Wireless Internet Security and Wardriving

BY: Jose Rodriguez

Topics

- What is Wireless Internet Security?
- Different types of wireless encryption
- What is Wardriving?
- Software available to sniff, collect and crack wireless encryptions
- My experiment
- Securing your wireless network
- Conclusion

Wireless Internet Security

- The prevention of unauthorized access or damage to computers using wireless networks.
- Is your computer safe?
- Wireless is essentially insecure
  - This is because all data going over a wireless connection is being broadcasted on a radio channel.
  - So anyone with a sniffing software can read the data being broadcasted.

Wireless Encryption

- WEP (wired equivalent protection)
  - Intended to make wireless networks as secure as wired networks.
- WPAv1
  - Pre-shared Shared Key (PSK)
  - 8 to 63 character passphrase
- WPAv2
  - The primary enhancement is the inclusion of the AES-CCMP algorithm
Wardriving

"The act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer or PDA."

Software

- BackTrack3
  - http://www.remote-exploit.org/backtrack.html
- Aircrack-ng

Experiment

- No Wardriving Today!
- Monitor the wireless networks from the comfort of my own home.
- Sniff the traffic from my own network
IV’s

“What’s an IV?”
WEP uses an Initialization Vector (IV) along with the user-entered "shared secret" key to produce a different RC4 key for each encrypted packet.

The reasons why WEP can be cracked boil down to:
- The IV is sent in cleartext, which makes it easily readable.
- The keystream generated by RC4 is slightly biased in favor of certain sequences of bytes.
- The statistics for the first few bytes of output keystream are strongly non-random, "leaking" information about the key.”
What did I learn?

- Never use WEP on my router
- IF you know anyone that is using WEP, suggest to change it quickly.

Some other suggestion!

- Change encryption to WAPv1 or v2
- Change administrator password and username on your router
- Enable MAC filtering to allow access to only MAC address you know are on your network
- Disable DHCP and take a few minutes to configure static address on your PCs

Conclusion

- Even with the suggestions that I mentioned before it is not 100% secure to use wireless connection.
Reference

- http://www.smallnetbuilder.com/content/view/30114/98/