Understanding Wireless Encryption

Michael Sweatt
Garold Wahnee
IT 4444 Capstone
19 April 2013
Abstract: This paper contains a brief look over 802.11 wireless standards that are used by today's commercially available wireless access points. Secondly, we will look at the different encryption algorithms that are commonly used to secure these access points; security threats that will be discussed as well. Next, we will look at an experiment designed to capture and analyze broadcast signals from access points in the wild, and make sense of all the data. Finally, some implications and final thoughts from the authors about the results.

Introduction: Wireless technology is built into almost every type of personal electronic device that people own. Laptops, MP3 players, phones, gaming systems, and even televisions can have a wireless network card built around the 802.11 wireless standard. All of these home devices communicate with the Internet and to each other through a central router, usually located inside of the home. If these wireless routers are not password protected then all of the devices connected to it are vulnerable to an attacker. All of the data transmitted using an 802.11 wireless signal, including credit card information, social security numbers, private emails, and a multitude of other private information can be collected by anyone with a wireless device that is within range of the wireless network's signal. Finding wireless access points is as easy as driving down the street. This technique is called “Wardriving.” All a person needs is a device, such as, a laptop or cellphone, a wireless network card, and a program that will collect data transmitted over wireless protocols. With this combination of devices, anyone with even basic computer technical skills could find and use an open wireless access points. If a person has enough time, they could crack a wireless routers password and use it as they please. Once an intruder has access to the router, they can collect sensitive data that is being transmitted by other wireless devices or even perform illegal acts such as downloading copyrighted intellectual property illegally or downloading child pornography. So are people securing their routers with some form of wireless encryption? This is what we aim to find out in our experiment.

Thesis: Any professional security worker will tell you that network perimeter security starts at the gateways, such as routers and access points. While this may be obvious for most, some still neglect this step and leave the entrance to their networks wide open. Specifically with wireless access points, improving the security of your wireless traffic can be as easy as a click of the mouse. We know that older 802.11 encryption standards are susceptible to password attacks, in some cases revealing a password in under 30 seconds, and an entire process from initial router acknowledgment to password crack in less than 2 minutes. 802.11 Wireless encryption standards haven't changed much lately, the most recent being Wi-Fi Protected Access(WPA), or 802.11i [5]. Although newer wireless routers default to WPA2, not all do. The purpose of our experiment was to survey router broadcasts to see how many were protected with up to date encryption standards, and who was vulnerable to wireless attacks.

Previous Work: Wardriving has been around since the late 1990's when the IEEE drew up the first 802.11 wireless specification. The term “wardriving” is derived from “wardialing” which was introduced in the 1983 movie War Games[2]. Wardialing was a discovery technique using a computer connected to a modem that dialed a broad spectrum of phone numbers looking for another computer connected to another modem. Wardriving is essentially the same concept, except a computer is used to scan a spectrum of wireless radio signals. This can be done with something as common as a cell phone. Android devices are great to “sniff” wireless networks, and with their built in GPS and WIFI cards, a map can be generated of where each wireless access point is located[1]. An exercise called World Wide Wardriving, done in 2003, found that 67.7% of wireless access points had not even the basic wireless security enabled.[3]. The original inspiration for this project was a video from the Defcon hacker conference, entitled The Safety Dance - Wardriving The Public Safety Band,[4] where the speakers gave a lecture on wardriving 4.9GHz public safety networks. Unfortunately there is not implementation of a 4.9GHz public safety band in an area near to test.
**Encryption Standards**: Wireless 802.11 broadcasts can be secured with a couple of different options where it comes to encrypting traffic. Wired Equivalent Privacy (WEP), as outlined in the 1999 IEEE 802.11 document[8], Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) outlined in IEEE 802.11i-2004[12], are the current standards used for 802.11 encryption.

**Wired Equivalent Privacy (WEP)**: WEP is now considered a vulnerable encryption scheme and poses a security problem. This encryption method relies on an RC4 cipher, which in theory should never be repeated twice. However, on a busy network this is impossible to accomplish. We know that a plain-text WEP frame \( M \) is combined with its checksum to give us the equation \( M \cdot c(M) \). Next, each packet is prepended with an initialization vector (\( IV \)) and a secret key (\( K \)), creating a packet key \( IV \cdot K \). Lastly, the output bytes are exclusive-ored with the checksum plaintext, yielding \( C = ( M \oplus (M \cdot R \cdot C) \cdot K ) \). According to Fluhrer, Marting, and Shamir [7] a 24-bit IV will repeat after 5000 packets 50% of the time.

This is the weakness with WEP encryption, even networks without as much traffic are susceptible to replay attacks that generate traffic. These sort of attacks harvest enough IV packets to run a brute-force attack on, which will usually complete in seconds; a quick search on Google will give you many tutorials and guides of people completing a the process from initial router contact to network access in minutes.

**Wireless Protected Access**: WPA was released in 2004 as an answer to WEP's security problems. WPA's significant improvement was the deployment of the Temporal Key Integrity Protocol (TKIP). The TKIP protocol issues a separate 128-bit key for each packet that is broadcast, making a brute-force attack almost impossible. This encryption method also employs a method integrity check called “Michael” that is stronger than the cyclic redundancy checks that WEP uses. WPA uses the RC4 cipher like WEP does, however WPA makes use of the TKIP protocol along with Michael and a longer key. This combination is what makes WPA more secure than WEP.

IEEE 802.11i-2004 also introduced the 4-way handshake, as shown in figure 1. During the 4-way handshake, encryption keys known as pairwise transient keys (PTK) are agreed on and generated by concatenating both the access point and station's MAC addresses and Cryptographic Nonces, and then running that string through a SHA-512 algorithm.

Wireless Protected Access II was introduced in 2006 by the Wi-Fi Alliance as a replacement for WPA and WEP. WPA2 works in almost the same fashion as WPA, however there is another security layer built in. Counter Cipher Mode with Block Chaining Message Authentication Code Protocol or CCMP is an encapsulation schema for data that is based on the AES standard.[6]
No Encryption: Using no encryption on a wireless access point poses many threats to both a corporate or home user. When using an open, non-secure wireless router, all traffic is open to eavesdropping, leaving the user to rely on other forms of encryption while surfing the web, such as Secure Socket Layer, among others. These methods may work for some services, but not all provide adequate protection from snoopers watching traffic on a network. Encryption is a vital part of keeping information safe on any network. Also, users that do not implement passwords on devices, such as laptops and desktop PCs, leave their systems open to be compromised by an intruder. The computer system is left open to data being altered, destroyed, or stolen. Backdoor programs and key loggers can be loaded onto a victim's computer to steal sensitive data such as login passwords and even credit card information without the victim's knowledge.

Experiment: Our experiment was designed to gather as much data as possible, minimizing the traveling distance. We were not sure how many data points to expect from our harvesting session, but in the end, we got more data points than initially thought. We packed up our vehicle with a laptop running our software, and our antenna mounted on the rear of the vehicle. Our total route from start to finish was a little over 30 miles, yielding close to 3000 broadcast signals. Upon later review, not all of the signals we logged were access points, but rather stations that were authenticating with a particular router.
Hardware: At first, the decision was made to make our own high gain antenna to save money for other pieces of the project. This process was both enlightening and frustrating to say the least. Following this guide [9] we built our antenna around a cardboard potato chip can that was lined with metallic foil. Previous attempts including using a metallic coffee can, a soup can, and metal piping.

We calculate the wavelength of a 2.4GHz signal to be 0.125 meters (4.92 inches) using the formula $\lambda = \frac{v}{f}$. A female N-Type connector with a modified probe was placed at the one-quarter wavelength mark. The one-quarter wavelength mark is significant in that this is the perfect spot in a single cycle for collecting information. This location is the peak of the positive side of the signal, which may be replicated as the negative side of the signal, as shown in figure 2.

Tests of our final antenna design proved that a directional antenna was not the way to go. The limited beam width of the antenna would only capture a small fraction of the available signals. We also noticed a considerable rise in packet loss beyond 75 yards on a flat surface without obstructions. This was simply too unreliable for our purposes, so we decided to look for other suitable antennas. Luckily, we came into a +13DBi omnidirectional antenna. With this new antenna, we were able to see broadcasts at approximately 130 yard in all directions.

Software: We chose two different pieces of software to capture the packets that we were looking for. The first piece is the newest version of Aircrack-ng Suite, which is a software suite that can detect, sniff, and crack wireless routers running 802.11a/b/g. We were particularly interested in the tool airodump-ng. This tool is a simple command line executable that is capable of logging broadcasts picked up by our antenna. Aircrack-ng includes many parameters that can be used to filter out channels, SSIDs, and encryption types. Unfortunately, Airodump-ng was not able to keep up with amount of traffic coming into the antenna, and subsequently crashed out less than five minutes into the experiment process.
Kismet, an open source intrusion detection tool, is the program that we turned to when Airodump-ng failed. Kismet employs a lot of the same filtering techniques that the previous tool did but without crashing. We also found that Kismet presented the information in a more user friendly manner, showing a full count of unique SSIDs captured, as well as how long the program was running and a detailed status box of the traffic received. Later, we analyzed the dump files using the Kismet Log Viewer and Open Office to crunch the numbers.

**Results:** Our findings show that among the 2082 broadcasting access points in our area, 64% of those were secured with current WPA or WPA2 encryption, 21% secured with WEP encryption, and the remaining 15% were not secured with any type encryption. With the vulnerabilities in WEP we can assume that 36% of these access points pose security risks for the users. These findings show that a majority of access points are considered safe based off of the encryption algorithm they are using, however this assumption is being made without any further interaction with the client.

**Final Thoughts:** Wireless access points that are using the latest encryption standards are not 100% safe and secure. For example, using a common password leaves the broadcasting client open to brute-force dictionary attacks. Other precautionary measure should be taken to ensure that only stations that are familiar to the administrator can connect to it, such as MAC filtering, but even this is not enough on it's own. MAC addresses can be easily spoofed to circumvent these filters. Network security is a layered practice, with many different processes built on top of each other to create a system of access control.

**Future Work:** Our next step in this project is to expand the number of unique access points in order to get a more clear picture of encryption algorithms in use. We plan to double or even triple the number of data points by choosing another more populous location to perform our wardriving experiment. We also plan to branch out into the 4.9 GHz public safety band for an in-depth look at encryption standards and protocols.
Bibliography


