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

christoph.schnidrig@csnc.ch

802.11

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

The limits of the access to data…

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

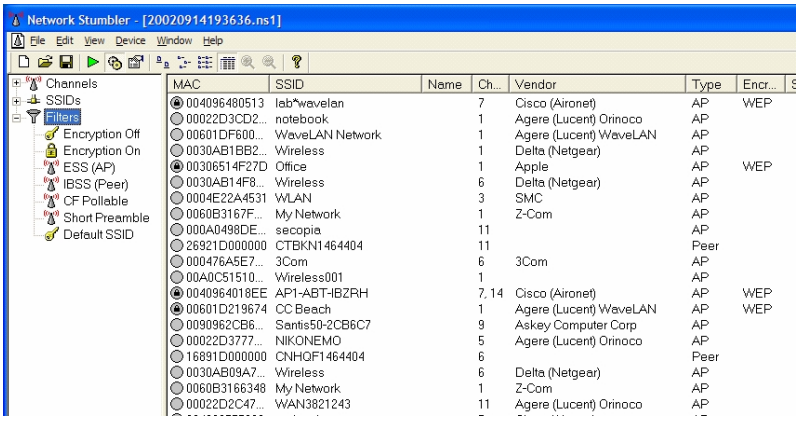
No security measures are enabled

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

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

Demo of NetStumbler



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

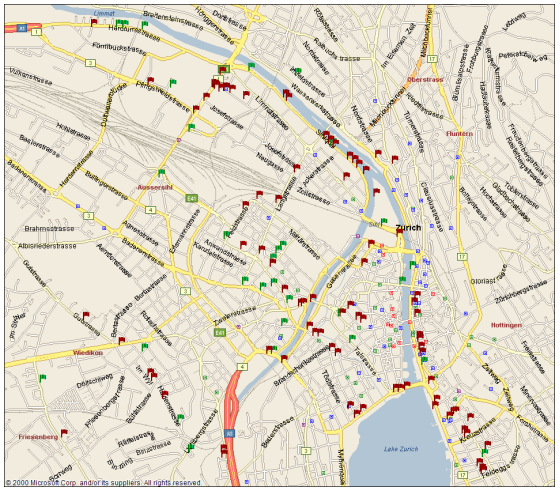
Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

Own Experience

1 hour

210 Networks

75% without WEP



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

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

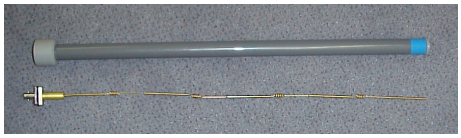
GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

Antennas

– Significantly extending the range

Omnidirectional



Yagi Directional

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

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

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

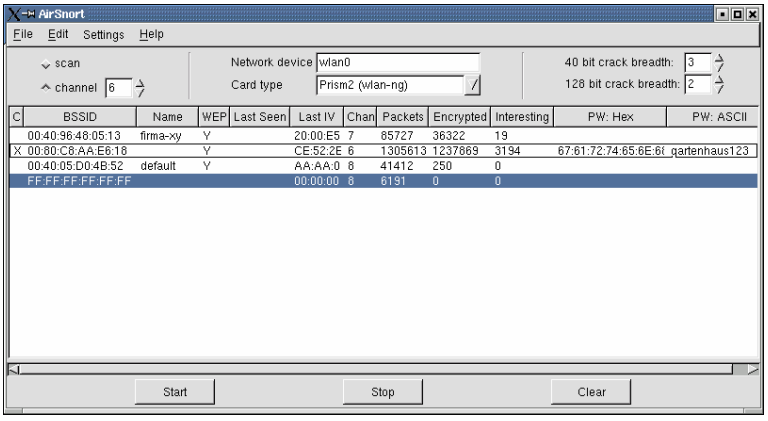
Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

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

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

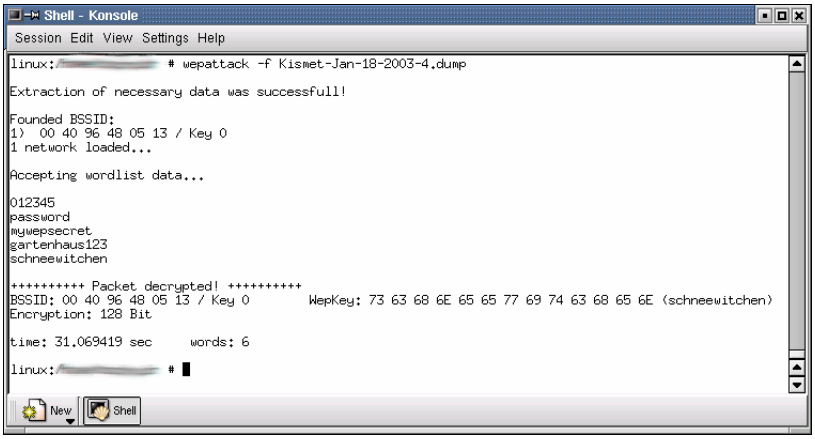
Demo of Airsnort (A)



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

Demo of WEPAttack (B)



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

- 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

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

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.

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

Demo of Pong

```
C:\event\CHRIGI>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...............
01f0  ff ff ff 00 00 00 00 00 dc 05 00 00 73 65 63 65   ............sece (SSID)
0200  76 65 6e 74 00 61 6e 00 00 00 00 00 00 00 00 00   vent.an.........
0210  00 00 00 00 00 00 00 00 00 00 00 00 00 01 06 30   ...............0
0220  00 01 01 02 00 00 00 00 00 00 00 00 00 00 00 00   ................
0230  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0240  00 00 00 00 00 12 34 ab cd ff 00 00 00 00 00 00   ......4.........
0250  00 00 00 00 00 00 00 00 00 00 67 61 72 74 65 6e   ..........gartenh (WEP Key)
0260  61 75 73 31 32 33 30 30 30 30 30 30 30 30 30 30   aus1230000000000
```

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

Other Vulnerabilities / Problems II

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

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

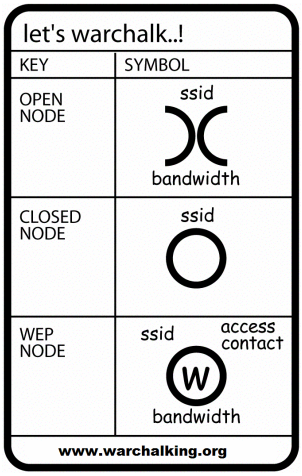
Countermeasures III (Miscellaneous)

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

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

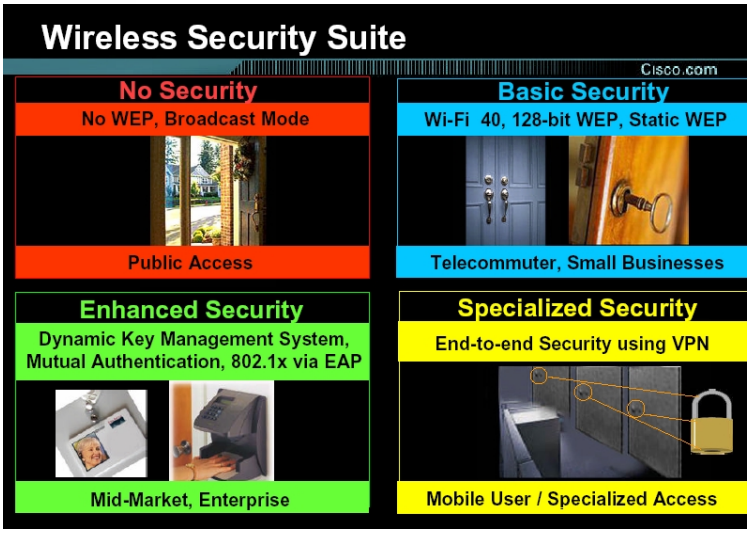
Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

- Wardriving becomes more and more popular



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

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

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch

Any questions?

Thank you for attention.

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

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
info@csnc.ch www.csnc.ch