CWSP Guide to Wireless Security

Passive Wireless Discovery

Objectives

- Explain how security information can be gathered by social engineering, phishing, and other techniques
- Define wardriving
- List the hardware and software used for wardriving
- Explain how a packet sniffer can be used in a WLAN

CLIP on hacking

http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm

General Information Gathering

- Includes:
  - Social engineering
  - Phishing
  - Improperly recycled equipment
  - Search engine scanning
  - Dumpster diving

Article: CEO steals employee identities: http://seattlepi.nwsource.com/business/1310AP_CEO_Identity_Theft.html

Social Engineering

- Relies on tricking someone to access a system
- Common characteristic
  - No technical skills are needed to break into the system
- Relies on the friendliness, frustration, or helpfulness of a company employee
  - To reveal information necessary to access a system
- Best defense against social engineering: written policy

Phishing

- Electronic version of social engineering
- Involves sending an e-mail or displaying a Web announcement
  - Falsely claims to be from a legitimate enterprise
  - Attempt to trick the user into surrendering information
- Difficult to distinguish between legitimate and fraudulent messages and Web sites

Phishing (continued)



Figure 3-1 e-Bay phishing Web message

Phishing (continued)

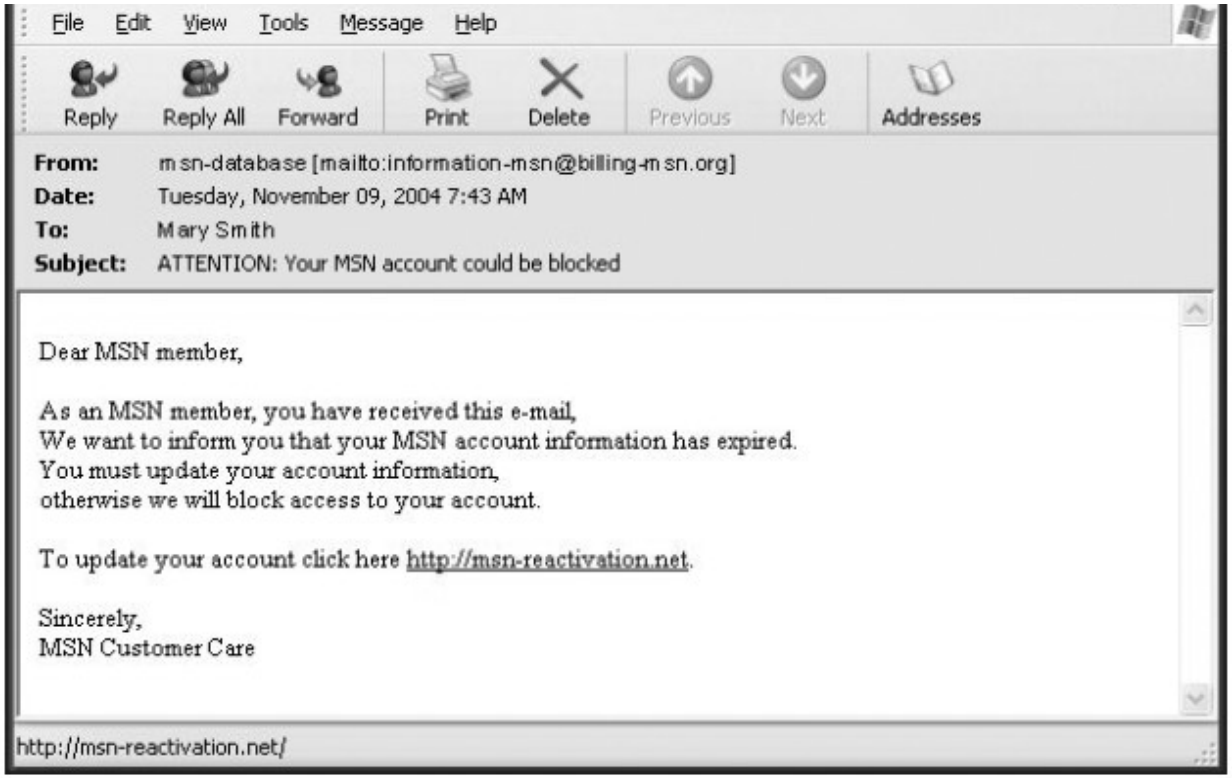
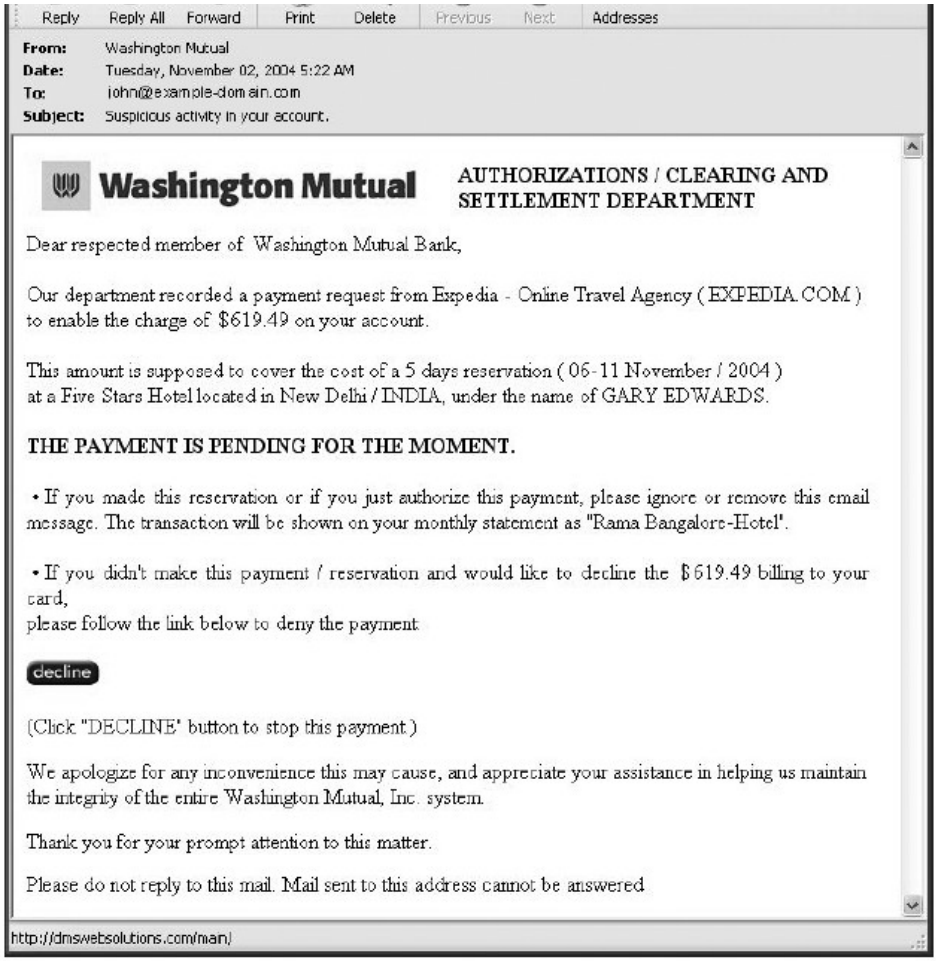


Figure 3-2 MSN phishing e-mail message

Phishing (continued)



Reply | Reply All | Forward | Print | Delete | Previous | Next | Addresses

From: Washington Mutual
Date: Tuesday, November 02, 2004 5:22 AM
To: john@example-domain.com
Subject: Suspicious activity in your account.

Washington Mutual AUTHORIZATIONS / CLEARING AND SETTLEMENT DEPARTMENT

Dear respected member of Washington Mutual Bank,

Our department recorded a payment request from Expedia - Online Travel Agency (EXPEDIA.COM) to enable the charge of $619.49 on your account.

This amount is supposed to cover the cost of a 5 days reservation (06-11 November / 2004) at a Five Stars Hotel located in New Delhi / INDIA, under the name of GARY EDWARDS.

THE PAYMENT IS PENDING FOR THE MOMENT.

• If you made this reservation or if you just authorize this payment, please ignore or remove this email message. The transaction will be shown on your monthly statement as "Rama Bangalore-Hotel".

• If you didn't make this payment / reservation and would like to decline the $619.49 billing to your card,
please follow the link below to deny the payment

decline

(Click "DECLINE" button to stop this payment)

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire Washington Mutual, Inc. system.

Thank you for your prompt attention to this matter.

Please do not reply to this mail. Mail sent to this address cannot be answered

http://dmswebsolutions.com/main/

Figure 3-3 Washington Mutual phishing Web message

Phishing (continued)

- Variations on phishing attacks
  - Spear phishing targets only specific users
  - Pharming automatically redirects user to the fake site
  - Google phishing involves phishers setting up their own search engines to direct traffic to illegitimate sites
- Ways to recognize phishing messages
  - Deceptive Web links
  - E-mails that look like Web sites
  - Fake sender's address

Phishing (continued)

- Ways to recognize phishing messages (continued)
  - Generic greeting
  - Poor grammar, formatting, or misspellings
  - Pop-up boxes and attachments
  - Unsafe Web sites
  - Urgent request

Improperly Recycled Equipment

- Many organizations and individuals recycle older equipment
  - By donating them or by selling them online
- Information that should have been deleted from the equipment often is still available
- With many operating systems, simply deleting a file does not necessarily make the information irretrievable
- Data can be retrieved by an attacker

Search Engine Scanning

- Search engines are important tools for locating information on the Internet
- Search engines offer advanced search tools
  - That can narrow criteria for more specific information
- Attackers can use search engines to scour the Internet for important attack information

Search Engine Scanning (continued)

Table 3-1 Search engine scanning techniques

Search Operator	Description	Example	Why Used by Attackers
site	Search a specific Web site for a certain term	*site:www.microsoft.com security*	Provides a listing of every Web page on the site that has information about security
filetype	Search for specific types of documents that contain a certain term	*filetype:pdf security*	Returns a listing of documents that contain security-related information
intitle	Search Web sites that contain a certain term in the title of the page	*intitle:index of "parent directory"*	Provides a list of files and directories on a Web page that can be used to identify desired information and how the Web server is organized

Dumpster Diving

- Dumpsters can be a source of secure information
  - Files, letters, memos, passwords, and similar sensitive data can be found in dumpsters
- Heightened emphasis on security today has resulted in sensitive documents being shredded

Wardriving

- Scanning the radio frequency airwaves for a signal
  - Can identify and map the location of a wireless network

What Is Wardriving?

- Wireless location mapping
  - Used to refer to passive wireless discovery
    - Process of finding a WLAN signal and recording information about it
- Technically involves using an automobile to search for wireless signals over a large area
  - Warflying uses airplanes instead of automobiles
- Wardriving is in itself not an illegal activity
  - Using that RF signal to connect to networks without the owner's permission can be illegal

What Is Wardriving? (continued)

- Techniques used by wardrivers
  - Driving at slower speeds
  - Creating a plan
  - Repeating over time

Wardriving Hardware

- Mobile computing devices
  - Laptop computer
  - Tablet computer
    - Designed for truly mobile computing
    - Can be operated with a stylus instead of a keyboard
    - Types: convertible and slate
    - Advantages
      - Users can write rather than type
      - Handwritten notes are immediately digitized
      - Ideal for drawings, formulas, signatures, and other graphical objects

Wardriving Hardware (continued)



Figure 3-4 Convertible tablet

Wardriving Hardware (continued)



Figure 3-5 Slate tablet

Wardriving Hardware (continued)

- Mobile computing devices (continued)
  - Handheld PC
    - Small enough to be held in a single hand
    - Has many of the features of a laptop computer
  - Personal digital assistant (PDA)
  - Smartphones
    - Combine functions of a PDA and a cellular telephone

Wardriving Hardware (continued)



Figure 3-6 Handheld PC

Wardriving Hardware (continued)



Figure 3-7 PDA

Wardriving Hardware (continued)

Table 3-2 Mobile computing devices

Device	Advantages	Disadvantages
Laptop computer	Portable	Limited battery life
Tablet computer	Recognize handwriting	High cost; limited battery life
Handheld PC	Same applications as desktop	Bulky design and small keyboard
Personal digital assistant	Fits in one hand	Replaced by smartphones
Smartphone	Combines several features into single device	High cost

Wardriving Hardware (continued)

- Wireless network interface card
  - Allows mobile computing device to detect a wireless signal
  - Also called a wireless client network adapter
  - WNICs shapes and styles
    - Standalone USB
    - USB Key fob
    - CardBus card
    - Mini PCI card
    - Type II PC card
    - CompactFlash (CF) card (may require an optional sled)

Wardriving Hardware (continued)

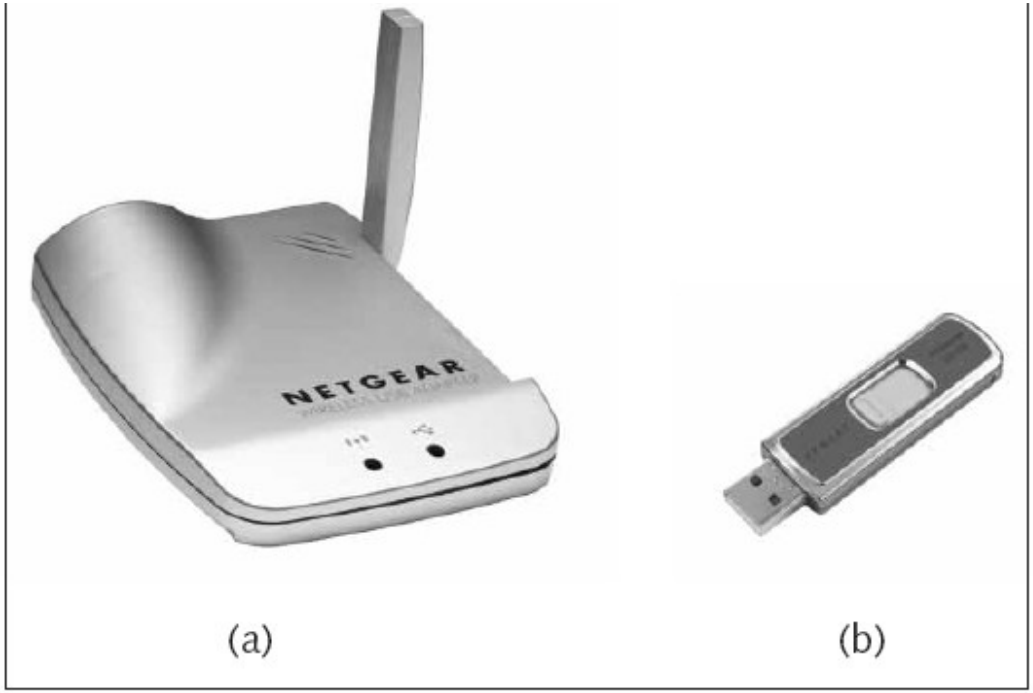
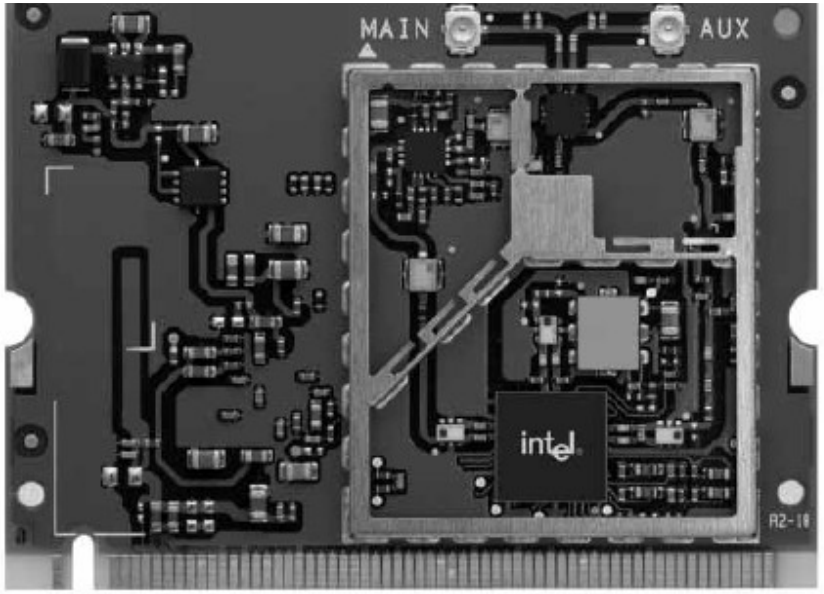


Figure 3-8 USB wireless NICs: (a) standalone USB device and (b) USB key fob

Wardriving Hardware (continued)



(a)



(b)

Figure 3-9 Wireless NIC PC Card adapters: (a) CardBus card and (b) Mini PCI card

Wardriving Hardware (continued)



Figure 3-10 Wireless CompactFlash card

Wardriving Hardware (continued)

- Wireless network interface card (continued)
  - Promiscuous mode
    - Allows a wired NIC to capture all the packets it receives
    - Promiscuous mode will not work on a WLAN

Wardriving Hardware (continued)

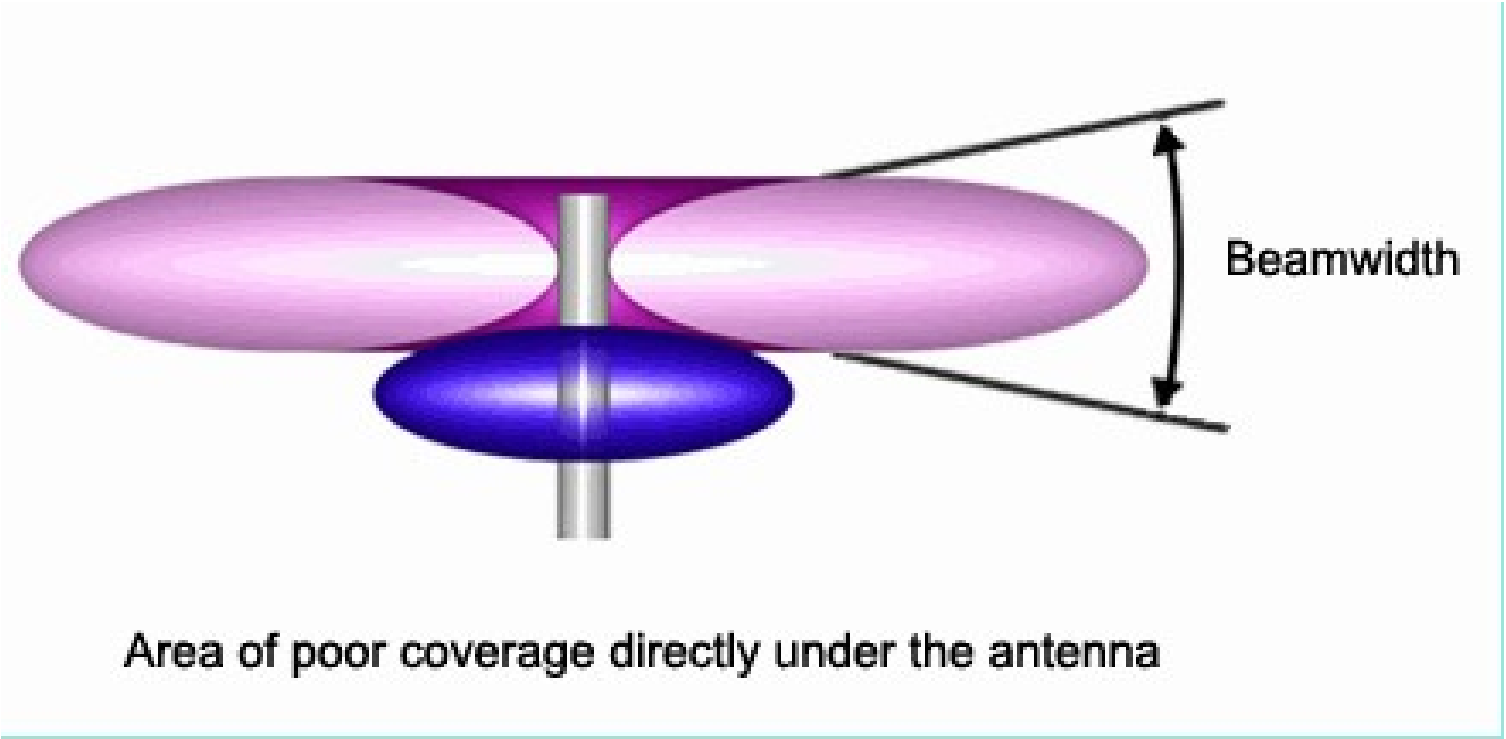
- Antennas
  - Attaching an external antenna will significantly increase the ability to detect a wireless signal
  - Fundamental characteristics
    - As the frequency increases, wavelength decreases
      - This means that the size of the antenna is smaller
    - As antenna gain increases, the coverage area narrows
      - High-gain antennas offer longer coverage areas

Wardriving Hardware (continued)

- Antennas (continued)

Basic categories

  - Omni-directional
    - Also called a dipole antenna
    - Detects signals from all directions equally



Wardriving Hardware (continued)

Sample semi-directional antennas

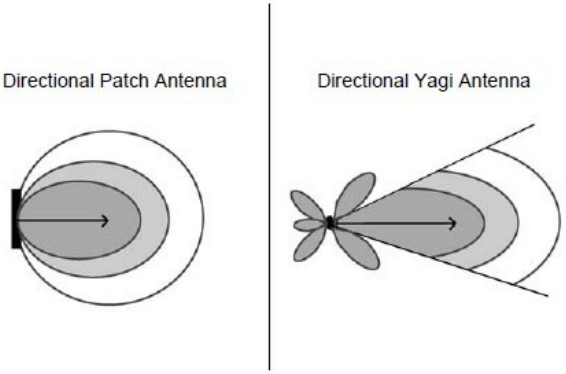


Yagi Antenna | Patch Antenna | Panel Antenna

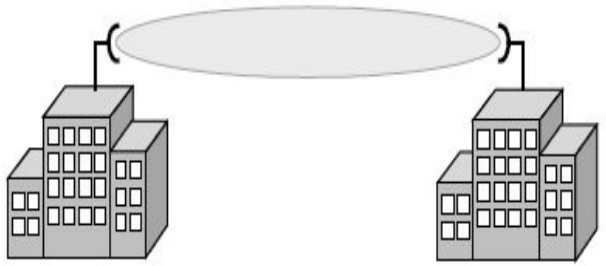
Semi-directional

– Focuses the energy in one direction

Coverage area of a semi-directional antenna



Point-to-point link using semi-directional antennas



Wardriving Hardware (continued)

- Highly directional
  - Sends a narrowly focused signal beam
  - Generally concave dish-shaped devices



Wardriving Hardware (continued)

- Global Positioning System (GPS)
  - Used to precisely identify location of a GPS receiver
  - GPS device is optional when wardriving

Wardriving Hardware (continued)

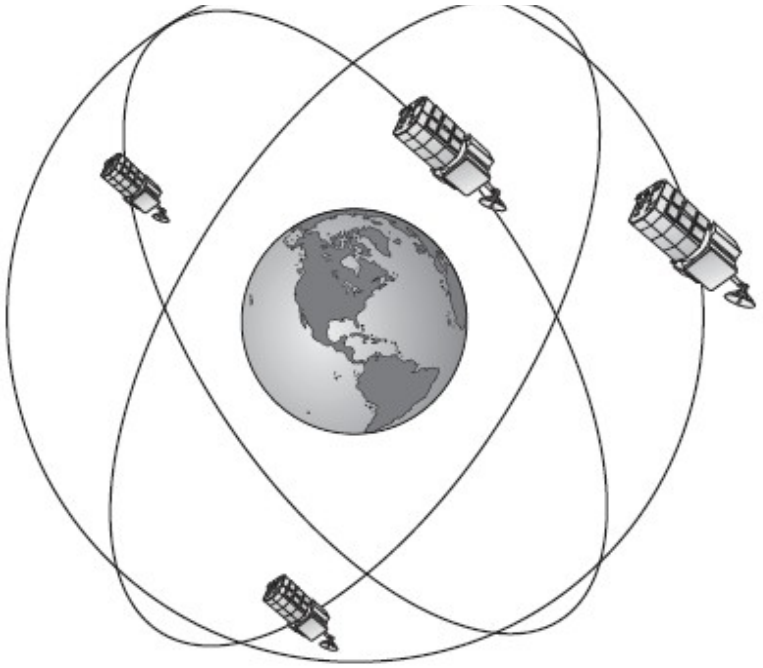


Figure 3-11 Global positioning system (GPS)

Wardriving Hardware (continued)



Figure 3-12 USB GPS

Wardriving Hardware (continued)

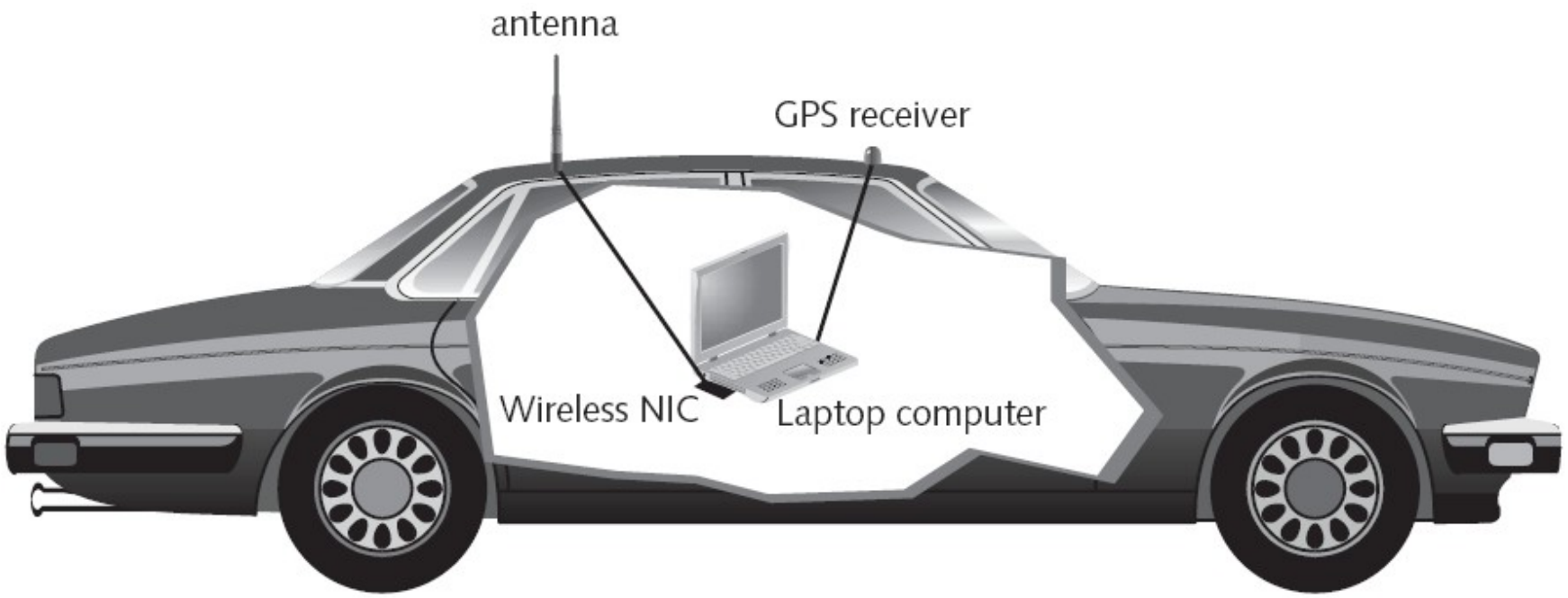


Figure 3-13 Wardriving hardware

Wardriving Software

- Client utilities
  - When WLANs first appeared, operating systems were not equipped to be aware of their presence
  - Used to detect a wireless signal and then connect to that network
- Integrated operating system tools
  - Microsoft's Wireless Zero Configuration (WZC)
    - Tightly integrated with Windows XP Service Pack 2 (SP2) and Windows Server 2003
    - Facilitates roaming between different WLANs

Wardriving Software (continued)

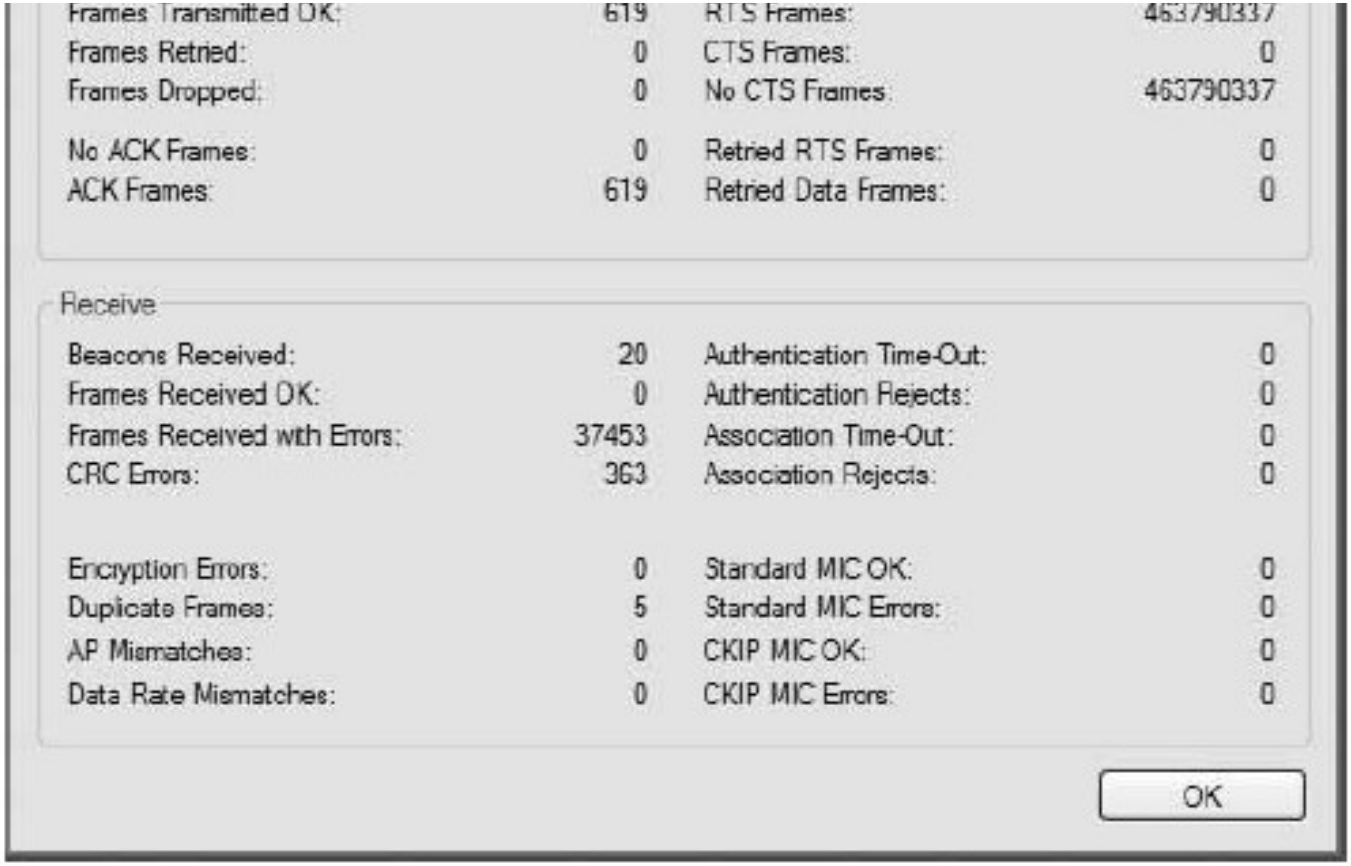


Figure 3-14 Client utility statistics

Wardriving Software (continued)

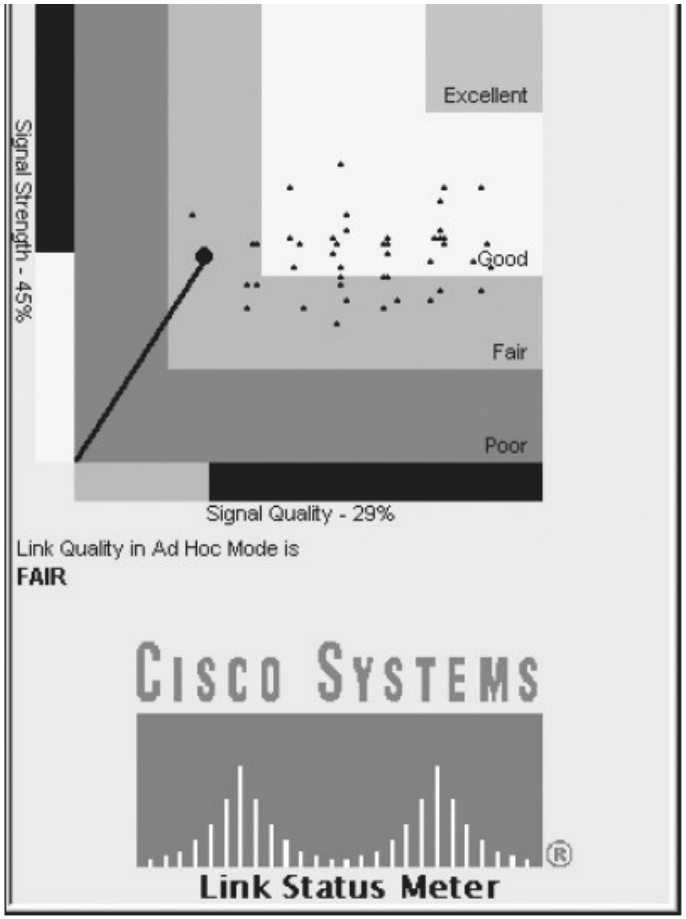


Figure 3-15 Client utility signal strength meter

Wardriving Software (continued)

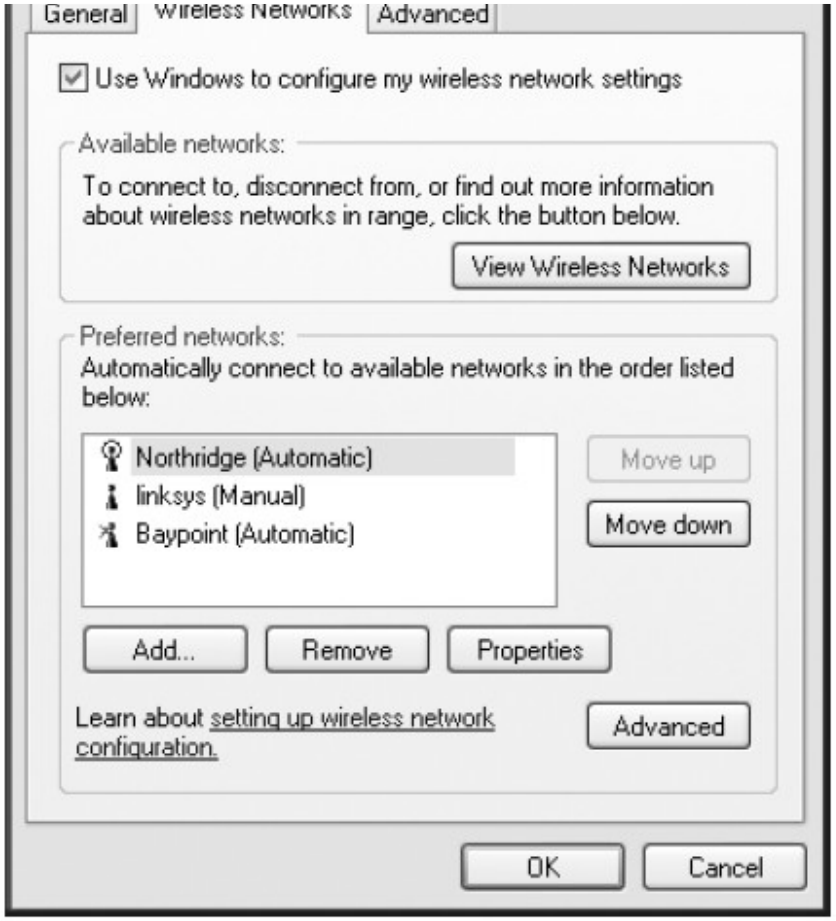


Figure 3-16 Wireless Network Connection Properties window

Wardriving Software (continued)

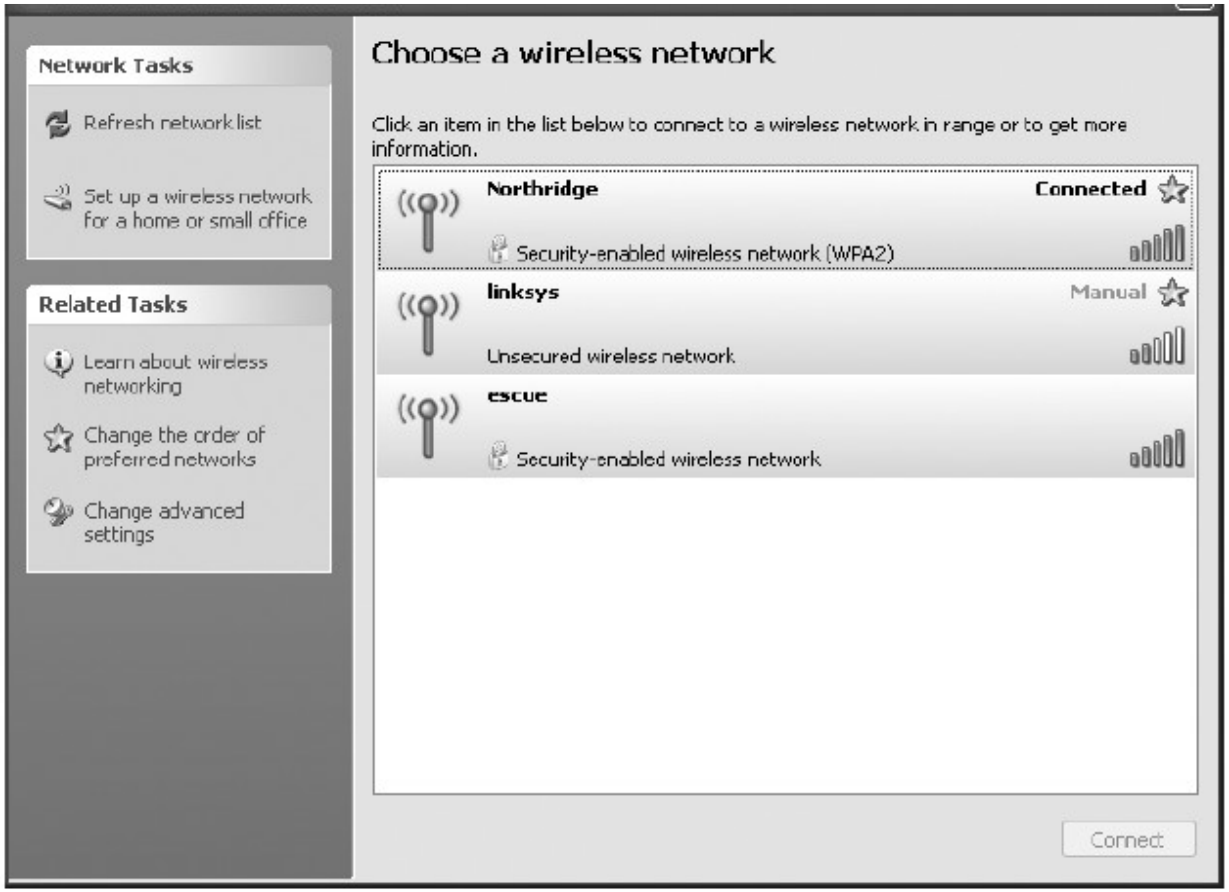


Figure 3-17 Choose a wireless network dialog box

Wardriving Software (continued)

- Freeware discovery applications
  - Specifically designed to pick up a radio frequency WLAN signal
  - NetStumbler
    - Probably the most widely used
    - Can determine an access point's location using a GPS device to mark locations
    - Cannot capture and decode wireless packets, monitor utilization, or make automatic connections
    - Cannot report all types of encryption
      - Such as IP Security (IPSec)

Wardriving Software (continued)

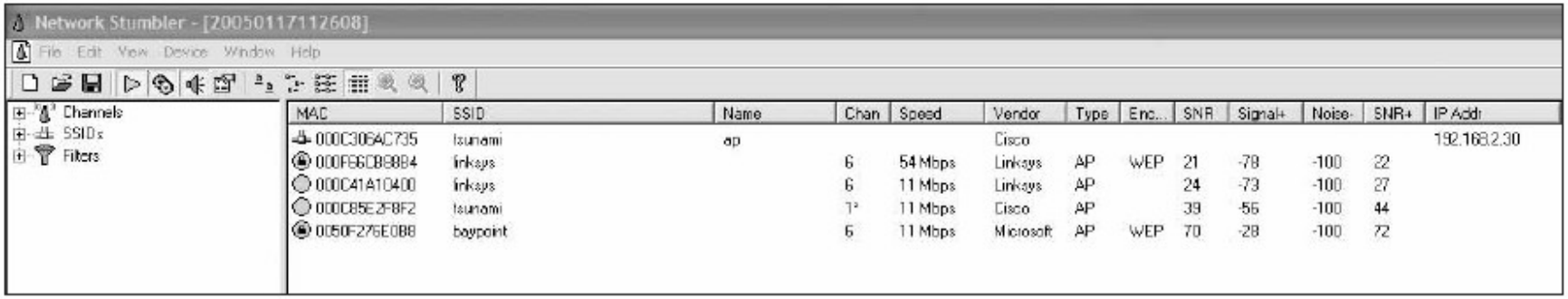


Figure 3-18 NetStumbler main screen

Wardriving Software (continued)

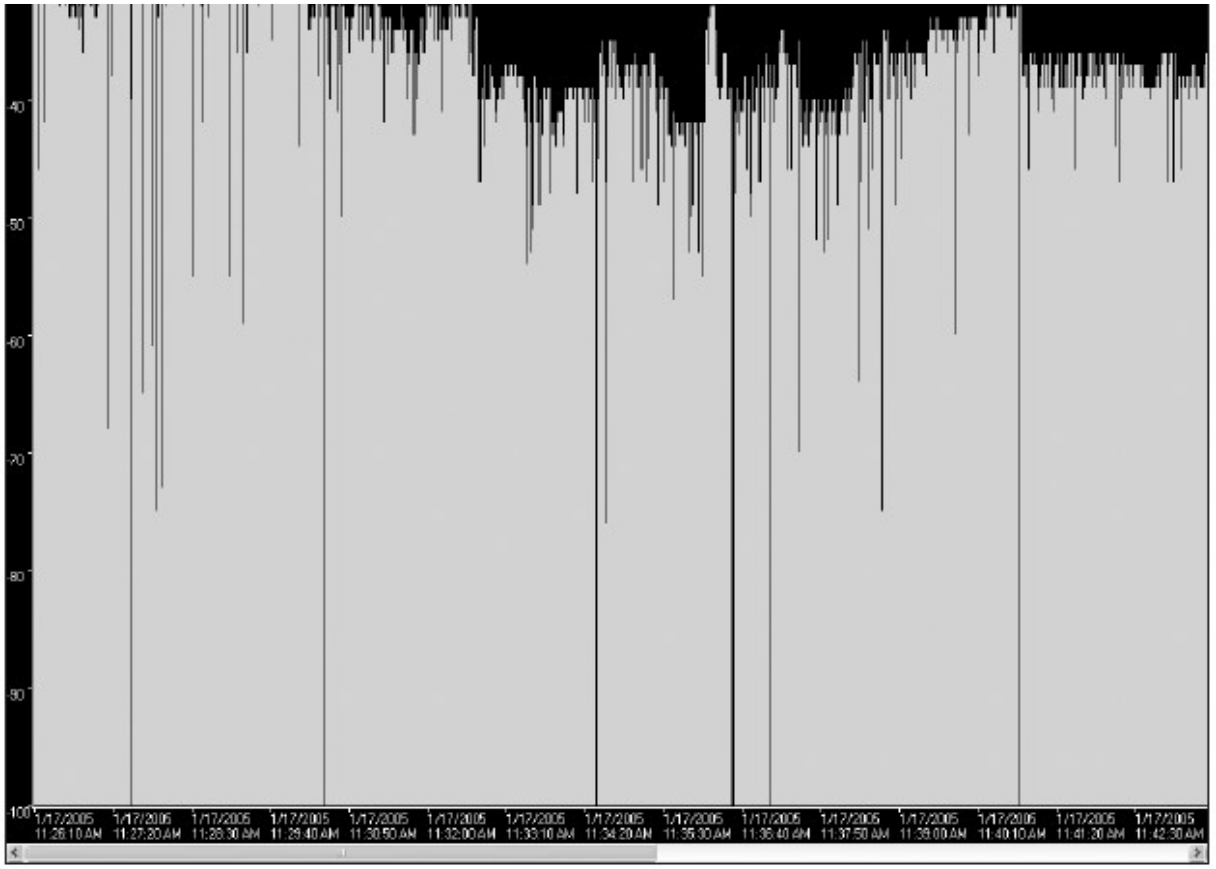


Figure 3-19 NetStumbler signal-to-noise ratio

Wardriving Software (continued)

- Freeware discovery applications (continued)
  - Kismet
    - Runs under the Linux operating system
    - Can report similar information as NetStumbler
    - Also supports GPS
    - Can capture packets and dump them to a file
  - KisMAC
    - Kismet application for Apple MacOS X
  - Script kiddies
    - Novice attackers that lack advanced technical skills

Public Mapping Sites

- Final step in wardriving
  - Document and then advertise the location of the wireless LANs
- Warchalking
  - Wireless networks were identified by drawing on sidewalks or walls around the area of the network
  - Has been replaced by public online databases and mapping sites

Public Mapping Sites (continued)

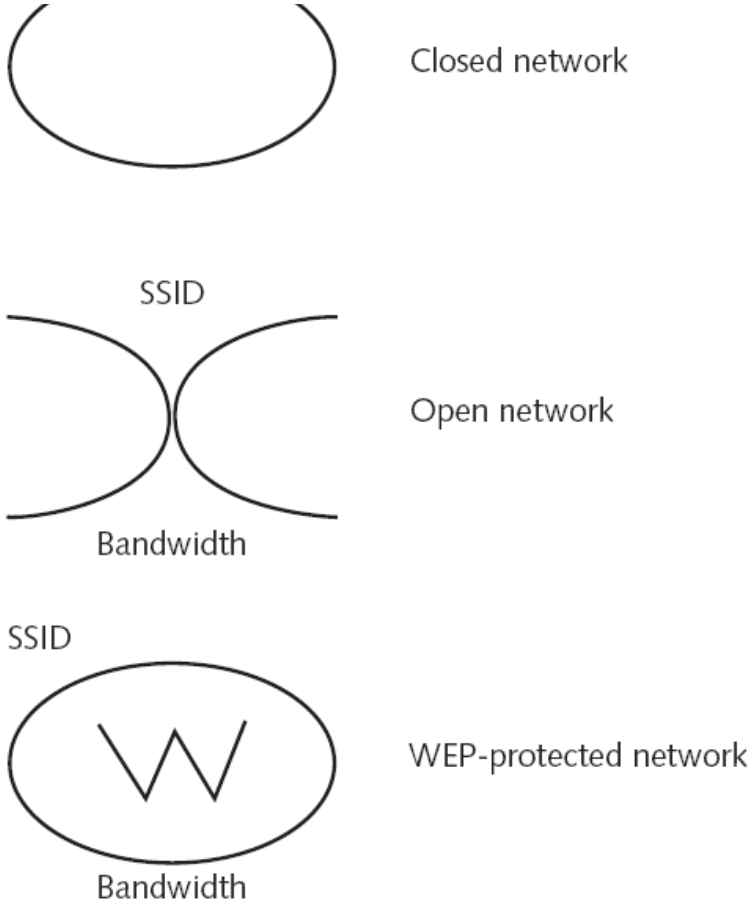


Figure 3-20 Warchalking symbols

Public Mapping Sites (continued)

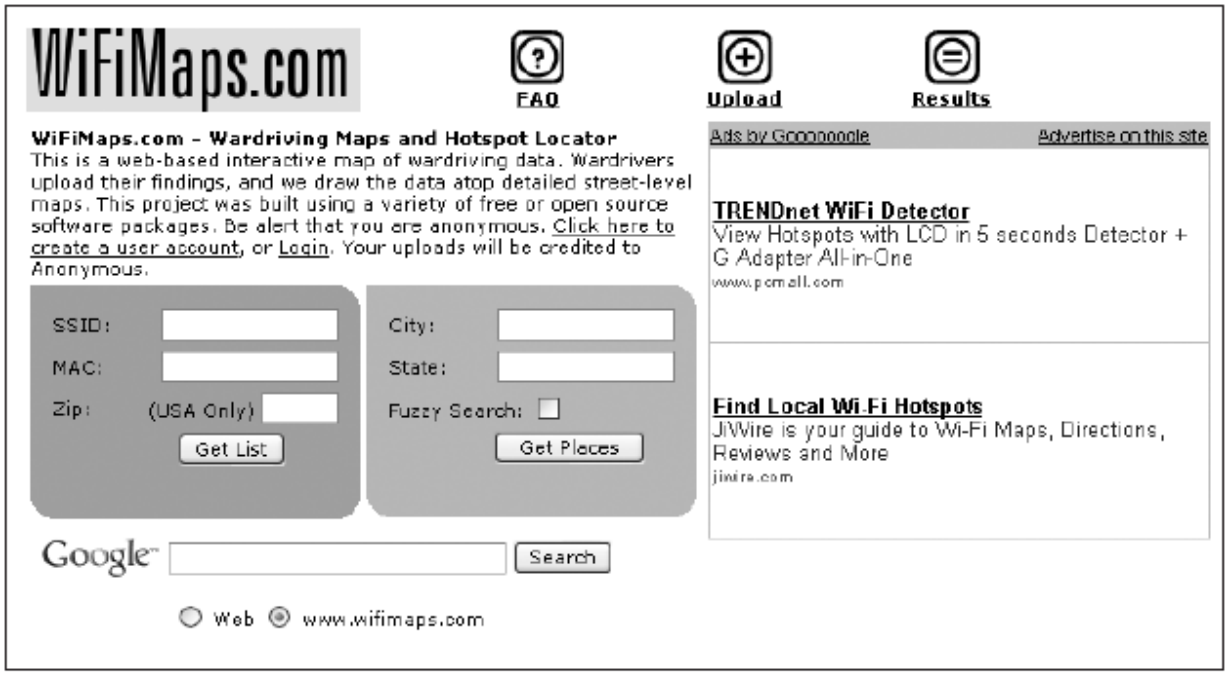


Figure 3-21 Recording WLAN information

Public Mapping Sites (continued)

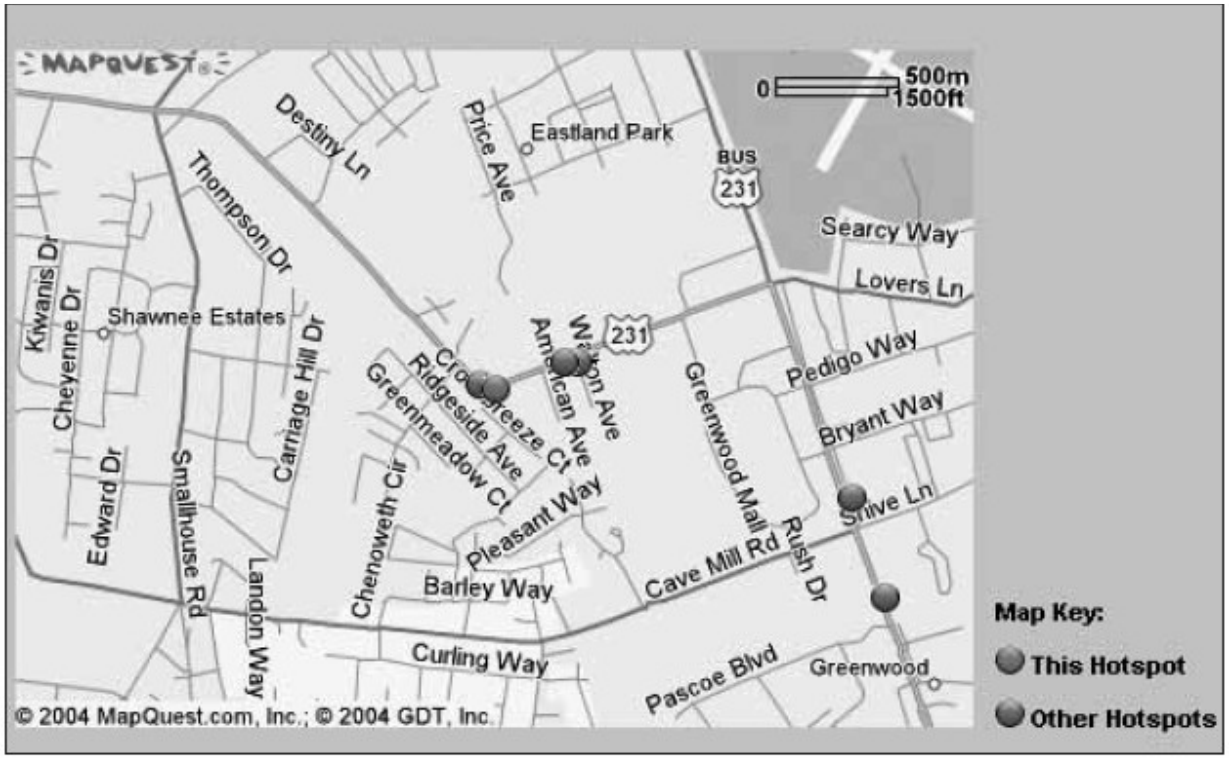


Figure 3-22 WLAN hotspots

Wireless Packet Sniffers

- Monitoring network traffic is important to determine the health of a network
- Simple Network Management Protocol (SNMP)
  - Part of the TCP/IP protocol suite
  - Allows computers and network equipment to gather data about network performance
  - Software agents are loaded onto each network device that will be managed
    - Monitor network traffic
    - Store info in a management information base (MIB)

Wireless Packet Sniffers (continued)

- Simple Network Management Protocol (SNMP) (continued)
  - SNMP management station
    - Communicates with the software agents and collects the data stored in the MIBs
  - First two versions of SNMP used community strings
    - Acted like a password to allow or deny access to the information that was collected
- Packet sniffer
  - Captures TCP/IP packets as they are transmitted

Wireless Packet Sniffers (continued)

- Packet sniffer (continued)
  - Categories based on their functions
    - Counts the number of packets transmitted
    - Shows general characteristics of traffic
    - Provides a detailed analysis of all protocols
- Wireless packet sniffer
  - Can capture data frames and management frames

Wireless Packet Sniffers (continued)

- Wireless packet sniffer (continued)
  - Helps reveal the following WLAN problems:
    - An access point that is advertising its SSID when it is intended to be turned off
    - An access point with encryption disabled
    - A wireless client that is sending a high rate of low-speed packets
    - An access point that is transmitting an excessive number of beacon frames

Summary

- General information gathering relies on deception and digging to obtain information about networks
- Social engineering relies on deceiving someone to access a system
- Wireless location mapping, or wardriving, refers to passive wireless discovery
  - Finding a WLAN signal and recording information about it
- Wardriving software
  - Integrated operating system tools

Summary (continued)

- Wardriving software (continued)
  - Client utilities
  - Freeware discovery applications
- Wireless packet sniffers
  - Play an important role in analyzing network traffic and identifying problems
  - Can capture data frames and management frames
  - Can also be used by attackers to capture unencrypted packets and view their contents

Quiz

1. The _____ is the group of integrated circuits that provide the functionality of the wireless NIC.

2. A(n) _____ antenna focuses the energy in one direction.

3. _____ relies on tricking and deceiving someone to access a system.

4. _____ involves phishers setting up their own search engines to direct traffic to illegitimate sites.

5. The integrated operating system tool for a Windows-based computer is Microsoft's _____ service.

6. True or False: NetStumbler can check for wireless networks and their signal strength, review which channels are being used, and then compare competing networks to monitor interference.

7. Wireless networks were identified by drawing on sidewalks or walls around the area of the network, a practice known as _____.

8. _____ allows computers and network equipment to gather data about network performance.