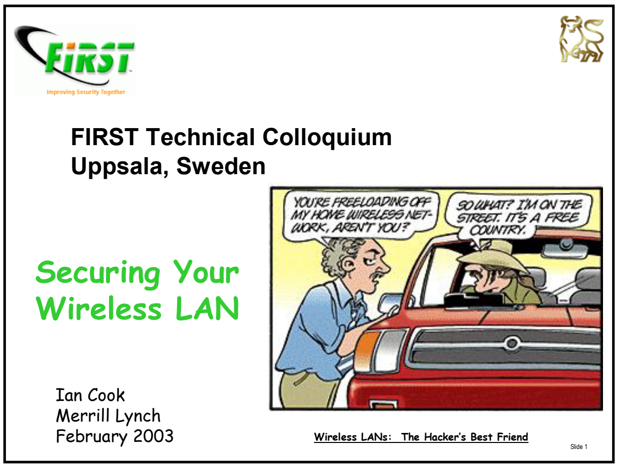


FIRST Technical Colloquium
Uppsala, Sweden

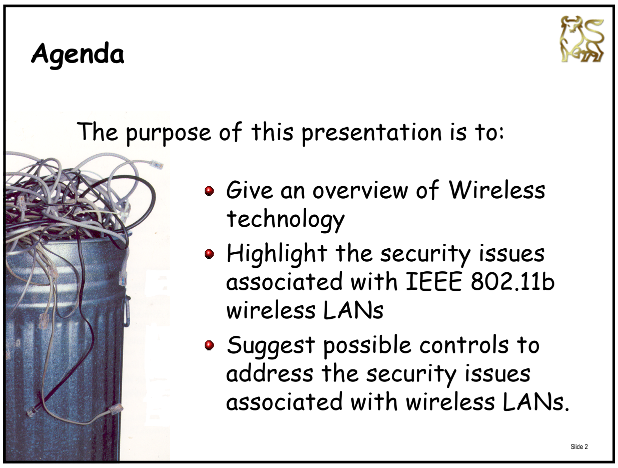
Securing Your Wireless LAN

Ian Cook
Merrill Lynch
February 2003

Wireless LANs: The Hacker's Best Friend

Improving Security Together
YOU'RE FREELOADING OFF MY HOME WIRELESS NETWORK, AREN'T YOU?
SO WHAT? I'M ON THE STREET. IT'S A FREE COUNTRY.

Slide 1

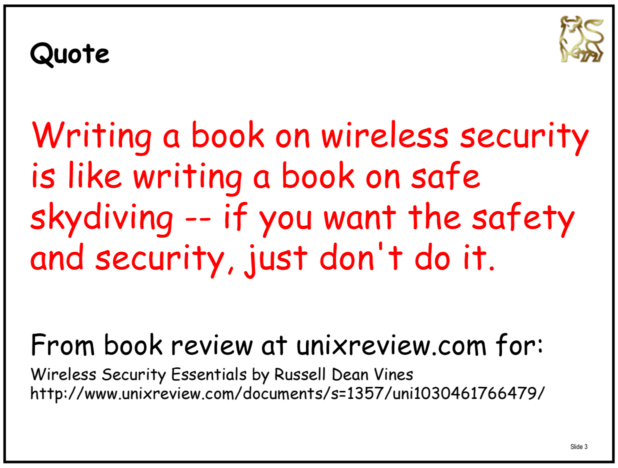


Agenda

The purpose of this presentation is to:

- Give an overview of Wireless technology
- Highlight the security issues associated with IEEE 802.11b wireless LANs
- Suggest possible controls to address the security issues associated with wireless LANs.

Slide 2

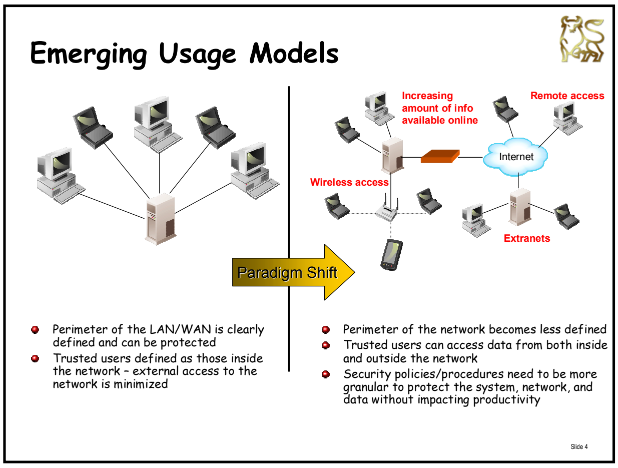


Quote

Writing a book on wireless security is like writing a book on safe skydiving -- if you want the safety and security, just don't do it.

From book review at unixreview.com for:
Wireless Security Essentials by Russell Dean Vines
http://www.unixreview.com/documents/s=1357/uni1030461766479/

Slide 3

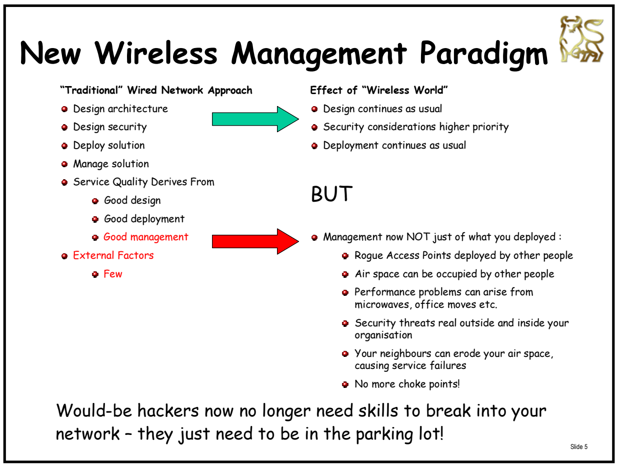


Emerging Usage Models

- Perimeter of the LAN/WAN is clearly defined and can be protected
- Trusted users defined as those inside the network – external access to the network is minimized

- Perimeter of the network becomes less defined
- Trusted users can access data from both inside and outside the network
- Security policies/procedures need to be more granular to protect the system, network, and data without impacting productivity

Slide 4



New Wireless Management Paradigm

"Traditional" Wired Network Approach

- Design architecture
- Design security
- Deploy solution
- Manage solution
- Service Quality Derives From
  - Good design
  - Good deployment
  - Good management
- External Factors
  - Few

Effect of "Wireless World"

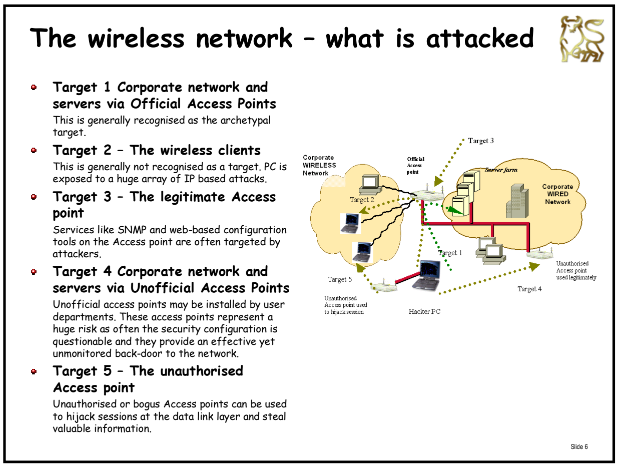
- Design continues as usual
- Security considerations higher priority
- Deployment continues as usual

BUT

- Management now NOT just of what you deployed :
  - Rogue Access Points deployed by other people
  - Air space can be occupied by other people
  - Performance problems can arise from microwaves, office moves etc.
  - Security threats real outside and inside your organisation
  - Your neighbours can erode your air space, causing service failures
  - No more choke points!

Would-be hackers now no longer need skills to break into your network – they just need to be in the parking lot!

Slide 5



The wireless network – what is attacked

- **Target 1 Corporate network and servers via Official Access Points**
  This is generally recognised as the archetypal target.
- **Target 2 – The wireless clients**
  This is generally not recognised as a target. PC is exposed to a huge array of IP based attacks.
- **Target 3 – The legitimate Access point**
  Services like SNMP and web-based configuration tools on the Access point are often targeted by attackers.
- **Target 4 Corporate network and servers via Unofficial Access Points**
  Unofficial access points may be installed by user departments. These access points represent a huge risk as often the security configuration is questionable and they provide an effective yet unmonitored back-door to the network.
- **Target 5 – The unauthorised Access point**
  Unauthorised or bogus Access points can be used to hijack sessions at the data link layer and steal valuable information.

Target 3
Corporate WIRELESS Network
Official Access point
Server farm
Corporate WIRED Network
Target 2
Target 1
Unauthorised Access point used legitimately
Target 5
Target 4
Unauthorised Access point used to hijack session
Hacker PC

Slide 6

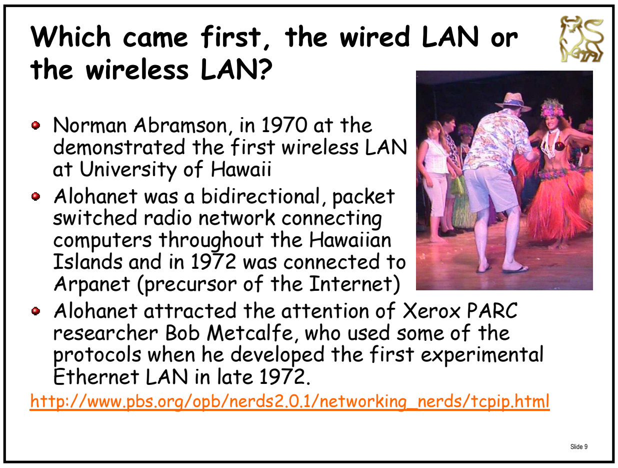
Questions You Should Ask Yourself

- Where are my access points?
- Are they all mine? i.e. are there any rogue access points?
- Are they vulnerable to attack?
- Where is my network perimeter?
- Are malicious third parties able to intercept and read my wireless network traffic from outside the building
- Is there any radio interference from other wireless networks which is interfering with my network traffic and thus reducing network capacity or availability

Quick Quiz

Which came first:

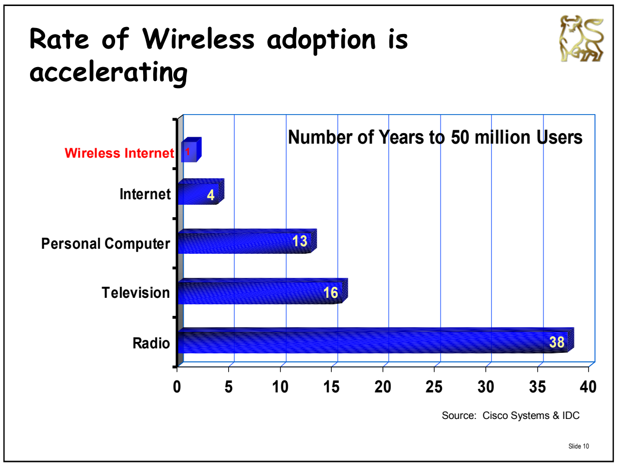
The wired LAN or the wireless LAN?



Which came first, the wired LAN or the wireless LAN?

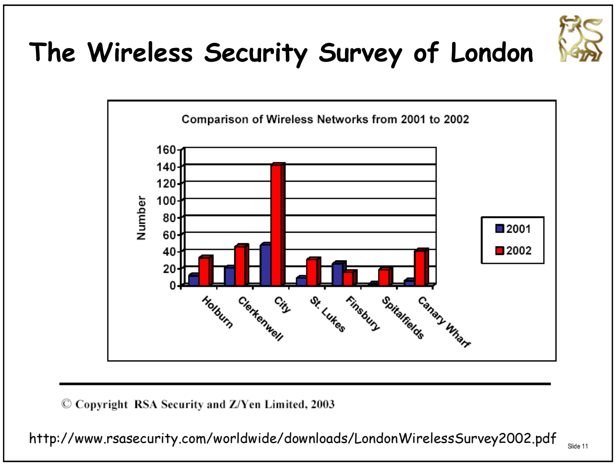
- Norman Abramson, in 1970 at the demonstrated the first wireless LAN at University of Hawaii
- Alohanet was a bidirectional, packet switched radio network connecting computers throughout the Hawaiian Islands and in 1972 was connected to Arpanet (precursor of the Internet)
- Alohanet attracted the attention of Xerox PARC researcher Bob Metcalfe, who used some of the protocols when he developed the first experimental Ethernet LAN in late 1972.

http://www.pbs.org/opb/nerds2.0.1/networking_nerds/tcpip.html



Rate of Wireless adoption is accelerating

Source: Cisco Systems & IDC



The Wireless Security Survey of London

Comparison of Wireless Networks from 2001 to 2002

http://www.rsasecurity.com/worldwide/downloads/LondonWirelessSurvey2002.pdf

Free Wireless ISPs

StockholmOpen.net
The access network with a freedom of choice

- *AN UNDERGROUND MOVEMENT* to deploy free wireless access zones in metropolitan areas is taking hold.
- The movement, called by some the "parasitic grid" and by others more simply the "free metro wireless data network," has already installed itself in New York, San Francisco, Seattle, Aspen, Portland, British Columbia, and London.
- Offers attackers and intruders anonymous access
- Anonymity surpasses payphone and acoustic coupler
- The most up-to-date listings of wireless community networks can be found at http://www.personaltelco.net/index.cgi/WirelessCommunities

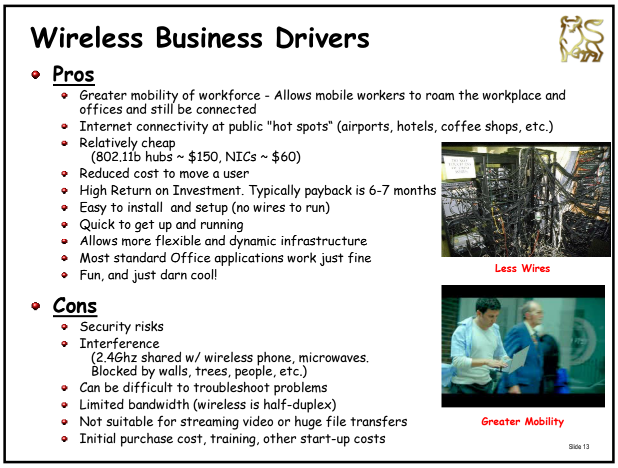
Consume

nycwireless

WIRELESSANARCHY

FREE NETWORKS.ORG

manchesterwireless.net



Wireless Business Drivers

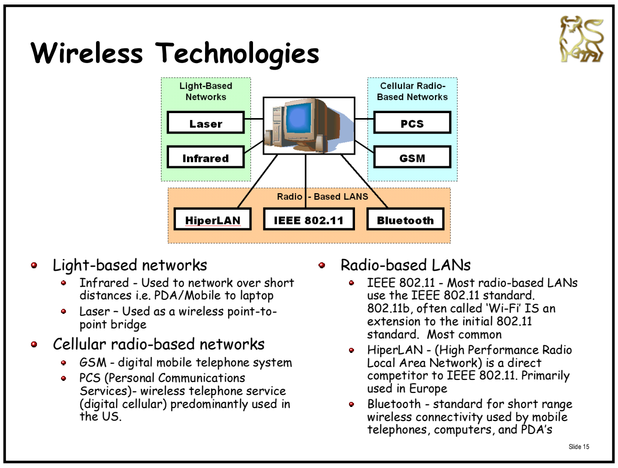
- **Pros**
  - Greater mobility of workforce - Allows mobile workers to roam the workplace and offices and still be connected
  - Internet connectivity at public "hot spots" (airports, hotels, coffee shops, etc.)
  - Relatively cheap
    (802.11b hubs ~ $150, NICs ~ $60)
  - Reduced cost to move a user
  - High Return on Investment. Typically payback is 6-7 months
  - Easy to install and setup (no wires to run)
  - Quick to get up and running
  - Allows more flexible and dynamic infrastructure
  - Most standard Office applications work just fine
  - Fun, and just darn cool!
- **Cons**
  - Security risks
  - Interference
    (2.4Ghz shared w/ wireless phone, microwaves.
    Blocked by walls, trees, people, etc.)
  - Can be difficult to troubleshoot problems
  - Limited bandwidth (wireless is half-duplex)
  - Not suitable for streaming video or huge file transfers
  - Initial purchase cost, training, other start-up costs

Less Wires

Greater Mobility

Slide 13

Slide 14



Wireless Technologies

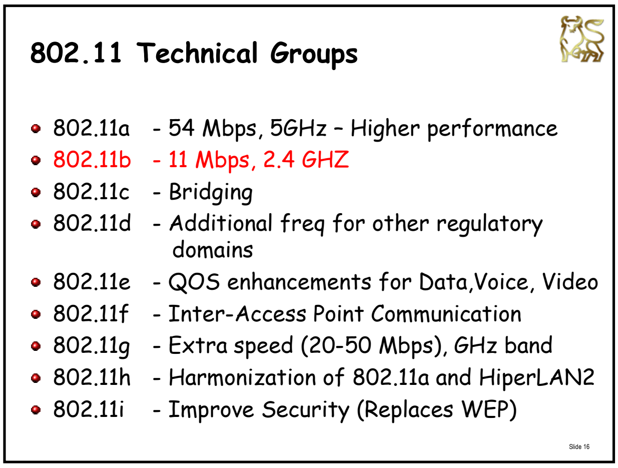
Light-Based Networks: Laser, Infrared

Cellular Radio-Based Networks: PCS, GSM

Radio - Based LANS: HiperLAN, IEEE 802.11, Bluetooth

- Light-based networks
  - Infrared - Used to network over short distances i.e. PDA/Mobile to laptop
  - Laser – Used as a wireless point-to-point bridge
- Cellular radio-based networks
  - GSM - digital mobile telephone system
  - PCS (Personal Communications Services)- wireless telephone service (digital cellular) predominantly used in the US.
- Radio-based LANs
  - IEEE 802.11 - Most radio-based LANs use the IEEE 802.11 standard. 802.11b, often called 'Wi-Fi' IS an extension to the initial 802.11 standard. Most common
  - HiperLAN - (High Performance Radio Local Area Network) is a direct competitor to IEEE 802.11. Primarily used in Europe
  - Bluetooth - standard for short range wireless connectivity used by mobile telephones, computers, and PDA's

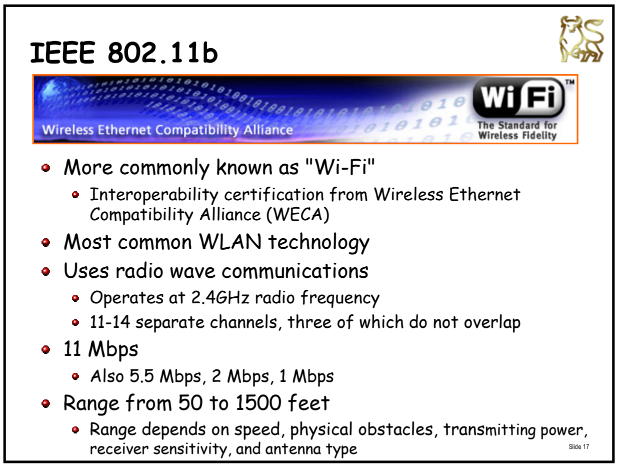
Slide 15



802.11 Technical Groups

- 802.11a - 54 Mbps, 5GHz – Higher performance
- 802.11b - 11 Mbps, 2.4 GHZ
- 802.11c - Bridging
- 802.11d - Additional freq for other regulatory domains
- 802.11e - QOS enhancements for Data,Voice, Video
- 802.11f - Inter-Access Point Communication
- 802.11g - Extra speed (20-50 Mbps), GHz band
- 802.11h - Harmonization of 802.11a and HiperLAN2
- 802.11i - Improve Security (Replaces WEP)

Slide 16



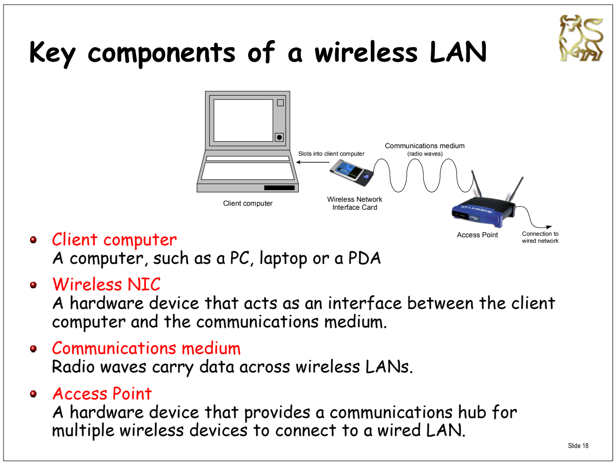
IEEE 802.11b

Wireless Ethernet Compatibility Alliance

Wi Fi™
The Standard for Wireless Fidelity

- More commonly known as "Wi-Fi"
  - Interoperability certification from Wireless Ethernet Compatibility Alliance (WECA)
- Most common WLAN technology
- Uses radio wave communications
  - Operates at 2.4GHz radio frequency
  - 11-14 separate channels, three of which do not overlap
- 11 Mbps
  - Also 5.5 Mbps, 2 Mbps, 1 Mbps
- Range from 50 to 1500 feet
  - Range depends on speed, physical obstacles, transmitting power, receiver sensitivity, and antenna type

Slide 17



Key components of a wireless LAN

Client computer

Slots into client computer

Wireless Network Interface Card

Communications medium (radio waves)

Access Point

Connection to wired network

- Client computer
  A computer, such as a PC, laptop or a PDA
- Wireless NIC
  A hardware device that acts as an interface between the client computer and the communications medium.
- Communications medium
  Radio waves carry data across wireless LANs.
- Access Point
  A hardware device that provides a communications hub for multiple wireless devices to connect to a wired LAN.

Slide 18

Wireless Network Cards: Hermes Chip Set

- Hermes cards (compatible with NetStumbler)
  - Orinoco (aka Wavelan Turbo, Gold & Silver)
  - Dell TrueMobile 1150
  - IBM High Rate Wireless LAN
  - Toshiba 802.11b Wireless
  - Compaq WL110
  - Cabletron Roamabout
  - ELSA AirLancer
  - ARtem ComCard
  - 1stWave 1ST-PC-DSS11
  - Buffalo Airstation WLI-PCM-L11

Wireless Network Cards: Prism2 Chip Set

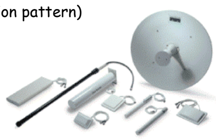
- Prism2 cards (widely supported by Linux, may work with some newer freeware war driving tools):
  - 3COM Airconnect
  - Cisco Aironet 340/350
  - Compaq WL100
  - Dell Treumobile 1100
  - D-Link DWL-650
  - GemTek (Taiwan) WL-211
  - Linksys WPC11
  - Samsung SWL-2000N
  - SMC 2632W
  - Z-Com XI300
  - Zoom Telephonics
  - ZoomAir 4100

Prism cards are very "hackable"

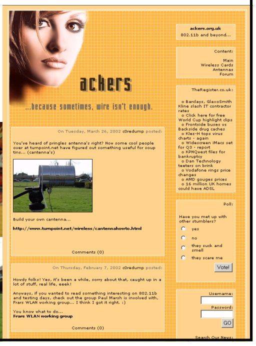
Wireless Range Extending Antennas

- An antenna is an optional piece of hardware, used to extend range of wireless card.
- The average card, without antenna can go about 1000 feet within line of sight)
- There are two main types of antenna:
  - Directional (increases coverage distance at the expense of coverage angle)
  - Omni directional (360-degree transmission pattern)
- Antenna on the Cheap

  http://www.turnpoint.net/wireless/cantennahowto.html
  http://www.oreillynet.com/cs/weblog/view/wlg/448
  http://verma.sfsu.edu/users/wireless/pringles.php
  http://www.netscum.com/~clapp/wireless.html



A Dual-Use Product


ackers.org.uk
802.11b and beyond...

Content:
Main
Wireless Cards
Antennas
Forum

ackers
...because sometimes, wire isn't enough.

On Tuesday, March 26, 2002 c0redump posted:

You've heard of pringles antenna's right? Now some cool people over at turnpoint.net have figured out something useful for soup tins... (cantenna's)

Build your own cantenna...

http://www.turnpoint.net/wireless/cantennahowto.html

Comments (0)

On Thursday, February 7, 2002 c0redump posted:

Howdy folks! Yes, it's been a while, sorry about that, caught up in a lot of stuff, real life, eeek!

Anyways, if you wanted to read something interesting on 802.11b and testing days, check out the group Paul Marsh is involved with, Frars WLAN working group... I think I got it right. :)

You know what to do...
Frars WLAN working group

Comments (0)

TheRegister.co.uk:

- Barclays, GlaxoSmith Kline slash IT contractor rates
- Click here for free World Cup highlight clips
- Frontside buses vs Backside drug caches
- Klez-H tops virus charts - again
- Widescreen iMacs set for Q3 - report
- KPNQwest files for bankruptcy
- Dan Technology teeters on brink
- Vodafone rings price changes
- AMD gouges prices
- 16 million UK homes could have ADSL

Poll:

Have you met up with other stumblers?

○ yes
○ no
○ they suck and smell
○ they scare me

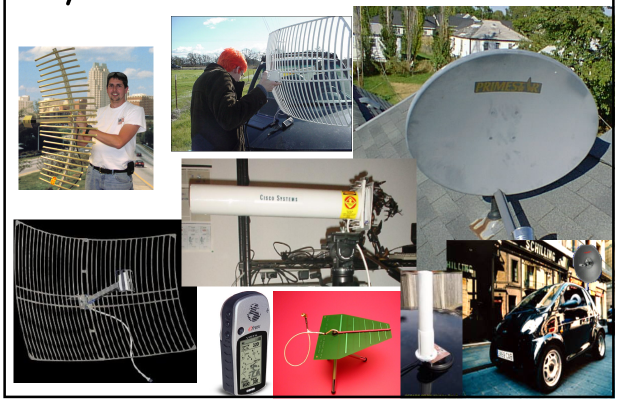
Username:
Password:

Search Our News:

You'll need:

- A N-Female chassis mount connector.
- Four small nuts and bolts
- A bit of thick wire
- An old can

Toys for Hackers



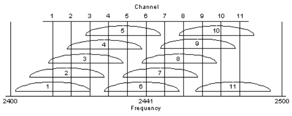
Access Point

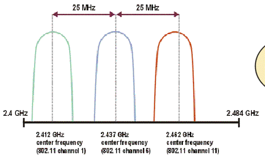
- An Access Point is a hardware device that provides a communications hub for multiple wireless devices to connect to a wired LAN.
- Individual Access Points have a range typically limited to a few hundred meters.
- Install multiple Access Points in order to allow a wireless network user to roam around a building and maintain communication.
- Access Points have a number of settings that can be configured, such as the network name (SSID) and encryption keys. (WEP)

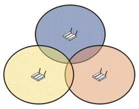
  (Covered Later)

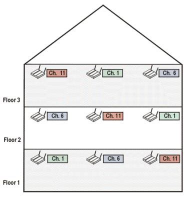
Wireless 802.11x – Channel Allocation

- Europe 13 channels
- USA 11 channels
- Japan 14 channels









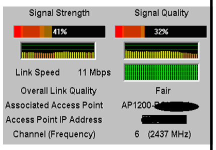
Source: *The IEEE 802.11 Handbook: A Designer's Companion*

Design Questions to Consider

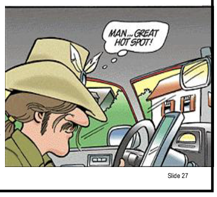
- How many access points do I need?
  - How many users and where are they?
- Where do I put the access points?
  - Do a site survey
- Will access points interfere with each other?
  - Channel assignments
- Can I move around and not lose my connection?
  - IP network design
  - Third-party products
- Does it scale?
  - Multiple co-located access points
  - Smaller cell sizes
- Can I make it secure?
  - How much security do you need?

Access Point Placement Issues

- Interference, dead zones (walls, large fish tanks, metal cabinets, wireless phones, etc.)
- Design in three dimensions
- Factor in antenna design and transmitting power
- Assign channels in a grid
- In multi-tenant buildings check traffic contention
- Put access points in the middle of the building to reduce risk of signal leakage outside the building
  This is not a strong defence and doesn't stop it!
- 11 mbit traffic travels about 40 metres or so but 2 mbit management traffic travels MUCH further!

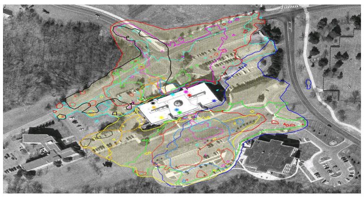


Signal Strength 41%
Signal Quality 32%
Link Speed 11 Mbps
Overall Link Quality Fair
Associated Access Point AP1200-[redacted]
Access Point IP Address [redacted]
Channel (Frequency) 6 (2437 MHz)



Example: RF Leakage

A single network composed of nine access points (AP's). Each AP is denoted by an asterisk. The complete network coverage is shown by the shaded area while the unique field for each AP is bounded by its respective colour.



University of Kansas

Wireless Network Visualization Project

http://www.ittc.ku.edu/wlan/index.shtml

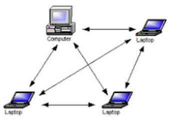
Wireless Lan Features

- Wireless LAN's typically include a number of features that can be used to strengthen their security.
- Features:
  - Alternative operating modes, i.e. 'Ad-Hoc' or 'Infrastructure'
  - Network identification using the Service Set Identifier (SSID)
  - MAC address filtering
  - Data encryption using the Wired Equivalent Privacy (WEP) protocol
  - User authentication using the IEEE 802.1x standard

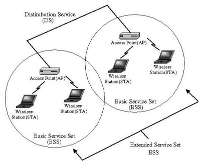
IEEE 802.11 Operating Modes

In IEEE's proposed standard for wireless LANs (IEEE 802.11), there are two different ways to configure a network: ad-hoc and infrastructure.

AD Hoc



Infrastructure



Basic Service Set
An AP forms an association with one or more wireless clients

Extended Service Set
Where additional AP's are added to increase the range and coverage of the wireless network,

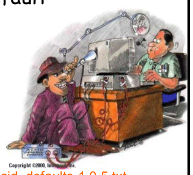
Service Set ID (SSID)

- The Service Set Identifier (SSID), often referred to as a Network Name, is a unique identifier up to 32 characters in length, that is attached to the header of packets sent over a wireless LAN
- The SSID differentiates one wireless LAN from another and was initially provided to give a network a logical name. (e.g. Accounting, finance or public)
- During the initial AP "association" the SSID is past to the AP, in clear text. - if they match then connection is established.
- Can be thought of as a password – but its widely known, travels in clear text, is broadcast periodically by the AP in beacon packets which can be sniffed.

Default Server Set ID (SSID)

- Each make of AP comes with a default SSID.
- Attackers can use these default SSID's to attempt to penetrate AP's that are still in their default configuration.
- Here are some default SSIDs:

"tsunami"	- Cisco
"comcomcom	- 3Com AirConnect
"Compaq"	- Compaq
"WLAN"	- Addtron
"intel"	- Intel
"linksys"	- Linksys



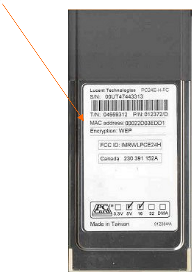
More at www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults/ssid_defaults-1.0.5.txt

- Change the Default SID
- Turn off SSID broadcasting
  - reduces casual observation only
- Don't Turning off Beaconing
  - it creates administrative pain, with no real security benefit
  - common tools can easily crack this level of security

MAC address filtering

- Each WLAN card has a hard coded MAC address
- Can control access by allowing only defined MAC addresses to connect to the network
- Does not scale, as lists of allowed MAC addresses must be compiled, maintained, and distributed to each access point
- Easy to sniff for an allowed address
- Easy to spoof legitimate MAC addresses

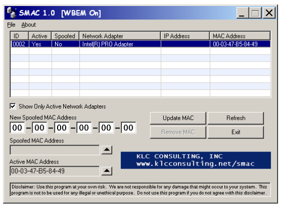
How to find your Mac address


Lucent Technologies PC24E-H-FC
S/N: 00UT47443313
T/N: 04559312 P/N: 012372/D
MAC address: 00022D03EDD1
Encryption: WEP
FCC ID: IMRWLPCE24H
Canada 230 391 152A
PC Card™ □ 3.3V ☑ 5V ☑ 16 □ 32 □ DMA
Made in Taiwan
012384/A

MAC Addresses Can Be Modified

- In Windows 2000 if you have a card that supports Clone MAC address :
  - Go to Start->Settings->Control Panel->Network and Dial-up Connections.
  - Right click on the NIC you want to change the MAC address and click on properties.
  - Under "General" tab, click on the "Configure" button
  - Click on "Advanced" tab
  - Under "Property section", you should see an item called "Network Address" or "Locally Administered Address", click on it.
  - On the right side, under "Value", type in the New MAC address you want to assign to your NIC. Usually this value is entered without the "-" between the MAC address numbers.
  - At command prompt type "ipconfig /all" to verify the changes.
  - If successful, reboot your Windows 2000 system.

Use SMAC to Modify MAC Addresses



ID	Active	Spoofed	Network Adapter	IP Address	MAC Address
0002	Yes	No	Intel(R) PRO Adapter		00-03-47-B5-84-49

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 00 - 00 - 00 - 00 - 00

Spoofed MAC Address:

Active MAC Address: 00-03-47-B5-84-49

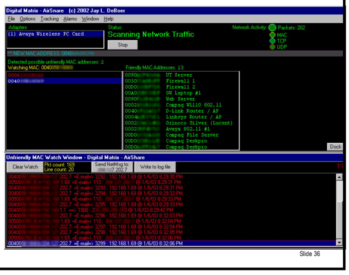
KLC CONSULTING, INC
www.klcconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

- With W2k or XP if you have a card that doesn't support Clone MAC address, use free SMAC GUI tool, which allows users to change MAC address for almost any Network Interface Cards (NIC). http://www.klcconsulting.net/smac/
- In Linux use MAC Changer http://www.alobbs.com/macchanger

AirSnare Wireless IDS

- AirSnare will alert you to unfriendly MAC addresses on your network http://home.attbi.com/~digitalmatrix/airsnare/index.htm
- Alert you to DHCP requests taking place.
- If AirSnare detects an unknown MAC address you have the option of tracking the MAC address's access to IP addresses and ports or by launching Ethereal upon a detection.


Digital Matrix - AirSnare (c) 2002 Jay L. DeBoer
File
Options
Tracking
Alarms
Window
Help
Stop
Dock
Unfriendly MAC Watch Window - Digital Matrix - AirShare
Clear Watch
Write to log file

Adapters: (1) Avaya Wireless PC Card

Status: Scanning Network Traffic

Network Activity: Packets: 202 MAC TCP UDP

*** NEW MAC ADDRESS: 0040[redacted]

Detected possible unfriendly MAC addresses: 2

Watching MAC: 0040[redacted]

```
0006[redacted]
0040[redacted]
```

Friendly MAC Addresses: 13

```
0090[redacted]  UT Server
0050[redacted]  Firewall 1
00D0[redacted]  Firewall 2
00A0[redacted]  GW Laptop #1
0090[redacted]  Web Server
0002[redacted]  Compaq WL110 802.11
0040[redacted]  D-Link Router / AP
0004[redacted]  Linksys Router / AP
0002[redacted]  Orinoco Silver (Lucent)
0002[redacted]  Avaya 802.11 #1
00D0[redacted]  Compaq File Server
00D0[redacted]  Compaq Deskpro
00D0[redacted]  Compaq Deskpro
```

Pkt count: 169
Line count: 20

Send NetMsg to: [redacted]7.202.7

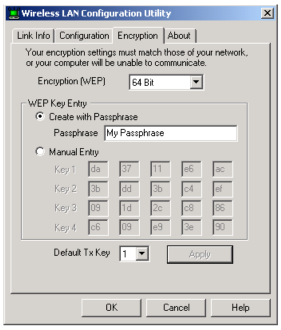
```
00400[redacted]202.7 =E-mail=> 3292 : 192.168.1.69 @ 1/6/03 8:29:30 PM
00500[redacted]1.69 =E-mail=> 110 : [redacted] @ 1/6/03 8:29:31 PM
00400[redacted]202.7 =E-mail=> 3293 : 192.168.1.69 @ 1/6/03 8:29:31 PM
00400[redacted]202.7 =E-mail=> 3294 : 192.168.1.69 @ 1/6/03 8:29:32 PM
00500[redacted]1.69 =E-mail=> 110 : [redacted] @ 1/6/03 8:29:33 PM
00400[redacted]202.7 =E-mail=> 3295 : 192.168.1.69 @ 1/6/03 8:29:33 PM
00400[redacted]1.1 ==> 1900 : 2[redacted]0 @ 1/6/03 8:29:42 PM
00400[redacted]202.7 =E-mail=> 3296 : 192.168.1.69 @ 1/6/03 8:32:03 PM
00500[redacted]1.69 =E-mail=> 110 : [redacted] @ 1/6/03 8:32:04 PM
00400[redacted]202.7 =E-mail=> 3297 : 192.168.1.69 @ 1/6/03 8:32:04 PM
00400[redacted]202.7 =E-mail=> 3298 : 192.168.1.69 @ 1/6/03 8:32:05 PM
00500[redacted]1.69 =E-mail=> 110 : [redacted] @ 1/6/03 8:32:06 PM
00400[redacted]202.7 =E-mail=> 3299 : 192.168.1.69 @ 1/6/03 8:32:06 PM
```

Wired Equivalent Privacy (WEP)

- WEP is a security protocol designed to provide a WLAN with the equivalent level of security as a wired LAN.
- WEP aimed to:
  - Prevent unauthorized access
    - WEP provides a method for devices to authenticate clients to access points
  - Prevent eavesdropping
    - WEP provides 40bit or 128bit keys
  - Prevent alteration of transactions
    - WEP provides a message integrity checksum
- Designed to be computationally efficient, self-synchronizing, and exportable

Slide 37

WEP KEY Entry Example



Wireless LAN Configuration Utility

Your encryption settings must match those of your network, or your computer will be unable to communicate.

Encryption (WEP): 64 Bit

WEP Key Entry

● Create with Passphrase

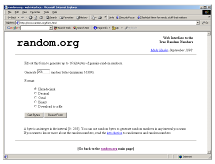
Passphrase: My Passphrase

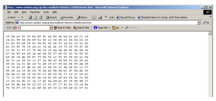
○ Manual Entry

Key 1	da	37	11	e6	ac
Key 2	3b	dd	3b	c4	ef
Key 3	09	1d	2c	c8	86
Key 4	c6	09	e9	3e	90

Default Tx Key: 1

Go to the Random.org website and select Hexadecimal.





Keys are can be selected from this hex block by designating a starting place by row. Manually key into the AP and each laptop

Slide 38

Securing Access Points - Summary

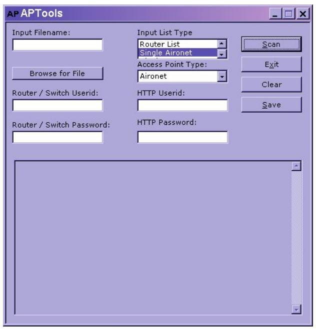
- There are three basic ways to secure wireless access points on a 802.11 network:
  - SSID: Service Set Identifier
    - Identifies a wireless network (a set of access points)
    - LAN adapters need to know SSID in order to access the network, BUT access points broadcast SSID in default configuration
    - Designed for network selection, not security - thwarts casual intruders
  - MAC: Media Access Control Filtering
    - Every 802.11 network card has a unique MAC address
    - Access points can have a list of MAC addresses that they will associate with
    - Impractical to maintain large list of cards - manual process
    - MAC addresses can be spoofed
  - WEP: Wired Equivalency Privacy
    - Encryption key (128 bit max) is manually entered into access points and notebooks
    - Keys must match for client to associate with access point
    - Protects against intrusion - encrypts all traffic
    - All clients in network share the same key
    - "Shared secret" - not a true form of user authentication

Don't forget to change SNMP public and private strings!!

Slide 39

AP Configuration Checker

- Developed and Tested on Cisco Products
- Audits Access Point Settings via HTML
- Does not support SSH.
- Good that its free…



APTools

Input Filename:

Input List Type: Router List / Single Aironet

Access Point Type: Aironet

Router / Switch Userid:

HTTP Userid:

Router / Switch Password:

HTTP Password:

http://aptools.sourceforge.net/

Slide 40

Rogue Access Points

- Network users often set up rogue wireless LANs to simplify their lives
- Rarely implement security measures
- Network is vulnerable to War Driving and sniffing and you may not even know it
- Could be installed by *Bad Actors* for easy access to your internal network
- This is a major risk

Problems with WEP

- WEP is broken…
- Key management is tough and inflexible, and updating keys can be difficult
- All users of a given access point share the same static encryption key
- Data headers remain unencrypted so anyone can see the source and destination of the data stream
- Authentication method provides information to help determine WEP key
- Vulnerable to attack
  - Passive attacks to decrypt traffic based on statistical analysis
  - Active attacks to inject new traffic from unauthorized mobile stations, based on known plaintext
  - Dictionary-building attack that, after analysis of a day's worth of traffic, allows real-time automated decryption of all traffic
- Tools available to automate attacks and crack WEP

Slide 42

WEP Attack Tools

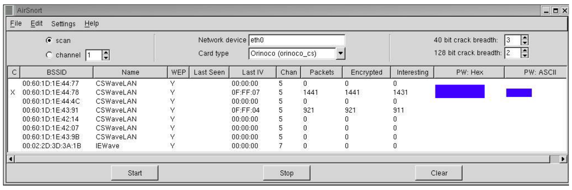
- Airsnort.
  - Listens in real time and brute forces the WEP key when enough packets have been gathered.

  http://freshmeat.net/projects/airsnort/
- WEPCrack.
  - Used against captured data.
  - Written in Perl

  http://sourceforge.net/projects/wepcrack
- Decrypt
  - Used to decrypt captured data once WEP key has been obtained.

  http://sourceforge.net/projects/airsnort

Airsnort



● scan
○ channel 1

Network device eth0
Card type Orinoco (orinoco_cs)

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASCII
	00:60:1D:1E:44:77	CSWaveLAN	Y		00:00:00	5	0	0	0		
X	00:60:1D:1E:44:78	CSWaveLAN	Y		0F:FF:07	5	1441	1441	1431		
	00:60:1D:1E:44:4C	CSWaveLAN	Y		00:00:00	5	0	0	0		
	00:60:1D:1E:43:91	CSWaveLAN	Y		0F:FF:04	5	921	921	911		
	00:60:1D:1E:42:14	CSWaveLAN	Y		00:00:00	5	0	0	0		
	00:60:1D:1E:42:07	CSWaveLAN	Y		00:00:00	5	0	0	0		
	00:60:1D:1E:43:9B	CSWaveLAN	Y		00:00:00	5	0	0	0		
	00:02:2D:3D:3A:1B	IEWave	Y		00:00:00	7	0	0	0		

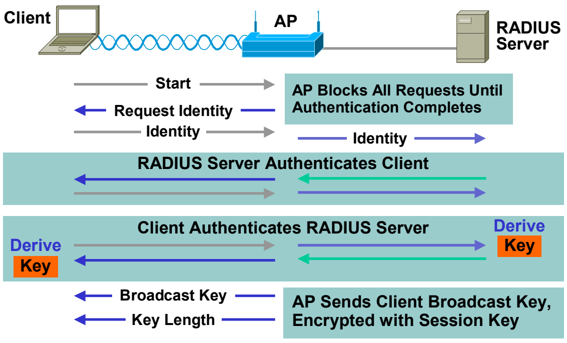
Airsnort is tool which cracks encryption keys on 802.11b WEP networks.

AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

Augmenting WEP

- Since WEP by itself is insufficient to secure a wireless network, additional security mechanisms are required
- Need dynamic, per-user, per-session WEP keys
- 802.11i provides dynamic key management
- Extensible Authentication Protocol (EAP)
  - Currently available from CISCO (LEAP)
  - Built into Windows XP

LEAP Authentication Process



Client

AP

RADIUS Server

Start

Request Identity

Identity

AP Blocks All Requests Until Authentication Completes

Identity

RADIUS Server Authenticates Client

Client Authenticates RADIUS Server

Derive Key

Derive Key

Broadcast Key

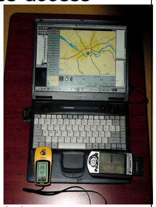
Key Length

AP Sends Client Broadcast Key, Encrypted with Session Key

Wardriving

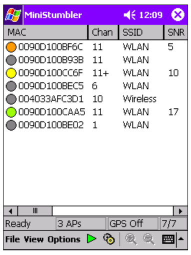
- WarDriving: Locating and logging wireless access points while in motion
- Necessary Equipment:
  - Laptop Computer - At least a Pentium100 with a free PCMCIA slot and serial port for GPS.
  - 802.11b-compliant wireless Ethernet card card
  - The Software, Linux, BSD, Windows, Mac
  - List of default SSID's and passwords

    www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults/
  - Optional: GPS receiver for location tracking.
  - A way to get around, a car, bus, subway, walking, bike.
- While you drive attack software listens and builds map of all 802.11 networks found
- To find closed access points you need a sniffing tool



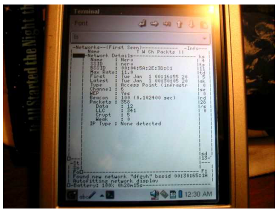
Wardriving HOW TO http://www.wardriving.com/doc/Wardriving-HOWTO.txt

Wardriving – Who needs a laptop



MAC	Chan	SSID	SNR
0090D100BF6C	11	WLAN	5
0090D100B93B	11	WLAN	
0090D100CC6F	11+	WLAN	10
0090D100BEC5	6	WLAN	
004033AFC3D1	10	Wireless	
0090D100CAA5	11	WLAN	17
0090D100BE02	1	WLAN	

Ready | 3 APs | GPS Off | 7/7



Wireless scanning and the law

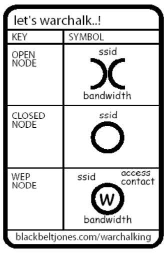
A recent FBI advisory states that wireless network discovery is not illegal in itself.

> *"Identifying the presence of a wireless network may not be a criminal violation, however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations."*

http://www.politechbot.com/p-03884.html

War Chalking – What is it?

- War Chalking is the practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access.
- Was developed to help Wi-Fi users find wireless access points - good or bad
- It was inspired by the practice of hobos during the Great Depression to use chalk marks to indicate which homes were friendly.



let's warchalk..!

KEY	SYMBOL
OPEN NODE	ssid)(bandwidth
CLOSED NODE	ssid ○
WEP NODE	ssid access contact Ⓦ bandwidth

blackbeltjones.com/warchalking

http://www.warchalking.org/

Wireless Access Point Discovery Software

- NetStumbler/MiniStumbler: www.netstumbler.org
  - Platforms: Win9x, Win2K, WinXP.
  - Cards: PRISM2
- ISS Wireless Scanner: www.iss.net
  - Platforms: Win2K
  - Cards: Hermes (Lucent/Agere/Orinoco Gold, Compaq WL110)
- BSD AirTools: www.dachb0den.com
  - Platform: FreeBSD, OpenBSD, NetBSD
  - Cards: PRISM2
- Airopeek: www.wildpackets.com
  - Platforms: Win2K, WinNT4, 95, 98, ME
  - Cards: Numerous
- Aerosol: www.sec33.com/sniph/aerosol.php
  - Platforms: Win2K
  - Cards: PRISM 2

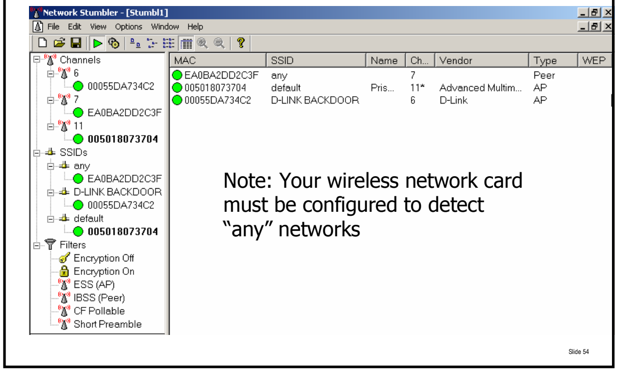
Wireless Access Point Discovery Software

- Wavestumbler: www.cqure.net/wavestumbler
  - Platforms: Linux
  - Cards: Hermes
- gtk-scanner: www.sourceforge.net/projects/wavelan-tools/
  - Platforms: Linux
  - Cards: Hermes
- Perlskan: www.sourceforge.net/projects/wavelan-tools/
  - Platforms: Linux (PERL)
  - Cards: Hermes
- ApTools: www.aptools.sourceforge.net
  - Platforms: Win2K, Solaris 8, FreeBSD?
  - Cards: Detects access points from wired ethernet lan
- Wellenreiter: www.remote-exploit.org
  - Platforms: Linux
  - Cards: Hermes

Wireless Access Point Discovery Software

- Kismet: www.kismetwireless.net
  - Platform: Linux
  - Cards: Hermes
- Freestumble: www.uix.com/freestumble/
  - Platforms: FreeBSD
  - Cards: Hermes
- THC-Wardrive/THC-Rut: www.thehackerschoice.com
  - Platforms: Linux
  - Cards: Hermes

Locating Wireless Access Points: NetStumbler

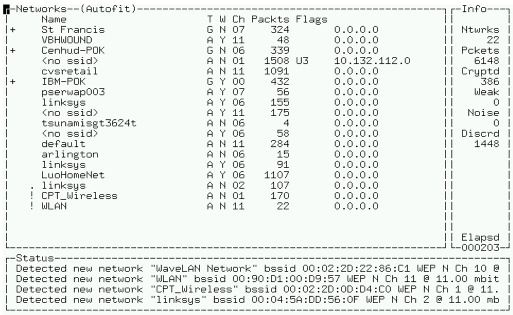


```
Channels
  6
    00055DA734C2
  7
    EA0BA2DD2C3F
  11
    005018073704
SSIDs
  any
    EA0BA2DD2C3F
  D-LINK BACKDOOR
    00055DA734C2
  default
    005018073704
Filters
  Encryption Off
  Encryption On
  ESS (AP)
  IBSS (Peer)
  CF Pollable
  Short Preamble
```

MAC	SSID	Name	Ch...	Vendor	Type	WEP
EA0BA2DD2C3F	any		7		Peer	
005018073704	default	Pris...	11*	Advanced Multim...	AP	
00055DA734C2	D-LINK BACKDOOR		6	D-Link	AP	

Note: Your wireless network card must be configured to detect "any" networks

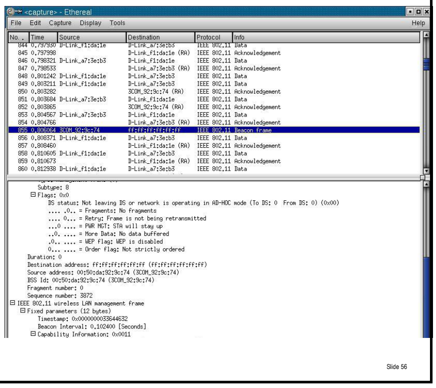
Locating Wireless Access Points: Kismet



```
┌-Networks--(Autofit)------------------------------------------------┐┌-Info---┐
|       Name                    T W Ch Packts Flags                   ||        |
|+      St Francis              G N 07    324        0.0.0.0          || Ntwrks |
|       VBHWOUND                A Y 11     48        0.0.0.0          ||     22 |
|+      Cenhud-POK              G N 06    339        0.0.0.0          || Pckets |
|       <no ssid>               A N 01   1508 U3     10.132.112.0     ||   6148 |
|       cvsretail               A N 11   1091        0.0.0.0          || Cryptd |
|+      IBM-POK                 G Y 00    432        0.0.0.0          ||    386 |
|       pserwap003              A Y 07     56        0.0.0.0          ||   Weak |
|       linksys                 A Y 06    155        0.0.0.0          ||      0 |
|       <no ssid>               A Y 11    175        0.0.0.0          ||  Noise |
|       tsunamisgt3624t         A N 06      4        0.0.0.0          ||      0 |
|       <no ssid>               A Y 06     58        0.0.0.0          || Discrd |
|       default                 A N 11    284        0.0.0.0          ||   1448 |
|       arlington               A N 06     15        0.0.0.0          ||        |
|       linksys                 A Y 06     91        0.0.0.0          ||        |
|       LuoHomeNet              A Y 06   1107        0.0.0.0          ||        |
|     . linksys                 A N 02    107        0.0.0.0          ||        |
|     ! CPT_Wireless            A N 01    170        0.0.0.0          ||        |
|     ! WLAN                    A N 11     22        0.0.0.0          ||        |
|                                                                    ||        |
|                                                                    ||        |
|                                                                    || Elapsd |
└--------------------------------------------------------------------┘└-000203-┘
┌-Status-----------------------------------------------------------------------┐
| Detected new network "WaveLAN Network" bssid 00:02:2D:22:86:C1 WEP N Ch 10 @ |
| Detected new network "WLAN" bssid 00:90:D1:00:D9:57 WEP N Ch 11 @ 11.00 mbit |
| Detected new network "CPT_Wireless" bssid 00:02:2D:0D:D4:C0 WEP N Ch 1 @ 11. |
| Detected new network "linksys" bssid 00:04:5A:DD:56:0F WEP N Ch 2 @ 11.00 mb |
└------------------------------------------------------------------------------┘
```

Ethereal

Captures Data "off the wire" from a live network connection, or read from a capture file.

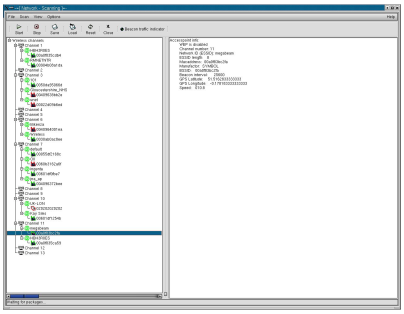


```
No. . Time     Source            Destination            Protocol     Info
844 0.797930 D-Link_f1:da:1e   D-Link_a7:3e:b3        IEEE 802.11  Data
845 0.797998                   D-Link_f1:da:1e (RA)   IEEE 802.11  Acknowledgement
846 0.798321 D-Link_a7:3e:b3   D-Link_f1:da:1e        IEEE 802.11  Data
847 0.798533                   D-Link_a7:3e:b3 (RA)   IEEE 802.11  Acknowledgement
848 0.801242 D-Link_f1:da:1e   D-Link_a7:3e:b3        IEEE 802.11  Data
849 0.803211 D-Link_f1:da:1e   D-Link_a7:3e:b3        IEEE 802.11  Data
850 0.803282                   3COM_92:9c:74 (RA)     IEEE 802.11  Acknowledgement
851 0.803684 D-Link_a7:3e:b3   D-Link_f1:da:1e        IEEE 802.11  Data
852 0.803865                   3COM_92:9c:74 (RA)     IEEE 802.11  Acknowledgement
853 0.804567 D-Link_a7:3e:b3   D-Link_f1:da:1e        IEEE 802.11  Data
854 0.804766                   D-Link_a7:3e:b3 (RA)   IEEE 802.11  Acknowledgement
855 0.806064 3COM_92:9c:74     ff:ff:ff:ff:ff:ff      IEEE 802.11  Beacon frame
856 0.808371 D-Link_f1:da:1e   D-Link_a7:3e:b3        IEEE 802.11  Data
857 0.808460                   D-Link_f1:da:1e (RA)   IEEE 802.11  Acknowledgement
858 0.810605 D-Link_f1:da:1e   D-Link_a7:3e:b3        IEEE 802.11  Data
859 0.810673                   D-Link_f1:da:1e (RA)   IEEE 802.11  Acknowledgement
860 0.812938 D-Link_f1:da:1e   D-Link_a7:3e:b3        IEEE 802.11  Data
```

```
      Subtype: 8
    ⊟ Flags: 0x0
        DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0  From DS: 0) (0x00)
        .... .0.. = Fragments: No fragments
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = WEP flag: WEP is disabled
        0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:50:da:92:9c:74 (3COM_92:9c:74)
    BSS Id: 00:50:da:92:9c:74 (3COM_92:9c:74)
    Fragment number: 0
    Sequence number: 3872
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (12 bytes)
      Timestamp: 0x000000003364632
      Beacon Interval: 0.102400 [Seconds]
    ⊟ Capability Information: 0x0011
```

Wellenreiter

- Audits 802.11b networks.
- Linux & Perl
- You can view details about the consistency and signal strength of the network.
- Its scanner window can be used to discover access-points, networks, and ad-hoc cards.
- Records the network location with GPS support.



```
Wireless channels
  Channel 1
    HBH3R0ES
      00a0f835cdb4
    RMNETNTR
      00904b08a1da
  Channel 2
  Channel 3
    101
      0050da95066d
    Gloucestershire_NHS
      00409638bb2e
    unet
      00022d09b6ed
  Channel 4
  Channel 5
  Channel 6
    lilikenza
      0040964001ea
    Wireless
      0030ab0ac8ee
  Channel 7
    default
      00055df2168c
    OII
      0060b3162a6f
    ingenta
      00601df0fbe7
    jna_ap
      004096372bee
  Channel 8
  Channel 9
  Channel 10
    UK-LON
      020202020202
    Kay Sims
      00601df1254b
  Channel 11
    megabeam
      00a0f83bc2fa
    HBH3R0ES
      00a0f835ca59
  Channel 12
  Channel 13
```

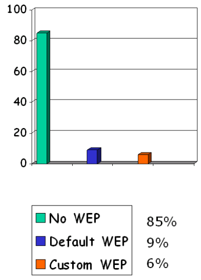
```
Accesspoint info:
    WEP is disabled
    Channel number: 11
    Network ID (ESSID): megabeam
    ESSID length:  8
    Macaddress:  00a0f83bc2fa
    Manufactor:  SYMBOL
    BSSID:   00a0f83bc2fa
    Beacon interval:     25600
    GPS Latitude:    51.5162833333333
    GPS Longitude:   -0.178183333333333
    Speed:   010.8
```

Waiting for packages...

War Driving in London

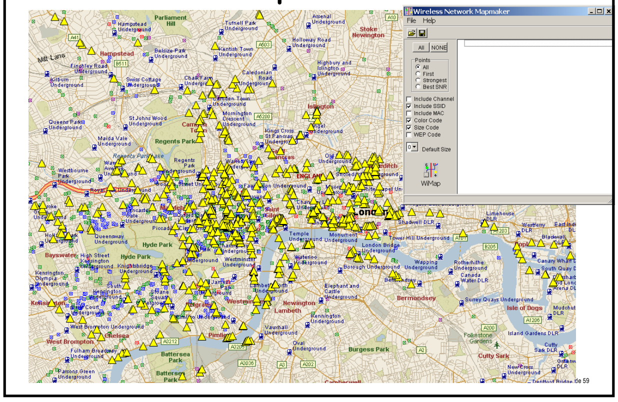
WEP utilisation is patchy

- 260 access points found in one evening. 5000 over a period of 6 months
- 85% had no WEP encryption
- 9% used default WEP encryption keys.
- Only 6% were found to be using non standard default WEP encryption keys
- About 25% used manufacturer's default SSID
- Similar to results from other cities available on the Web



Wireless Audit Map - London

wirelessaudit.co.uk



Key security issues affecting 802.11b wireless LANs

- Radio interference
  - Malicious radio jamming
  - Radio interference from other wireless networks
  - Radio interference from other sources
- Radio propagation
  - Interception of data in transit
- Wired Equivalent Privacy (WEP) weaknesses
  - WEP not enabled
  - Inadequate encryption
  - Lack of WEP key management
- Poor network address management
  - Disclosure of the network name (SSID)
  - Connection not limited to identified client computers
- Lack of user authentication
  - No integrated user authentication functionality
- Unauthorised or inappropriate hardware implementation
  - Installation of rogue Access Points
  - Poor placement of Access Points
  - Poor interoperability of wireless networking equipment
- Client computer attacks
  - Client-to-client computer attack
  - Connection to a cloned Access Point
  - Loss or theft of a client computer with wireless Network Interface Card

INFORMATION SECURITY FORUM

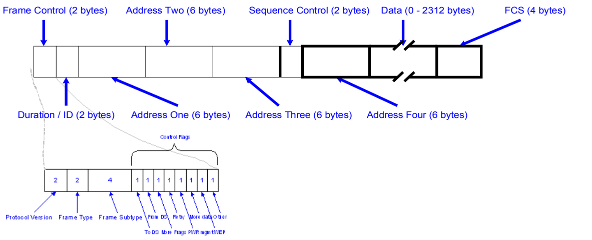
To Recap

- Wireless Networks can be secured if the AP's are correctly configured.
- Main risks are:
  - Wrongly configured AP's
  - Rogue AP's
  - Weak Encryption

Wireless Tool

- What we needed was a centrally managed automated tool that:
  - Passively monitors wireless traffic
  - Verifies that wireless access points are secure
  - Identifies unauthorised (rogue) AP's
  - Identifies when the wireless network is being attacked (Wireless IDS)
  - Helps you manage Wireless Networks
  - Reports to central management console
- Nothing this extensive in the market – so we worked with small local company to develop one

802.11 Frame Layout



00 - Management Frame Type

0000 - association request
0001 - association response
0010 - reassociation request
0011 - reassociation response
0100 - probe request
0101 - probe response
1000 - beacon
1010 - disassociation
1011 - authentication
1100 - deauthentication

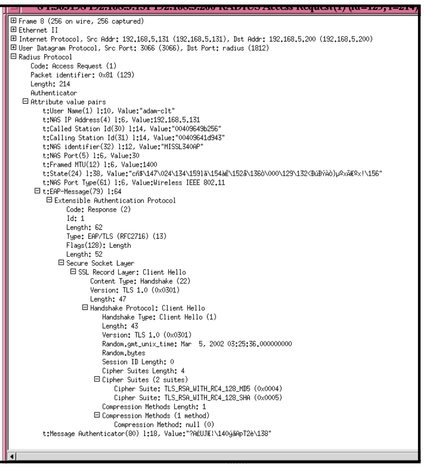
01 - Control Frame Type

1010 - power save poll
1011 - RTS
1100 - CTS
1101 - ACK
1110 - CF-end
1111 - CF-end + CF-ACK

10 - Data Frame Type

0000 - data
0001 - data + CF-ACK
0010 - data + CF-poll
0011 - data + CF-ACK + CF-poll
0100 - NULL (no data)
0101 - CF-ACK (no data)
0110 - CF-poll (no data)
0111 - CF-ACK + CF-poll (no data)

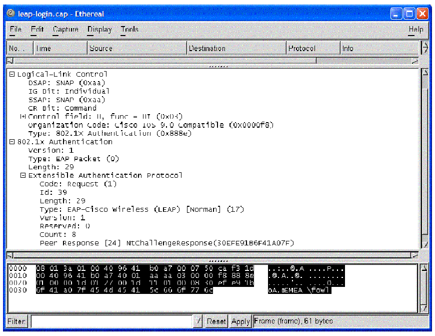
Lots of Info you can use in a Management Tool



```
61.365158 192.168.5.131 192.168.5.200 RADIUS Access Request(1) (id=129, l=214)
⊞ Frame 8 (256 on wire, 256 captured)
⊞ Ethernet II
⊞ Internet Protocol, Src Addr: 192.168.5.131 (192.168.5.131), Dst Addr: 192.168.5.200 (192.168.5.200)
⊞ User Datagram Protocol, Src Port: 3066 (3066), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access Request (1)
    Packet identifier: 0x81 (129)
    Length: 214
    Authenticator
  ⊟ Attribute value pairs
      t:User Name(1) l:10, Value:"adam-clt"
      t:NAS IP Address(4) l:6, Value:192.168.5.131
      t:Called Station Id(30) l:14, Value:"00409649b256"
      t:Calling Station Id(31) l:14, Value:"00409641d943"
      t:NAS identifier(32) l:12, Value:"MISSL340AP"
      t:NAS Port(5) l:6, Value:30
      t:Framed MTU(12) l:6, Value:1400
      t:State(24) l:38, Value:"cñ$\147\024\134\159lä\154àÊ\152å\136ò\000\129\132<ÐúÐÝÀò)µºxÄÆºx!\156"
      t:NAS Port Type(61) l:6, Value:Wireless IEEE 802.11
    ⊟ t:EAP-Message(79) l:64
      ⊟ Extensible Authentication Protocol
          Code: Response (2)
          Id: 1
          Length: 62
          Type: EAP/TLS (RFC2716) (13)
          Flags(128): Length
          Length: 52
        ⊟ Secure Socket Layer
          ⊟ SSL Record Layer: Client Hello
              Content Type: Handshake (22)
              Version: TLS 1.0 (0x0301)
              Length: 47
            ⊟ Handshake Protocol: Client Hello
                Handshake Type: Client Hello (1)
                Length: 43
                Version: TLS 1.0 (0x0301)
                Random.gmt_unix_time: Mar  5, 2002 03:25:36.000000000
                Random.bytes
                Session ID Length: 0
                Cipher Suites Length: 4
              ⊟ Cipher Suites (2 suites)
                  Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
                  Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
                Compression Methods Length: 1
              ⊟ Compression Methods (1 method)
                  Compression Method: null (0)
      t:Message Authenticator(80) l:18, Value:"?AÉUJÆ¦\140ýãApT2è\138"
```

Capture of Leap Login

Capture of Leap packets could be used to authenticate MAC address



```
⊟ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  ⊞ Control field: U, func = UI (0x03)
    Organization Code: Cisco IOS 9.0 Compatible (0x0000f8)
    Type: 802.1X Authentication (0x888e)
⊟ 802.1x Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 29
  ⊟ Extensible Authentication Protocol
      Code: Request (1)
      Id: 39
      Length: 29
      Type: EAP-Cisco Wireless (LEAP) [Norman] (17)
      Version: 1
      Reserved: 0
      Count: 8
      Peer Response [24] NtChallengeResponse(30EFE91B6F41A07F)

0000  08 01 3a 01 00 40 96 41  b0 a7 00 07 50 ca f3 1d   ..:..@.A ....P...
0010  00 40 96 41 b0 a7 40 01  aa aa 03 00 00 f8 88 8e   .@.A..@. ........
0020  01 00 00 1d 01 27 00 1d  11 01 00 08 30 ef e9 1b   .....'.. ....0...
0030  6f 41 a0 7f 45 4d 45 41  5c 66 6f 77 6c            oA..EMEA \fowl
```

Frame (frame), 61 bytes

Isomair Wireless Sentry^{TM}

isomair
security for a wireless world

- A small appliance which:
  - Continually Monitors your Air Space
  - Supports 802.11b today and 802.11a in future
  - On-Air Auditing, real-time 24 hour - no more walkabouts
  - On-Air automatic wireless intrusion detection (IDS)
  - On-Air performance monitoring
  - On-Air fault finding
  - On-Air packet capture – anywhere, anytime.
  - Platform for future wireless security and managemen functionality

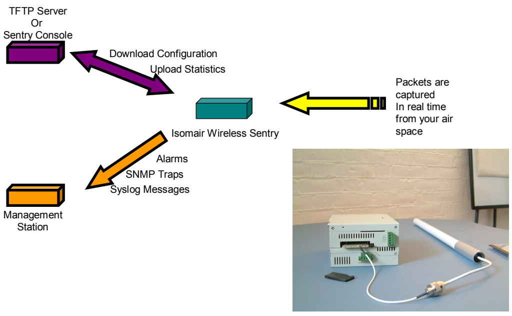
- Low unit costs permits corporate-wide deployment
- Patented

So What does it do?

- Discovers ALL new devices – access points, stations, print servers – permanently - 24 hours a day
- Discovers Infrastructure AND ad-hoc mode networks
- Discovers NON-WEP configurations and identifies insecure access points and stations
- Intrusion Detection – watches for 802.11b specific anomalous traffic patterns. NOT an Ethernet packet filter, but a purpose-built Wireless IDS
- Finds potential Denial of Service attacks automatically
- Finds ANY device using a manufacturer default SSID
- Finds faulty or failing stations BEFORE they call your helpdesk
- Finds Signal and Noise quality issues automatically
- Finds Low Transmit Speed situations instantly
- Finds Wireless Hot Spots automatically
- Finds over-utilised or congested Wireless LANs automatically
- Does remote real-time packet capture – capture any conversation off the air anywhere !

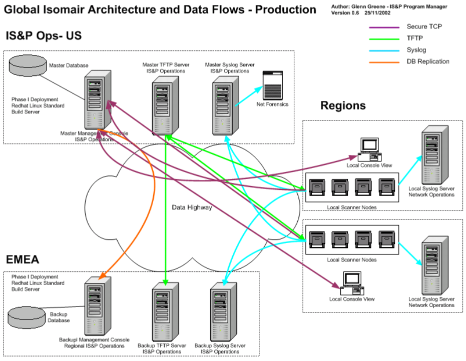
Slide 67

Wireless Sentry Information Flows



Slide 68

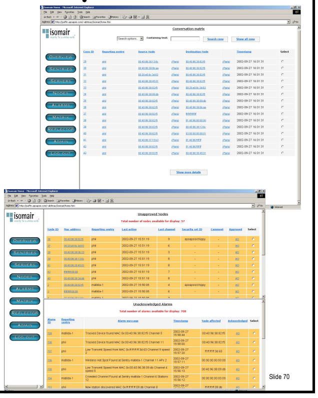
Isomair Architecture



Slide 69

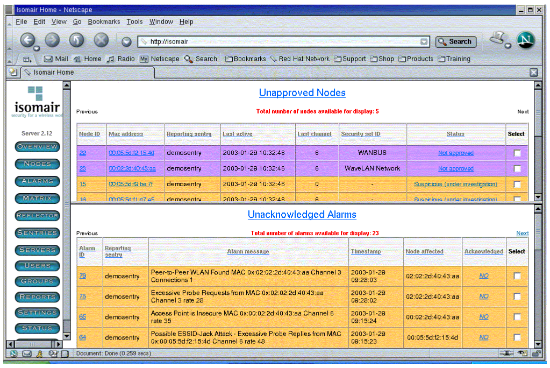
Isomair Wireless Sentry Console

- Web based multi-user console system
- Sentry -> Sentry-TCP -> SQL database -> Sentry Console Web interface
- Consolidated industry standard SQL database back-end
- Software product, runs on RedHat Linux and Sun Solaris.
- Interactive management features - Approve nodes, Acknowledge alarms
- Search and view alarms & database for station information, browse.
- Track user ownership and details of wireless stations
- Automatic management of Sentry devices



Slide 70

London Wardrive Jan 29th 2003


Isomair Home - Netscape
File Edit View Go Bookmarks Tools Window Help
http://isomair
Search
Mail Home Radio Netscape Search Bookmarks Red Hat Network Support Shop Products Training
Isomair Home
isomair
security for a wireless wor
Server 2.12
OVERVIEW
NODES
ALARMS
MATRIX
REFLECTOR
SENTRIES
SERVERS
USERS
GROUPS
REPORTS
SETTINGS
STATUS

Unapproved Nodes

Previous

Total number of nodes available for display: 5

Next

Node ID	Mac address	Reporting sentry	Last active	Last channel	Security set ID	Status	Select
22	00:05:5d:f2:15:4d	demosentry	2003-01-29 10:32:46	6	WANBUS	Not approved	□
23	00:02:2d:40:43:aa	demosentry	2003-01-29 10:32:46	6	WaveLAN Network	Not approved	□
15	00:05:5d:f9:be:7f	demosentry	2003-01-29 10:32:46	0	-	Suspicious (under investigation)	□
16	00:05:5d:f1:d7:e5	demosentry	2003-01-29 10:32:46	6	-	Suspicious (under investigation)	□

Unacknowledged Alarms

Previous

Total number of alarms available for display: 23

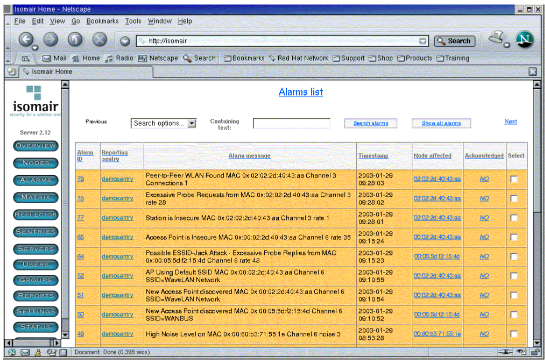
Next

Alarm ID	Reporting sentry	Alarm message	Timestamp	Node affected	Acknowledged	Select
79	demosentry	Peer-to-Peer WLAN Found MAC 0x:02:02:2d:40:43:aa Channel 3 Connections 1	2003-01-29 09:28:03	02:02:2d:40:43:aa	NO	□
78	demosentry	Excessive Probe Requests from MAC 0x:02:02:2d:40:43:aa Channel 3 rate 28	2003-01-29 09:28:02	02:02:2d:40:43:aa	NO	□
65	demosentry	Access Point is Insecure MAC 0x:00:02:2d:40:43:aa Channel 6 rate 35	2003-01-29 09:15:24	00:02:2d:40:43:aa	NO	□
64	demosentry	Possible ESSID-Jack Attack - Excessive Probe Replies from MAC 0x:00:05:5d:f2:15:4d Channel 6 rate 48	2003-01-29 09:15:23	00:05:5d:f2:15:4d	NO	□

Document: Done (0.259 secs)

Slide 71

London Wardrive Jan 29th 2003



Alarms list

Previous

Containing text:

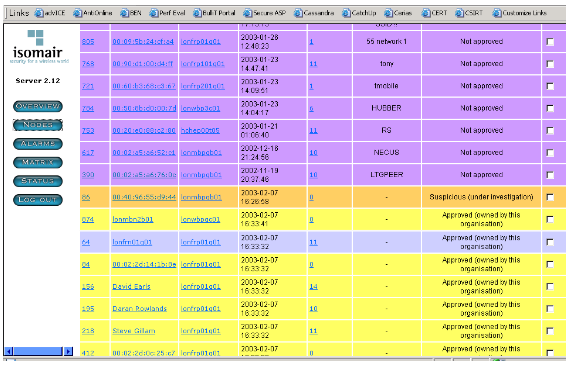
Next

Alarm ID	Reporting sentry	Alarm message	Timestamp	Node affected	Acknowledged	Select
79	demosentry	Peer-to-Peer WLAN Found MAC 0x:02:02:2d:40:43:aa Channel 3 Connections 1	2003-01-29 09:28:03	02:02:2d:40:43:aa	NO	□
78	demosentry	Excessive Probe Requests from MAC 0x:02:02:2d:40:43:aa Channel 3 rate 28	2003-01-29 09:28:02	02:02:2d:40:43:aa	NO	□
77	demosentry	Station is Insecure MAC 0x:02:02:2d:40:43:aa Channel 3 rate 1	2003-01-29 09:28:01	02:02:2d:40:43:aa	NO	□
65	demosentry	Access Point is Insecure MAC 0x:00:02:2d:40:43:aa Channel 6 rate 35	2003-01-29 09:15:24	00:02:2d:40:43:aa	NO	□
64	demosentry	Possible ESSID-Jack Attack - Excessive Probe Replies from MAC 0x:00:05:5d:f2:15:4d Channel 6 rate 48	2003-01-29 09:15:23	00:05:5d:f2:15:4d	NO	□
52	demosentry	AP Using Default SSID MAC 0x:00:02:2d:40:43:aa Channel 6 SSID=WaveLAN Network	2003-01-29 09:10:55	00:02:2d:40:43:aa	NO	□
51	demosentry	New Access Point discovered MAC 0x:00:02:2d:40:43:aa Channel 6 SSID=WaveLAN Network	2003-01-29 09:10:54	00:02:2d:40:43:aa	NO	□
50	demosentry	New Access Point discovered MAC 0x:00:05:5d:f2:15:4d Channel 6 SSID=WANBUS	2003-01-29 09:10:52	00:05:5d:f2:15:4d	NO	□
49	demosentry	High Noise Level on MAC 0x:00:60:b3:71:55:1e Channel 6 noise 3	2003-01-29 08:53:28	00:60:b3:71:55:1e	NO	□

Document: Done (0.398 secs)

Slide 72

Automated MAC Address Checking



Links advICE AntiOnline BEN Perf Eval BulliT Portal Secure ASP Cassandra CatchUp Cerias CERT CSIRT Customize Links

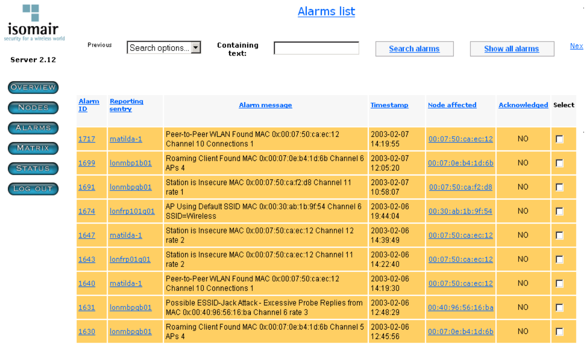
isomair
security for a wireless world

Server 2.12

OVERVIEW
NODES
ALARMS
MATRIX
STATUS
LOG OUT

805	00:09:5b:24:cf:a4	lonfrp01q01	2003-01-26 12:48:23	1	55 network 1	Not approved	□
768	00:90:d1:00:d4:ff	lonfrp101q01	2003-01-23 14:47:41	11	tony	Not approved	□
721	00:60:b3:68:c3:67	lonfrp201q01	2003-01-23 14:09:51	1	tmobile	Not approved	□
784	00:50:8b:d0:00:7d	lonwbp3c01	2003-01-23 14:04:17	6	HUBBER	Not approved	□
753	00:20:e0:88:c2:80	hchep00t05	2003-01-21 01:06:40	11	RS	Not approved	□
617	00:02:a5:a6:52:c1	lonmbpqb01	2002-12-16 21:24:56	10	NECUS	Not approved	□
390	00:02:a5:a6:76:0c	lonmbpqb01	2002-11-19 20:37:46	10	LTGPEER	Not approved	□
86	00:40:96:55:d9:44	lonmbpqb01	2003-02-07 16:26:58	0	-	Suspicious (under investigation)	□
874	lonmbn2b01	lonwbpqc01	2003-02-07 16:33:41	0	-	Approved (owned by this organisation)	□
64	lonfrn01q01	lonfrp01q01	2003-02-07 16:33:32	11	-	Approved (owned by this organisation)	□
84	00:02:2d:14:1b:8e	lonfrp01q01	2003-02-07 16:33:32	0	-	Approved (owned by this organisation)	□
156	David Earls	lonfrp01q01	2003-02-07 16:33:32	14	-	Approved (owned by this organisation)	□
195	Daran Rowlands	lonfrp01q01	2003-02-07 16:33:32	10	-	Approved (owned by this organisation)	□
218	Steve Gillam	lonfrp01q01	2003-02-07 16:33:32	11	-	Approved (owned by this organisation)	□
412	00:02:2d:0c:25:c7	lonfrp01q01	2003-02-07	0	-	Approved (owned by this	□

Alarm List



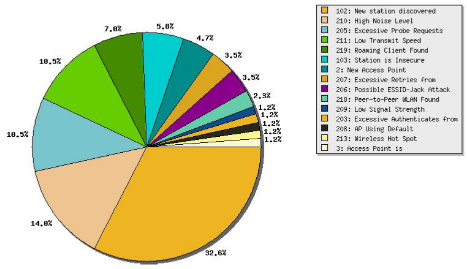
Server 2.12

Alarms list

Alarm ID	Reporting sentry	Alarm message	Timestamp	Node affected	Acknowledged	Select
1717	matilda-1	Peer-to-Peer WLAN Found MAC 0x:00:07:50:ca:ec:12 Channel 10 Connections 1	2003-02-07 14:19:55	00:07:50:ca:ec:12	NO	□
1699	lonmbp1b01	Roaming Client Found MAC 0x:00:07:0e:b4:1d:6b Channel 6 APs 4	2003-02-07 12:05:20	00:07:0e:b4:1d:6b	NO	□
1691	lonmbpqb01	Station is Insecure MAC 0x:00:07:50:ca:f2:d8 Channel 11 rate 1	2003-02-07 10:58:07	00:07:50:ca:f2:d8	NO	□
1674	lonfrp101q01	AP Using Default SSID MAC 0x:00:30:ab:1b:9f:54 Channel 6 SSID=Wireless	2003-02-06 19:44:04	00:30:ab:1b:9f:54	NO	□
1647	matilda-1	Station is Insecure MAC 0x:00:07:50:ca:ec:12 Channel 12 rate 2	2003-02-06 14:39:49	00:07:50:ca:ec:12	NO	□
1643	lonfrp01q01	Station is Insecure MAC 0x:00:07:50:ca:ec:12 Channel 11 rate 2	2003-02-06 14:22:40	00:07:50:ca:ec:12	NO	□
1640	matilda-1	Peer-to-Peer WLAN Found MAC 0x:00:07:50:ca:ec:12 Channel 10 Connections 1	2003-02-06 14:19:30	00:07:50:ca:ec:12	NO	□
1631	lonmbpqb01	Possible ESSID-Jack Attack - Excessive Probe Replies from MAC 0x:00:40:96:56:16:ba Channel 6 rate 3	2003-02-06 12:48:29	00:40:96:56:16:ba	NO	□
1630	lonmbpqb01	Roaming Client Found MAC 0x:00:07:0e:b4:1d:6b Channel 5 APs 4	2003-02-06 12:45:56	00:07:0e:b4:1d:6b	NO	□

London Wardrive Overview

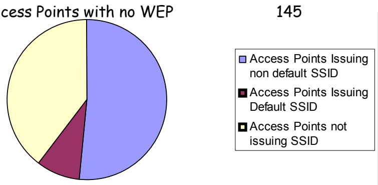
Isomair Wireless Sentry Alerts



London Wardrive Overview

SSID/WEP Breakdown

Access Points Issuing non default SSID	114
Access Points Issuing Default SSID	20
Access Points not issuing SSID	88
Access Points with WEP	77
Access Points with Default WEP	52
Access Points with no WEP	145



Merrill Lynch
Wireless LAN –Top Tips

KPMG

isomair
security for a wireless world

Merrill Lynch

Top Tips - Introduction

- This document contains guidelines for the secure configuration of an 802.11 wireless LAN
- Although the guide is designed to be simple, brief and straight forward, it has been designed for a more technical audience, so end-users may require further explanation.
- This document was written jointly by Merrill Lynch, Isomair and KPMG

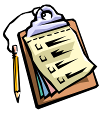
KPMG

isomair
security for a wireless world

Merrill Lynch

Top Tips - Overview

Tip 1 Avoid Unnecessary Signal Leaks
Tip 2 Disable Broadcast SSID
Tip 3 Change Access Points default settings
Tip 4 Use Extensible Authentication Protocol (EAP) Encryption
Tip 5 Segregate WLAN Connections
Tip 6 Monitor Your Environment
Tip 7 Review WLAN System and security logs
Tip 8 Prepare for Incident Response
Tip 9 Harden Laptops
Tip 10 Know the common flaws



Tip 1

Avoid Unnecessary Signal Leaks

Tip

Locate Access Points in the middle of the building, use directional antenna and reduced access point's signal strength to reduce signal leakage outside of the building.

Why

Standard wireless equipment can transmit a useable signal that exceeds the perimeter of a typical building. Depending on the location, this can encourage detection of the network and promote its unauthorized use.

Impact

This ease-to-achieve, low cost obfuscation technique, called RF signal shaping, reduces the risk of unauthorized access (but does not eliminate it).

Tip 2

Disable Broadcast SSID

Tip

Don't allow Broadcast SSID connections.

Why

A wireless client, that doesn't know the correct SSID can determine all the networks in an area by actively scanning for AP's by sending out broadcast Probe Request messages with a Zero or Null SSID. By default, many 802.11 Access Points send out their SSID when probed in this manner - allowing hackers to connect even if they do not know the name of the network.

Impact

This change of configuration costs nothing but will only deter the casual War-drivers and hackers. Hackers can discover the network name with a packet sniffer.

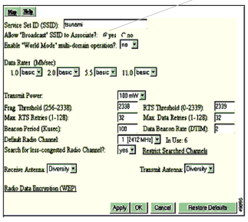
To further obscure your network AP Beaconing can also be switched off. However, if both Beaconing and Broadcast SSID are disabled your AP will become cloaked which can make it difficult to administer and use.

Tip 2

Disable Broadcast SSID - more detail

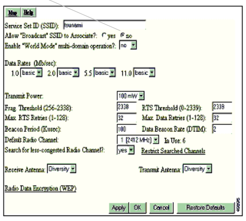
Screen shot from the Cisco Aeronet manager shows:

Automatic Association with the Broadcast SSID or ANY SSID should be disabled



Service Set ID (SSID): tsunami
Allow "Broadcast" SSID to Associate?: ● yes ○ no
Enable "World Mode" multi-domain operation?: no
Data Rates (Mb/sec): 1.0 basic 2.0 basic 5.5 basic 11.0 basic
Transmit Power: 100 mW
Frag. Threshold (256-2338): 2338 RTS Threshold (0-2339): 2339
Max. RTS Retries (1-128): 32 Max. Data Retries (1-128): 32
Beacon Period (Kusec): 100 Data Beacon Rate (DTIM): 2
Default Radio Channel: 1 [2412 MHz] In Use: 6
Search for less-congested Radio Channel?: yes Restrict Searched Channels
Receive Antenna: Diversity Transmit Antenna: Diversity
Radio Data Encryption (WEP)

BEFORE



Service Set ID (SSID): tsunami
Allow "Broadcast" SSID to Associate?: ○ yes ● no
Enable "World Mode" multi-domain operation?: no
Data Rates (Mb/sec): 1.0 basic 2.0 basic 5.5 basic 11.0 basic
Transmit Power: 100 mW
Frag. Threshold (256-2338): 2338 RTS Threshold (0-2339): 2339
Max. RTS Retries (1-128): 32 Max. Data Retries (1-128): 32
Beacon Period (Kusec): 100 Data Beacon Rate (DTIM): 2
Default Radio Channel: 1 [2412 MHz] In Use: 6
Search for less-congested Radio Channel?: yes Restrict Searched Channels
Receive Antenna: Diversity Transmit Antenna: Diversity
Radio Data Encryption (WEP)

AFTER

Tip 3

Change Access Points default settings

Tip

Harden any Access Points and WLAN equipment by:

- Changing all default passwords.
- Changing default SSIDs - use SSIDs that do not entice or provide an incentive to the hacker.
- Change default SNMP community strings with non guessable alternatives.
- Turn on MAC address filtering.
- Encrypt your wireless traffic by turning on WEP, minimum of 128 bit and change the default key
- Checking your authentication options. Typically allows settings of: Closed (also known as shared), Open or Both. Both or Open allows unencrypted traffic.
- Prevent over-the-air management features.

Why

The access point is a primary target for abuse.There are many web sites which provide details of default settings and how to use them to obtain network access. If you've paid for these security features – use them.

Impact

These measures significantly reduce the likelihood of unauthorised access.

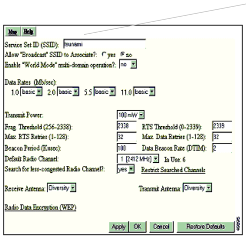
Tip 3

Change Access Points default settings

(more detail)

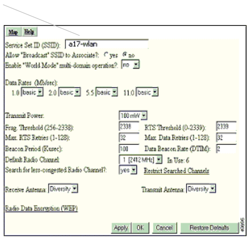
Screen shot from the Cisco Aeronet manager shows:

Change default SSID



Service Set ID (SSID): tsunami
Allow "Broadcast" SSID to Associate?: ○ yes ● no
Enable "World Mode" multi-domain operation?: no
Data Rates (Mb/sec): 1.0 basic 2.0 basic 5.5 basic 11.0 basic
Transmit Power: 100 mW
Frag. Threshold (256-2338): 2338 RTS Threshold (0-2339): 2339
Max. RTS Retries (1-128): 32 Max. Data Retries (1-128): 32
Beacon Period (Kusec): 100 Data Beacon Rate (DTIM): 2
Default Radio Channel: 1 [2412 MHz] In Use: 6
Search for less-congested Radio Channel?: yes Restrict Searched Channels
Receive Antenna: Diversity Transmit Antenna: Diversity
Radio Data Encryption (WEP)

BEFORE



Service Set ID (SSID): a17-wlan
Allow "Broadcast" SSID to Associate?: ○ yes ● no
Enable "World Mode" multi-domain operation?: no
Data Rates (Mb/sec): 1.0 basic 2.0 basic 5.5 basic 11.0 basic
Transmit Power: 100 mW
Frag. Threshold (256-2338): 2338 RTS Threshold (0-2339): 2339
Max. RTS Retries (1-128): 32 Max. Data Retries (1-128): 32
Beacon Period (Kusec): 100 Data Beacon Rate (DTIM): 2
Default Radio Channel: 1 [2412 MHz] In Use: 6
Search for less-congested Radio Channel?: yes Restrict Searched Channels
Receive Antenna: Diversity Transmit Antenna: Diversity
Radio Data Encryption (WEP)

AFTER

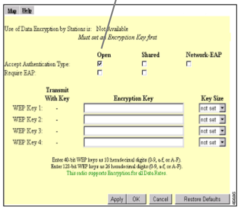
Tip 3

Change Access Points default settings

(more detail)

Screen shot from the Cisco Aeronet manager shows:

The open Authentication type permits any workstation to *JOIN* with the ***service set.*** This should be restricted



Map Help

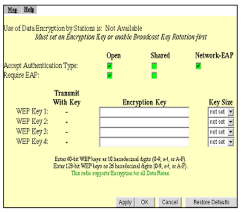
Use of Data Encryption by Stations is: Not Available
Must set an Encryption Key first

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	□	□
Require EAP:	□	□	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	-		not set
WEP Key 2:	-		not set
WEP Key 3:	-		not set
WEP Key 4:	-		not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

BEFORE



Map Help

Use of Data Encryption by Stations is: Not Available
Must set an Encryption Key or enable Broadcast Key Rotation first

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	🟩	☑
Require EAP:	☑	🟩	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	-		not set
WEP Key 2:	-		not set
WEP Key 3:	-		not set
WEP Key 4:	-		not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

AFTER

Tip 4

Use Extensible Authentication Protocol (EAP) Encryption

Tip

Use a stronger encryption scheme than 128 bit WEP to provide stronger encryption like Leap, EAP-TLS, WPA or IPSEC VPNs and provide better key handling.

Why

WEP has known weaknesses and can be compromised using freely available tools. WEP has static keys which periodically needs to be manually changed which has a high administration overhead.

Impact

Greatly improves the security of your 802.11 network and protects not only your data but also the integrity of your network session from password sniffing or session stealing.

Tip 5

Segregate WLAN Connections

Tip

Connect WLAN Access Points into their own VLAN or Segment and install a properly configured firewall between the wired infrastructure and the wireless network..

Why

This creates a Choke-Point between your internal wired network and the outside to increases your ability to control access and apply security.

Impact

Provides cost benefits for administration and improved monitoring and provides improved access control. But don't forget about Rogue access points.

Tip 6

Monitor Your Environment

Tip

Perform frequent security scans and assessments, either automated or manual and continually monitor your Air-Space 24X7.

Why

Your environment is not your Access Point so you need to monitor your Air-Space for threats and intrusions, ensure that your official Access Points' configurations conform to policy and that Rogue Access Points are not present. This is automated by the Isomair Wireless Sentry.

Impact

Enables you to address security weaknesses before they get out of control.

Tip 7

Review WLAN System and security logs

Tip

Review WLAN System and security Access Point Logs.

Why

Many attacks occur at the 802.11 management level – these are not identified by standard IDS or network monitoring tools. Reading the AP Logs can provide some information.

A dedicated 802.11 Air-Space monitoring system will detect 802.11 attacks. Isomair Wireless Sentry Console will reduce the need for reviewing general for signs of attacks by providing specific security events - you still need to make sure the event messages are received by the right people.

Impact

Huge benefit but potentially a high manual overhead - the Isomair system will reduce this.

Tip 8

Prepare for Incident Response

Tip

Prepare for Incident Response by having a clear incident response policy defined, agreed, and ready.

Why

To enable you to be prepared if something does go wrong.

This a new technology so you must have identified the threats, managed the risk and be prepared to execute the response.

Standard Login authentication systems are susceptible to wide-spread DOS by account lock-out.

Wireless LANs are still vulnerable to jamming RF interference (blocking) resulting in (either a unintentional or purposeful) DOS attacks.

Even with LEAP, EAP or Ipsec, Access Points are vulnerable to disassociation (monkey-jack) attacks.

Impact

Low cost, huge benefit. Often the most critical component of an integrated wireless management framework

Tip 9

Harden Laptops and Workstations

Tip

Ensure workstations connected to your WLANs are secured.

Why

WLANs are external, potentially public networks. This means that workstations connected to them are exposed to hostile threats – and they are not protected by a corporate firewall. Laptops connected to WLANs should:

- Have latest security patches installed
- Have antivirus product installed and kept updated
- Have Personal Firewall installed
- Disable file sharing
- Disable 'ad hoc mode'

Impact

Minimizes the risk of wireless client being compromised.

Tip 10

Keep Abreast of New Vulnerabilities

Tip

Be aware of know the threats, errors and the attacks which require extensive manual intervention or occur frequently and ensure that your Access point firmware is updated.

Why

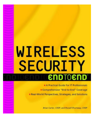
To enable you to secure your environment and address Access Point software vulnerabilities before they are used against you.

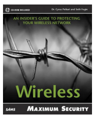
Impact

Being prepared for new threats and addressing security vulnerabilities quickly greatly increases your ability to withstand concerted attacks against your wireless network.

Additional Resources

- NIST Special Publication 800-48 Wireless Network Security: 802.11, Bluetooth and Handheld Devices http://csrc.nist.gov/publications/
- Wireless Security End-to-end
  Brian Carter & Russell Shumway
  John Wiley & Sons Inc;
  ISBN: 0764548867
- Maximum Wireless Security
  Cyrus Peikari & Seth Fogie
  Sams;
  ISBN: 0672324881
- Google is your Friend





Feedback