Global Information Assurance Certification Paper

Erik Montcalm
GSEC Practical Version 1.4b
Option 1 – Research on Topics in Information Security

How to Avoid Ethical and Legal Issues In Wireless Network Discovery

1.0 Executive Summary

A very important subject with any new technology is deciding how current laws deal with new issues that this new generation of products might raise. Several actions that we used to take for granted now could possibly be perceived as illegal. This paper deals with the legal gray area that is specific to wireless network analysis and discovery tools. These tools are very useful for security networking experts, wireless network enthusiasts and malicious hackers alike. This paper takes the position that wireless network discovery tools are similar in nature to port scanners. Therefore, the same criteria should be applied to both when deciding what is ethical or legal. Using both these types of tools in a completely legal manner usually requires a combination of honorable intentions, making sure not to adversely affect the networks we are probing and taking necessary configuration and procedural steps to stay on the good side of the law.
This paper provides basic background information about wireless network security, explains the legal and ethical issues that might arise, categorizes the type of people that might use these discovery tools and attempts to give recommendations for each category

2.0 Introduction

The market for wireless applications and hardware is growing at a phenomenal rate. As with most new technologies that gains market acceptance, the deployment phase is usually followed by the discovery of security issues and subsequent “tweaking”. A good example of this pattern is Internet transactions. In the early nineties, most people didn’t even know what the Internet was. By the end of the 90’s, the Internet was quite the rage and online transactions were booming. But unfortunately, it is estimated that “in the period from 1998-2000, 50% of non-bank online banking had existing vulnerabilities.” [2]

3.0 Current State of Wireless Security

3.1 Basics

At the moment, there are competing standards in wireless LANs. The most popular standard is the IEEE 802.11x suite of standards. This is what this paper

will focus on when talking about “wireless technologies”. Other standards, including Bluetooth and HomeRF have their own set of specifications and security issues and will not be discussed.

Most 802.11 networks use what are called Access Points (AP) in order for the client machine to connect to the network. These APs act as centralized service providers for the wireless network. This mode of communications is called Basic Service Set (BSS). BSS used a single access point for all communication. But an access point is not necessary in order to implement a wireless LAN. Stations can communicate directly with each using the Independent Basic Service Set (IBSS) mode (Peer mode). But in practice, this is not used very much.

3.2 Security issues

The 802.11 suite of standards includes some mechanisms to insure the security of transmitted information. A lot of papers have already been written about the fact that these mechanisms are clearly insufficient from a security standpoint, so only a short summary of them will be given. The main issue we face when dealing with wireless security is the lack of control we have over the communications medium. Radio waves do not care where property lines are drawn. Physical access to copper or fiber wiring was a lot easier to prevent. If we break down the possible types of attacks against wireless networks into the well-known CIA (confidentiality, integrity, availability) model for security, we can analyze the defenses present in the 802.11 standard to overcome these attacks.

Confidentiality:

802.11b has a built-in form of encryption that was designed to make sure that somebody eavesdropping would not be able to understand the information. This provision goes by the name of WEP (Wireless Equivalent Privacy) and is based on the RC4 cipher.

The Ars Technica web site has a very comprehensive explanation of WEP and its problems [10]. This paper will attempt to summarize their findings below.

Known problems with WEP:

a) Attack on the length of the Initialization Vector (IV):

Because there are only 24 bits in the IV, only around 16 million distinct initialization vectors exist. A busy network will have a massive amount of packets flowing through it. Anybody capturing packets on target wireless networks will begin to see the IV repeat itself after a short amount of time. Software can be found to infer the WEP key from this traffic.

b) Attack on weak initialization vectors.

Certain numbers do not work well when used as IVs for the RC4 encryption algorithm. By running packets encrypted with these IVs through a mathematical function, it is possible to obtain part of the WEP key. When enough of these "weak packets" have been obtained, the attacker discovers the WEP key.

c) No key management

The lack of key management is also a big problem for WEP.
So if a key were compromised, a network administrator would need to change the WEP key. The WEP key must be changed not only on the Access point, but also on every client accessing that AP. This is obviously a very tedious and expensive process that could lead to corporations not changing the WEP keys as often as they should.

Availability:

Nothing is included in the 802.11b suite of standards to address availability.
A Denial of Service (DOS) attack is possible using traditional methods (SYN flood, Smurf attack, etc) where the target is saturated with network requests and cannot serve the ones from legitimate clients. The new issue brought to the table regarding the availability of a wireless network is frequency DOSing. In fact, papers have already been written about the vulnerability of 802.11 networks to the jamming of radio waves that it uses. Mika Stallberg has proven that most 802.11b network can be jammed. He even states that jamming can easily be done with "relatively simple equipment sold in open markets"[4].

The only limiting factor for this type of attack is physical proximity. The attacker jamming the network would need to be in the same geographical area as the AP and users. This is somewhat easier to defend against than a DDOS (Distributed Denial of Service) attack that can happen from anywhere on the Internet (i.e. the world).

Integrity:

At the most basic level (layer1), the 802.11b protocol uses Direct Sequence Spread Spectrum (DSSS) mode to transmit data over radio waves. DSSS is a type of spread spectrum radio communications that combines the sending station's data stream with a chipping code. Because the chipping code is a

redundant bit pattern, most transmission errors can be recovered. [5] As we go up the OSI model, most other layers and protocols have their own integrity and error-correction mechanisms.

4.0 Basics of Port Scanning and Methodology

The ISS definition of a port scan is :

"Port Scanning is one of the most popular reconnaissance techniques hackers use to discover services they can break into. A potential victim computer runs many 'services' that listen at well-known 'ports'. By scanning which ports are available on the victim, the hacker finds potential weaknesses that can be exploited." [11]

A port scan usually implies multiple ports. If packets are only sent to one or a few ports, then the word probe or strobe is used.

Because port scanning is in essence network discovery (or reconnaissance), our contention is that it is similar enough in nature to wireless network discovery tools to warrant a comparison. If we start by analysing how to use port scanning tools ethically and legally, we can apply the same criteria to war driving (the act of discovering wireless networks).

So the question now becomes: Is port scanning legal? Is it ethical?

Shaun Jamieson has good reasoning for this in his paper about this very topic that can be found in the SANS reading room

"Whether or not scanning is ethical is a delicate tricky question. While scanning is widely held to be a malicious activity, professionals use the technique regularly to diagnose network problems and to detect vulnerabilities on their own network. The legitimacy of a port scan is often determined by the circumstances surrounding the incident in an attempt to establish intent." [12]

Intent seems to be one component of what makes a port scan legal or ethical. Are there any other factors that weigh into making a port scan legal or ethical?

According to a judgement last year by US judge Thomas Thrash, port scanning victims cannot sue the person scanning if they did not suffer any damage [6]

He also goes on to declare the money spent investigating a port scan cannot be considered damage.

As we can see, the effect on the target network is another component in the equation for calculating the ethicality and legality of a port scan. We

will use these two factors to compare the legality and ethicality of a port scan to those of a wireless network discovery tool.

5.0 Wireless auditing, why it is important?

Most corporations have a security policy that tells users how to use computers in a secure fashion. As pointed out in the first Security Essentials Course book, any way of bypassing the controls put in place to enforce this policy is an added risk to the company from a security standpoint. [9]

Just like corporations previously had problems with users circumventing what they consider overly restrictive security policies controls with unauthorized modems, they will now face the same problems with rogue wireless access points.

Most end-users want the kind of freedom that wireless technologies can give them. With wireless access points becoming cheaper and easier to configure everyday, it is not hard to see why rogue access points might become a problem. And just like war-dialing (scanning for rogue dial-in modems) became part of a standard security audit a few years ago, wardriving is now fast becoming part of the professional security analyst's toolkit. Proof of this can be found by looking at the growing list of professional level wireless network discovery tools.

For example:

1. AirMagnet www.airmagnet.com
2. Sniffer Wireless www.nai.com (Network Associates)
3. AiroPeeks www.wildpackets.com
4. The Wireless Security Auditor www.ibm.com
5. Netstumbler www.netstumbler.com
6. Kismet www.kismetwireless.net/

5.1 Wireless scanning and the law

A recent FBI advisory states that wireless network discovery is not illegal in itself.

"Identifying the presence of a wireless network may not be a criminal violation, however, there may be criminal violations if the

network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations." [14]

This is in agreement with all we have seen up until now. Wardriving to find wireless networks without malicious intent and without causing any harm to it should not be any different than port scanning. The same criteria for ethicality and legality should apply. The FAQ page on Wardriving.com seems to agree with this paper in this regard. In their opinion:

"Simply driving around a city searching for the existence of wireless networks, with no ulterior motive cannot be deemed illegal." [7]

On the other hand, if somebody is trying to get free Internet access, hack into a network, or inadvertently breaks the network, then it will probably be considered a crime.

5.2 Problems with the current law

The reasoning for current laws was acceptable back when every network was wired. At that time, it was easy to determine whom we were connecting to. With wireless networks, this is not always so easy to determine where we are connected.

What if we are moving around or own property and inadvertently connect to the neighbors AP just because its signal is more powerful than our own? We do not have any malicious intent, but we could easily be causing unintended damage to their network by using their bandwith or other resources.

This is exactly what happened to Dave Salvator, from the ExtremeTech web site. He had been using his AP to surf the web from outside his house. He one day discovered that he had unknowingly connected to the Internet through his new neighbors AP. He found the explanation for this after a little bit of research:

"Turns out that the signal to my AP is somewhat weak in the front of my house, and my neighbor's network provides better coverage there. Thus the email/web surfing station I have there only associates with my neighbor's AP, and not mine." [8]

Should Mr. Salvatore be held responsible if his neighbor gets a billed for exceeding his bandwidth usage from his ISP? The problem with current laws regarding this sort of issue seems to be that it is the burden of the end-user to make sure he complies with local law. This would be fine if most products came configured in a way that made inadvertent connections unlikely, but most

wireless products come with Plug And Play fully turned on. Furthermore, most end-users do not have the kind of technical skills required to make sure that this does not happen by accident. It took Dave Salvator (an experienced computer user and computer journalist) a few hours of research and consulting with friends to find a way to make sure he does not connect to his neighbors AP. What are the rest of us supposed to do?

I propose the following categories of people that would use software for to Find APs. These categories are based on the intentions of the person scanning for wireless networks. The different issue that are involved for each issues will be explained and we will later give recommendations according to these categories.

a) Malicious wardrivers (for hacking/cracking reconnaissance)

This category of wardriver should be prosecuted to the full extent of the law. These people are why these laws are needed. This type of scanning will often be a precursor to the real crime, which would be the actual attack on the wireless network.

The problem in this case is one of tracing back the perpetrators. Wireless LANs bring a whole new issue to the table. How are we to trace wireless hackers? The only real way is to triangulate their position, but only while the signal lasts.

b) Hobbyists (wardriving as game, studies)

A lot of people around the world have made a game out of finding wireless access point. DEFCON now has a Wardriving contest that has actual rules and points. [13]

People are building their own antennas to find a greater number of access points at a further range. Other people enjoy hooking their wireless cards to a GPS system and mapping out APs. This way then can trend the adoption rate of this new wireless technology and also do reports and keep metrics on how many use WEP encryption and other interesting facts.

The main problem in this case is finding the legal limit under which they operate.
General consensus is that this type of activity, if performed with benign intentions, is not illegal. But what happens if somebody inadvertently affects the network they just found? This is not supposed to happen, but is something to keep in mind.

c) Professional Security testers/auditors

As discussed previously, network security professionals are increasingly interested in finding unauthorized access points that might bypass the standard company security infrastructure. This is exactly the sort of thing that network security professionals have been doing on wired networks for many years with rogue dial-in devices

If the penetration tester has obtained sufficient permission from the network owner, this should not be a problem. Finding the rogue Access Point is not illegal. But once a list of rogue access points has been obtained, how are we to supposed find out where they are and who was responsible for the breach of company policy?

The simplest way would to do this would probably be to connect to the AP and try to figure out where is connected to the corporate network using standard tools (ping, traceroute, etc). But by doing this, the security professional has no way of confirming if he is connecting to a rogue network or an Access Point that is not hooked up to the company network but just happens to be within its range. If this is the case, then performing the reconnaissance on the AP might be very illegal because we would be doing so on a private network, without the owner's authorization.

This never used to happen with wired networks because it is very easy to determine if the connection is on the company network just by obtaining a list of IP or phone numbers that belong to the company. But with wireless networks, it is a lot harder to determine exactly whom we are connecting to. The Service Set Identifier (SSID) and network name for the Access Point can be used help determine if we are connecting to the right place. But if the network we are looking for devices in the first place, there is no reason it will follow the corporate naming convention in any way.

d) Public APs (open) seekers for wireless Internet use

The wireless technologies seem to have been adopted by the public at a greater pace then companies can roll out commercial services to respond to the growing demand. People want to use their laptops and PDAs in public areas: parks, restaurants, and coffee shops. Certain restaurants and coffee shops are using free Internet access to attract customers. Other people just like sharing and are setting up free Internet access within the range of their access point. Whether the free access point is setup for commercial purposes or just to be helpful to others, we will use the word "public" to describe them. A public access point is a wireless network that was INTENTIONNALY left open, to be used by all. These access points are usually configured with WEP disabled and have a DHCP server handing out IP addresses to anybody who wants one.

The difficulty then becomes differentiating a public AP from a merely insecure one. If we take into account that many access points come configured this way out-of-the-box, this task becomes next to impossible. If the AP is set to broadcast its SSID and gives a DHCP lease to anybody who asks, should it be the user's responsibility to make sure he is connecting to correct AP? Even if we consider that this is the case, how is the user supposed to do this if he is at the correct location for the public AP?

For example:

If I walk into a coffee shop that is supposed to have free Internet access, and sit next to the window. Am I really to blame if I obtain an IP from a private AP across the street?

6.0 Conclusions and Recommendations

This paper has shown the existence of certain legal gray areas in current computer laws dealing with network intrusions with regards to finding wireless networks. Even the most well-intentioned people could be in danger of breaking our current laws. Since most of the issues brought up in this paper have not been tested in court yet, it is hard to say how they really apply in the real world. We will find out in time where the exact line is between illegally finding wireless networks and finding them in an ethical/legal manner. In the mean time, it is best to err the side of caution. Consult the local laws in your areas and make sure to stay well within its boundaries. Finally, here are some specific recommendations to limit their risk of criminal prosecution. We will base the recommendations on the categories of people scanning for wireless networks previously identified.

1) Malicious Hackers

In this case, the recommendations are not to protect this category of person, but to protect one's network from these would-be hackers

- Don't use default configurations (turn off the DHCP service, turn of broadcasting the SSID) .
- Don't rely on built-in encryption, but turn it on anyways.
- Use some form of proven, strong encrypted tunnel (SSH, IPSEC, etc).
- Use some form of authentication (RADIUS, Domain, etc).
- Use MAC address filtering (if available)

It might seem pointless to turn on WEP and turn off broadcasting the SSID if these measures can be bypassed. But in the case where criminal prosecution might become necessary against the malicious hackers, these items prove that the network owner configured the AP with due diligence and that the hacker was knowingly breaking into a network. WEP might be easy to break, but it

does require some specialized software to do so.

2) Hobbyist who wardrive for fun.

- Disable DHCP on the client side in order not to use the network inadvertently
- Do not run any sniffers or capturing software
- Do not clone MAC address
- Do not Clone SSID

In this case, disabling DHCP is not recommended for securing the network, but for making sure we do not inadvertently obtain an IP on the WLAN. Turning off DHCP (or TCP/IP altogether) seems to be the best way to avoid getting an IP on the newly found networks. It is in fact so important, that
The World Wide Wardrive organizers wrote a little page about how to do it correctly [3].

3) Public Networks Seekers

- Do not advertise public networks with warchalking symbols
- Only try and connect to APs you KNOW are public (from lists, sites, name of the AP)
- Make sure the AP you are connected to is your intended target AP

Warchalking is the process of advertising wireless networks and their current state with chalk diagrams on building. Connecting to only to access points with a known name and SSID is the only real of being absolutely sure we have permission from the network owners. Also, once connected to what we think is a known AP, it would be wise to double check that we are actually connected to the correct network.
Confirming the name, the signal strength and that the IP we obtained is in the correct subnet should be standard precaution.

4) Professionals

- Get written permission
- Make sure to use due diligence
    1. Tell customer to make backup
    2. Stay within range of the companies premises
- Turn OFF DHCP for the initial mapping of APs (turn it back on if needed once it is ascertained that the APs belong to the company)
- Use the Signal to Noise ratio readout (signal strenght) to determine if an AP is on company land

It should be much easier to get security professionals to follow these types of recommendations because, by definition, they are more receptive to this sort of legal or ethical requirement. A more comprehensive checklist for professional security testers can be found in the Open Source Security Testing Methodology Manual. [1]

These recommendations might seem either pointless or self-evident, but they might provide some protection from legal action in the case the network owner decides to prosecute the wardriver. If intent is such an important component of these laws, then using these precautions could prove to the court that the network discovery was not malicious.

Works Cited

[11]Unknown, Port Scanning. ISS. 20 August 2002 http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Port_Scan/default.htm

[10]Dismukes, Trey. Wireless Security Blackpaper. Ars Technica. 30 September 2002 http://arstechnica.com/paedia/w/wireless/security-1.html.

[7]FRED, . Wardriving HOW-TO. Wardriving.com. 13 Spetember 2002 http://www.wardriving.com/doc/Wardriving-HOWTO.txt Section_3.1

[1]Herzog, Pete. Open Source Testing Methodology Manual. Ideahamster Organization. 12 September http://www.ideahamster.org/download.htm.

[12]Jamieson, Shaun. The Ethics and Legality of Port Scanning. SANS. 22 October 2002 http://rr.sans.org/audit/ethics.php.

[6] Poulsen, Kevin. Port scans legal, judge says. SecurityFocus.org. 22 October 2001 http://online.securityfocus.com/news/126

[8]Salvator, Dave. Opinion: Plugging Neighborhood 802.11b Leaks . ExtremeTech. October 3rd, 2002 http://www.extremetech.com/article2/0,3973,586818,00.asp.

[2] Junnarkar, Sandeep . Anatomy of a hacking. CNET. 20 May 2002 http://news.com.com/2009-1017-893228.html.

[9]SANS Security Essentials I : Information Security : The Big Picture. 2001, Section 2-4.

[4] Stallberg, Mika. Radio Jamming Against two Popular Wirless Networks . Helsinki University. http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers/stahlberg.pdf

[13] DefCon 10 WarDriving Contest Announcement and Rules. SecurityTribe. Septeber 29th, 2002 http://www.securitytribe.com/wardrive.html.

[14] Shore, Bill. Wireless networks - Warchalking/Wardriving. FBI. October 21st,2002 http://www.politechbot.com/p-03884.html.

[5] DSSS. Webopedia.com. 15 August 2002

http://www.webopedia.com/TERM/D/DSSS.html.

[3] WAYS TO AVOID ACCIDENTALLY GETTING A DHCP ADDRESS AND ACCESSING A NETWORK. World War Drive. September,2002 http://worldwidewardrive.org/nodhcp.html