

Practical WLAN Attack & Defense: A Pragmatic Hacker's Primer

Presented by Adam Boileau

Who am I?

- Adam Boileau, Security Consultant at Security-Assessment.com
- Australaisian pure-play security consultancy and research company, offices in Sydney, Auckland, and Wellington, with ~25 staff.
- Penetration testing, Web App testing, Policy & Governance, Architecture reviews, Code auditing, PCI-compliance, Incident Response
- We don't sell equipment, we don't do integration, we don't do implementation. Independant, vendor agnostic company.
- We do research. SA staff regularly present at events like Blackhat, Defcon, Ruxcon, AusCERT, Bluehat, Syscan
- Recent research uncovered vulnerabilities in:
 - Skype
 - An unnamed airline ticketing system
 - 3COM IDS
 - VMWare
- as well as kernel-mode antiforensic-rootkits, SANs, Firewire...



Who am I?

- What Job Do You Do?
 - Unix Systems Programmer
 - ISP Network Engineer & ISP “Security Guy”
 - A Security Consultant (twice now)
 - Linux (Embedded) Systems Engineer
 - Lead Architect for the NZ Supercomputer Centre
- In my spare time...
 - Geek around with wireless stuff :)
 - Spread Python bigotry
 - Play bass for a bad-80s-hair-metal covers band...



Practical WLAN Attack & Defense: A Pragmatic Hacker's Primer

- Attacks against wireless networks
 - Reconnaissance
 - Wireless Network Attacks
 - Client Attacks
 - Useless Defenses
- Integrating WLANs into your environment
- 802.11i's role, attacks against it, and what I do and don't like about it
- A very cunning attack
- What can you do?
- What do I do?
- Questions



What I'm Trying To Say...

- Fit the technical issues into the larger picture, to give some perspective
- How & why did WEP fail, from a design point of view
- And how do we know that the solution's you're being sold actually solve these problems?
- Cut through the hype and the sales, and give you an honest, independent assesment of the technology and security choices you're making.

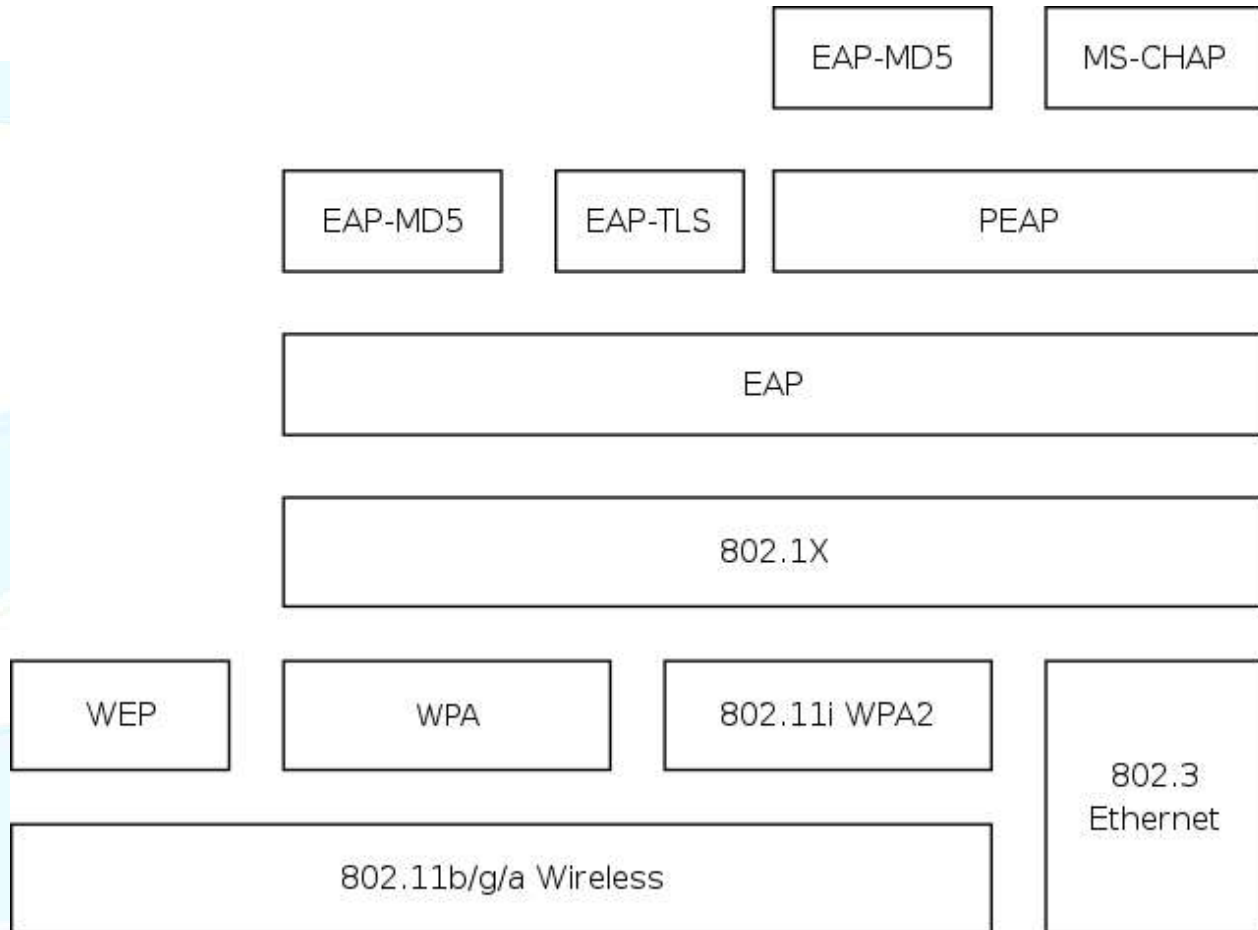


A whirlwind of eight-oh-two-dot-stuff

- 802.11a/b/g – Wireless LAN standards, including WEP “security”
 - Not equivalent to wired privacy at all!
 - Shonky crypto, basic mistakes
 - No per-station auth, only per-network auth
 - Hardware provides RC4 crypto only
- 802.1X wired ethernet port security
 - generic enough to apply to 802.11a/b/g
- 802.11i RSN “Robust Security Network”
 - another name for WPA2
 - 802.11a/b/g + new crypto (AES) + 802.1X
- WPA
 - 802.11a/b/g + bits of 802.11i
 - RC4 + Temporal Key (TKIP) + 802.1X + better ICV (MIC)
 - for legacy hardware that lacks support for WPA2 (has RC4-hardware crypto, but not AES)



802.soup



Reconnaissance

What can we learn from observing a network?

- Sniffing / Stumbling / War-Driving
- Mapping AP Coverage
- Direction Finding stations and APs
- L2 Topology discovery

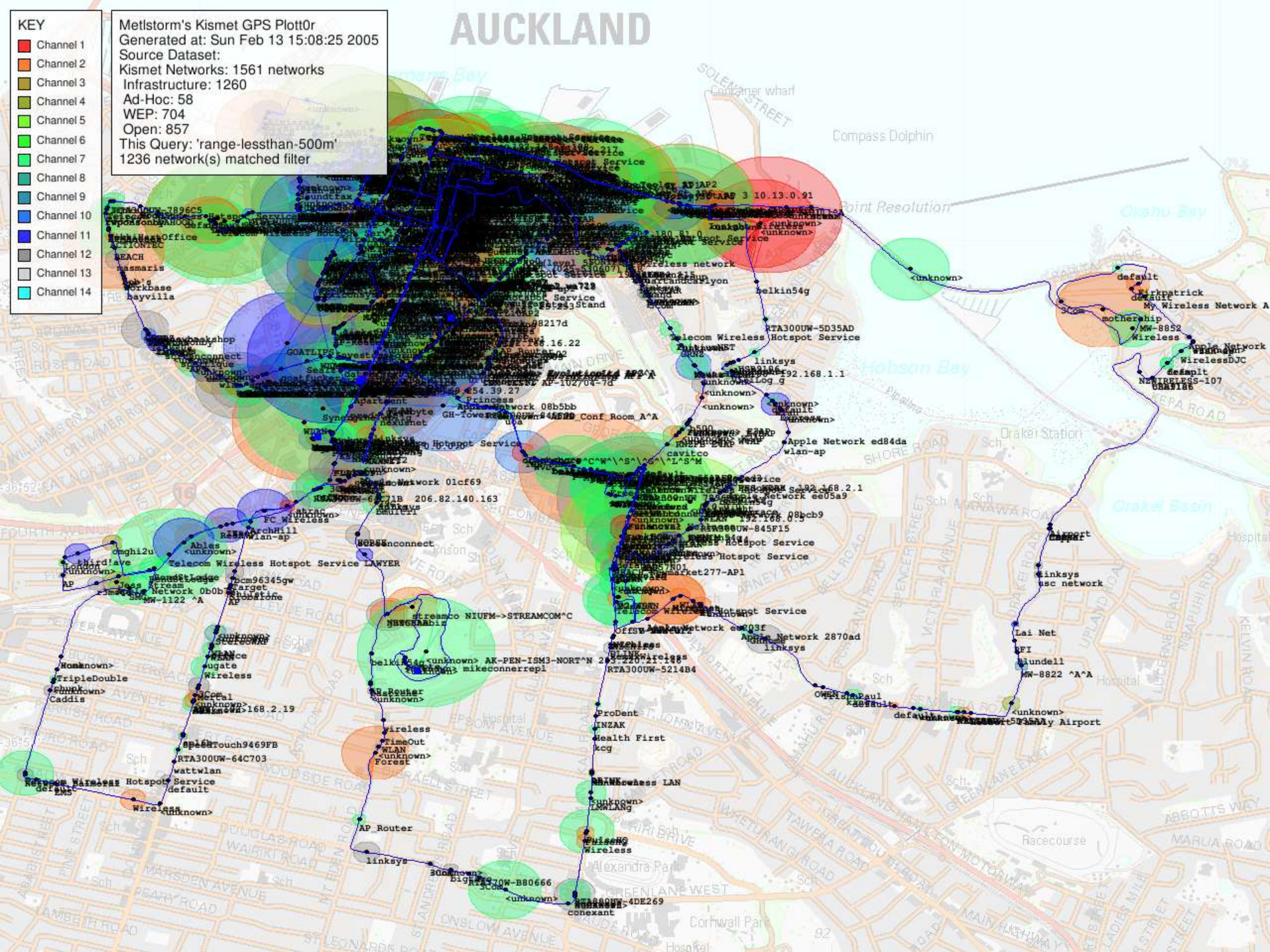


AUCKLAND

KEY

- Channel 1
- Channel 2
- Channel 3
- Channel 4
- Channel 5
- Channel 6
- Channel 7
- Channel 8
- Channel 9
- Channel 10
- Channel 11
- Channel 12
- Channel 13
- Channel 14

Metlstorm's Kismet GPS PlottOr
Generated at: Sun Feb 13 15:08:25 2005
Source Dataset:
Kismet Networks: 1561 networks
Infrastructure: 1260
Ad-Hoc: 58
WEP: 704
Open: 857
This Query: 'range-less-than-500m'
1236 network(s) matched filter



Direction Finding

- Like mapping, but
 - with a directional antenna
 - and you have to record the azimuth and elevation of your antenna per packet
 - post-process with relation to your antenna's spread pattern
- Basic tech has been around since radio was invented, home brew totally possible.
- Advanced, ex-military tech like GHz phased-arrays beginning to enter private sector as “wireless switches”
- Might make WIDS actually useful for something
- Research being done on using existing, authorized wireless nodes to triangulate unauthorised transmitters



Met! War Tri Pod tripod closeup
A: Lego Mindstorms RCX v1.5
B: Pan mechanism
C: Tilt mechanism
D & E: Microswitches to detect tilt extents
F: Opto rotation sensor (10 x light/dark segments on a wheel)
G: Lego IR TX/RX tower
H: 16dbi Yagi
I & J: Yagi retention mechanism



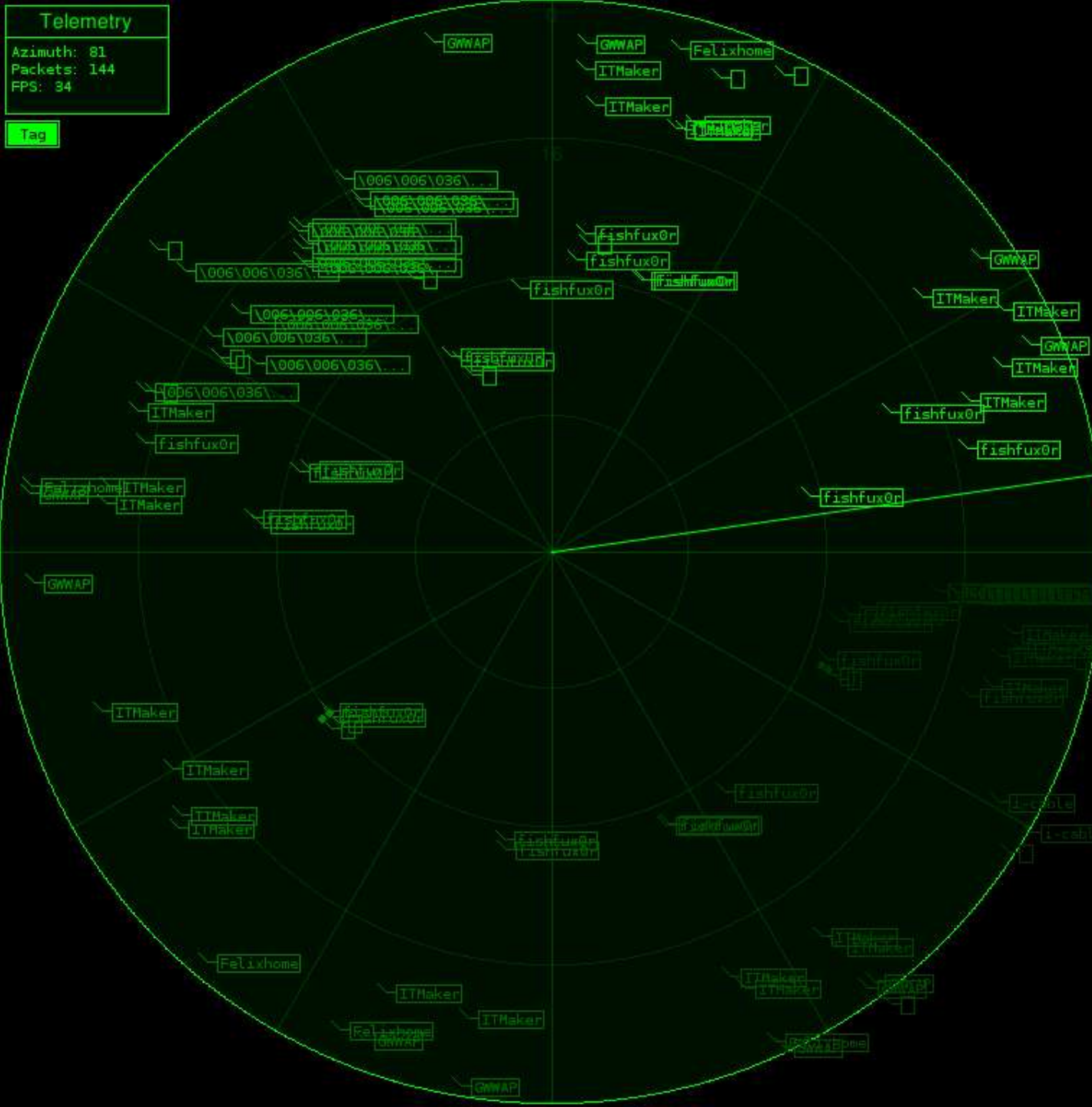
- Metl War Tri Pod Components
A: Metl War Tri Pod, lego mindstorms, brickOS
B: 16dbi Yagi
C: Lego IR TX/RX Tower
D: Zcom 300mW PCMCIA card
E: Kismet
F: MWTP-Kismet client
G: Visualisation bit of MWTP-Kismet
H: LNP Lego Networking daemon
I: MWTP Tripod Telemetry daemon
J: MWTP Logging daemon
K: MWTP Remote Controller interface
L: USB Gamepad, remote tripod controller
M: Moses, token blasphemy
N: Gin & Tonic



Telemetry

Azimuth: 81
Packets: 144
FPS: 34

Tag



Packet Log

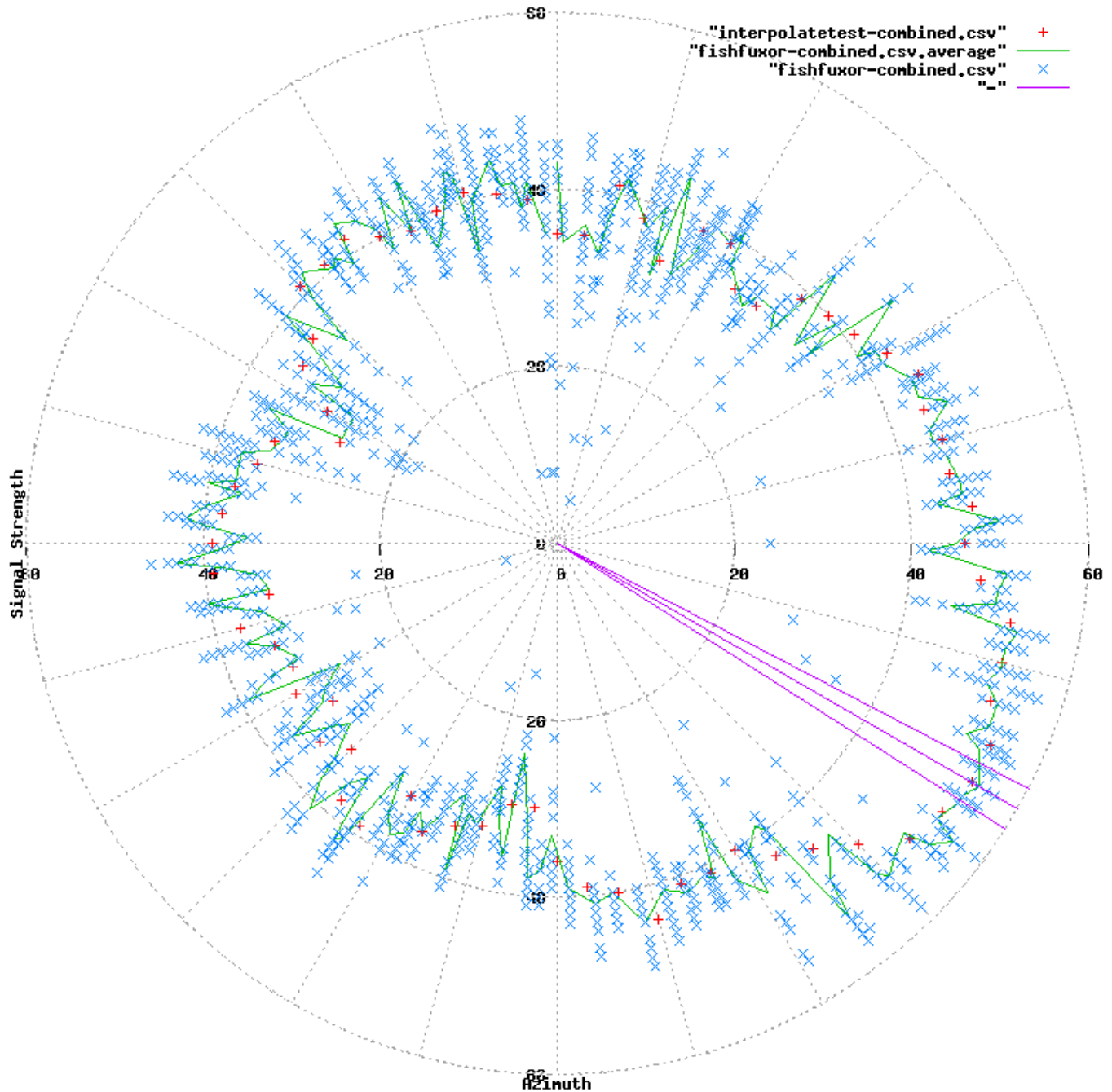
M 7	ITMaker:	00:0F:85:28:F7:14
M 4	GWAP:	00:90:96:B5:03:7F
M 7	ITMaker:	00:0F:85:28:F7:14
M 4	GWAP:	00:90:96:B5:03:7F
M 29	fishfux0r:	00:40:96:30:99:18
M 11	ITMaker:	00:0F:85:28:F7:14
M 26	fishfux0r:	00:0E:35:AD:73:DD
M 11	ITMaker:	00:0F:85:28:F7:14
M 26	fishfux0r:	00:0E:35:AD:73:DD
M 27	:	00:0E:35:AD:73:DD
M 3	Felixhome:	00:0D:54:FB:59:08
M 12	ITMaker:	00:0F:85:28:F7:14
M 30	fishfux0r:	00:0E:35:AD:73:DD
M 12	ITMaker:	00:0F:85:28:F7:14
M 30	fishfux0r:	00:0E:35:AD:73:DD
M 12	ITMaker:	00:0F:85:28:F7:14
M 30	fishfux0r:	00:40:96:30:99:18
M 11	ITMaker:	00:0F:85:28:F7:14
M 5	:	00:12:F0:76:06:85
M 2	:	00:12:F0:76:06:85
M 12	ITMaker:	00:0F:85:28:F7:14
M 4	GWAP:	00:90:96:B5:03:7F
M 5	ITMaker:	00:0F:85:28:F7:14
M 4	GWAP:	00:90:96:B5:03:7F
M 22	fishfux0r:	00:0E:35:AD:73:DD
M 8	ITMaker:	00:0F:85:28:F7:14
M 13	ITMaker:	00:0F:85:28:F7:14
M 15	fishfux0r:	00:40:05:DF:2C:E2
M 34	fishfux0r:	00:40:96:30:99:18

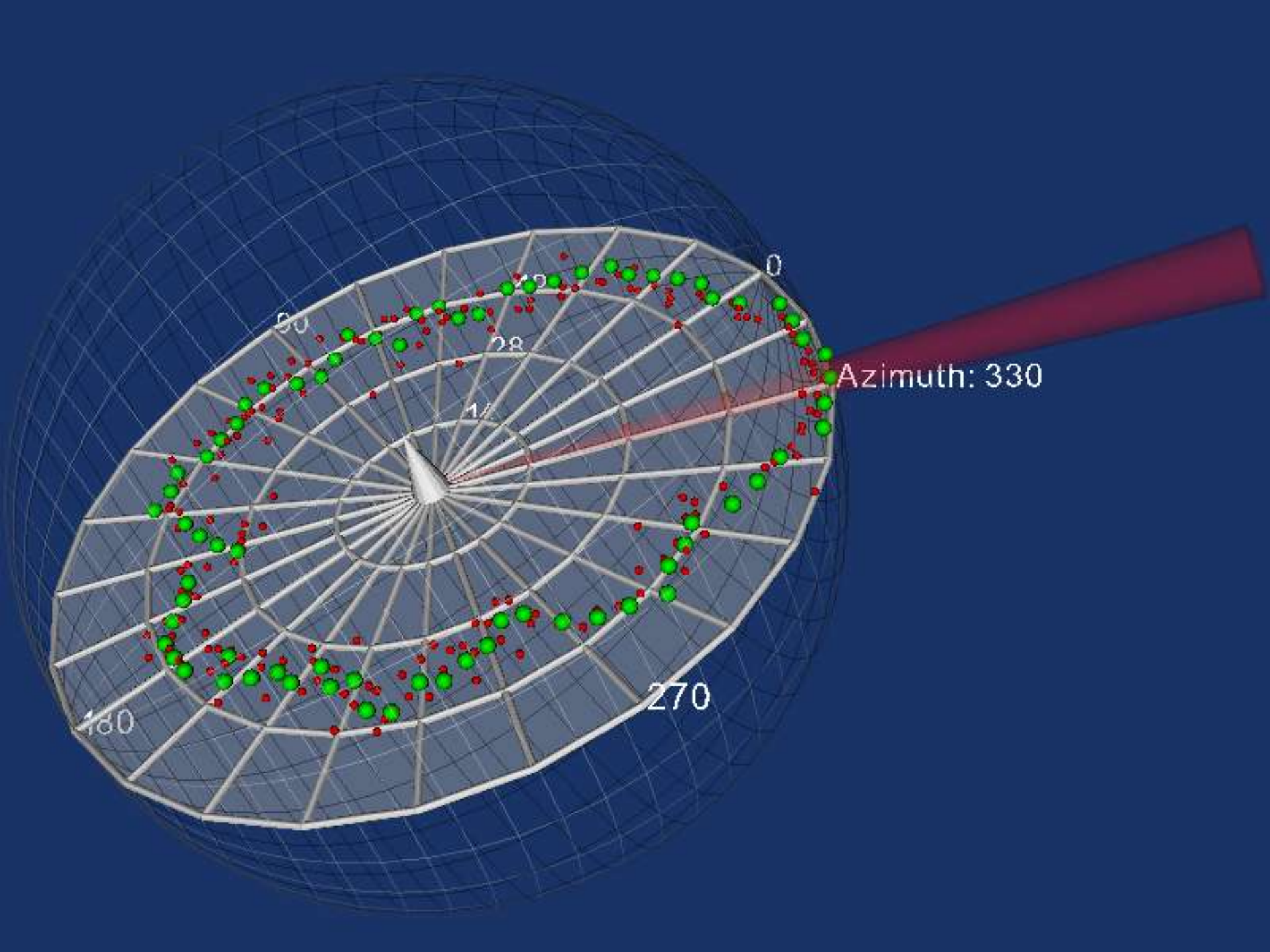
Channel Utilization

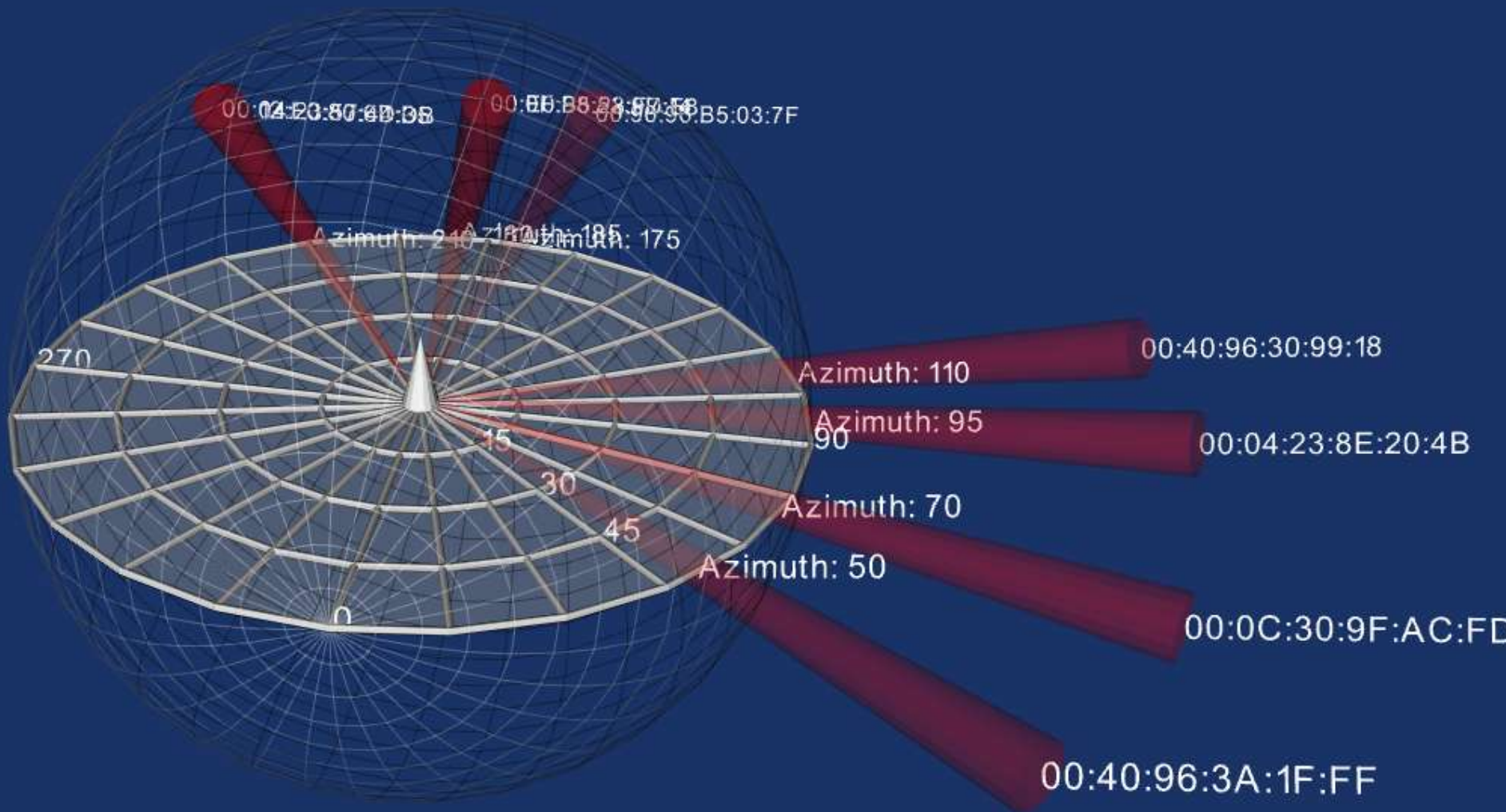


Hopping

Antenna Pattern





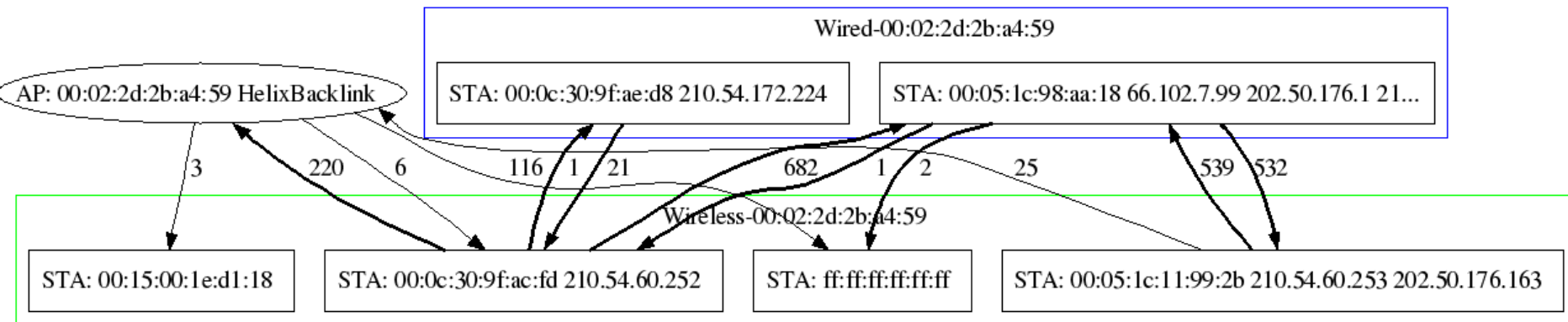


Layer 2 Topology Discovery

- Passive sniffing not only reveals presence of networks...
- ... can also divulge data about design and architecture of network
- Future war-driving tools could identify juicier networks, pick out interesting stations, networks, or relationships between hosts
- Even traffic analysis of encrypted data can still reveal interesting things
 - Timing attacks on one-character-per-packet passwords?



Early work on a L2 Topology Mapper



Attacks on Wireless Networks

The classics



Denial of Service

- ISM and UNII bands are public spectrum...
- ... and hence vulnerable to jamming, interference
- But people who are going to break the law anyway don't care about RF emission regulations
- Not a solveable problem. Can you afford the downtime for the M.E.D. to get their Direction-Finding truck to come around and look for the source of interference?
- Treat it as a DR/Business-Continuity issue
- If it's mission-critical, say, more than a couple of nines uptime, it should have a wire. Probably more than one.
- Watch out for Nutters with Magnetrons. You can buy WW2-era military radar magnetrons for \$15.



What's so bad about WEP?

- Why did WEP fail?
- Not designed or reviewed by cryptographers
- Poor choice of cipher
- No replay protection
- Integrity checking is not cryptographically secure
- Shared one-key-per-network auth
- No forward secrecy
- No key distribution
- Terrible exposure to known-plaintext attacks
 - “shared” auth protocol in the standard does this horribly!
- Not “equivilent to wired privacy” at all!
- All these individual issues can combine into a cascading failure

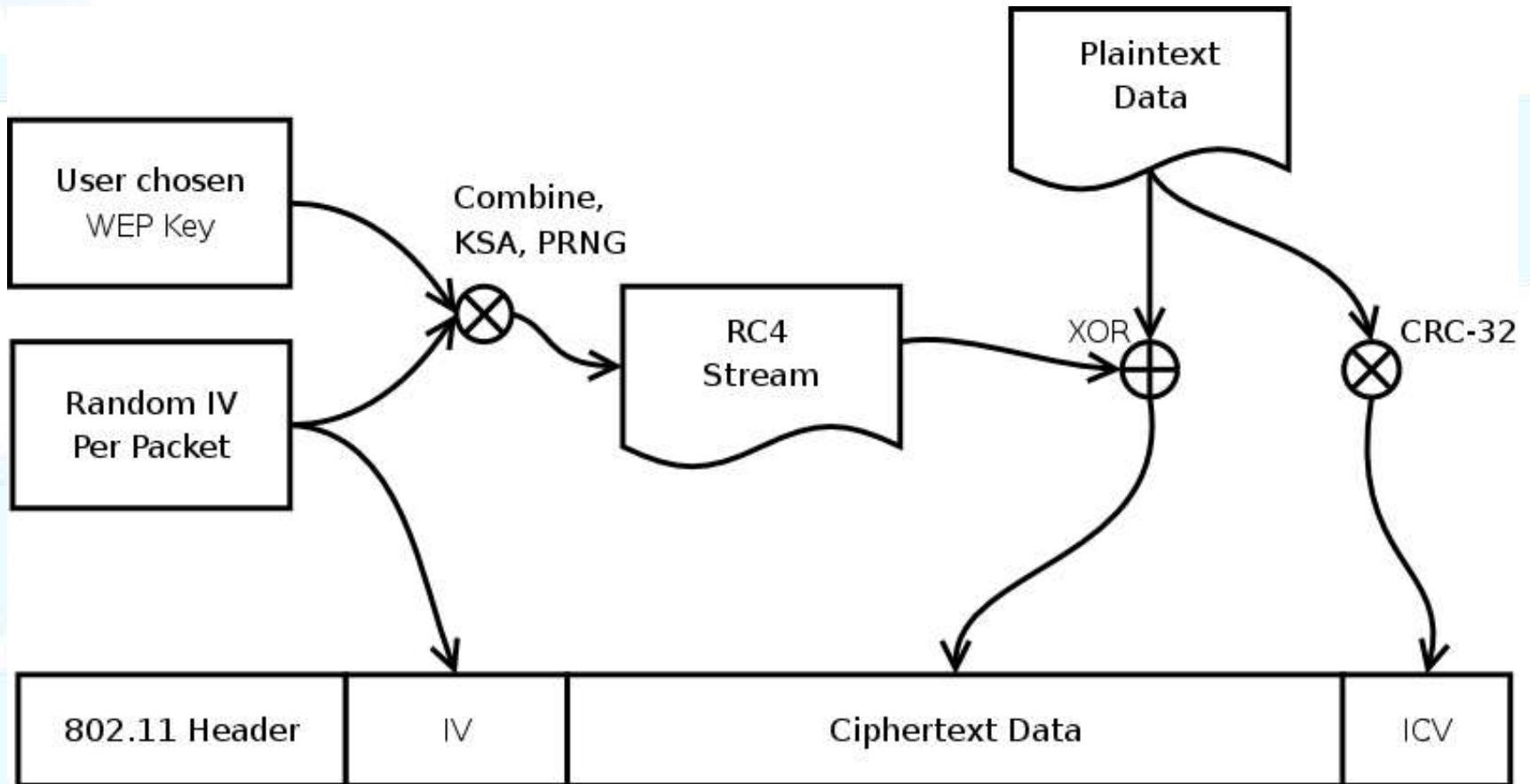


Attacks against authentication: WEP

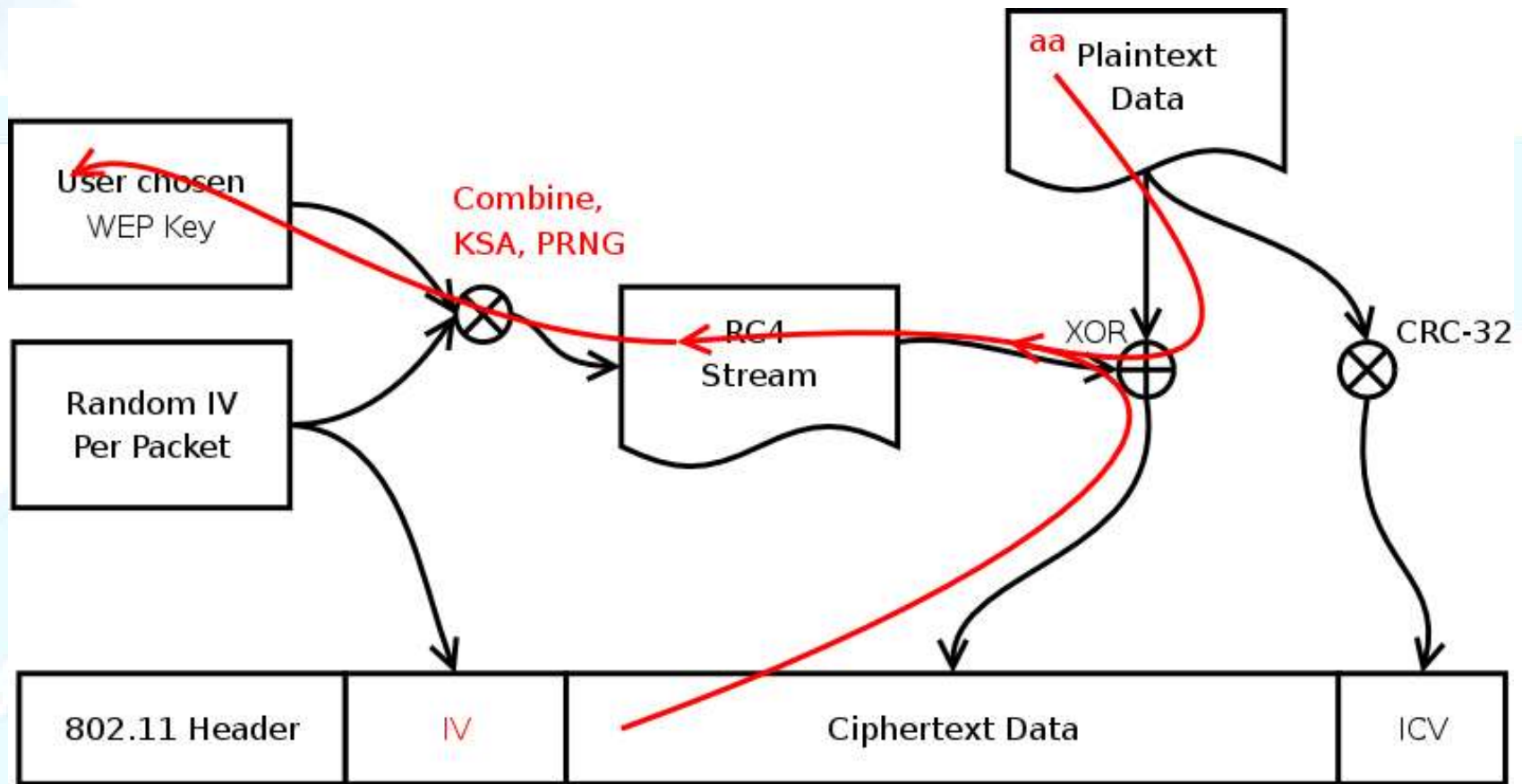
- Original observations by Tim Newsham regarding weakness in passphrase to key generation for 40bit WEP
 - Requires ~24GB of packet dumps to crack
 - Failure due to poor choice of key-generation algorithm
- FMS (Fluhrer, Mantin, Shamir) attack on the KSA (Key Scheduling Algorithm) for the RC4 stream cipher.
 - Statistical attack based on some packets leaking information about the key
 - Requires ~6m packets
 - Later refinement to 100-500k packets.
 - Failure due to poor choice of KSA, poor understanding of the cryptography



WEP Crypto Primer



WEP FMS Attack



For certain values of IV, KSA generates RC4 bytes which leak information about the state of the KSA, which tells us about the WEP Key. We must know some plaintext, but the standard says the first byte will be 0xAA!

Attacks against authentication: WEP

- Often people who have heard of WEP vulnerabilities still regard them as “theoretical” because Newsham and early FMS required impractical amounts of data.
- State of the art in WEP cracking is significantly more aggressive, faster and easier...



Accelerated FMS

- FMS WEP attack depends on having lots of packets with weak IVs
- Why wait for them? Cause them to be created.
- We can capture an encrypted packet, and replay it because WEP has no replay prevention.
 - This is one of the critical design flaws in WEP
 - Failure to learn lessons from other network crypto work
- Capture a packet that elicits a response, e.g. an ARP request, We can spot based on length and other metadata
- Replay packet repeatedly, collecting responses...
- ...at 54mbps and beyond!
- Totally feasible to crack a 128bit WEP network while you have coffee and a cupcake



**An idea so cunning, you could put a tail
on it...**

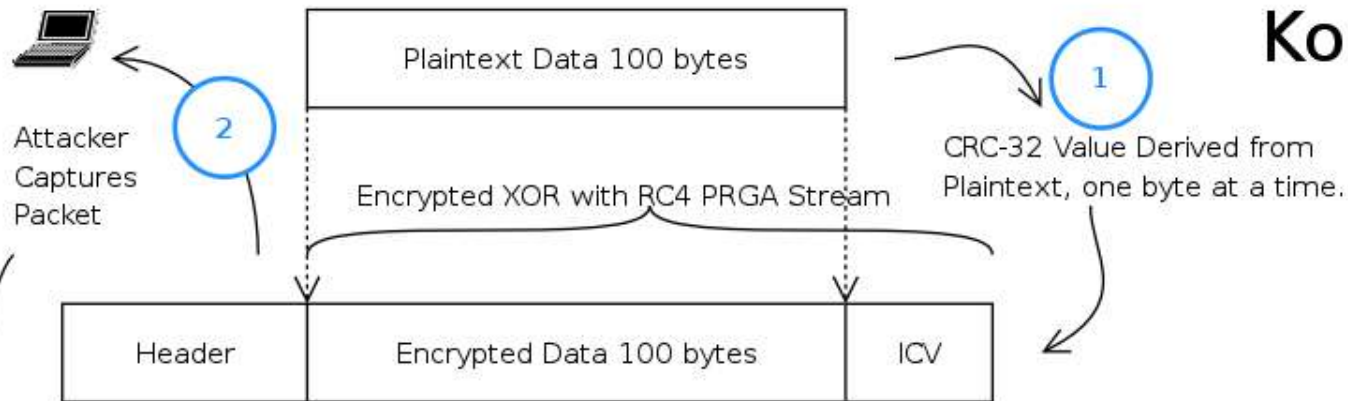
...and call it a weasel.



Korek's Chopchop attack against WEP

- Performs a per-byte recovery of keystream for a given packet, permitting us to:
 - decrypt previous/future packets of equal or lesser length with the same IV
 - generate our own new packets without the WEP key
- We can use this to:
 - decrypt interesting packets to learn about the network (is it worth WEP cracking?)
 - forge SNMP packets
 - blind portscan the network
 - or manufacture the perfect ARP request to accelerate our FMS WEP cracking
- Failure due to inappropriate use of CRC-32 as the ICV algorithm, and the choice of RC4 as the stream cipher
- Attack uses the AP as an “oracle” to validate guesses about the plaintext.
- A little complex to follow...

KoreK Chopchop Attack



ICV is a CRC-32 Integrity check, not a proper cryptographic hash. The XOR operation allows us to modify the ciphertext to have a predictable result on the plaintext, without knowing the plaintext.



Remove encrypted byte from message, ICV now invalid.



Assume plaintext byte was 0x00, update ICV by removing influence of 0x00



Send new, shorter packet to AP



Other Useless “defenses”

- Closed/Hidden SSIDs
 - Only hidden in beacons, not in probe responses, trivially detected
- 802.11b “Shared” auth
 - Actually *worse* than open association, because it leaks RC4 PRGA!
- MAC Filtering
 - Every single packet has a valid source MAC in it
 - Trivially bypassed: `ip link set wlan0 address 00:de:ad:be:ef:00`
 - Multiple stations with the same MAC works just fine
- Manual WEP Key rotation
 - “We change our keys once a week!”, oh how cute.
- Pre-WPA Proprietary WEP Enhancements
 - Generally don't address all WEP's problems – typically just implement WEP rotation or weak IV avoidance, don't address poor choice of ICV algorithm or provide replay protection
- Any or all of the above
 - Still broken!



Attacks against the client: Rogue AP

- An attacker pretends to be an AP the Station wants to talk to – the “Man in the Middle”
- Station hands over it's auth credentials to the Rogue, who reuses them to auth to the real AP
- Can be done at L2, to MitM 802.1X auth
- Or, in non 802.1X networks, at L3 to MitM application layer auth, like SSL
- Or at public hot spots to fool user – fake “captive portal” logins. How do you know that Telstra or Telecom Hotspot you gave your Xtra account details to was really a Telecom one?
- Shmoo Group released Linksys WRT-54G firmware to do Rogue AP with a Web interface, fake portal, SSL MITM at Blackhat Vegas 2005.
- Insidious, defeats all auth methods, human or crypto, that don't have strong mutual authentication (PKI!)



Attacks against the client: Classic

- Attacker joins same network as client (internet, Rogue AP, at a public hotspot, wherever)
- Attacker spots client probing, creates new AP to match
- Attack client via non-wireless-specific attack (network services, MITM, Bonzai Buddy, virus)
- Steal WEP keys, certificates, keylog user, backdoor system
- Defense
 - policy
 - prevent Stations associating with non-corporate APs
 - host firewalling
 - patch management
 - user education
 - Difficult!



The Bigger Picture

Where do WLANs fit into your network architecture?



Integrating WLANs into your environment

- Where do wireless networks fit into your architecture?
- Where SHOULD they?
- Wireless Networks can be used for different things:
 - Corporate wired LAN replacement
 - Access network (e.g. campuses, Wireless ISPs)
 - Point-to-Point links
 - Commercial Hotspots
- Each type of use has differing security models

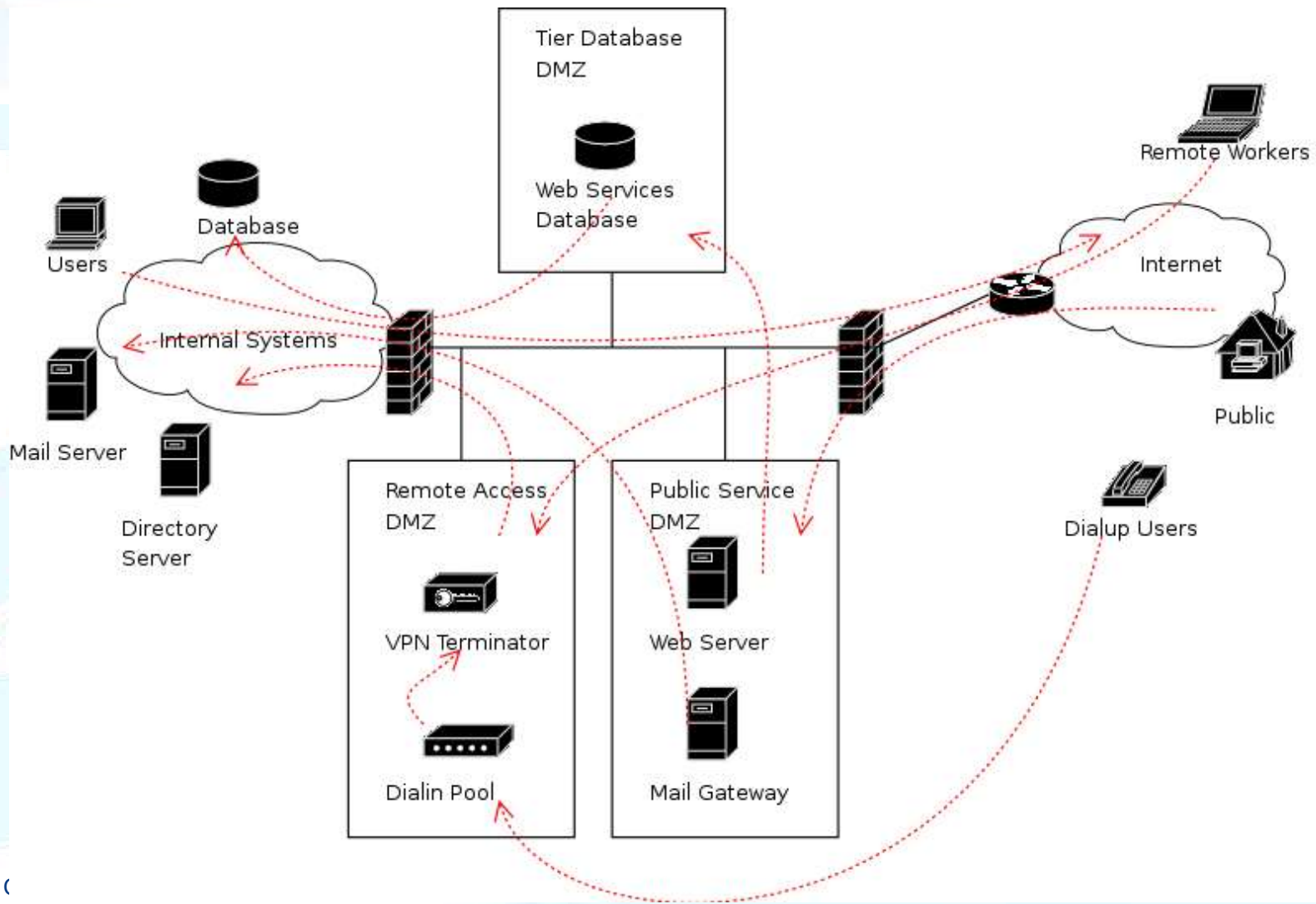


Traditional Wireless LAN Environments

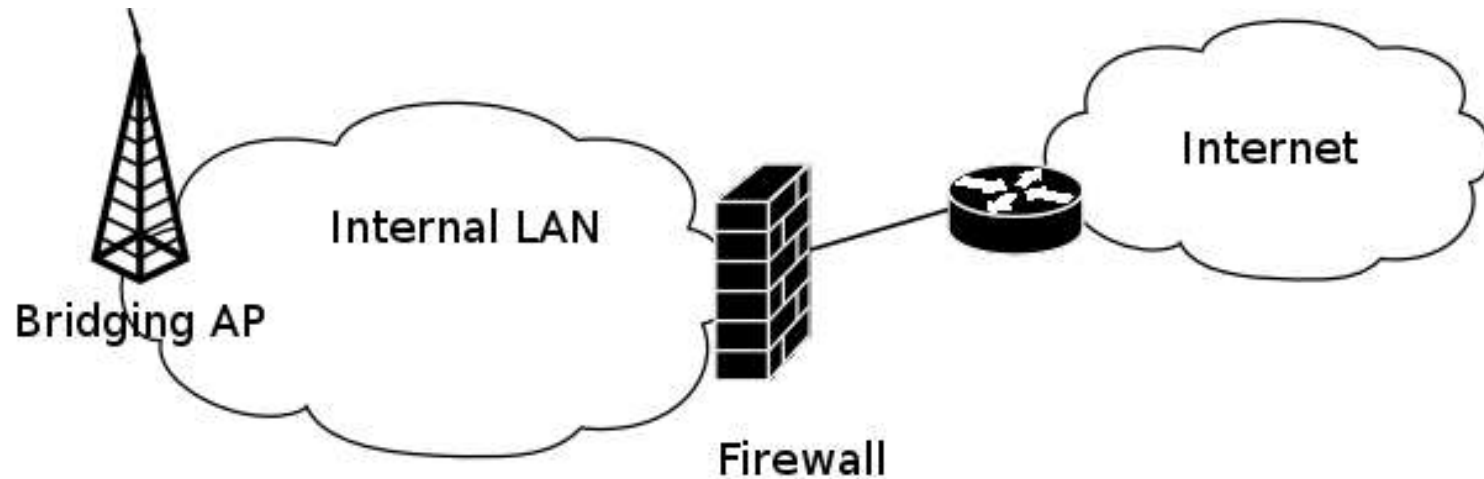
Use	Concern	Typical Solution	OK?
Corporate LAN	Protection of corporate network	WEP or WPA, sometimes plus VPN	✗
Access Network	Protect management functions	Open, MAC Filtering, separate management plane	✓
Point-to-Point	Privacy, availability	WEP or WPA	✗
Commercial Hotspot	Integrity of billing, ease of use	Open, Captive Portal	✓



Where Does a Corporate WLAN Go?

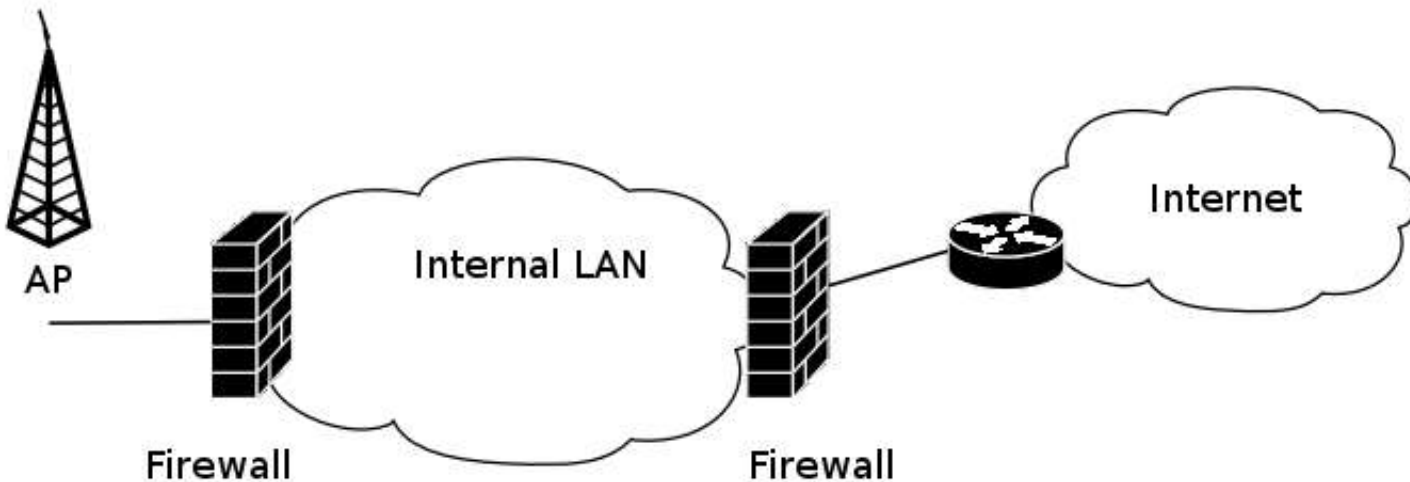


Flat Network Architecture



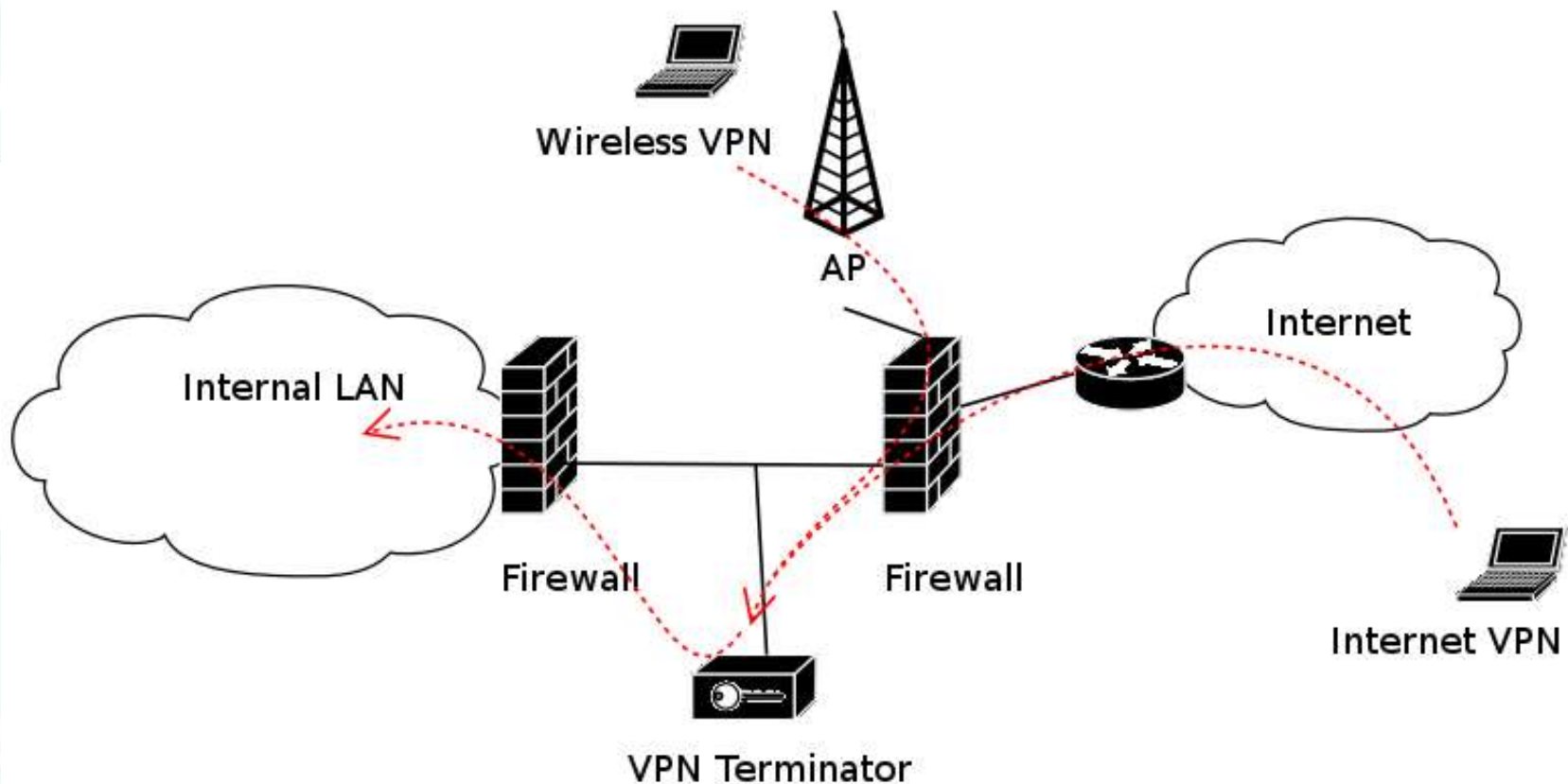
- Flat network
 - AP bridges onto internal network
 - WLAN is just like the LAN
- Terrible, disturbingly common

Wireless Segment Firewalling



- Dedicated wireless segment firewall
- Better, but dedicated WLAN kit not considered “part of the perimeter”
- Vendors want you to do this, with their special wireless-only kit

The Sad Truth



- The WLAN is part of your remote-access VPN

A WLAN is not a LAN

- A Wireless Network is not like a LAN...
- ... it's like the Internet.
- WLANs are part of your untrusted network perimeter, including the stations on it
- So are the bits of WLAN equipment – APs, routers, other wireless aware gadgets
- You need to take as much care with the WLAN bits of your perimeter as you would with your internet facing firewalls and systems.



Identify Your Perimeter

- Step 1 of a Mastercard/Visa PCI audit goes: “Identify the perimeter”
- Perimeter is anywhere external access to your network is controlled
- Not necessarily where you want it to be
- Systems that move between trust zones create a “temporal perimeter”
- WLAN stations, APs, and gadgets are as much part of the perimeter as your DMZ webserver and firewall
- Wireless laptops:
 - move between trust zones
 - have auth tokens, confidential data
 - are out of reach of corporate patching/policy
 - and they get used in the worst of places (like security conferences, filled with dirty wireless hackers!)
- Vulnerable to the full suite of “Classic” attacks while off corporate-net.



The Solution

802.11i?



802.11i's role

- 802.11i has:
 - strong auth
 - strong crypto
 - proper integrity checking
 - replay protection
 - key management
 - per-user, per-session keys
 - Does this sound like a VPN to you?
- Basically implements 802.1X + AES as a layer-2 specific, non-routable VPN technology
- Which is great!
- But... all the hassle of a VPN (complex client software, complex auth, PKI, user education)
- Provides the first step towards managing the reality of your perimeter...
- ... a path which ends with proper endpoint security



Attacks against authentication: 802.1X

- Some EAP methods are better than others
- Back to classic dictionary attacks, available offline against EAP-MD5, EAP-LEAP
- Some specific combinations are vulnerable also – the “Compound Binding Problem”
 - e.g. EAP-TLS over PEAP
- My favorite little fishhook: a quote from the IEEE 802.11i specification, section 8.1.4:
“An RSNA assumes the following:
...
b) When IEEE 802.1X authentication is used, the specific EAP method used performs mutual authentication. This assumption is intrinsic to the design of RSN in IEEE 802.11 LANs and cannot be removed without exposing both the STAs to man-in-the-middle attacks.”
- If this is the case why do vendors provide the option to only one-way auth?



What I Like about 802.11i

- Proper auth of WLANs, finally. They're no longer an instant liability.
- Decent crypto, replay prevention
- Per user, per session keying
- They've thought about things like broadcast and multicast, and actually handled them sensibly, unlike WEP
- Delegate the auth back to something clever/proper
- At least they're honest about the requirement for mutual authentication... in the depths of the IEEE standard.
- I think they've learnt their lesson from WEP, and have taken the time to do it properly... I hope.
- If you've got 802.1X on your wired ethernet already, it's a great idea (or vice versa, if 802.11i helps you push 802.1X onto your wired network, also great)



What I Don't Like about 802.11i

- Yet another fine VPN technology, with all the baggage that brings
- A general principle: Complexity == Insecurity, and there's loads of complexity
- The whole EAP-Zoo confuses people
- Centralised auth promotes password reuse
 - Centralised auth is about ease of administration, not necessarily improving security
 - Is it appropriate to use the same password for your remote access VPN as your internal mail server? your FTP server?
 - (This is a gripe about remote-access auth in general, really)
- Weasel words about PKI – don't want to scare people with “requires a PKI and Directory Services and Identity Management and...” bullet point. Standard says you can't be secure without it, why do vendors implement one-way auth?



What can you do?

- There is no excuse, ever, ever, ever to run WEP. It is the network security equivalent of a joke rubber-nose-with-glasses-and-moustache.
- WPA at the bare minimum
- WPA2/802.11i RSN with Mutual Authentication
- Remember that 802.11i still only provides security on the wireless side – if your backhaul is untrusted, you'll need something more.
- Do you still need a “real” VPN?
 - Users who are always within your boundaries, 802.11i is perfect
 - Users who roam outside of your administrative control (outside of your 802.11i cloud) still require a L3 VPN & host firewalling
- Protect your client systems – proper authentication is the first step towards endpoint security



What do I do?

- I distrust the internet as much as I distrust my WLAN. I have no expectation of privacy without end-to-end-crypto.
- Public open, cleartext ad-hoc WLAN
- Static IP allocation
- No VPN, cleartext HTTP, DNS etc.
- Application layer crypto (SSH, SSL) where required
- Aggressive host firewalling
- Gateway is a Linux box with a standard distribution, automatic updates



A Brief Promotional Interlude

**S-A runs a 1 day seminar called S4
Afternoon session is about RF tech; RFID, 802.11
I'll be running a hands on wireless hacking training
session...**

- **11th July Wellington**
- **13th July Auckland**

www.security-assessment.com



Links

More about my personal wireless (and other) projects & tools

<http://www.storm.net.nz>



Questions ?

<http://www.security-assessment.com>

adam.boileau@security-assessment.com

