the antenna connector is not advertised. In several cases, it has been found that the external antenna connector of Hermes based cards are plugged with an easily removable piece of plastic.

It proves to be difficult to find a Prism based wireless LAN card with an external antenna connector. Unlike Hermes based cards, if a Prism card does not advertise an external antenna connector, it most likely does not have one. Therefore, it is wise to seek a Prism card that actually advertises an external antenna connector.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Lastly, Aironet wireless LAN cards will require some modification to access the external antenna connector. This modification involves removing the top cover of the antenna section of the card (Spurrier, p.1).

External Antenna

External antennas are not a requirement to participate in the wardriving activity, however, any equipment that can be used to extend the range of a wireless LAN card will allow one to detect more wireless access points with less distance traveled. Antennas come is a variety of sizes, shapes and specifications and they have become the defining aspect of a wardriving rig. Since 802.11b wireless networks operate in the 2.4 Ghz spectrum, a proper wardriving antenna will support this same frequency.

Attaching an external antenna to a wireless LAN card will require the use of a cable called a *pigtail* (Positive, p.1). A pigtail is usually a short 1 to 2 foot cable that converts connectors from your wireless LAN card's proprietary connector to a standard antenna connector. An N-male connector is usually used for the other end of the pigtail and it connects with the N-female cable of the antenna.

There are two main antenna behaviors: directional and omni-directional. Directional antennas are primarily used for fixed point-to-point wireless transmissions. These antennas are unpopular amongst wardrivers because they focus the radio wave transmission and reception in one specific direction. Since the task of a wardriver is to scan an entire area for access points, the only logical antenna choice is an omni-directional antenna. Many omni-directional antennas take the form of whips or blades that offer between 4 and 15.4 dBi power increases (Schafer, p.1).

Under FCC law, if you are using an omni-directional antenna in the 2.4 Ghz range, your rig must not exceed a total output of 1 watt, or 30 dBi (Federal Communications Commission, p.90) (Pozar, p.3) (Young, p.3). Since many wireless LAN cards produce an output that is well under this limit, an external antenna is used to increase the overall power output.

Finally, investigate how the antenna is mounted. Since you will be attaching the antenna to your car, magnetic-mount antennas are preferable.

Amplifiers

Most wireless cards, combined with a 15.4 dBi omni-directional antenna, will achieve power levels very close to the 1-watt FCC limit. However, many wardrivers become fanatical about increasing the range of their wireless cards and may opt to employ the use of an amplifier. Some wardrivers may use a 500mW or 1 watt amplifier to overcome signal loss produced by long cables and multiple cable connectors. While there is no documentation of wardriving rigs that include amplifiers above 1 watt, amplifiers can be found in varieties of up to 50 watts.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

GPS Device

Data collected from a wardriving session would simply be incomplete without also recording the geographic location of the wireless access point. Collection of this data has been automated with the use of common GPS devices. Many GPS devices come equipped with a serial cable that can be attached to a laptop or PDA, therefore wireless network scanning software may have access to the GPS data.

Any GPS device that is capable of NMEA output through the serial port will be compatible with most wireless network scanning programs (Kismet Website, p.2) (Thorn, p.2).

Not all GPS devices are created equal. Some devices acquire GPS satellite fixes faster, while other GPS devices update their coordinates more frequently. Typically, GPS units will update the position every second and will have cold startup times ranging from 45 to 120 seconds.

The most basic of GPS devices will suit your needs for wardriving. The only function required of a GPS device is to provide the current GPS coordinates to the computer system. Inexpensive GPS devices are available that have no displays and no added functionality -- they just provide coordinates.

III. Scanning Software

As mentioned in the pervious section, many different operating systems may be used in a rig. I will discuss popular and free scanning software available for each of these platforms, but this will in no way be an exhaustive list. Many commercial programs are available that specialize in wireless access point detection and troubleshooting. However, most wardrivers are hobbyists and do not usually spend thousands of dollars on software targeted for wireless access point deployment in a business setting. Commercial scanning programs often do not contain certain features, GPS logging for instance, that are found in free and open source software. Security corporations have also been found to be using free and open-source scanning software rather than commercial products (Noguchi, p.8).

Mac OS X - MacStumbler

MacStumbler (http://homepage.mac.com/macstumbler), authored by korben, is the most prominently used wireless network scanner available for Mac OS X. MacStumbler will only function with the proprietary Apple Airport wireless card. According to the author, it was a challenge writing a wireless network scanner for Mac OS X because, “Apple hasn't provide [*sic*] any information on interfacing with their airport card driver.” Korben notes that he “had to reverse engineer the functions required to actually preform [*sic*] the scans.”

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

MacStumbler contains the following features:

- Active scanning for wireless access points
- Logs access points to a plain text file (not wi-scan compliant)

In the future, korben plans to add GPS support to MacStumbler.

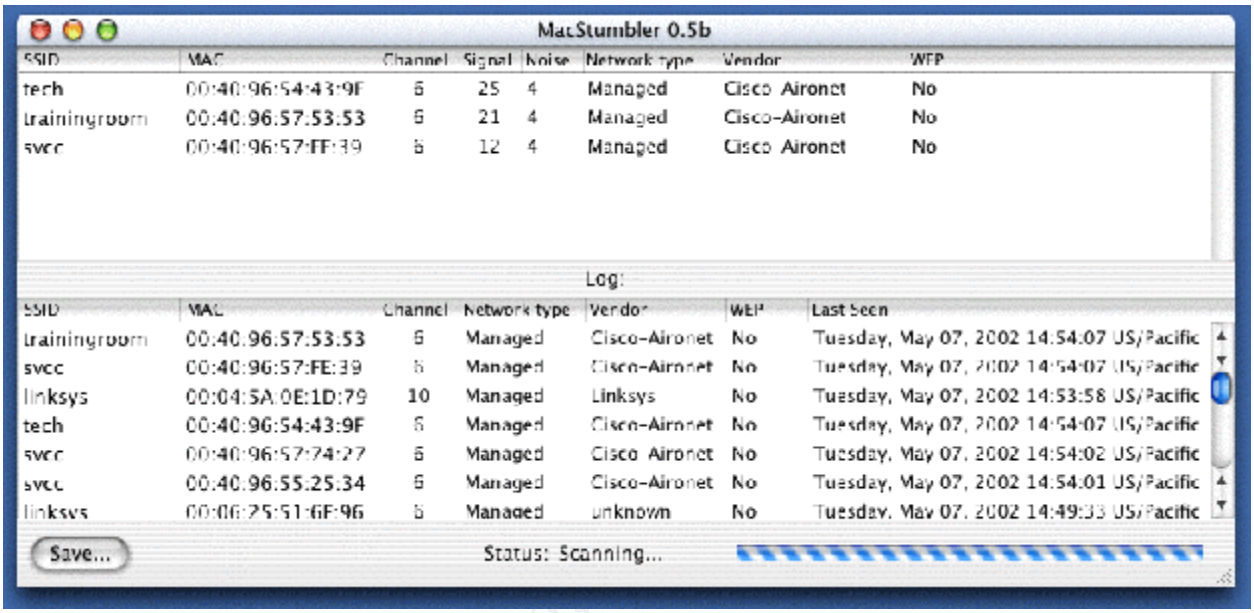

Figure 1: Screenshot of MacStumbler, by korben, from http://homepage.mac.com/macstumbler/

<u>Windows - Network Stumbler (NetStumbler)</u>

NetStumbler (http://www.stumbler.net), by Marius Milner, is the easiest to setup and most popular scanner used on the Windows platform. NetStumbler functions by emitting 802.11b probes that ask wireless access points to respond if they are nearby. Wireless access points are configured by default to respond to these probes, but this option may be turned off to thwart wardrivers from detecting your wireless access point, otherwise known as “cloaking” (Morrissey, p.3).

NetStumbler supports Hermes and Aironet-based wireless LAN cards. Prism support is included with Windows XP.

NetStumbler contains the following features:

- Active scanning for wireless access points
- GPS support
- Logs access points to NS1, extended and summary wi-scan, and plain text files

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

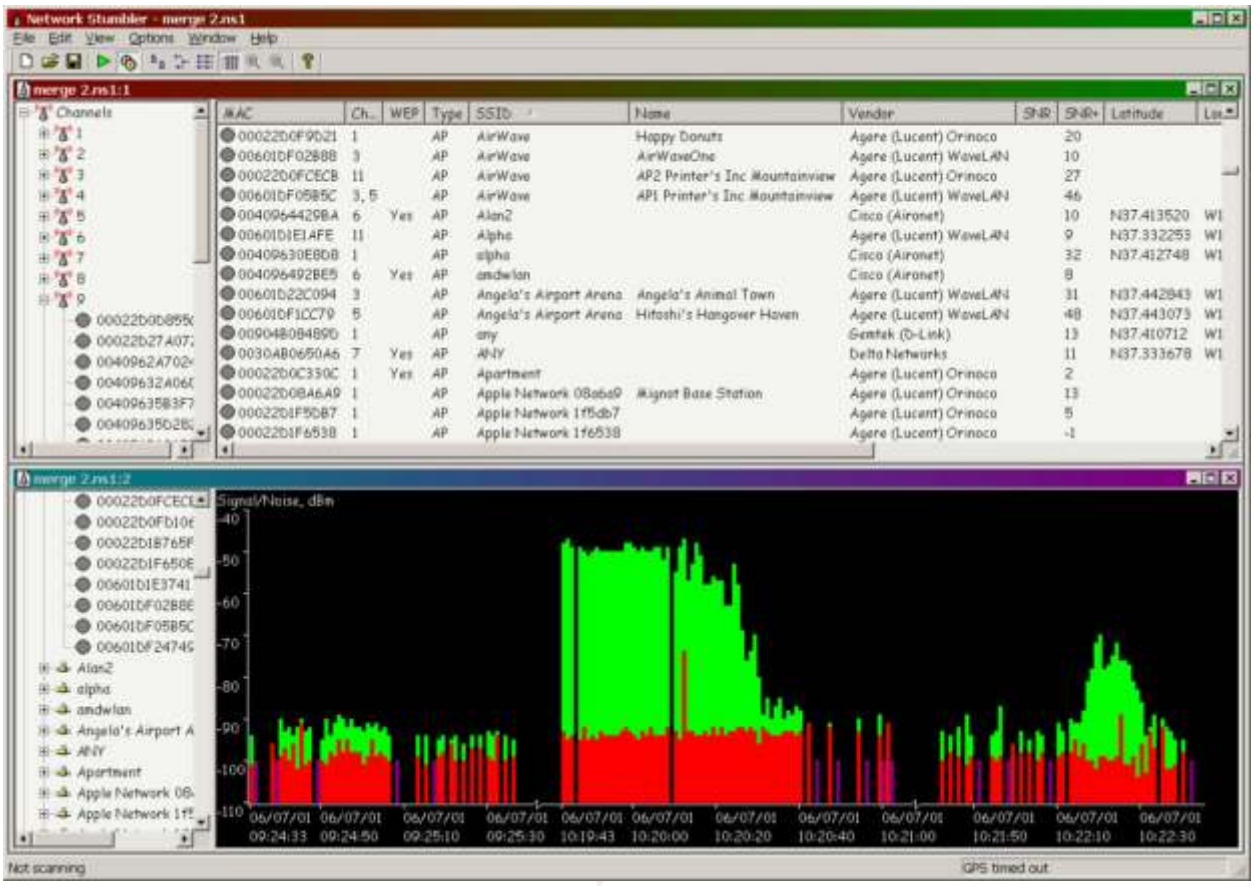

Figure 2: Screenshot of NetStumbler, by Marius Milner, from http://home.pacbell.net/mariusm/

© SANS Institute 2002,

Pocket PC (PDA) - MiniStumbler

MiniStumbler (http://home.pacbell.net/mariusm), also by Marius Milner, is a slimmed down version of NetStumbler that operates on the Pocket PC platform.

MiniStumbler contains the following features:

- Active scanning for wireless access points
- GPS support
- Logs access points to a NS1 file

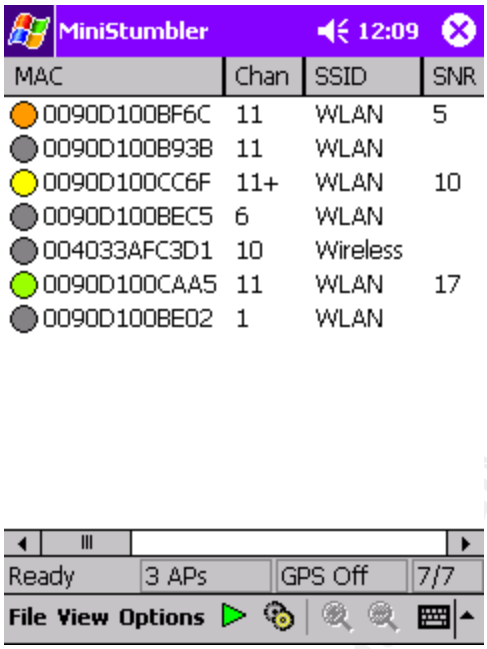

Figure 3: Screenshot of MiniStumbler, by Marius Milner, from http://home.pacbell.net/mariusm/

Kismet – Linux

Kismet (http://www.kismetwireless.net), by Mike Kershaw, is different from MacStumbler, NetStumbler, and MiniStumbler because it is completely passive. Kismet does not send probe requests. Instead, it just listens for access point beacons and network traffic that is traveling through the air. This allows Kismet to also detect "cloaked" wireless access points that are transmitting data, but not emitting beacon packets. In order to achieve this passive behavior, Kismet requires that the wireless LAN card be put into a monitor mode. Up until recently, only the Prism and Aironet-based wireless LAN cards were able to support monitor mode. However, a patch has been created for Linux that allows the Hermes-based cards to achieve monitor mode (Snax, p.1).

Kismet functions on computers and PDAs loaded with the Linux operating system.

Kismet contains the following features:

- Passive scanning for wireless access points
- Detects "cloaked" access points
- GPS support
- Logs access points to Kismet log files (CSV, XML, GPS)
- Logs raw packet data to .dump files
- Includes 'Kismet to CWGD' converter program and gpsmap mapping program

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

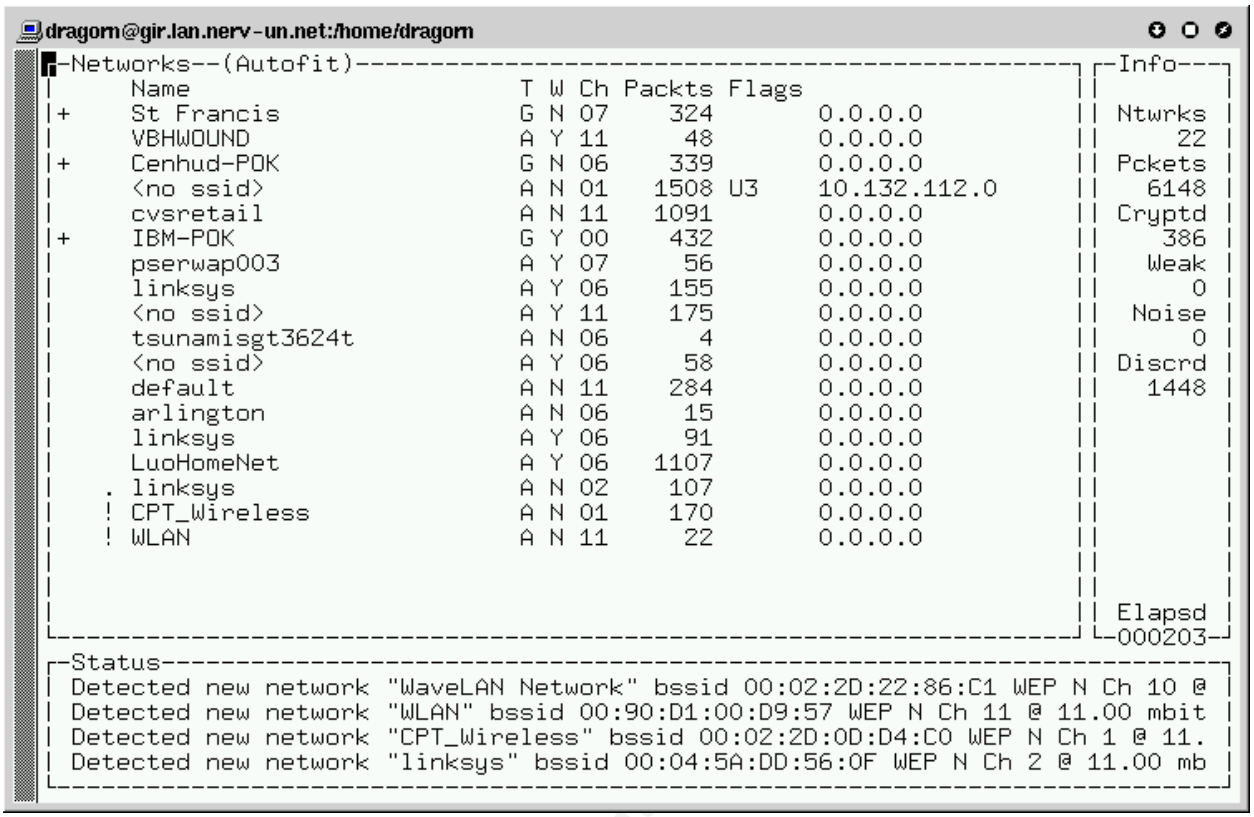

Figure 4: Screenshot of Kismet, by Mike Kershaw, from http://www.kismetwireless.net/screenshot.shtml

IV. Hitting the Road

The typical configuration for a wardriving rig is to place the laptop in the passenger-side seat, place the GPS unit on the dashboard and to magnetically-mount the external antenna to the top of the car.

Several strategies can be employed to maximize the number of wireless access points detected. One common sense strategy is to avoid backtracking down streets that you have already driven through. It helps to keep in mind the range of your external antenna so that you may be able to skip driving down side streets that you know your rig would be able to detect from a distance.

If completeness is not your goal and you are simply looking to detect the most amount of access points in the least amount of time, a little bit of research prior to your wardrive can go a long way. Densely populated areas with higher than average household incomes are ideal grounds to wardrive. Given the cost of a wireless access point and the technical expertise required to set-up and operate one, these demographics make sense. Websites, such as MSN HomeAdvisor (http://homeadvisor.msn.com), will be able to assist in locating these areas. Also, schools, retail businesses and corporate offices are likely to have multiple wireless access points. It is known that bar code

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

readers used in retail stores operate in the 2.4 Ghz frequency and that many corporations are experimenting with 802.11b access points.

As far as the speed of your driving is concerned, take note that your average GPS device will only update every second and it takes Kismet about 4 seconds to hop through all of the channels of the 802.11b protocol. NetStumbler will quickly detect wireless access points because it is actively seeking access points and utilizing the 802.11b protocol that aids in the quick discovery of access points.

V. Mapping

Once a wardriving session has been completed, it is time to present the data in a visual form that is easy to understand. The de-facto standard for doing this is to plot all of the wireless access points on a map and to color the markers red for WEP encrypted and green for no encryption.

This process can be completed by uploading your data to a web site that serves as a global repository for discovered access points or to use readily available software on your computer to generate your own maps.

Two websites exist that allow wardrivers to upload access point information and locations. This data is compiled into a master list and plotted on a map in real time. The two websites are:

- http://www.wigle.net
- http://mapserver.zhrodague.net

A central website is a great method of sharing data with others across the world, but it may be difficult to isolate and analyze the results from your specific wardriving session.

One popular mapping utility that is used to visualize wardriving data is called StumbVerter (http://www.sonar-security.com). StumbVerter is a Windows program that uses maps from Microsoft Map Point 2002 and imports wireless access point data in wi-scan formats.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

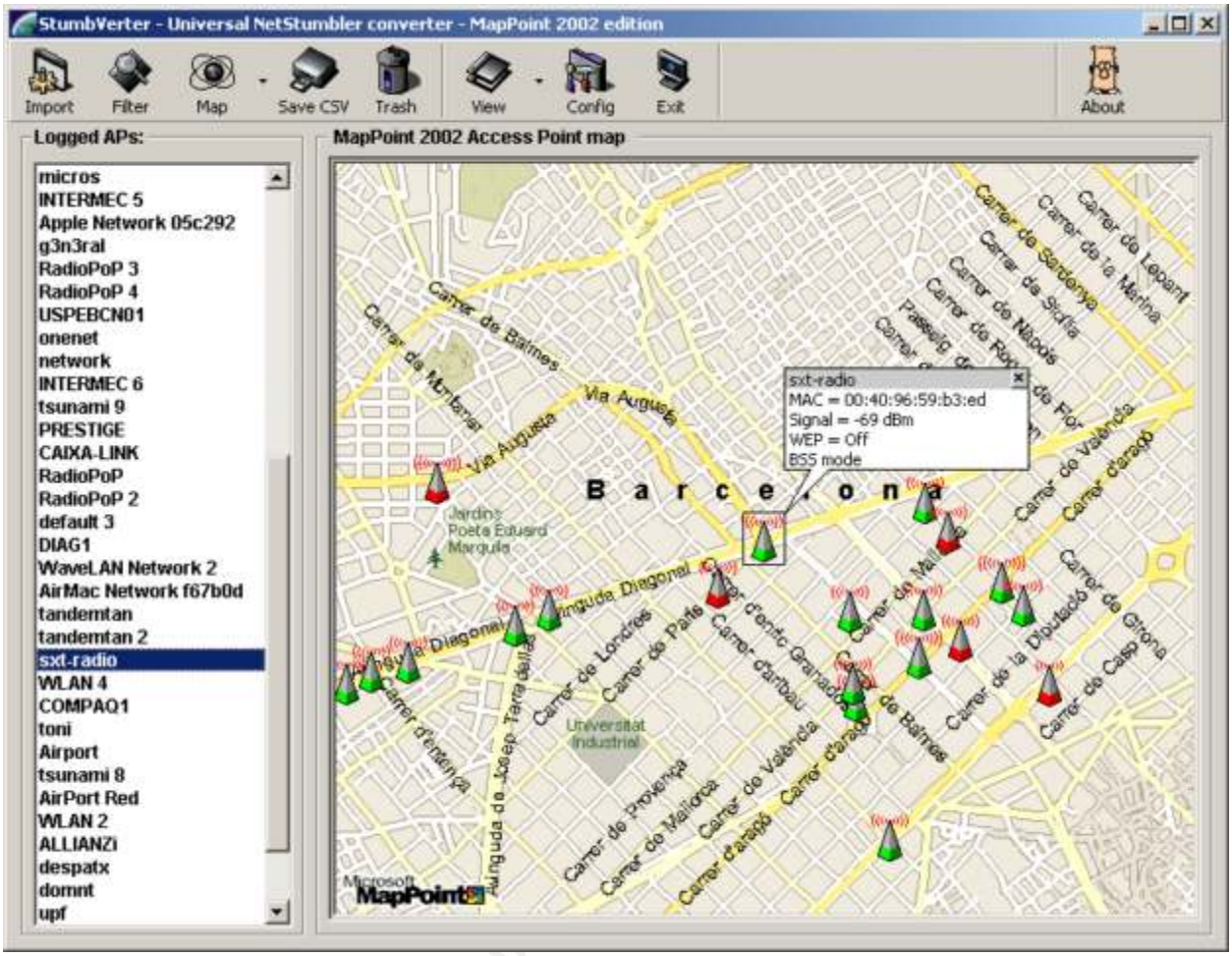

Figure 5: StumbVerter, by Michael Puchol (Sonar Security), from http://www.sonar-security.com

NetStumbler and Kismet log wireless access point and GPS data to their own specified file formats, binary formatted .NS1 for NetStumbler and a combination of .CSV .GPS .XML text and xml formats for Kismet. As you can see, a conversion process is needed to convert data into wi-scan format for StumbVerter.

Just as an overview, there are several different file formats that are used to log wardriving sessions. At least five file formats exist:

- Wi-scan summary
- Wi-scan extended
- CWGD (Common Wireless GPS Data)
- Netstumbler .NS1
- Kismet .GPS .CSV .XML

An open-source project called WarGlue (http://sourceforge.net/projects/warglue/) will allow wardrivers to convert between these data formats. Meanwhile, NetStumbler's built-in converters and several scripts written by Medic and c0nv3r9 are available and sufficient for converting between these formats (blackwave, p.1).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

With Kismet, you have another option for visualizing your wardriving data. A Linux program, *gpsmap*, is bundled with Kismet. Given a Kismet GPS file, gpsmap will download a map from Expedia, Mapblast, and Terraserver and plot the wireless access points. Gpsmap also allows you to visualize the route taken during the wardriving session.

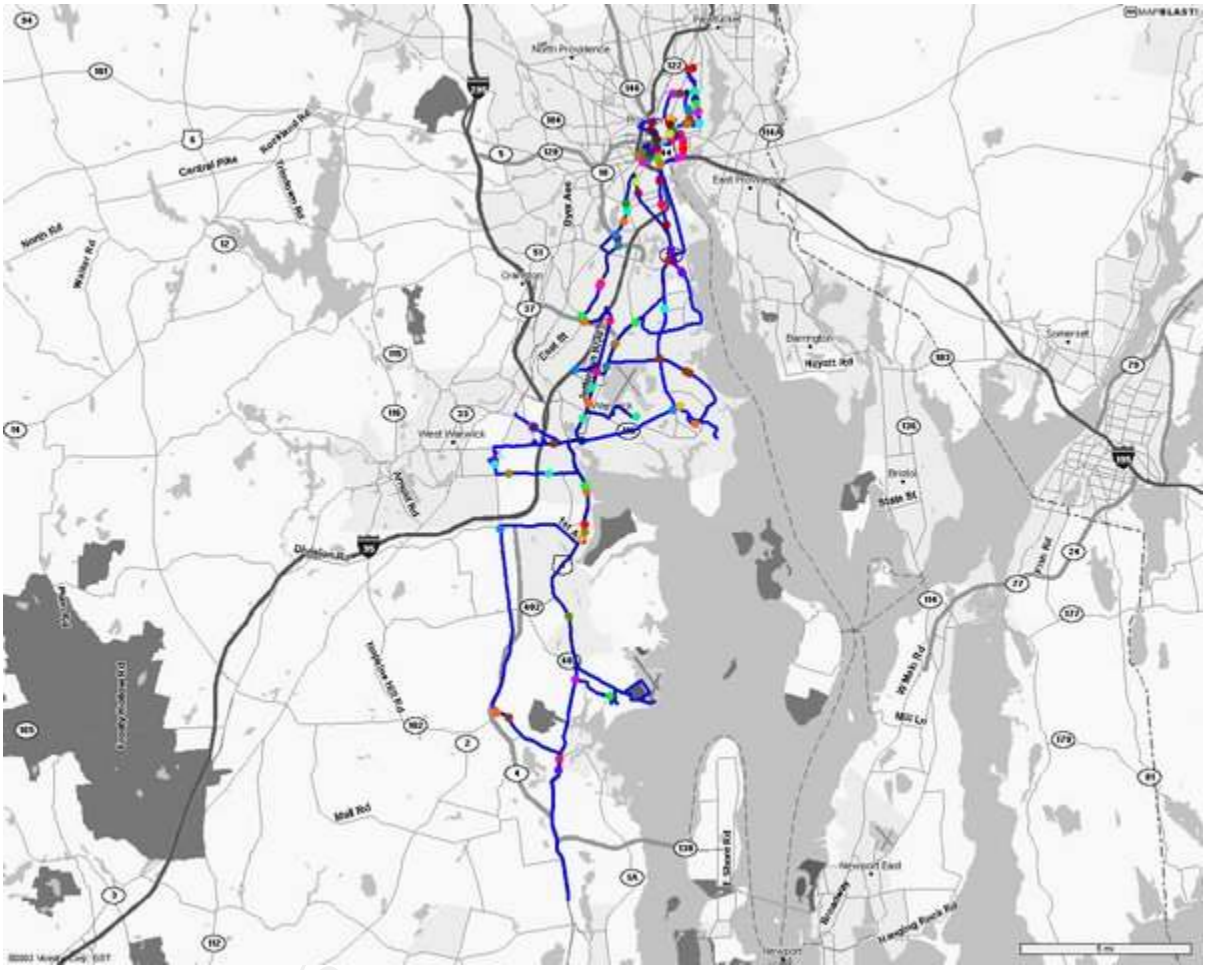

Figure 6: Gpsmap, included in the Kismet package, from http://www.kismetwireless.net/screenshot.shtml

VI. Two Methods of Detecting Wardrivers

Now that you are familiar with the hardware and software that wardrivers use to detect wireless access points, I will discuss two methods that could be used to detect passing wardrivers. The first method is only effective in detecting users of NetStumbler. The second method can be used to detect users of NetStumbler, MiniStumbler, and MacStumbler. Since Kismet is a passive scanner, these methods cannot be used to detect users of that program.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Both of these methods involve setting up a stationary computer with a wireless LAN card and running the Kismet program 24 hours a day. The computer will not be attached to the wireless network; it will simply be in "listen mode."

Method 1: Listening for NetStumbler signatures

A recent addition to the Kismet scanning program is the ability to detect nearby wardrivers that are using NetStumbler. A unique behavior of NetStumbler is that it emits a packet of data after it has detected a wireless network. This packet has a signature that can now be identified by Kismet (Kershaw, p.1).

Method 2: Listening for excessive 802.11b probe requests

A less accurate method of detecting wardrivers is to simply listen for an excess amount of 802.11b probe requests. This will not positively identify all wardrivers because even legitimate 802.11b clients emit 802.11b probe requests. In my own tests, I have found that, on average, NetStumbler emits probe packets more frequently than legitimate 802.11b clients. Further, if you know what devices are legitimately using your network, you may deduce that all foreign 802.11b probe requests are from wardrivers and other unauthorized users.

VII. Conclusion

Wardriving is an activity that many can participate in with low cost and minimal technical expertise. Wardrivers simply record the name, location, and security setting of your wireless access point and the results of this activity point to a large problem of insecure wireless access points. According to Peter Shipley, the inventor of wardriving, "WEP usage is now 33%" (Shipley, p.2). The number of wireless access points that do not enable any form of wireless protection are plentiful. Not enabling WEP encryption on your wireless access point is inviting unauthorized and accidental access to your local network. No protection is perfect, but the use of WEP encryption on your wireless access point will deter most unauthorized access attempts.

VIII. References

Atwood, Mark, *et al*. "Lucent Wireless Card." Version 65. 30 August 2002. URL: http://www.seattlewireless.net/index.cgi/LucentWirelessCard (3 September 2002).

blackwave. "kismet->wi-scan converters posted here." 29 July 2002. URL: http://www.kismetwireless.net/Forum/General/Messages/1027904934.958515 (3 September 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Federal Communications Commission. “PART 15 - RADIO FREQUENCY DEVICES.” 20 August 2002. URL: http://www.fcc.gov/oet/info/rules/part15/part15_8_23_02.pdf (3 September 2002).

Fred. “Wardriving HOWTO (Un-official).” Version 1.0. 4 April 2002. URL: http://www.wardriving.com/doc/Wardriving-HOWTO.txt (3 September 2002).

Gomes, Pedro. “War Dialing and Driving.” 5 May 2002. URL: http://www.infosatellite.com/news/2002/05/p070502wardriving2.html (3 September 2002).

Johanson, Eric, *et al*. “Hardware Comparison.” Version 100. 3 September 2002. URL: http://www.seattlewireless.net/index.cgi/HardwareComparison (3 September 2002).

Kershaw, Mike. “Re: [KISMET] NetStumbler detection.” 22 August 2002. URL: http://www.kismetwireless.net/archive.php?mss:2720:200208:gdceanfbgamhinnacdpp (3 September 2002).

Kismet Website. “Kismet Frequently Asked Questions.” 14 July 2002. URL: http://www.kismetwireless.net/faq.shtml (3 September 2002).

Morrissey, Peter and Advani, Dilip. “Sneak an AiroPeek at WLAN Stats.” 27 May 2002. URL: http://www.networkcomputing.com/1311/1311f33.html (3 September 2002).

Noguchi, Yuki. “High Wireless Acts.” 28 April 2002. URL: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A60405-2002Apr27&notFound=true (3 September 2002).

Positive, Jay Prime, *et al*. “Pig Tail.” Version 36. 30 July 2002. URL: http://www.seattlewireless.net/index.cgi/PigTail (3 September 2002).

Pozar, Tim. “Regulations Affecting 802.11 Deployment.” 6 June 2002. URL: http://www.lns.com/papers/part15/Regulations_Affecting_802_11.pdf (3 September 2002).

Schafer, Marlon K.. “How to Pick the Right Antenna.” 2001. URL: http://www.odessaoffice.com/wireless/antenna/how_to_pick_the_right_antenna.htm (3 September 2002).

Shipley, Peter. “About Pete Shipley.” URL: http://www.dis.org/shipley/ (3 September 2002).

Shand, Adam, *et al*. “Prism2Card.” Version 65. 1 September 2002. URL: http://www.personaltelco.net/index.cgi/Prism2Card (3 September 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Snax. “Orinoco Monitor Mode Patch Page.” URL: http://airsnort.shmoo.com/orinocoinfo.html (3 September 2002).

Spurrier, Andrew and Samin, John. “Cisco Aironet 350 PCMCIA Modifications.” 13 October 2001. URL: http://www.mrx.com.au/wireless/AironetModifications.htm (3 September 2002).

Thorn. “NetStumbler FAQ.” 15 May 2002. URL: http://forums.netstumbler.com/showthread.php?s=&threadid=1797 (3 September 2002).

Young, Michael. “dMystifying the dB.” 23 August 2001. URL: http://www.isp-planet.com/fixed_wireless/equipment/2001/dMystifying_dB.html (3 September 2002).

© SANS Institute 2002, Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced