

WIRELESS NETWORKS

Nigel Pentland
August 2002

Introduction

This is largely meant as an aide mémoire for myself.

Background and Basics

Wireless Networking aka Wireless Ethernet aka WiFi (Wireless Fidelity) aka 802.11b

Here is a very readable overview of the 802.11b facts -

http://www.oreillynet.com/pub/a/wireless/2001/03/02/802.11b_facts.html

As an indicator of the growing prevalence of Wireless Networking note the reference to IBM "i Series" ThinkPads coming with built-in Wireless Networking!

More detailed reference – <http://grouper.ieee.org/groups/802/11/index.html>

SSID – Service Set Identifier

WEP – Wired Equivalence Protection (uses RC4 symmetric encryption)

2.4 GHz unlicensed radio band which is broken into 14 overlapping 22-MHz channels and used one at a time.

11mbit (closer to 6mbit usable)

Designed for up to 1500 feet but with enhanced antennas plus clear line of sight, several miles is possible.

802.11b defines two different modes of operation:

1. **Infrastructure mode** – client to AP (access point) only
2. **Ad-hoc mode** – client to client directly

Common packet types:

-  Beacon
-  Probe
-  Data
-  Ad-hoc

Ad-hoc packets are simply data packets sent in Ad-hoc mode as opposed to Infrastructure mode.

Network Detection

Active Detection

NetStumbler – <http://www.netstumbler.com/>

Passive Detection

Kismet - <http://www.kismetwireless.net/>

Wellenreiter - <http://www.remote-exploit.org/>

Airsnort - <http://airsnort.shmoo.com/>

Cloaking and Non-Beaconing

WEP only encrypts data packets!

Cloaking is where the SSID is blocked from beacon packets. However, once a client joins the network the SSID is sent by the client and the AP in clear.

Neither cloaking nor non-beaconing provide any significant protection.

Securing Wireless Networks

- ✚ Use application or network layer encryption
- ✚ Use proper authentication – MAC addresses can be easily spoofed
- ✚ Use properly tuned equipment – always use minimum power possible

Community Wireless Networks

Check out what's happening near you, you'll be surprised!

<http://wirelessanarchy.com/>

<http://www.glasgow.net/>