Practical Wireless Network Security

Derek Williams
CPSC 5157
Columbus State University
+1-770-704-7146
williams_james15@colstate.edu

ABSTRACT

Security measures are available to protect data communication over wireless networks in general, and IEEE 802.11 (Wi-Fi) in particular. Unfortunately, these measures are not widely used, and many of them are easily circumvented. While Wi-Fi security risks are often reported in the technical media, these are largely ignored in practice. This report explores reasons why.

To understand the scope and degree of the problem, I examined the practical aspects of Wi-Fi security, and sought to answer several key questions. For example, are insecure wireless networks truly widespread? What are the real risks in using these networks? Do eavesdropping and circumventing ("cracking") Wi-Fi security mechanisms require such a high degree of skills, time, or resources that the threat is only a remote possibility? Why do users fail to take proper security precautions? What steps can be done to improve the situation?

To answer these questions, I present the results of studies and experiments, which include academic research, opinion surveys, "wardriving", and laboratory "cracking" and "spoofing" exercises.

My high-level conclusion is that the security risks are very real and prevalent, and are far greater than most users understand. I found that the tools and techniques for wireless cracking are so readily available and are so easy to use that the number of attackers will likely continue to grow. At the same time, the number of Wi-fi networks and users (potential targets) continues to rise, leading to an escalating situation. The situation is ripe for large-scale and/or high-profile attacks to become commonplace. I believe that a fundamental shift in public awareness is needed to demand and use higher levels of security.

Categories and Subject Descriptors

C.2.0 **[Computer-Communication Networks]:** Security and protection; C.2.1 **[Computer-Communication Networks]:** Wireless communication

General Terms

Measurement, Security, Experimentation, Verification.

Keywords

Wireless LAN, 802.11, Wi-Fi, Security, Eavesdropping, Cracking, Wired Equivalent Privacy (WEP)

1. INTRODUCTION

The past few years have seen an explosion in the deployment, acceptance, and use of 802.11 (Wi-Fi) technology. ABI Research estimates that over 140 million Wi-Fi enabled devices shipped in 2005, and predicts that number will increase to 450 million devices by 2009. ABI Research further reports 106,000 *commercial* Wi-Fi hotspots in North America [2], which includes 47% growth in 2006. Jupiter Research estimates that there are 14.3 million *home-based* Wi-Fi access points in the United States [6]. Gartner Research reports that by the end of 2006, there will be 89,000 *public* Wi-Fi network access points and more than 99 million Wi-Fi users worldwide.

We also find that Wi-Fi hotspots are being used for increasingly more sensitive, yet unprotected data. A November 2006 Steganos survey of Wi-Fi users in the United Kingdom found that only 8% encrypted their data and only 14% used a secure, encrypted link to the internet. Of these users, 28% said they use Wi-Fi connections for internet banking, 51% send work emails, and 23% shop online.

It should not surprise us, then, that news reports of costly and embarrassing Wi-Fi security breaches are becoming common. In 2003, three college students successfully hacked the Wi-Fi network of a Lowe's store in Southfield, Michigan to steal credit card information and software. That same year, an information security consultant used the Wi-Fi network of a Raleigh, North Carolina clinic to access 2,000 patient records. And the threat is worldwide; for example, hackers in Haifa, Israel used a Wi-Fi connection to break into a post office network and obtain account numbers which they later used to steal money [3].

In spite of great efforts by vendors and consultants to improve security and publicize the risk, there is little or no improvement in the vast majority of Wi-Fi networks. To paraphrase author Charles Dudley Warner, it seems everyone talks about wireless security, but too few people do anything about it. That is, there is a large *implementation gap* between what is available for secure Wi-Fi use and what is put in practice.

To better understand why this is the case, I put forth five key questions to answer.

1. ***Perception:*** Why do users fail to take proper security precautions?
2. ***Scope:*** Are insecure wireless networks truly widespread?
3. ***Severity:*** What are the real risks in using these networks?
4. ***Feasibility:*** Do eavesdropping and circumventing ("cracking") Wi-Fi security mechanisms require such a high degree of skills, time, or resources that the threat is only a remote possibility?
5. ***Solution:*** What steps can be done to improve the situation?

Each of these questions is addressed below.

2. PERCEPTION

Security measures are often highly dependent on human factors. Take a simple example: if homeowners do not know how to lock their house doors or underestimate the risk of a break-in and do not bother to "lock up", then the quality of the door locks is not relevant. The same holds for computer security, which is why David Mackey, IBM's director of security intelligence stated, "I think that in 2006 we're going to continue to see the computer user being the weak link." So, as a first step to understanding the *implementation gap*, I sought to answer the question, "Why do users fail to take proper security precautions?"

I draw my answers from two sources: 1) research of prior studies in this area, and 2) my own opinion survey to fill gaps and address areas not covered in prior surveys.

2.1 Research

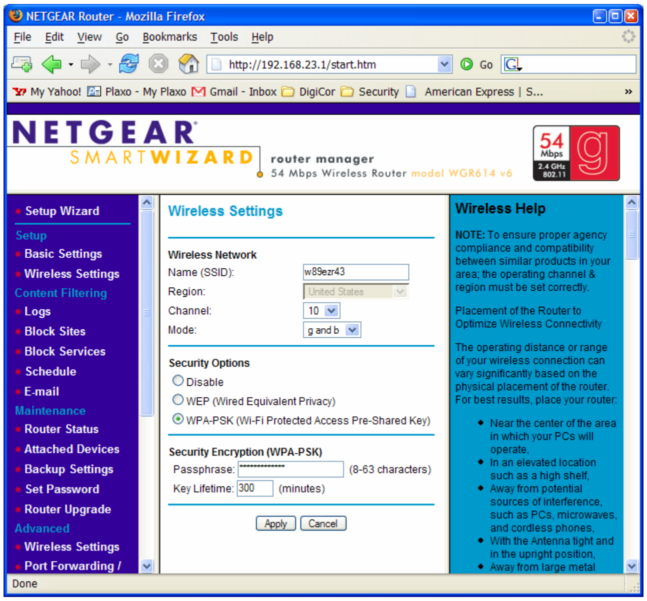
There is much reported in the literature about wireless network security risks, but not significant coverage of the reasons why. I did, however, discover trends that indicated these factors:

1. a lack of *knowledge* - owners of Wi-Fi routers and access points often do not know *how* to adequately secure these devices,
2. a lack of *awareness* –wireless users are not fully aware of how vulnerable they are, and
3. a lack of *urgency* – Wi-Fi owners and users owners may be aware of the potential risk, but do not feel it is great enough to warrant an urgent response.

For example, Humphrey Cheung, editor of the technology Web site *tomshardware.com* had this to say about people who buy wireless routers: "Most people just plug the thing in. Ninety percent of the time it works. You stop at that point and don't bother to turn on its security." [7]

Indeed, many wireless networking vendors disable security by default, particularly on consumer devices, in order to make them easier to use, and to reduce potential support calls and product returns.

I found, however, that, while users may be intimidated by the terminology and perceived difficulty of securing a wireless network, the process is usually quite simple. I conducted a simple experiment with a common Wi-Fi router (a NETGEAR WGR614) and two users (albeit fairly skilled with computers) to see how much time was required to configure WPA encryption on the router and the two Windows XP laptop computers that use it. In both cases, the entire process was completed in less than 20 minutes, using the router's web interface (see *Figure 1*). It was necessary to use a wired connection to the router to configure it, and, in two cases, the users had to refer to the router's (conveniently located) online help text, but both accomplished the task without outside help and without even referring to manuals. Through this process, we did discover room for improvement, which is discussed in the *SOLUTION* section below.



Wireless Settings

Wireless Network
Name (SSID): w89ezr43
Region: United States
Channel: 10
Mode: g and b

Security Options
○ Disable
○ WEP (Wired Equivalent Privacy)
● WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)

Security Encryption (WPA-PSK)
Passphrase: ************** (8-63 characters)
Key Lifetime: 300 (minutes)

Wireless Help

NOTE: To ensure proper agency compliance and compatibility between similar products in your area; the operating channel & region must be set correctly.

Placement of the Router to Optimize Wireless Connectivity

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the router. For best results, place your router:

- Near the center of the area in which your PCs will operate,
- In an elevated location such as a high shelf,
- Away from potential sources of interference, such as PCs, microwaves, and cordless phones,
- With the Antenna tight and in the upright position,
- Away from large metal

Figure 1 - Wireless Router Configuration - Web Interface

Perhaps what lacks more than the "how to" *knowledge* of securing a wireless network is the *awareness* of the vulnerabilities. Most wireless network owners do not think of their LAN as a miniature "radio station" broadcasting their computer communication to anyone in range who wants to listen when, in reality, that's exactly what it is.

Almost by definition, *public* wireless networks are insecure; otherwise, they would not be easily available. The risk in this context is that users are lured into a false sense of security in thinking that their wireless messages cannot be read when they can be, often quite easily.

The Cheung study report demonstrates the lack of *urgency*, such as the case of Martha Ramirez of Miami, Florida. Ms. Ramirez said she had not thought much about securing her wireless internet connection until she found a man outside her condominium with a laptop pointed at her building. When she asked the man what he was doing, he said he was stealing a wireless internet connection because he did not have one at home. She was amused but later had an unsettling thought: "Oh my God. He could be stealing *my* signal." Yet some six months later, Ms. Ramirez still had not secured her network. [7]

2.2 Opinion Survey

One topic that I found that was not well addressed in prior research is exactly how threatened people feel by the possibility of an attack.

To help answer this question, I conducted surveys both online (using SurveyMonkey, www.surveymonkey.com, and email) and in person. I asked 10 questions, including, "What do you think the likelihood is that someone will steal information from your home wireless network?" Among those who had open networks or only weak encryption, 13% answered "Impossible", 47% responded "Highly Unlikely", and 23% answered "Somewhat unlikely." Out of these responders, only 17% answered "Somewhat likely" or "Highly likely."

I asked a similar question for public Wi-Fi hotspots; that is, "What do you think the likelihood is that someone will steal information from you while you use a public Wi-Fi network?" In this case, 8% answered "Impossible", 20% responded "Highly Unlikely", and 41% answered "Somewhat unlikely." Only 31% answered "Somewhat likely" or "Highly likely."

To summarize, many Wi-Fi users are not concerned enough about security risks to be motivated to invest the time to secure their networks.

2.3 Conclusion

I found that the majority of Wi-Fi users carry a false sense of security about their network use, and, indeed, the computer user is often the weak link in the solution. An increasing urgency and awareness is needed to motivate users to learn and apply simple security measures.

3. SCOPE

To understand the scope of the problem, I sought to answer the simple question, "Are unsecured (or inadequately secured) wireless networks truly widespread?"

As stated earlier, there are over 14.3 million *home* wireless networks and over 89,000 *public* Wi-Fi access points in the United States. And the number of Wi-Fi enabled devices is expected to grow by over 320% by 2009. So two questions that follow are, "how many of these networks are unsecured?" and "is the situation improving?"

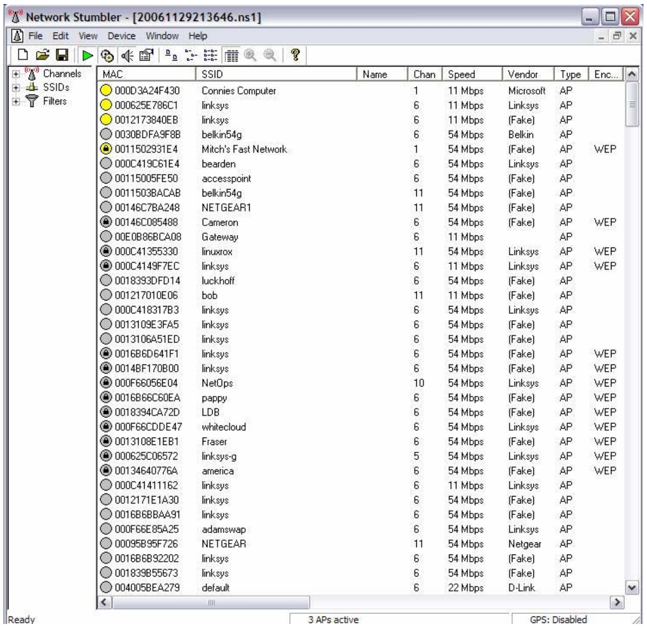
3.1 Wardriving

To understand this further, I conducted my own *wardriving*[1] experiments of neighborhoods in the Canton, Georgia area. I used a laptop computer running the *NetStumbler* auditing software to collect and log Wi-Fi access points in residential neighborhoods. I did not include public or commercial networks, and NetStumbler not report networks where the SSID was "hidden"[2]. I used the laptop's standard features with no special equipment or antenna. In short, I used tools that nearly any laptop computer owner could configure and use in just a few minutes. *Figure 2* shows a sample screen shot of networks logged in these experiments.

Columbus State University, CPCS 5157, December 2006, Canton, GA, USA.

[1] *Wardriving* means to search for Wi-Fi networks by laptop computer or other network detection device while driving around. It is named after the practice of *wardialing* (searching for networks by automatic dialing) demonstrated in the 1983 movie *WarGames*.

[2] Other tools I used, such as *Kismet*, would display networks with hidden SSIDs. But I used *NetStumbler* more often because of its ease of use and my focus on open networks.



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...
000D3A24F430	Connies Computer		1	11 Mbps	Microsoft	AP	
000625E786C1	linksys		6	11 Mbps	Linksys	AP	
0012173840EB	linksys		6	11 Mbps	(Fake)	AP	
0030BDFA9F8B	belkin54g		6	54 Mbps	Belkin	AP	
0011502931E4	Mitch's Fast Network		1	54 Mbps	(Fake)	AP	WEP
000C419C61E4	bearden		6	54 Mbps	Linksys	AP	
00115005FE50	accesspoint		6	54 Mbps	(Fake)	AP	
0011503BACAB	belkin54g		11	54 Mbps	(Fake)	AP	
00146C7BA248	NETGEAR1		11	54 Mbps	(Fake)	AP	
00146C085488	Cameron		6	54 Mbps	(Fake)	AP	WEP
00E0B86BCA08	Gateway		6	11 Mbps		AP	
000C41355330	linuxrox		11	54 Mbps	Linksys	AP	WEP
000C4149F7EC	linksys		6	11 Mbps	Linksys	AP	WEP
0018393DFD14	luckhoff		6	54 Mbps	(Fake)	AP	
001217010E06	bob		11	11 Mbps	(Fake)	AP	
000C418317B3	linksys		6	54 Mbps	Linksys	AP	
0013109E3FA5	linksys		6	54 Mbps	(Fake)	AP	
0013106A51ED	linksys		6	54 Mbps	(Fake)	AP	
0016B6D641F1	linksys		6	54 Mbps	(Fake)	AP	WEP
0014BF170B00	linksys		6	54 Mbps	(Fake)	AP	WEP
000F66056E04	NetOps		10	54 Mbps	Linksys	AP	WEP
0016B66C60EA	pappy		6	54 Mbps	(Fake)	AP	WEP
0018394CA72D	LDB		6	54 Mbps	(Fake)	AP	WEP
000F66CDDE47	whitecloud		6	54 Mbps	Linksys	AP	WEP
0013108E1EB1	Fraser		6	54 Mbps	(Fake)	AP	WEP
000625C06572	linksys-g		5	54 Mbps	Linksys	AP	WEP
00134640776A	america		6	54 Mbps	(Fake)	AP	WEP
000C41411162	linksys		6	11 Mbps	Linksys	AP	
0012171E1A30	linksys		6	54 Mbps	(Fake)	AP	
0016B6BBAA91	linksys		6	54 Mbps	(Fake)	AP	
000F66E85A25	adamswap		6	54 Mbps	Linksys	AP	
00095B95F726	NETGEAR		11	54 Mbps	Netgear	AP	
0016B6B92202	linksys		6	54 Mbps	(Fake)	AP	
001839B55673	linksys		6	54 Mbps	(Fake)	AP	
004005BEA279	default		6	22 Mbps	D-Link	AP	

Figure 2 - NetStumbler - Finding Open Wireless Networks

Out of more than 500 networks logged, 54.8% were open with no encryption. Also, it was very common to find access points with SSIDs set to a default name (typically a brand name). As discussed below, use of a common SSID is a security risk. Some of the more commonly-deployed SSIDs I found were:

SSID	% (Out of 509)
belkin54g	2.9
linksys	27.8
NETGEAR	7.0

3.2 Research

In April, 2004, a study by Humphrey Cheung (cited earlier) found similar results. He sought to determine how common open wireless networks had become at that time. He and some colleagues flew two single-engine airplanes over metropolitan Los Angeles with two wireless laptops. Their study logged more than 4,500 wireless networks, and only about 30 percent of those had encryption enabled. [7]

Later that same year, Mike Outmesguine, owner of a technical services company did an 800-mile "wardrive" from Los Angeles to San Francisco. He found over 3,600 networks (compared to 100 on that same route in 2000), and nearly 40% did not have a single change in the (completely unsecured) default settings. [5]

Between the Cheung study and my own samples, we find an increase in the percentage of secured (vs. open) networks – from 30% (April, 2004) to 45.2% (November, 2006). This is encouraging, although there may be other contributing factors.

4. Conclusion

The answer to the question, "are insecure wireless networks truly widespread?" is a clear "yes". While awareness is growing and security is improving, the world of wireless LANs is very much a "wild west frontier," and there remain millions of completely open Wi-Fi networks in the U.S. with no security. It is truly a "target rich environment" for even the simplest forms of hacking.

5. SEVERITY

Clearly, open wireless networks are common and widespread, but how significant is this? In other words, what are the real risks in using these networks? For example, if the digital content flowing over these networks consisted only of streaming digital music, having adequate security is not important.

These questions remind us of the days when analog cellular telephones were commonplace. As with many wireless networks today, users of analog cell phones slowly began to learn that their telephone conversations could be fairly easily monitored (in that case, using common radio scanners). But public habits and behaviors did not begin to change until some high-profile eavesdropping cases were reported.

In once instance, a Florida couple recorded a cell phone conversation between U.S. Representative John Boehner and U.S. House Speaker Newt Gingrich. It provided evidence that Gingrich may have violated his agreement with the House Ethics Committee, and became very politically damaging, not only for Gingrich, but for many of the politicians involved.

In 1998, freelance journalist Eric Ford used a scanner to record a cell phone conversation between Tom Cruise and Nicole Kidman describing their marital problems. Mr. Ford sold the information to *The Globe* which reported it in a story that was picked up by other media outlets.

In both cases, the unwelcome attention and speculation caused many to rethink their cell phone usage, and led to increased public caution in cell phone conversations and greater demand for the more secure digital cell phones.

U.S. Representative Mike Honda from California believes that the broad problem of inadequate wireless internet security is so great that it has become a national security issue. At a briefing in March, 2006, Rep. Honda stated, "Sales of laptops and portable devices continue to skyrocket as more and more Americans demand mobile Internet access, but with this increased usage come added security risks... Reliance on computers and computer networks raises the vulnerability of the nation's critical infrastructures to cyber-attacks." [13]

We sense that this feeling is shared by terrorist organizations when we hear reports such as the December 1, 2006 National Security Alert of a possible Al-Qaeda cyber attack. When viewed at the national level, wireless internet security is indeed a "weakest leak" problem. That is, even if 99% of all accessible wireless networks in the U.S. were to be secured, nearly 150,000 open networks would remain, more than enough to launch crippling distributed denial of service (DDoS) attacks.

The broad increased availability of "hacking" tools have made attacks so widespread that organizations such as DShield, a free public, non-profit "distributed intrusion detection system" now report global attack statistics in real-time. DShield maintains a free public database for sharing intrusions from millions of firewall logs around the world. Global security "dashboards", such as the Talisker Computer Network Defense Operational Picture (http://securitywizardry.com/radar.htm) demonstrate how internet security attacks are continual and highly frequent. And the major vendors offer their own regular reports, such as IBM's

Security Threats and Attack Reports and Symantec's *Internet Security Threat Reports*. Together, these ongoing monitors, alerts, and reports provide a sobering view of the onslaught of network security attacks.

For example, phishing[3] attacks now number more than 33 million a week, instant messaging attacks grew more than 2200% from 2004 to 2005 [4], and medium- to large- internet sites typically see thousands of port scans a day. Certainly not all of these threats and attempts result in successful attacks but the sheer volume of attacks creates a struggle for many organizations to maintain viable networks.

In the literature, we find the following possible threats to insecure wireless networks:

1. Identity theft

   Identity theft involves collecting sensitive private to impersonate someone else, often to steal money from existing accounts, or open and use new accounts in that person's name.

   A recent study by the U.S. Department of Justice found that identity theft losses cost an estimated $6.4 billion each year. The study found that, in the first six months of 2004, an estimated 3.6 million U.S. families were hit by some form of identity theft; that's nearly 3% of all U.S. households. [8]

   The 2005 Javelin Identity Fraud Survey Report found that about 11.6% of all known identity fraud cases came from online channels. The most common enablers of identity theft remain "offline" methods such as a lost or stolen, wallet, checkbook, or credit card, yet online identity theft is growing. [14]

2. Account fraud

   Account fraud involves gaining enough confidential account information to illegally access another person's account and withdraw money. This includes stealing such things as credit card numbers and authentication information (expiration dates, credit card verification numbers, etc.) and checking account numbers with personal identification numbers (PINs).

   A Gartner Research study found that nearly two million Americans have had their checking accounts raided by criminals in 2004. Consumers reported an average loss per incident of $1,200, pushing total losses higher than $2 billion for the year. Many customers surveyed did not know how their account information was disclosed, but experts report that online mechanisms could be the cause of up to half of the takeovers.

   As with identity theft, "offline" channels may remain the largest source of account fraud, yet the resulting new security fears (perceptions) are themselves becoming very costly. For example, an August, 2006 Gartner study estimates that more than 9 million adults in the U.S. have stopped using online banking because of security concerns and 23.7 million will not start due to these same concerns. The study further estimates that nearly $2 billion in potential sales is lost each year due to security concerns of online shoppers.

3. Viruses, spyware, and malware

   Insecure wireless networks can provide the vehicle to access a person's computer and plant viruses, spyware, and other unwanted programs on it. Kelly Martin of SecurityFocus puts it plainly: "With the consumer Wi-Fi explosion, launching a virus into the wild has never been easier and more anonymous than it is today. Like a sneeze in a crowded subway, it's hard to find the human source of the latest viral infection."

   Craig Mathias, security expert with the Farpoint Group said this about wireless networks: "security measures are ... still an issue... the fear is those who are malicious, and the threat of installing viruses or spyware onto a network and computer. Many of these attacks can be avoided if people take basic precautions, but many just don't know they should." [11]

4. DDoS attacks

   A distributed denial of service (DDoS) attack is a coordinated attack using many computers (often thousands of them) accessing a single target at once, in an attempt to overwhelm it and render it unusable to others. Historically, viruses (such as MyDoom) planted through conventional means (such as email attachments) have been used as the source of such attacks. But many speculate that open wireless networks will soon become a common source of planting DDoS agents.

5. Espionage

   Online espionage, or "netspionage" (network enabled espionage) is using the internet to illegally gather competitive information. It can involve hacks into corporate intranets or networks, or simply eavesdropping in the expectation that users will take shortcuts when working with proprietary information. As we will see later in this report, insecure wireless networks become a ready vehicle for gathering private information.

   It is difficult to understand the full scope of this problem, as it often takes time to realize information theft has occurred, and many companies do not want to openly admit they have been victimized. But a 2001 survey of 138 companies by the American Society for Industrial Security estimated the value of proprietary information and intellectual property lost through computer espionage by these companies to be between $53 and $59 billion. [1]

6. Phishing and pharming

   Internet phishing involves masquerading as a legitimate site (such as an online banking login page) to gather sensitive data. Pharming is similar, but further involves planting controls (such as malware or incorrect domain name server entries) to cause users to be redirected to a "spoofed" site. Open wireless networks can facilitate phishing and pharming through such means as "evil twin" access points and hacking the attached computers to plant controls. Wireless phishing (described below) is a practice becoming so common that it has its own new name: *wiphishing*.

[3] Phishing is the use of email messages that masquerade as legitimate sites to attempt to gather private information for identity theft or other types of fraud.

A 2004 Gartner study found that at least 1.8 million consumers had been tricked into divulging personal information in phishing attacks, most within that year.

7. Blackmail

   In our new bold Web 2.0 era, there is a web site for everything: something web designer Tom Scott fully recognized when he created the online blackmail and extortion site *extortr* (http://www.extortr.com/). Of course, the site is tongue-in-check, but it acknowledges the real and growing problem of online blackmailing. The means (enablers) of online blackmail are varied, but include such threats as disclosing sensitive information obtained through internet eavesdropping and cracking, possible DDoS attacks, and even new "ransomware" software that blocks access to data.

   For example, in early 2006, a Russian gang extorted more than $4 million from British companies by threatening DDoS attacks against them. Fortunately, the group was apprehended, due to a coordinated effort from law enforcement agencies in three countries.

   A recent Reuters story states that blackmailed threats of embarrassment to individuals is often a very real, but under-reported crime. The report cites a British cyber crime detective who commented that the typical victim quietly "puts it on her credit card and transfers the funds to the (suspect's online bank) account and hopes it goes away." [10]

8. Reduced computer performance and internet slowdowns (piggybacking)

   Persons who have been infected with computer viruses and malware are all too aware of how they can slow a PC's performance. Further, having bandwidth stolen from other users who "piggyback" on a wireless LAN can seriously harm its performance.

   Such was the case for Randy and Christine Brodeur of Los Angeles. Their wireless internet connection had slowed to the point of being practically unusable. Mrs. Brodeur told how they were at first puzzled by how this could occur, "I didn't know whether to blame it on the Santa Ana winds or what." [7] They eventually discovered that the source was neighbors who had secretly joined their wireless network.

   While a few Wi-Fi owners openly invite piggybacking, a history of harmful effects have caused governments such as the State of California and the United Kingdom to ban the practice. And piggybackers themselves are at risk, as an open wireless network may be a hacker's "honeypot[4]" for victimizing attached computers.

9. False prosecution (guilt by association)

   While this is a legal "gray area" for individuals, the "safe harbor" provisions in the Digital Millennium Copyright Act have been used to defend those whose Wi-Fi networks are unknowingly used to commit crimes. But the time and energy to participate in the legal process can be costly. Such was the case of some Venice, California residents, whose wireless internets were used in 2003 to send spam e-mails advertising pornographic Web sites. The victimized network owners were cleared, but without first being dragged into the legal process. [11]

Many of these are threats are inter-related and can be combined to create a compounding problem. For example, open networks can be used to plant malware that enables DDoS attacks along with wipharming tools to steal account information.

5.1 Wireless Data Value Experiments

While considering the seriousness of critical data flowing over wireless networks, I sought to determine whether obscurity was a valid defense. That is, could the occasional un-encrypted (yet highly sensitive) data packet be effectively hidden in the noise of volumes of streaming media and other non-critical data?

To answer this, I used freely-available protocol analyzers (wireless "sniffers") to collect wireless LAN packets. Eavesdropping laws not always clear in the area of wireless networks, yet for ethical reasons, I carefully avoided sniffing traffic from other users, and resorted to lab experiments with my own equipment to determine this.

I found the *Wireshark* (formerly *Ethereal*) sniffer running under Microsoft Windows and Linux to be a powerful and approachable tool, but I discovered a severe limitation – it would only sniff my own traffic and broadcast packets (such as ARP[5] packets)[6]. I found the problem to be that most drivers, particularly Microsoft Windows drivers, and many Wi-Fi adaptors do not support placing the Wi-Fi card into "monitor mode," which is necessary to collect all traffic. I did, however, find Linux drivers that supported monitor mode for the wireless card in one of my laptop computers (an Intel PRO/Wireless 220BG adapter). I had to use the *Kismet* sniffer running under Linux and also correct some scripts (such as *start-kismet*) that had faulty driver detection (the scripts incorrectly determined that newer driver versions would not work). I found that I could collect the packets under Kismet, save them to pcap files for analysis by *ngrep* and other tools, and even load them into Wireshark under Windows for handy browsing.

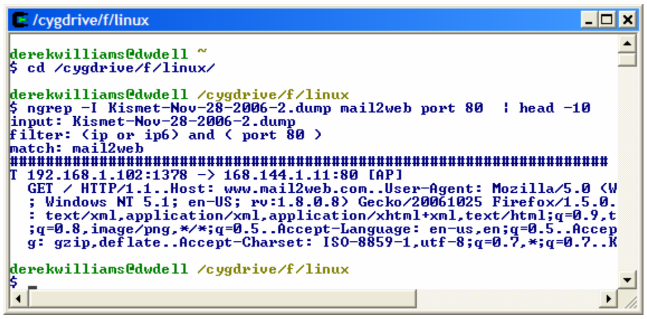
Tools such as *ngrep* solve the "needle in a haystack" problem when searching for vulnerabilities in very large dump files. *Figure 3* shows a simple example (the output is intentionally chopped to the first 10 lines to avoid revealing private information). This *ngrep* command example finds HTTP packets

[4] An internet *honeypot* is a site, computer, or network used to lure in and trap users. Honeypots can be used both ways – they can trap those seeking to cause harm and they can cause harm to those seeking common network use.

[5] ARP is Address Resolution Protocol, a mechanism that uses broadcast messages to map IP addresses to hardware addresses.

[6] In this regard, it behaved like a wired LAN sniffer running on a switched LAN. With switched LANs, sniffers can only "see" all packets if they are plugged into a monitor port of the switch, something LAN administrators would typically prevent. There are techniques (such as ARP spoofing to stage a man-in-the middle attack) to circumvent this, but generally, wired switch networks are naturally far less susceptible to eavesdropping than Wi-Fi networks or wired hubs.

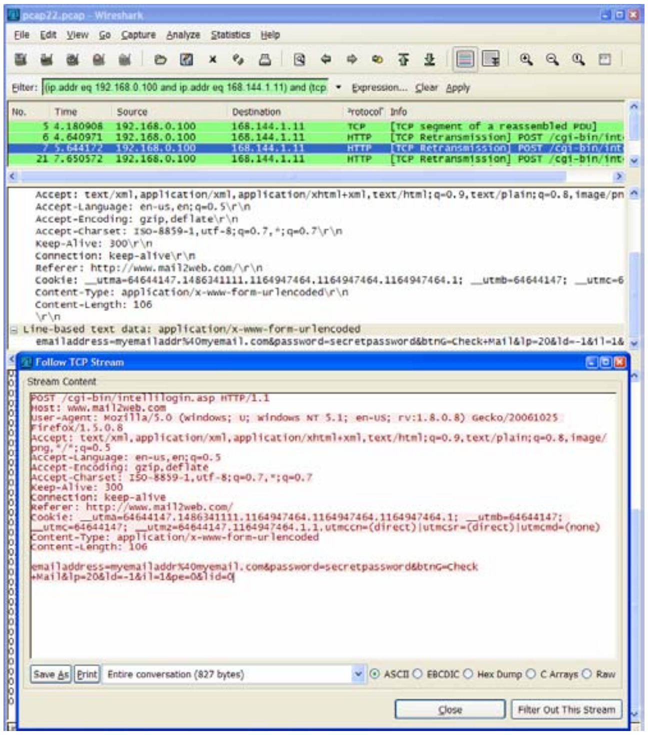
exchanged with mail2web.com. Mail2web, like many web email sites, is an easy target because it defaults to an open login screen without password mangling, SSL (secure socket layer), or other measures. Mail2web does offer a secure login path, but it is not the first one shown and many users do not bother to switch to it. Using *ngrep*, it is easy to write scripts to quickly and automatically scan for common vulnerabilities, such as sites known to collect private information without adequate security.



```
derekwilliams@dwdell ~
$ cd /cygdrive/f/linux/

derekwilliams@dwdell /cygdrive/f/linux
$ ngrep -I Kismet-Nov-28-2006-2.dump mail2web port 80  | head -10
input: Kismet-Nov-28-2006-2.dump
filter: (ip or ip6) and ( port 80 )
match: mail2web
###############################################################################
T 192.168.1.102:1378 -> 168.144.1.11:80 [AP]
  GET / HTTP/1.1..Host: www.mail2web.com..User-Agent: Mozilla/5.0 (W
  ; Windows NT 5.1; en-US; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.
  : text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,t
  ;q=0.8,image/png,*/*;q=0.5..Accept-Language: en-us,en;q=0.5..Accep
  g: gzip,deflate..Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7..K

derekwilliams@dwdell /cygdrive/f/linux
$ _
```

Figure 3 - Using ngrep to Filter Packet Dumps

I performed a simple experiment to determine how easy it is to steal someone's user ID and password with open services such as mail2web. I visited the mail2web site and entered a bogus email address (myemailaddr@myemail.com) and password (secretpassword) while using another laptop computer to sniff Wi-Fi packets. *Figure 4* shows how clearly the user ID and password appear in the message.



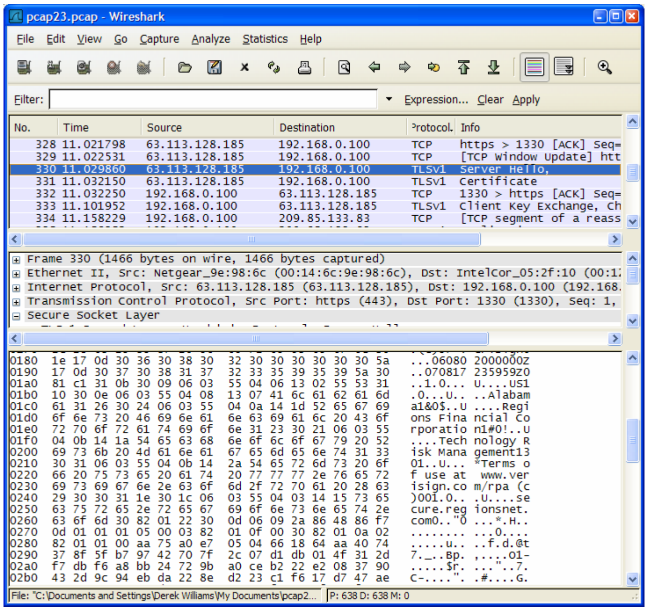
```
Filter: (ip.addr eq 192.168.0.100 and ip.addr eq 168.144.1.11) and (tcp

No.  Time      Source          Destination   Protocol  Info
   5 4.180908  192.168.0.100   168.144.1.11  TCP       [TCP segment of a reassembled PDU]
   6 4.640971  192.168.0.100   168.144.1.11  HTTP      [TCP Retransmission] POST /cgi-bin/int
   7 5.644172  192.168.0.100   168.144.1.11  HTTP      [TCP Retransmission] POST /cgi-bin/int
  21 7.650572  192.168.0.100   168.144.1.11  HTTP      [TCP Retransmission] POST /cgi-bin/int

    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/pn
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.mail2web.com/\r\n
    Cookie: __utma=64644147.1486341111.1164947464.1164947464.1164947464.1; __utmb=64644147; __utmc=6
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 106
    \r\n
⊟ Line-based text data: application/x-www-form-urlencoded
    emailaddress=myemailaddr%40myemail.com&password=secretpassword&btnG=Check+Mail&lp=20&ld=-1&il=1&
```

```
POST /cgi-bin/intellilogin.asp HTTP/1.1
Host: www.mail2web.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.8) Gecko/20061025
Firefox/1.5.0.8
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/
png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.mail2web.com/
Cookie: __utma=64644147.1486341111.1164947464.1164947464.1164947464.1; __utmb=64644147;
__utmc=64644147; __utmz=64644147.1164947464.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)
Content-Type: application/x-www-form-urlencoded
Content-Length: 106

emailaddress=myemailaddr%40myemail.com&password=secretpassword&btnG=Check
+Mail&lp=20&ld=-1&il=1&pe=0&lid=0

Entire conversation (827 bytes)   ● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw
```

Figure 4 – Wireshark Displaying a mail2web Capture

Gathering email passwords and eavesdropping on email content is also straightforward against users of email clients (such as Microsoft Outlook) that rely on the basic POP (post office protocol) and SMTP (simple mail transport protocol) mechanisms. These simple protocols are quite common, and private information is sent in clear text form, easily accessible from the sniffers described above.

Fortunately, due to careful website implementations, much of the confidential data that flows over the internet today is protected by encryption, using measures such as encryption in HTTP POST parameters, or secure socket layer (SSL). This is why it is important to first look for the closed padlock or unbroken key icon on the browser status bar before providing confidential information; this indicates that SSL being used and the data will be sent in encrypted form. *Figure 5* demonstrates the benefits of SSL: here, the sensitive information exchanged with an online banking site is strongly encrypted, so although it traveled over a completely open wireless network, it is highly unlikely that it will be compromised.


pcap23.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

```
Filter:

No.  Time       Source          Destination     Protocol  Info
 328 11.021798  63.113.128.185  192.168.0.100   TCP       https > 1330 [ACK] Seq=
 329 11.022531  63.113.128.185  192.168.0.100   TCP       [TCP Window Update] htt
 330 11.029860  63.113.128.185  192.168.0.100   TLSv1     Server Hello,
 331 11.032150  63.113.128.185  192.168.0.100   TLSv1     Certificate
 332 11.032250  192.168.0.100   63.113.128.185  TCP       1330 > https [ACK] Seq=
 333 11.101952  192.168.0.100   63.113.128.185  TLSv1     Client Key Exchange, Ch
 334 11.158229  192.168.0.100   209.85.133.83   TCP       [TCP segment of a reass

⊞ Frame 330 (1466 bytes on wire, 1466 bytes captured)
⊞ Ethernet II, Src: Netgear_9e:98:6c (00:14:6c:9e:98:6c), Dst: IntelCor_05:2f:10 (00:1
⊞ Internet Protocol, Src: 63.113.128.185 (63.113.128.185), Dst: 192.168.0.100 (192.168.
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: 1330 (1330), Seq: 1,
⊟ Secure Socket Layer

0180  1e 17 0d 30 36 30 38 30  32 30 30 30 30 30 30 5a   ...06080 2000000Z
0190  17 0d 30 37 30 38 31 37  32 33 35 39 35 39 5a 30   ..070817 235959Z0
01a0  81 c1 31 0b 30 09 06 03  55 04 06 13 02 55 53 31   ..1.0... U....US1
01b0  10 30 0e 06 03 55 04 08  13 07 41 6c 61 62 61 6d   .0...U.. ..Alabam
01c0  61 31 26 30 24 06 03 55  04 0a 14 1d 52 65 67 69   a1&0$..U ....Regi
01d0  6f 6e 73 20 46 69 6e 61  6e 63 69 61 6c 20 43 6f   ons Fina ncial Co
01e0  72 70 6f 72 61 74 69 6f  6e 31 23 30 21 06 03 55   rporatio n1#0!..U
01f0  04 0b 14 1a 54 65 63 68  6e 6f 6c 6f 67 79 20 52   ....Tech nology R
0200  69 73 6b 20 4d 61 6e 61  67 65 6d 65 6e 74 31 33   isk Mana gement13
0210  30 31 06 03 55 04 0b 14  2a 54 65 72 6d 73 20 6f   01..U... *Terms o
0220  66 20 75 73 65 20 61 74  20 77 77 77 2e 76 65 72   f use at  www.ver
0230  69 73 69 67 6e 2e 63 6f  6d 2f 72 70 61 20 28 63   isign.co m/rpa (c
0240  29 30 30 31 1e 30 1c 06  03 55 04 03 14 15 73 65   )001.0.. .U....se
0250  63 75 72 65 2e 72 65 67  69 6f 6e 73 6e 65 74 2e   cure.reg ionsnet.
0260  63 6f 6d 30 82 01 22 30  0d 06 09 2a 86 48 86 f7   com0.."0 ...*.H..
0270  0d 01 01 01 05 00 03 82  01 0f 00 30 82 01 0a 02   ........ ...0....
0280  82 01 01 00 aa 75 a0 e7  05 04 66 18 64 aa 40 74   .....u.. ..f.d.@t
0290  37 8f 5f b7 97 42 70 7f  2c 07 d1 db 01 4f 31 2d   7._..Bp. ,....O1-
02a0  f7 db f6 a8 bb 24 72 9b  a0 ce b2 22 e2 08 37 90   .....$r. ..."..7.
02b0  43 2d 9c 94 eb da 22 8e  d2 23 c1 f6 17 d7 47 ae   C-....". .#....G.

File: "C:\Documents and Settings\Derek Williams\My Documents\pcap2...   P: 638 D: 638 M: 0
```

Figure 5 - Wireshark Display of SSL Encrypted Data

Given SSL protection, hackers must resort to attacks other than simple eavesdropping to gather confidential information that is sent to SSL-secured websites. Techniques such as wiphishing are discussed further in *FEASIBILITY*, below.

5.2 Conclusion

The research data and experiments confirm that the ongoing use of common open wireless networks is a very real and significant risk. Obscurity is no defense: while private data may be buried deep in the sea of common internet traffic, tools to collect, locate, and extract this data are readily available and easy to use. Possible outcomes of these risks include reduced computer performance, loss of network capacity (available bandwidth), the stress and loss of time in correcting the lingering effects of an attack, financial loss, and even false criminal prosecution.

6. FEASIBILITY

There have been many reported stories of hackers working around the clock and going to great ends to break into a target. Such reports give the impression that hacking is a tiresome and difficult process reserved for the highly trained and aimed only at choice targets. Primarily through first-hand experiments, I sought to determine the extent of this. I searched out an answer to the following question: do eavesdropping and circumventing ("cracking") Wi-Fi security mechanisms require such a high degree of skills, time, or resources that the threat to an average user is only a remote possibility?

As explained in *SEVERITY*, above, I found it quite easy eavesdrop on open wireless networks. But two questions follow – what about networks that are not wide open, and can their security mechanisms be circumvented? These are answered in the sections below.

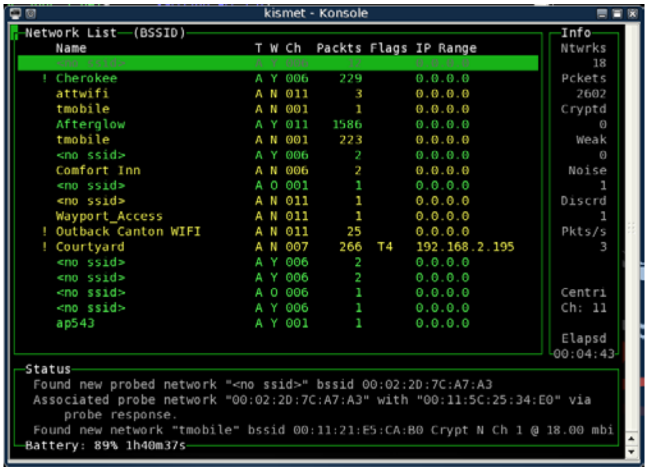
6.1 Cracking Secured Networks

Unfortunately, many of the basic common Wi-Fi security mechanisms offer only paper-thin protection. These mechanisms and the means to circumvent them are described below.

1. SSID cloaking

   SSID cloaking is simply turning off the broadcast of the service set identifier (SSID) by an access point or computer so that it is hidden from "browsing" computers. By disabling SSID broadcasts, the SSID can be set to a non-obvious name, and only computers that know that name can connect to it.

   But this only hides the SSID in broadcast (beacon) packets; the name is still contained in other Wi-Fi packets, a fact which can be exploited rather easily to reveal the hidden SSID. As shown in *Figure 6*, these "hidden" networks can still easily be found by tools such as Kismet, and then un-clocked by forcing another attached computer to "disassociate" and then re-associate, which exposes the SSID.

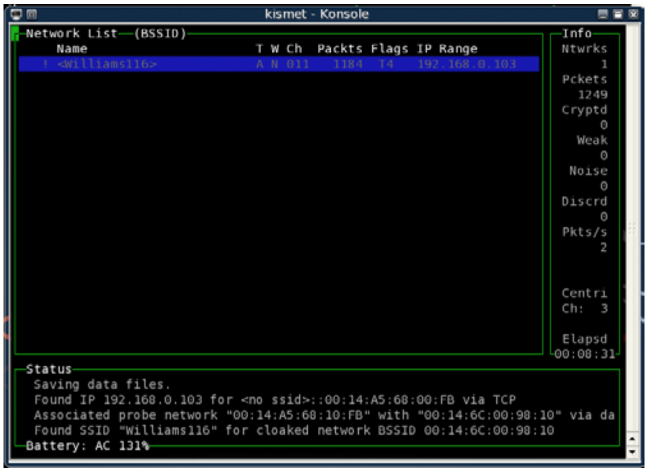


```
kismet - Konsole
Network List—(BSSID)                                       Info
    Name                   T W Ch  Packts Flags IP Range    Ntwrks
    <no ssid>              A Y 006     12       0.0.0.0         18
  ! Cherokee               A Y 006    229       0.0.0.0     Pckets
    attwifi                A N 011      3       0.0.0.0       2602
    tmobile                A N 001      1       0.0.0.0     Cryptd
    Afterglow              A Y 011   1586       0.0.0.0          0
    tmobile                A N 001    223       0.0.0.0       Weak
    <no ssid>              A Y 006      2       0.0.0.0          0
    Comfort Inn            A N 006      2       0.0.0.0      Noise
    <no ssid>              A O 001      1       0.0.0.0          1
    <no ssid>              A N 011      1       0.0.0.0     Discrd
    Wayport_Access         A N 011      1       0.0.0.0          1
  ! Outback Canton WIFI    A N 011     25       0.0.0.0     Pkts/s
  ! Courtyard              A N 007    266  T4   192.168.2.195     3
    <no ssid>              A Y 006      2       0.0.0.0
    <no ssid>              A Y 006      2       0.0.0.0
    <no ssid>              A O 006      1       0.0.0.0     Centri
    <no ssid>              A Y 006      1       0.0.0.0     Ch: 11
    ap543                  A Y 001      1       0.0.0.0
                                                            Elapsd
                                                          00:04:43
Status
 Found new probed network "<no ssid>" bssid 00:02:2D:7C:A7:A3
 Associated probe network "00:02:2D:7C:A7:A3" with "00:11:5C:25:34:E0" via
     probe response.
 Found new network "tmobile" bssid 00:11:21:E5:CA:B0 Crypt N Ch 1 @ 18.00 mbi
Battery: 89% 1h40m37s
```

Figure 6 - Kismet Display of "Hidden" Networks

   I intentionally avoided un-cloaking networks owned by others (such as the ones shown in *Figure 6*); rather, I did this in a "lab" experiment against my own router. *Figure 7* demonstrates the effect in Kismet; see the message, "Found SSID … for cloaked network."

   The entire operation took less than five minutes, proving that SSID hiding is not an effective security mechanism. However, it still provides a benefit: there are so many open networks with clear and default SSIDs (easier targets) that many potential hackers many not care to bother with this extra step of unlocking an SSID.



```
kismet - Konsole
Network List—(BSSID)                                       Info
    Name                   T W Ch  Packts Flags IP Range    Ntwrks
  ! <Williams116>          A N 011   1184  T4   192.168.0.103     1
                                                            Pckets
                                                              1249
                                                            Cryptd
                                                                 0
                                                              Weak
                                                                 0
                                                             Noise
                                                                 0
                                                            Discrd
                                                                 0
                                                            Pkts/s
                                                                 2

                                                            Centri
                                                            Ch:  3

                                                            Elapsd
                                                          00:08:31
Status
 Saving data files.
 Found IP 192.168.0.103 for <no ssid>::00:14:A5:68:00:FB via TCP
 Associated probe network "00:14:A5:68:10:FB" with "00:14:6C:00:98:10" via da
 Found SSID "Williams116" for cloaked network BSSID 00:14:6C:00:98:10
Battery: AC 131%
```

Figure 7 - Using Kismet to "Crack" a Hidden SSID

2. MAC address filtering

   For wireless Ethernet adaptors, MAC (media access control) addresses are the six-byte identifiers assigned to the card, typically by the firmware. With MAC address filtering, the access point only accepts connections from known computers whose addresses appear in a defined list.

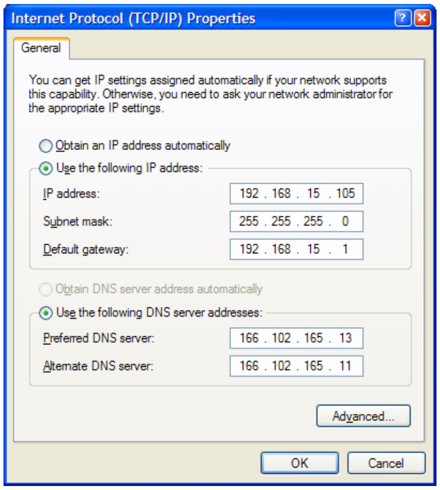
   The trouble with this scheme is that it is easy to determine (with a sniffer such as Wireshark or Kismet) the MAC addresses of all computers attached to the access point and then use one of these addresses to masquerade as a legitimate computer. I was able to do this very quickly under Linux, using *Kismet* to find an authorized MAC address, and then using *ifconfig* to override my own MAC address to this value.

   Since MAC address filtering limits network flexibility without providing significant security benefits, I do not recommend it.

3. Disabling DHCP and changing the IP subnet

   The dynamic host configuration protocol (DHCP) and the commonly used 192.168.0.x and 192.168.1.x subnets make it easy to quickly attach new computers to a network. When used, users do not have to change the network settings of their computers in order to connect.

   Disabling DHCP at the router and changing its IP subnet makes it far less likely that someone would accidentally connect to the network. But circumventing this is even easier than overcoming MAC address filtering, and the process is almost the same. A sniffer is used to gather the IP address range, which can then easily be keyed into the TCP/IP settings of virtually any operating system including Windows and Linux (see *Figure 8*).



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 15 . 105
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 15 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	166 . 102 . 165 . 13
Alternate DNS server:	166 . 102 . 165 . 11

Figure 8 - Overriding the IP Address in Windows XP

As with MAC address filtering, disabling DHCP limits network flexibility without significant benefits. Other measures, such as encryption and SSID hiding can be used to prevent accidental connections.

4. WEP encryption

WEP (wired equivalent privacy) was one of the first encryption technologies broadly deployed on Wi-Fi devices and is still often the "lowest common denominator" for encryption. It relies on a 64-bit or 128-bit secret key (shared by the access point and all attached devices) to encrypt and decrypt packets. As with all encryption methods, the key is the vital link, and if the key is compromised, the encryption becomes useless.

This is why key infrastructures are so important to security. Most WEP deployments have no true key infrastructure – it is up to the user to choose a key and enter it into the settings of the access point and all devices. If the key is ever revealed, the network owner or administrator should quickly change it by re-configuring all devices.

SSID cracking software tries to determine the key by choosing candidates one at a time and using each to see if it will decode certain "weak" encrypted packets (captured by a sniffer) into valid messages. There are three approaches to selecting a candidate key: 1) brute force – choose every possible key in the range of 64-bit or 128-bit values, 2) dictionary hack – choose likely keys based on the notion that people often use easy-to-remember values as passwords, and 3) statistical hack – like brute-force, but with information and analysis to greatly reduce the range of possible values.

A brute force attack typically requires too much processing time to be feasible. Dictionary hacks can be quickly successful against networks with a common key. These characteristics are generally true of all encryption schemes. But where WEP has fallen short is that statistical attacks (including packet injection methods) have been shown to be quickly effective.

New methods have been published to crack the strongest of WEP keys using around 500,000 captured encrypted packets that are sufficiently unique. Once these packets have been collected, a typical cracking program can determine the key within a few minutes. Of course, packet capture is the more time-consuming step, so packet injection techniques are used to speed the rate. These processes and algorithms have now been built into freely-available tools such as *Kismet* and *aircrack*, which removes the "security by obscurity" defense.

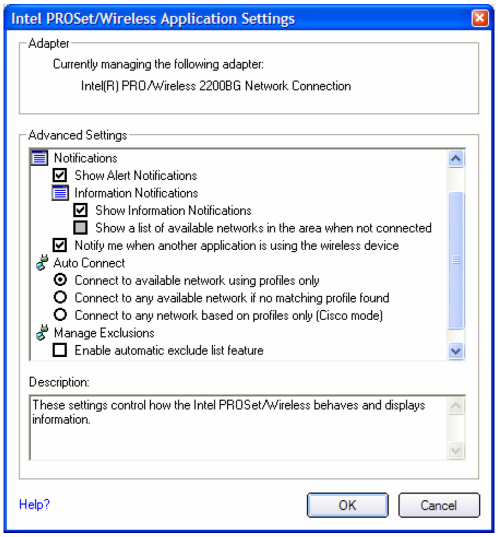
Because of this well-known weakness, I recommend using the stronger *Wi-Fi Protected Access* (WPA) encryption if all devices support it. The Pre-shared Key (PSK) variant of WPA is susceptible to some of the same shared key risks as WEP, but the WPA protocol has several critical advantages. For example, WPA uses longer initial vectors (IV) to avoid creating packets that are easy to crack, and it derives new keys from master keys, rather than using them directly. If the network must support older devices with only WEP encryption available, WEP is still far better than no encryption. That is, there are so many open networks with no encryption that many potential hackers would not bother with the WEP cracking process against a consumer wireless LAN.

As stated earlier, users are often the weakest link in security. So there will continually be new and creative ways to compromise security through simple "social engineering". For example:

- Hackers could gain encryption keys under the guise of providing technical support. Users may not understand the long-term significance of giving temporary access to a wireless LAN or to a wireless router's remote administration function. Once a key or administration password is disclosed, it should be changed immediately.
- Someone could gain brief, temporary physical access to a wired network to connect a hidden "rogue" (unauthorized) access point to an otherwise secure network. When combined with powerful Wi-Fi antennas that can receive signals from as far as miles away, a hacker would then have continual full network access while remaining far out of sight. Network administrators should periodically scan for such access points.

As described earlier, by using SSL-secured websites, private information such as user IDs, passwords, and account numbers can be encrypted and protected. However, this measure can be circumvented by rouge "evil twin" access points. Evil twins are computers acting as access points to perform "man in the middle" hacking. The evil twin passes through most internet traffic, but redirects certain web pages (such as online banking login pages) to its own replacement pages in order to gather data. An evil twin can be targeted at an individual by sniffing traffic to determine the SSID and websites used by that person, and then configuring the SSID and replacement web pages to match.

Even without targeted approaches, coaxing a Windows computer to connect to an evil twin access point is not difficult, particularly because the default configuration is to automatically connect to any access point that matches a known SSID. *Figure 9* shows common auto-connect settings, with do not support simply disabling auto-connect. Since a handful of common SSIDs (such as *linksys* and *NETGEAR*) are broadly used (see *Wardriving*, above), they occur in the "auto connect" profiles of many laptop coputers. By using one of these common SSIDs, an evil twin access point has "favored bait" to lure in unsuspecting victims.



Adapter

Currently managing the following adapter:

Intel(R) PRO/Wireless 2200BG Network Connection

Advanced Settings

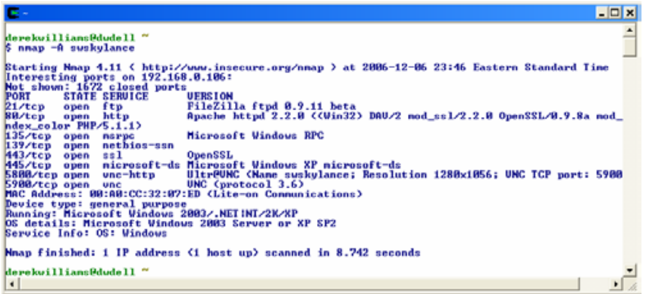
- Notifications
  - ☑ Show Alert Notifications
  - Information Notifications
    - ☑ Show Information Notifications
    - ☐ Show a list of available networks in the area when not connected
  - ☑ Notify me when another application is using the wireless device
- Auto Connect
  - ● Connect to available network using profiles only
  - ○ Connect to any available network if no matching profile found
  - ○ Connect to any network based on profiles only (Cisco mode)
- Manage Exclusions
  - ☐ Enable automatic exclude list feature

Description:

These settings control how the Intel PROSet/Wireless behaves and displays information.

Figure 9 - Wireless Adaptor Auto-connect Settings

Finally, many Wi-Fi wireless internet users do not realize the extent to which they provide "open doors" (open TCP/IP ports) into their computers that other computers on the same wireless LAN can access. Such open ports are typically hidden from the broad "outside world" of the internet because of the routers and proxy servers that intervene, but are often available to local computers. Simple and free port scanners, such as *nmap* and *SuperScan* expose open ports quickly and easily. Hackers use these scanners to find open ports and other information they can try to exploit. *Figure 10* shows the output from running *nmap*.



```
derekwilliams@dudell ~
$ nmap -A swskylance

Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2006-12-06 23:46 Eastern Standard Time
Interesting ports on 192.168.0.106:
Not shown: 1672 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.11 beta
80/tcp    open  http         Apache httpd 2.2.0 ((Win32) DAV/2 mod_ssl/2.2.0 OpenSSL/0.9.8a mod_
ndex_color PHP/5.1.1)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
443/tcp   open  ssl          OpenSSL
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
5800/tcp open  vnc-http     Ultr@VNC (Name swskylance; Resolution 1280x1056; VNC TCP port: 5900
5900/tcp open  vnc          VNC (protocol 3.6)
MAC Address: 00:A0:CC:32:07:ED (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows 2003/.NET|NT/2K/XP
OS details: Microsoft Windows 2003 Server or XP SP2
Service Info: OS: Windows

Nmap finished: 1 IP address (1 host up) scanned in 8.742 seconds

derekwilliams@dudell ~
```

Figure 10 - Nmap Scan of a Local Computer

Users can protect themselves by using personal firewalls and by running their own port scans to identify vulnerabilities.

6.2 Conclusion

While some forms of attack certainly require deep skills and a large investment of time, many common attacks can be pulled off quickly and easily, using common, freely-available tools. Such tools quickly enable the "hacker next door" and can bring the threat to wireless networks anywhere.

7. SOLUTION

Many of the results I found are alarming. Unsecured Wi-Fi networks are widespread, common, and are growing in number daily. As their use has extended to new applications (such as online banking and shopping) by more people, the stakes have risen. Hacking tools are broadly and freely available, and are easy to use. I believe that if significant changes do not occur rapidly, we will begin to see tremendous growth in both the number and cumulative cost of security attacks.

Fortunately, viable solutions are available. But as stated earlier, the primary problem is an *implementation gap*; that is, these effective Wi-Fi security measures are not broadly put into practice.

I have grouped by recommended solutions below into three general categories:

1. *Network recommendations* – simple, practical steps that can be done to secure the wireless network.
2. *Computer (client) recommendations* – tasks that can be done to protect computers and other devices that are attached to wireless networks.
3. *Industry recommendations* – steps that Wi-Fi vendors and organizations should take to address the general problem.

7.1 Network Recommendations

Network owners and/or administrators should take the following steps to secure their wireless LAN access points and routers:

1. Change the configuration password and SSID from the default values. Disable remote (web) configuration. Choose strong names; for example, use a combination of letters and numbers that is not common and does not occur in dictionaries. A simple test of password and SSID strength is to "google" it; if Google returns no matches, the name is a good one, but select a variant of the name after "googling" it.
2. Enable the strongest possible encryption available to the access point and attached devices. Use WPA; only use WEP if WPA is not available. For the pass phrase, choose a unique name, as was done for the password and SSID.
3. For routers, do not forward any ports unless absolutely necessary.
4. Periodically look for unauthorized network access by checking "attached devices" at the access point or router. Periodically run software such as *Kismet* or *NetStumbler* to locate and identify Wi-Fi computers in the area and check for rogue access points.
5. Consider turning off the access point or router when not in use. Some routers have built-schedule functions to turn off the radio automatically; if not, a simple lamp timer can be connected to the device.

7.2 Computer (Device) Recommendations

For all wireless-enabled computers and devices, do the following:

1. Enable encryption to match the access point or router.
2. If the only choice is an open wireless network (for example, at a public Wi-Fi hotspot), use a VPN (virtual private network) or SSH (secure shell) connection to direct all traffic through an encrypted "tunnel." If no VPN or SSH server is available, configure a computer at home to act as one.
3. Disable the ad-hoc network feature so that other computers cannot connect to it.
4. Turn off the automatic connection feature, if possible. This particularly applies to Windows XP computers.
5. Turn off the Wi-Fi radio when not in use.

6. Use security software (firewall, virus scanner, anti-spyware, etc) and keep it current through automatic subscriptions.

7.3 Industry Recommendations

Finally, there is much that the Wi-Fi industry can and should do to improve the situation. For example:

1. Get the word out. Vendors and industry groups should better publicize the risks associated with Wi-Fi networks and plainly communicate basic steps that users can follow to protect themselves. Organizations and web sites such as http://www.GetWirelessSecure.org are a step in the right direction.
2. Vendors should pre-configure wireless devices with non-obvious SSIDs, password expirations (and automatic 'change password' prompts, and with security enabled by default. Some invention may be possible here to help the situation; for example, to automatically generate a new pass phrase and help distribute it to all devices.
3. Vendors should work together to simplify the configuration problem. For example, in our experiments, we found that different vendors did not use the same acronyms in the drop-down lists used to select the encryption type. In one case, the participant simply had to use trial and error to see if the encryption choices were the same. Vendors may feel that there is little room for improvement, but even small changes can help new users. Much like the simple color coding of mouse and keyboard plugs introduced by the *PC 97* specification, simply using easily-matched terms in configuration screens can help speed the configuration process.
4. "White hat" hackers could get in the game by hacking into open wireless networks and leaving warning messages and instructions on how to protect it. This is a radical approach, but it would certainly get the attention of the network owners.

Taken together, these steps are not difficult and well worth the time to protect against "sleeping giant" of large-scale security risk.

8. ACKNOWLEDGMENTS

I would like to thank my son, Spencer Williams, for his participation in some of my experiments, and would like to thank those who participated in my survey.

9. REFERENCES

[1] American Society for Industrial Security, Trends in Proprietary Information Loss - Survey Report, Sep 2002

[2] ABI Research, *Wi-Fi Research Service Market Data*, Report Code MD-WLHS, Nov. 2, 2006.

[3] T. Bradley and B. Waring, Complete Guide to Wi-Fi Security, *JiWire*, Dec. 6, 2005

[4] *FaceTime Security Labs*, IMPact Report – Summary Analysis of IM and P2P Threats in 2005, http://www.facetime.com/securitylabs

[5] M. Fordahl, WiFi Popularity Overshadows Security Problems, *The Boston Globe*, June 1, 2004

[6] S. Ina, A. Wood, and M. Gartenberg, Home Automation: Finding Growth Among Connected Home Consumers, *Jupiter Research*, July 28, 2006

[7] M. Marriott, A. Zarate, and G. Ruethling, Hey Neighbor, Stop Piggybacking on My Wireless, *New York Times*, Mar. 5, 2006

[8] R. McMillan, Identity Theft Hit 3.6 Million in U.S. *IDG News Service*, March 31, 2006

[9] Michael Ossmann, WEP: Dead Again, *SecurityFocus*, Dec. 14, 2004.

[10] Reuters, Cyber Blackmail Targets Office Workers, Dec. 29, 2003.

[11] Richard Shim, Wardriving conviction is first under Can-Spam, *CNET News*, Sep. 30, 2004

[12] Robert Moskowitz, WLAN Testing Reports – Debunking the Myth of SSID Hiding, *ICSA Labs*, Dec. 1, 2003

[13] *United Press International*, Wireless-Security Campaign Steps Up, Mar 8, 2006.

[14] J. Van Dyke, 2005 Javelin Identity Fraud Survey Report, *Javelin Strategy and Research*, released by the Better Business Bureau, Jan. 26, 2005.