The Project

The purpose of my project is to raise the awareness of the security ramifications arising from the use of wireless Lans (WLAN) in the home and office community.

Presented here are the early results of a 18 month effort that started in fall of 2000.

Network Security and Wireless Lans

- The convenience and low cost of WLANs has resulted in their deployment at a feverish rate.
- This is very similar to the Web race a several years ago.
- Sadly this deployment has brought security back ten years.

Hardware

- “low end” Laptop with FreeBSD –stable or Windows 98
- External Antenna (>5db)
- GPS (Garmin eMAP)
- Lucent /Aironet 802.11 (Wi-Fi) card

Software

- “wi-scan” – perl script for FreeBSD
- Netstumbler – a Windows App.
- dStumbler – A FreeBSD App. (beta)

The native drivers for cards can also be used although the operation will not be as automated.

Detection Methods

Currently the WLANs are being detected with a 802.11 feature called “broadcast SSID” or “Null SSID”.

The Lucent card supports this feature that when you to set your SSID to (null) or “ANY” the card will detects a AP’s beacon and automatically associate with it.

Detection Methods

Currently I run a script that resets then polls the card every three to five seconds.

When a new WLAN is detected the script notes the SSID, Mac address, signal strength, channel, location (via. GPS) and security configuration.

Detection Methods

Currently we can drive at speeds of up to fifty-five miles a hour and successfully locate and identify wireless networks.

Long Distance ?

Some security officers feel that if AP is distanced from the street or on a high floor of a building they will be safe from network trespassers.

Experiments show that we are able to successfully make a network connection twenty-five miles away from hilltops and high-rise buildings.

Open WLANs
the early results of WarDriving

Peter Shipley
shipley@dis.org