Analyzing Wireless Security in Columbia, Missouri

Matthew Chittum
Clayton Harper
John Mixon
Johnathan Walton

Abstract

The current state of wireless security in most areas can be estimated based on trends and collected data, but the complete picture is often unknown. Without collecting the information on most wireless access points in a given area, we cannot compare different areas based on their security, get an accurate view of the areas as a whole, or relate wireless security with other factors in a given region. We have performed a wireless security audit of Columbia, MO. Information was collected on thousands of access points throughout the city in hopes of understanding a large area's use of wireless networking and its possible security flaws. The flaws of WEP encryption allow a supposedly secure computer to be breached and then compromised. We have demonstrated how simple it is to bypass WEP encryption using easily accessible software available on the Internet. We have determined that although Columbia's overall level of security is better than the national average, it still leaves much room for improvement.

Part 1:
Wardriving

Wardriving: The Basics

- Wardriving, in a basic sense, is the act of driving in a vehicle searching for and detecting wireless access points (APs) using a laptop or other hardware equipped with wireless capabilities.
- Wardriving Software
  - Netstumbler
  - Kismet/Kismac
  - Aircrack
  - Ethereal

Why Wardrive?

- Analyze the security vulnerabilities that are associated with APs over a given area.
  - Compare different areas based on their security
  - Get an accurate view of the areas as a whole
  - Relate wireless security with other factors in a given region.

Wardriving Ethics

- Laws (There are none prohibiting it)
- Netstumbler sends a probe and the AP responds. This is how wireless networking is supposed to work!
- As long as you don't gain access or use the WiFi connection then their aren't any ethical considerations.

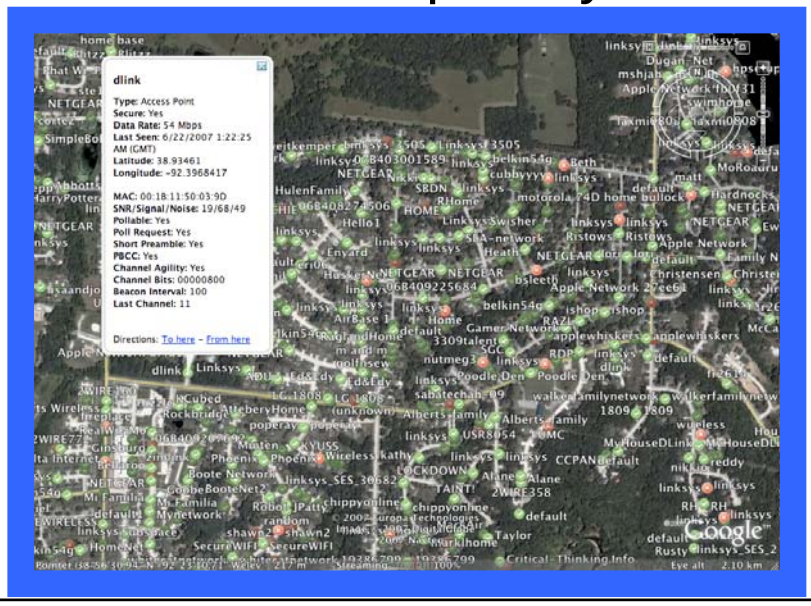
Our Software Choice: Netstumbler

- Why?
  - Supports nearly all wireless network adapters
  - Ease of use and a great support community
  - Reliable
  - High refresh rates
  - Decent amount of statistics
  - GPS/Mapping Support
- Overall a great piece of software!

The Setup

- Netstumbler v0.4.0 (http://www.netstumbler.com/downloads/)
- Earthstumbler (http://mboffin.com/earthstumbler/)
- Google Earth (http://earth.google.com/)
- Garmin Etrex and serial cable
- Dell Wireless 1370 WLAN Mini-PCI card
- Computer running Windows XP
- Car

GPS Capability



Statistics Of Interest

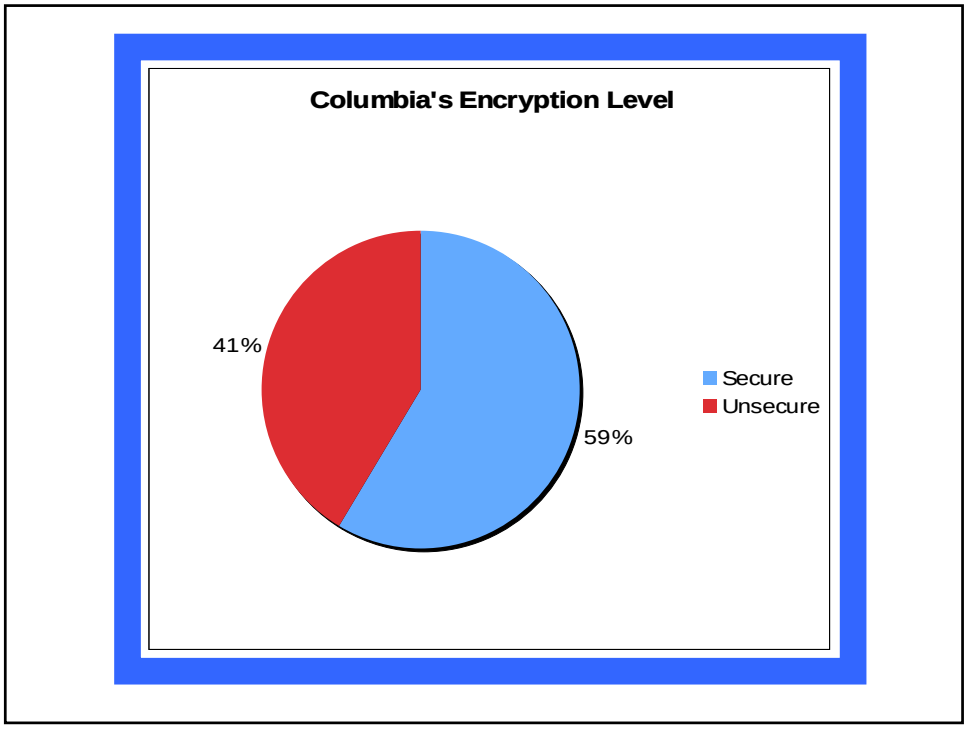
- Encryption or No Encryption
- Unique SSID
- DSSS Channel
- 802.11x standard (such as a,b,g)

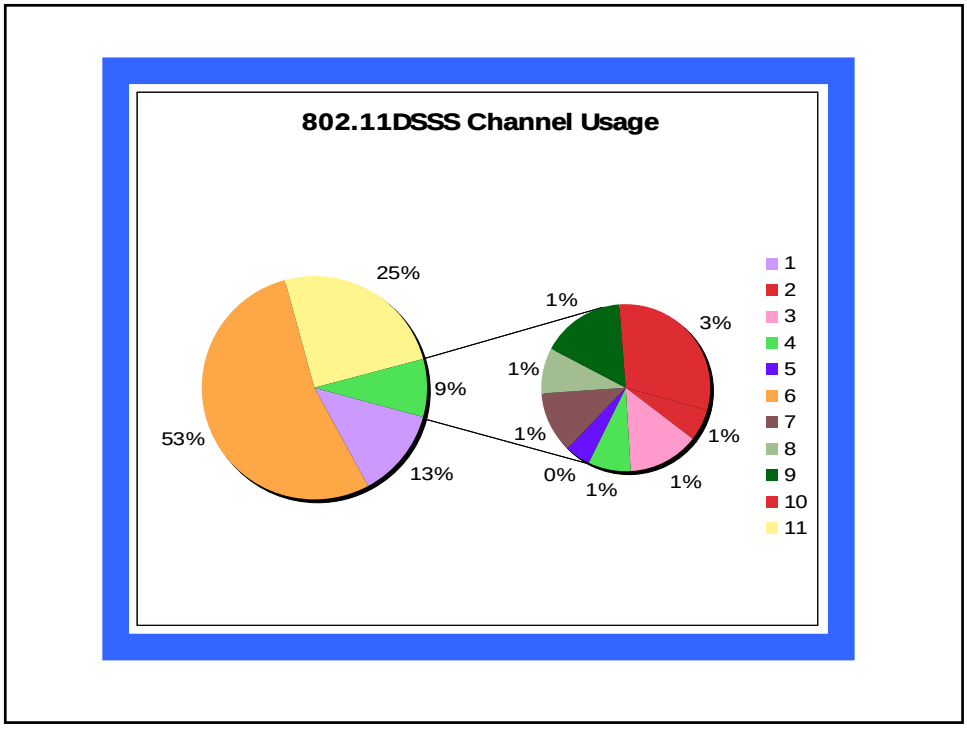
Statistics

- Surveyed 5,563 APs in Columbia
- Nearly 30% had a default SSID, 12% higher than the national average.
- 88.1% of APs in Columbia had 802.11g capability.
- 59% of discovered APs in Columbia were secure, nearly 20% higher than the national average.

Statistics Continued

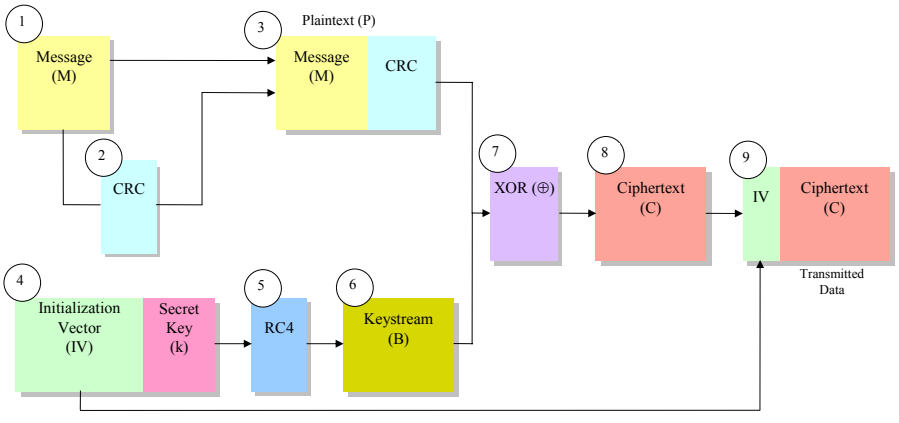
- 11,134,831 unique APs and their location have been uploaded to Wigle.net by 67,683 registered wardrivers.
- Channels 1, 6, and 11 comprise 91% of 802.11DSS channels used.
- It is possible to crack WEP security in as little as 10 minutes in a heavy traffic area; TigerNET uses WEP security.
- Since 2002 the growth rate of wireless network adoption has been exponential.


Columbia's Encryption Level
41%
59%
Secure
Unsecure


802.11DSSS Channel Usage
25%
9%
53%
13%
1%
3%
1%
1%
1%
0%
1%
1%
1
2
3
4
5
6
7
8
9
10
11

Part 2:
WEP Protocol

WEP Protocol (Encryption)



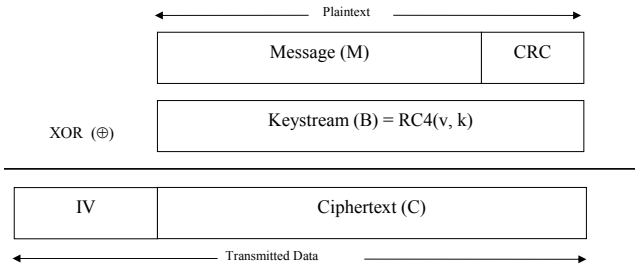
Explanation

1. The WEP encryption process begins with the Message (M) that needs to be transmitted.
2. A cyclic redundancy check (CRC) or integrity checksum is computed on the Message (M) for error handling.
3. The Message (M) and the CRC are concatenated together to form Plaintext (P).
4. An Initialization Vector (IV) is chosen.
5. The RC4 algorithm is applied to the IV and Secret Key (k).

Explanation Continued

6. The RC4 algorithm generates a Keystream (B) of pseudorandom bits.
7. The Plaintext (P) is XOR'ed with the Keystream (B).
8. The XOR operation creates the Ciphertext (C).
9. The IV and Ciphertext (C) are concatenated and are ready to be transmitted.

Another Look



Analytical Approach

Encryption:

- P = M + CRC
- B = RC4(IV, k) → B is a RC4 function of IV and k
- C = P ⊕ B = P ⊕ RC4(IV, k)

Decryption:

- P' = C ⊕ RC4(IV, k)
- = (P ⊕ RC4(IV, k)) ⊕ RC4(IV, k)
- = P

The checksum is then checked to verify that the data does not contain errors.

Problems

WEP encryption uses RC4, a stream cipher algorithm. Stream cipher algorithms work by taking a secret key and creating a pseudorandom keystream from that key. This keystream is then XORed with the plaintext to create the ciphertext. Stream cipher algorithms are relatively weak because encrypting two messages using the same IV can reveal information about both messages.

$C_1 = P_1 \oplus RC4(IV, k)$
$C_2 = P_2 \oplus RC4(IV, k)$

$C_1 \oplus C_2 = (P_1 \oplus RC4(IV, k)) \oplus (P_2 \oplus RC4(IV, k))$
$= P_1 \oplus P_2$

Problems Continued

- The result is both of the plaintexts XORed together. If the plaintext of one message is known the other is easily obtainable. Even if one of the plaintexts is not known there are simple techniques that can easily recover both of the plaintexts.
- One such technique is searching for two English phrases that when XORed together form the two plaintexts XORed together.

Attack Methods

The most common:

- Brute Force
- Keystream Reuse
- “Weak” IV

Brute Force

- Simplest method
- Tries all possible key combinations until the correct key is found.
- Because of the length of keys WEP uses it takes an extremely long time for this method to successfully find the correct key
- Inefficient and impractical.

Keystream Reuse

- If a keystream is known then it is possible to recover the data that was encrypted using that keystream.
- Only 2^24 (16 million) IVs exist (and even less if “weak” IVs are excluded) IVs can be repeated within the matter of hours.

Keystream Reuse Continued

- Problem: Encrypting two different messages using the same IV and secret key can reveal important information about both messages. (Previously Discussed)

$$C_1 = P_1 \oplus RC4(IV, k)$$
$$C_2 = P_2 \oplus RC4(IV, k)$$

$$C_1 \oplus C_2 = (P_1 \oplus RC4(IV, k)) \oplus P_2 \oplus RC4(IV, k))$$
$$= P_1 \oplus P_2$$

“Weak” IVs

- The secret key can be computed by capturing many packets some of which use “weak” IVs.
- One weak IV can reveal a correct key byte 5% of the time.
- With a large number of IVs the most probable key can be guessed.

Cracking WEP Times

- “We demonstrate an active attack on the WEP protocol that is able to recover a 104-bit WEP key using less that 40,000 frames with a success probability of 50%. In order to succeed in 95% of all cases 85,000 packets are needed.”
- http://eprint.iacr.org/2007/120.pdf

Cracking WEP Times Continued

- "With 40 bit keys, the median number of packets required to crack the key is one million. With two million packets, 80% of the 40-bit key could be obtained."
- Graphs on next slide

Graphs

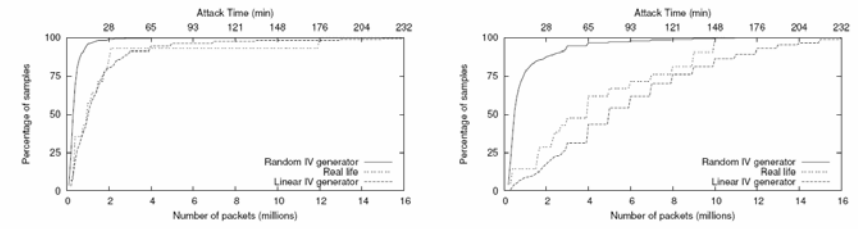


Figure 8. Cumulative distribution of packets required for cracking 40 bit (left plot) and 104 bit keys.

Conclusions

- Columbia's encryption level is considerably higher than the national average but there is still room for improvement.
- WEP encryption provides little protection because it is easily crackable.
- WPA is the best encryption standard today

Future Work

- Talk to residents
  - See if they are aware of what kind of security they use
  - What they know about wireless security in general
- Find more secure standards and attempts to find flaws in those and other existing standards

References

- [1] A. Bittau, M. Handley, and J. Lackey. The Final Nail in WEP's Coffin. http://tapir.cs.ucl.ac.uk/bittau-wep.pdf
- [2] D. Wagner. Weak Keys in RC4, 1995. www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys
- [3] E. Tews, R. Weinmann, A. Pyshkin. Breaking 104 bit WEP in less than 60 seconds. http://eprint.iacr.org/2007/120.pdf
- [4] L.M.S.C of the IEEE Computer Soceity. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Standard 802.11, 1999 Edition.
- [5] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
- [6] S. Fluhrer, I. Mantin, A, Shamir. Weakness in the Key Scheduling Algorithm of RC4. www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps
- [7] www.wigle.net