802.11b and the Joy of WarCycling in Dublin

David Malone

12 November 2002

Plan

1. 802.11 basics.
2. Wardriving.
3. Answers to selected problems.

802.11

Think coaxless thin Ethernet.

802.11b Most common variant. 2.4GHz, 11Mbps, 100m.

802.11a Faster variant. 5GHz, 54Mbps, 50m.

802.1x EAP based authentication.

e: Qos, g: faster 2.4GHz, h: mods to a, i: security.

802.11b Concepts

Channel Frequency for communication (1–14).

BSSID Group of communicating individuals (MAC).

SSID Network name (20 chars).

mode Infrastructure/ad-hoc (IBSS).

WEP

Built in security mechanism.

- Encrypts the body of frames.
- 40 (104) bit keys.
- Default or per-station.
- No key management.

WEP Problems

Has been shown to be flawed.

- Key is usually constant.
- First byte is `0xAA`.
- Initial Vector is observable.

Some IVs provide information about key.

Cards

Chipsets Lucent Hermes, Intersil PRISM, Aironet.

Sniffing Some chip sets more flexable than others.

Host AP Useful for building own networks.

Antenna Depends on packaging.

WEP Key size.

Access Point

High level dhcp, NAT, packet/MAC filter, radius,. . .

Low level See card features.

Dual card Not usually useful.

Future proof LEAP, 802.11i, 802.11a, . . .

Antennas

- Usually unnecessary.
- Omni, Parabolic, Sector, Yagi, . . .
- Good cabling important.
- Talk to radio HAMs.

Software

- Good driver support by/for usual suspects.
- Sniffing for networks: kismet, bsdairtools, NetStumbler, MacStumbler,. . .
- Sniffing for packets: tcpdump, AirSnort, bsdairtools,. . .
- Network surveying.

Why Wardrive?

- To understand WiFi better.
- Fun.
- Business.
- To walk the walk.

- Dry run around TCD.
- Expand to around town.
- Industrial Estates.
- Missing pieces.

Interesting Finds

- IFSC and friends.
- Big network in the docs.
- Public service use?
- Industrial estate spotting.

War Cycling

- Found MacStumbler.
- `antenna++, farady_cage--;`
- Took a bit of getting right.
- Route to work & Clontarf.

More finds

- Really Rapid Results.
- Eastpoint: must try harder.
- Deft HEA?
- Irishwan.

Talking to People

- Legal advice.
- Help with mapping.
- ‘Guys in a car. . . ’
- Feedback.

Serious Sniffing

- FreeBSD 4.7,
- Orinoco card,
- dsniff,
- *not just wireless problem.*

Dirty Wireless

- Put wireless on own network/VLAN.
- Do normal ingress/egress filtering.
- Application level security.
- Doesn't protect wireless network.

LEAP

- Cisco's quick 802.1x solution.
- Authenticates user and network.
- Frequent key changes.

IPsec/VPN

- Encryption to local gateway.
- Authenticate with local gateway.
- WEP shouldn't be a factor.