WARDRIVING

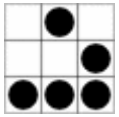
with small systems
and
wardriving-bots

www.wardriving.ch

Christoph Weber

Security Engineer

wardriver@wardriving.ch



WARNUNG:

- Alle hier gegeben Informationen und Anleitungen sind ausschliesslich für Forschungs- und Testzwecke zu benutzen. Wir übernehmen keinerlei Haftung für etwaige Verstösse von Usern gegen geltendes nationales oder internationales Recht !

Agenda

- Eine Idee entsteht
- Hard + Software / Konfiguration Tips
- Einsatzmöglichkeiten von Small Systems
- Praktische Beispiele
- Wardriving Bots
- Funktionen und Möglichkeiten

Eine Idee wird Geboren!

- Wie so bei mancher Idee, war auch hier der Grundgedanke bei einer philosophischen Grundsatzdiskussion im Freundeskreis entstanden.

Hauptziel

- Ein für Wireless optimiertes und kostengünstiges Gerät zu bauen und mit Opensource OS und Tools zu betreiben.
- Ziel ist es, nicht mehr selber Wardriving zu betreiben, sondern Wardriving Bots zu bauen, die selbständig Daten sammeln und „zurückkehren“, oder die angefallenen Daten zurücksenden.

Vorstufe

- Low Cost Wireless Equipment (keine Notebooks)
- Frei Konfigurierbar für den jeweiligen „Individuellen Einsatz“
- Lösung Technischer Probleme
- Neue Ideen sammeln und ausloten
- Möglichkeiten Überprüfen
- Daten werden noch Manuell ausgelesen.

Ziel

- optimierte Scripts + Tools
- Neue Tools entwickeln
- Optimierung der Hardware
- Feedback der Wardriving-Bots an den Bot-Kontroller und Operator
- selbständige Bots aufbauen
- Autonome Datenrücksendung
- Datenverschlüsselung
- Autoupdate der Bots
- Neue Sensoren integrieren

Wardriving Bots

Realität (Stufe 1)

- Auto fest Eingebaut
- Stationäre Bots
- Postpakete
- Rucksackmodell

Nahe Zukunft (Stufe 1)

- Taxi / Lastwagen
- Mietautos (Mobility)

Zukunft (Stufe 2)

- Zug / Bus
- LKW + Fernfahrer
- Alles was unterwegs ist

Ferne Zukunft (Stufe 2)

- Modell - Flugzeug
- Ballon
- Zeppelin
- .....

Aufbau

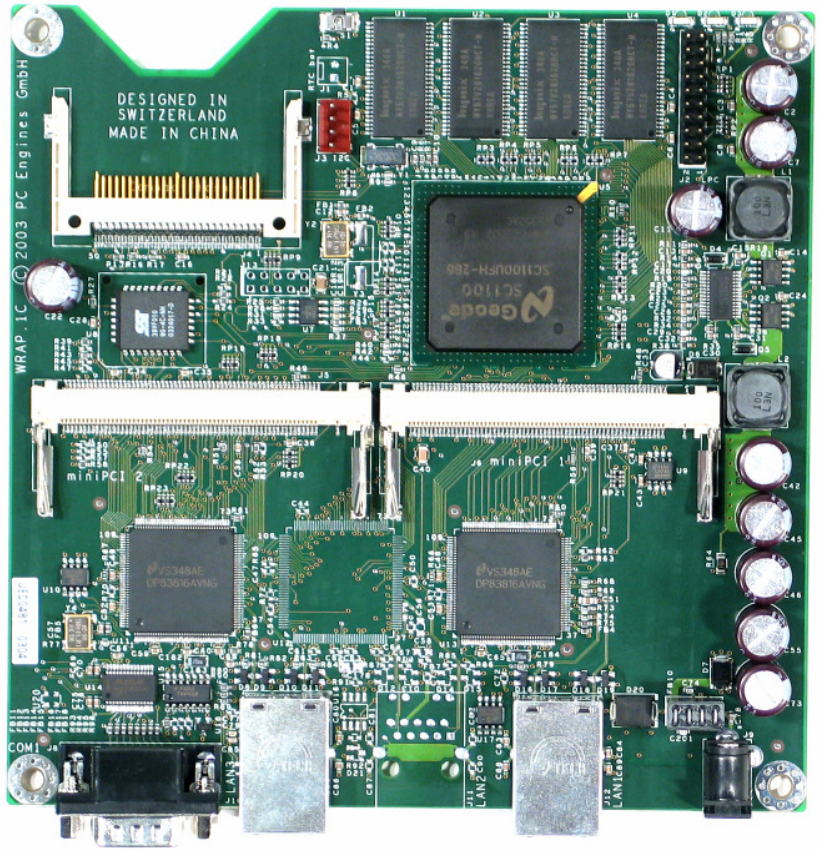
- Hardware
- Software
- Konfiguration
- Gelöste + Ungelöste Probleme

Hardware Anforderungen

- kleine Baugrösse, günstiger Preis
- geringer Strombedarf !!!
- anpassbar / ausbaubar / flexibel
- MiniPCI Anschlussmöglichkeit
- CF Slot (oder SD, MMC …)
- Externe Anschlussmöglichkeiten (RS 232/USB)
- keine Mechanischen Teile
- Keine grossen Wärmeentwicklung / keine Lüfter

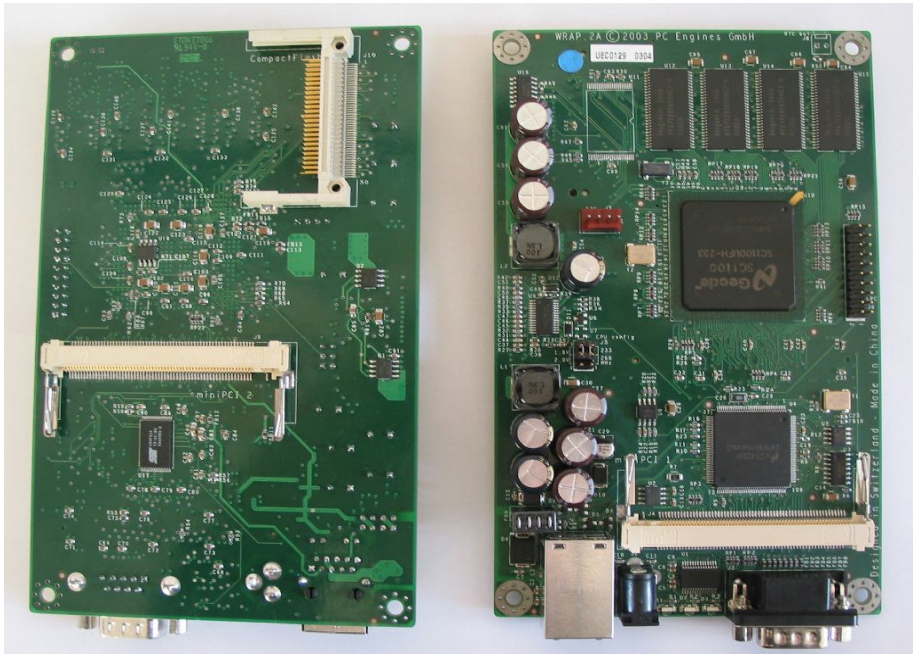
WRAP 1 (www.pcengines.ch)

- CPU: 266 AMD Geode
- 3-5 Watt / 12V
- 128 MB RAM
- 2 (3)LAN / 2(1) miniPCI
- RS232 (Console)
- I2C Anschluss
- CF Slot
- (USB)



WRAP 2 (www.pcengines.ch)

- CPU: 266 AMD Geode
- 3-5 Watt / 12V
- 128 MB RAM
- 1LAN / 2 miniPCI
- RS232 (Console)
- I2C Anschluss
- CF Slot
- Kompaktere Bauweise (100mm x 160mm)

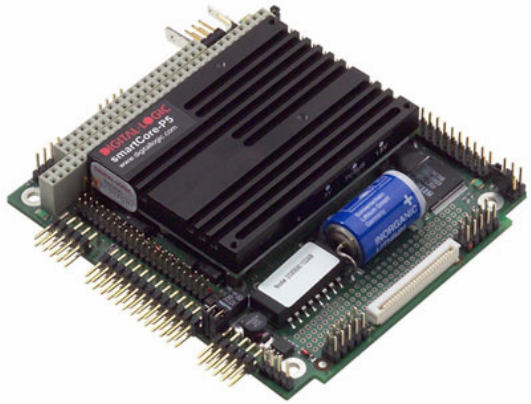


Soekris (www.soekris.com)

- 266 Mhz NSC SC1100
- 256 Mbyte RAM
- Power 15W (max.)
- 3 LAN
- 1 MiniPCI / 1 PCI
- USB (1.1)
- 2.ter RS232
- UltraDMA-33 Interface

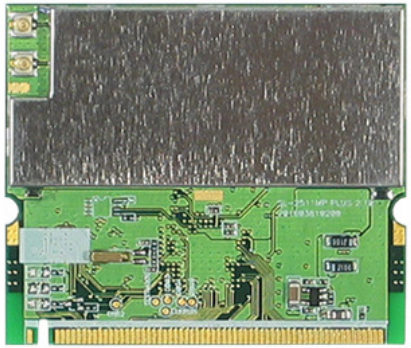
PC104 / Mini-ITX

- ab 66Mhz
- ab 256 MB RAM
- RS232 / USB
- PCI
- (kleiner PC)
- Div. Modelle



Mini PCI Wireless Karten

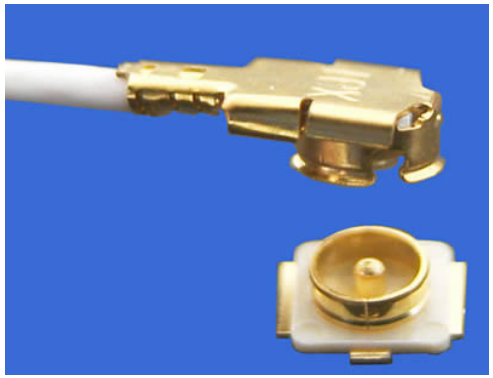
- NL-2511MP Plus (Senao)
- Atheros 2513 Chipset
- (WKM54G)



- Treiber Verfügbarkeit überprüfen (nicht für jedes OS aktuelle und funktionierende Treiber verfügbar)
- Wireless Karten benötigen viel Strom.
- 802.11b/g + 802.11a

Antennen + Kabel

- I-PEX Stecker auf den Mini-PCI Karten
- Reverse SMA an den Antennen



GPS

Problematik

- USB Treiber
- RS232-Anschlüsse
- Leistungsbedarf.

GPS Maus USB

Grösstes Problem

- Sicht zum Himmel !!

LCD Anzeigen

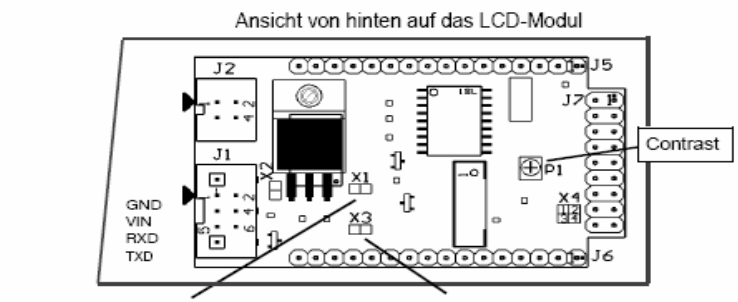
- 4 x 20 Zeichen
- 2 x 20 Zeichen
- Grün / Blau / Weiss

Anschluss via

- RS232
- I2C
- USB

Bsp. www.vtec.ch

Anschluss LCD



Jumper X1 f. Versorgungsspannung		
OPEN	7.5 - 20V	Ueber Regler
CLOSE	5 V	+- 10%
Für höhere Eingangsspannungen Version mit Schaltregler verlangen!		

Jumper X3 f. Baude Rate Selection	
OPEN	2400 Baud
CLOSE	9600 Baud

- Anschluss via RS232 Schnittstelle (2400 oder 9600 Baud)

- Simple Ansteuerung mit Steuersequenzen

Steuer – Befehle		
Clear screen	**"\D"**	
LED Backlight ON	**"\B"**	
LED Backlight OFF	**"\A"**	
LED Backlight intensity	**"\Lx"**	Helligkeit der Hintergrundbeleuchtung in Stufen von 0 .. 9. Dieser Wert bleibt im EEPROM gespeichert. Bei der Auslieferung ist der Wert 6 gesetzt. (bei OLED-Display nicht unterstützt)
Curser on "blink"	**"\E"**	
Curser on "line"	**"\F"**	
Curser off	**"\C"**	
Gehe zu Position (Zeile, Zeichen)	**"\llcc"**	"Zeile","Zeichen" es müssen je 2 Zeichen gesendet werden
Spezial - Zeichen definieren	**"\Z",d,c,c,c,c,c, c,c,c**	d= Custom character Adresse, 8 X c=Daten für Character Generator RAM (CG)
Firmware Version	**"\VV"**	Zeigt Firmware Version auf dem LCD. (ab aktueller Cursor Position)
Beispiel: \0109 nächstes gesendetes Zeichen geht auf Zeile 2, Pos. 10		

Power

- 12V Auto Adapter
- NIMH oder NICD Akkus (7.2 V / bis 3500mAh)
- Blei-Akkus
- Solarzellen
- 220V Adapter

Unser Hauptproblem:

Stromversorgung !

Bluetooth

- Bluetooth Dongle Classe I (100m)
- Mini PCI Karte mit externer Antenne (not testet)

Bluetooth MiniPCI

Bluetooth (USB 1.1)

Webcam (Geplant)

- Webcam Axis (Anschluss via Netzwerk)
- Webcam via USB (Treiber Problem !)
- Optional mit Microphon

Netz Webcams

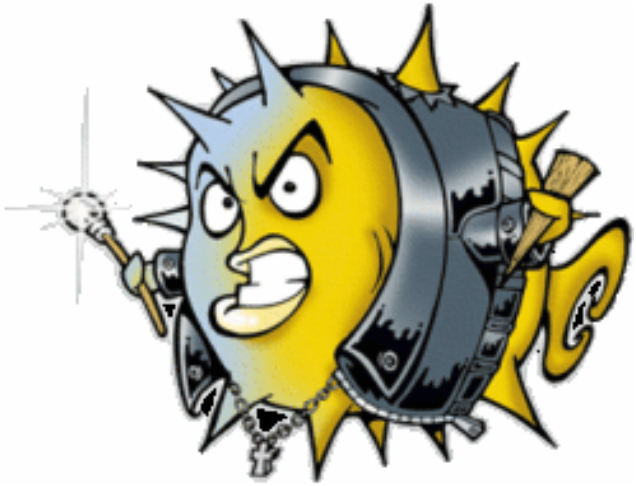
USB Webcams

Open-BSD

- OpenBSD 3.8
  OpenBSD 3.9 ab1.5.06

Gründe:

- extrem klein
- Open Source
- schnell
- anpassbar
- Kismet Unterstützung
- Wirelss Kartentreiber vorhanden.



Linux als Alternative

- Linux 2.4 / 2.6
- Aufwendiger zum Downsizen !

Gründe:

- Open Source
- schnell
- anpassbar
- Kismet Unterstützung
- Wirelss Kartentreiber vorhanden.

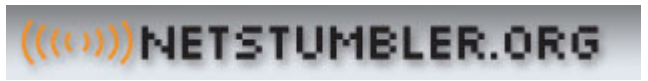
Keine Alternative !

- Windows XP
- Windows CE
- Windows 95

(c) 2003 by Microsoft

Gründe

- Nicht Opensource
- Zu Gross
- Ressourcenintensiv (CPU / MEM)
- Keine passende Software



Probleme und Lösungen

Wie erwartet viele Technische Probleme

- Speicherplatz / CPU Power
- Stromversorgung
- Hardware / passende Treiber
- Software + Konfigurationen
- Eigene neue Entwicklungen notwendig

Wir haben keine Probleme,
nur Punkte die „noch“ nicht gelöst sind!

System Konfiguration auf CF

- Problem: CF Lebensdauer
  - Max Anzahl Writes / pro CF Karte ist limitiert
    (MTBF bei 100.000 Schreib-/Lese-Zugriffen)
- - Daten müssen auf die CF
  - Keine HD möglich (Erschütterungen)
- Lösung:
  - Entwicklung und Test auf Normalem System
  - notwendige System Logfiles ins RAM
  - keine Swap Partition
  - Gesammelte Daten (komprimiert und verschlüsselt) auf CF schreiben.
  - alte und kleinere CF Karten „aufbrauchen“

System Erstellen

- Scripte und Binarys auf dem entwicklungs System erstellen.
- Tool für Erstellung bei OpenBSD ist **flashdist**.
  - flashdist.sh script anpassen (Systemabhängig)
  - erstellen von config files (rc / kismet.conf ...)
  - erstellen von flashdist.txt File mit allen notwendigen Files
  - erstellen vom Hardware abhängigen Kernel
  - flashdist.sh script anpassen (Systemabhängig)
  - CF in in Slot einfügen und flashdist.sh aufrufen.

  flashdist.sh sd0 flashwire.txt /usr/src/sys/arch/i386/compile/WRAP3/bsd /u/openbsd

- - allenfalls CF Parameter eingeben (C/H/S)
  - neues root Passwort eingeben

First Boot

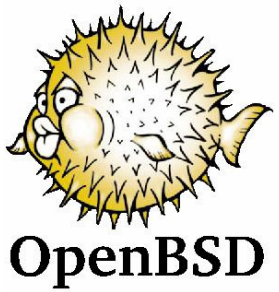
- Boot Meldung von WRAP Box
- BIOS / Speicher / CF Size / Serial Speed

```
PC Engines WRAP.2B/2C v1.11
640 KB Base Memory
130048 KB Extended Memory

01F0 Master 848A Flash Card
Phys C/H/S 1002/16/32 Log C/H/S 1002/16/32
Using drive 0, partition 3;
Loading;.....
probing: pc0 com0 pci mem[640K 127M a20=on]
disk: hd0
>> OpenBSD/i386 BOOT 2.10
switching console to com0
>> OpenBSD/i386 BOOT 2.10
com0: changing speed to 38400 baud in 5 seconds, change your terminal to
   match!
```

Links zu den Tools

- FLASHDIST
  http://www.nmedia.net/~chris/soekris/
- FLASHBOOT
  http://www.mindrot.org/flashboot.html
- OPENSBD
  www.openbsd.org



Anpassungen Kernel

- Integration aller Wireless Karten
- Nur Notwendige Treiber, restlichen machen Kernel zu gross!
- Notwendig sind z.B. USB (nur für Soekris 4801/ WRAP nur wenn USB eingebaut)
- Muster Config Files sind bald verfügbar auf www.wardriving.ch

```
# Wireless network cards
wi*     at pci? dev ? function ?        # Intersil Prism MiniPCI wireless card
ath*    at pci? dev ? function ?        # Atheros MiniPCI wireless card

#atw*   at pci?                         # ADMtek ADM8211 (802.11)
wi*     at pci?                         # WaveLAN IEEE 802.11DS
#an*    at pci?                         # Aironet IEEE 802.11DS
ipw*    at pci?                         # Intel PRO/Wireless 2100
#iwi*   at pci?                         # Intel PRO/Wireless 2200BG/2915ABG
#ral*   at pci?                         # Ralink RT2500
#rtw*   at pci?                         # Realtek 8180
```

Anpassunngen /etc/rc

- Individuellen Anpassungen
- DHCP starten
- kimset
- gpsd
- lcdd (Eigenentwicklung)
- Kontroll Scripts (im Aufbau)

```
echo ssh: starting daemon...
/usr/sbin/sshd
#
# CF auf RW setzen
#
mount -uo rw /
#
# Kismet starten
#
cd /home/trilobit
/bin/bash /home/trilobit/kismet-server.sh &
/bin/bash /home/trilobit/taster.sh &
/bin/bash /home/trilobit/kismet-test.sh &
```

USB + RS232

Anschlüsse RS232 / USB

- 1. RS 232 Anschluss ist für Serielle Console (Soekris 19200/ WRAP 38400 Baud)
- Soekris 4801 hat 2. RS232 Anschluss Onboard
- WRAP 1 hat USB Onboard, muss aber nachträglich eingebaut werden. (Löten) (Achtung: Spannungsversorgung)
- Soekris 4801 hat USB Port Ready for use.
- Soekris 4801 hat PCI Slot.

LED + Taster WRAP

- WRAP LED‘s für Statuskontrolle
  3 LED‘s für Kontrolle
  Script Steurerbar via `gpioctl(8)`
  (Devices müssen im Kernel integiert sein + MAKEDEV muss angepasst sein)
- Taster auslesbar
  auch via `gpioctl(8)`
  [root@chasmops:~] # gpioctl 40
  pin 40: state 0
- Temparatur auslesbar

```
[root@chasmops:~] # sysctl hw.sensors.0
hw.sensors.0=lmtemp0, TEMP, temp, 44.00 degC / 111.20 degF
```

Anschlüsse Soekris 4801

- 20 Pins Ansteuerbar (J5 Onboard) auch via `gpioctl(8)` ansteuerbar.
- IDE Disk Anschluss vorhanden.
- GPS an USB
- Bluetooth an USB
- USB Devices müssen im Kernel integriert sein und müssen mit MAKEDEV erstellt werden. Ansprechen von /dev/ttyU0 für USB-GPS
  `gpsd -p /dev/ttyU0`

Support: RTFM

- Wir haben nichts neues erfunden, nur bestehende Dinge sinnvoll zusammengefügt, deshalb können wir nur auf die jeweiligen Dokumentationen verweisen.
- www.google.ch war,ist und bleibt unser bester Supporter.
- Read the „Famous“ Manual...

Gelöste Probleme

- Filesystem Check nach Power Lost.
  Regelmässg Filesystem sync‘en und Daten schreiben.
  Bsp. Kismet (Default 300 Sec)

```
# How often (in seconds) do we write all our data files (0 to
disable)
writeinterval=60
```

Kismet Konfiguration

Anfallende Datenmenge begrenzen:

Kismet Logfiles

```
# File types to log, comma seperated
# dump    - raw packet dump
# network - plaintext detected networks
# csv     - plaintext detected networks in CSV format
# xml     - XML formatted network and cisco log
# weak    - weak packets (in airsnort format)
# cisco   - cisco equipment CDP broadcasts
# gps     - gps coordinates
# logtypes=dump,network,csv,xml,weak,cisco,gps
# logtypes=network,csv
logtypes=csv,dump
```

Kismet Scanner

Vorteile

- Unterstützung von mehr als einer Wirelesskarte zum Scannen.
- Optimierung ist möglich.
- Kismet lässt sich Optimal den Anforderungen anpassen (kismet.conf)
- Client – Server Software
- Zugriff auf Server via Perl ohne Probleme möglich.

Nachteile

- Wireless-Karte die für Kismet-Scanner benutzt wird, lässt sich nicht gleichzeitig zum Verbinden mit AP‘s benutzen.

http://www.kismetwireless.net/

Ungelöste Probleme

- Uhrzeit geht verloren bei Power Lost
  da keine interne Uhr !
  Mögliche Lösungen:
  - ntp abgleich via „Open Accesspoint“
  - Zeit von GPS übernehmen
- Filesystem Full
- Unterstützung neuer Wireless Karten (Bsp. Atheros-Chipsätze)
- Filesystem Type
- Keine Möglichkeit „fertige“ allgemeine Bootimages zu erstellen.
- Datenreduktion (Auswertung auf System)

Einsatzmöglichkeiten

- Mobil
  - Auto (Taxi / „Mami“ / Mobility / LKW)
  - Rucksack / Kinderwagen
  - Zug / Tram / Bus
  - Postpackete
  - Wearble Boxes
- Stationär
  - Audits
  - Wireless Netzwerk Überwachung

Test Einsätze

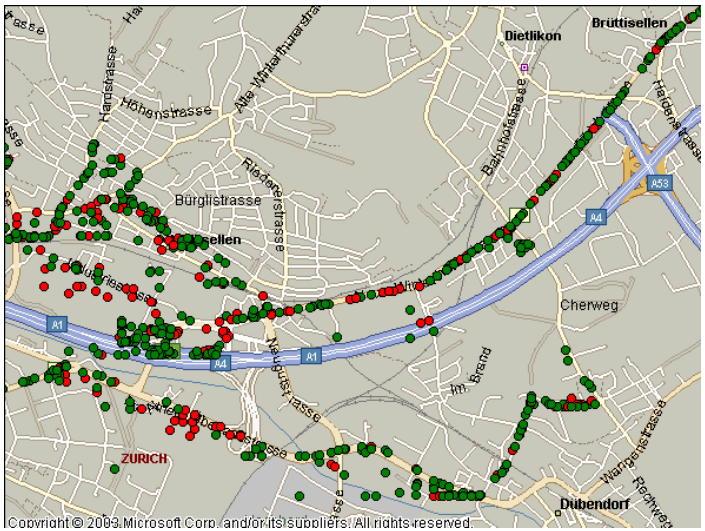
Bereit für Postpaket

Einsatz im Zug

Ohne GPS !

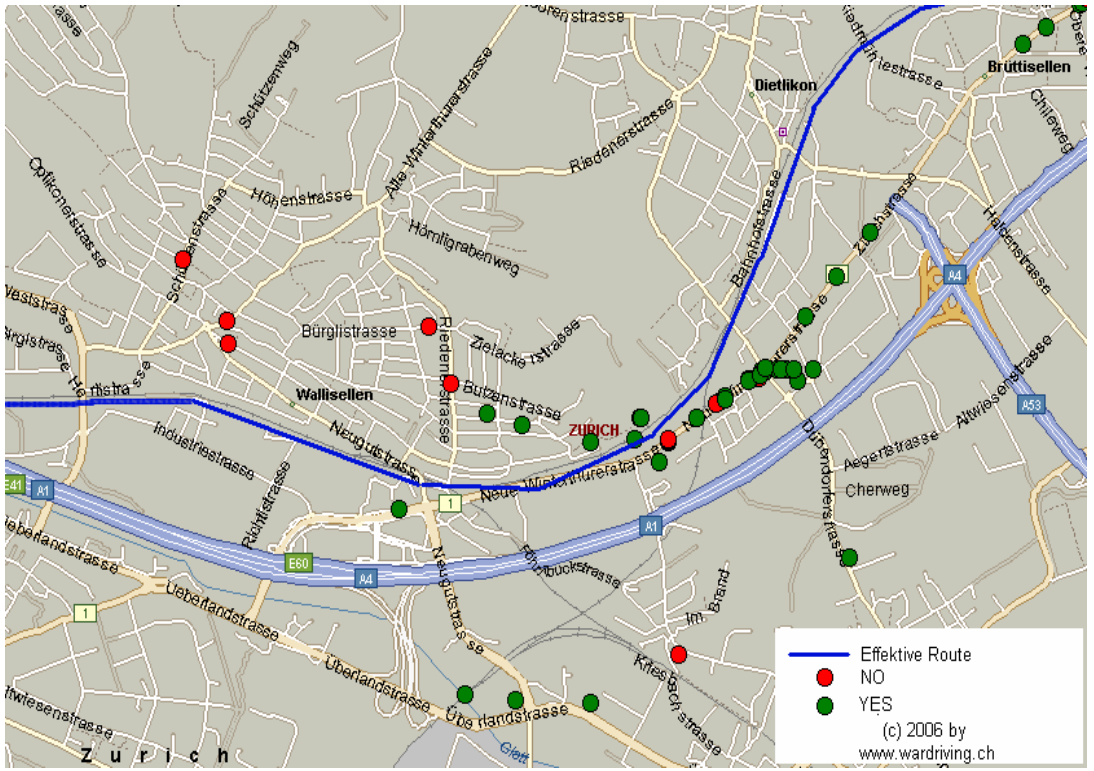
Sammeln von Daten.
(MAC + SSID)

Datenauswertung



Bekannte MAC/AP‘s

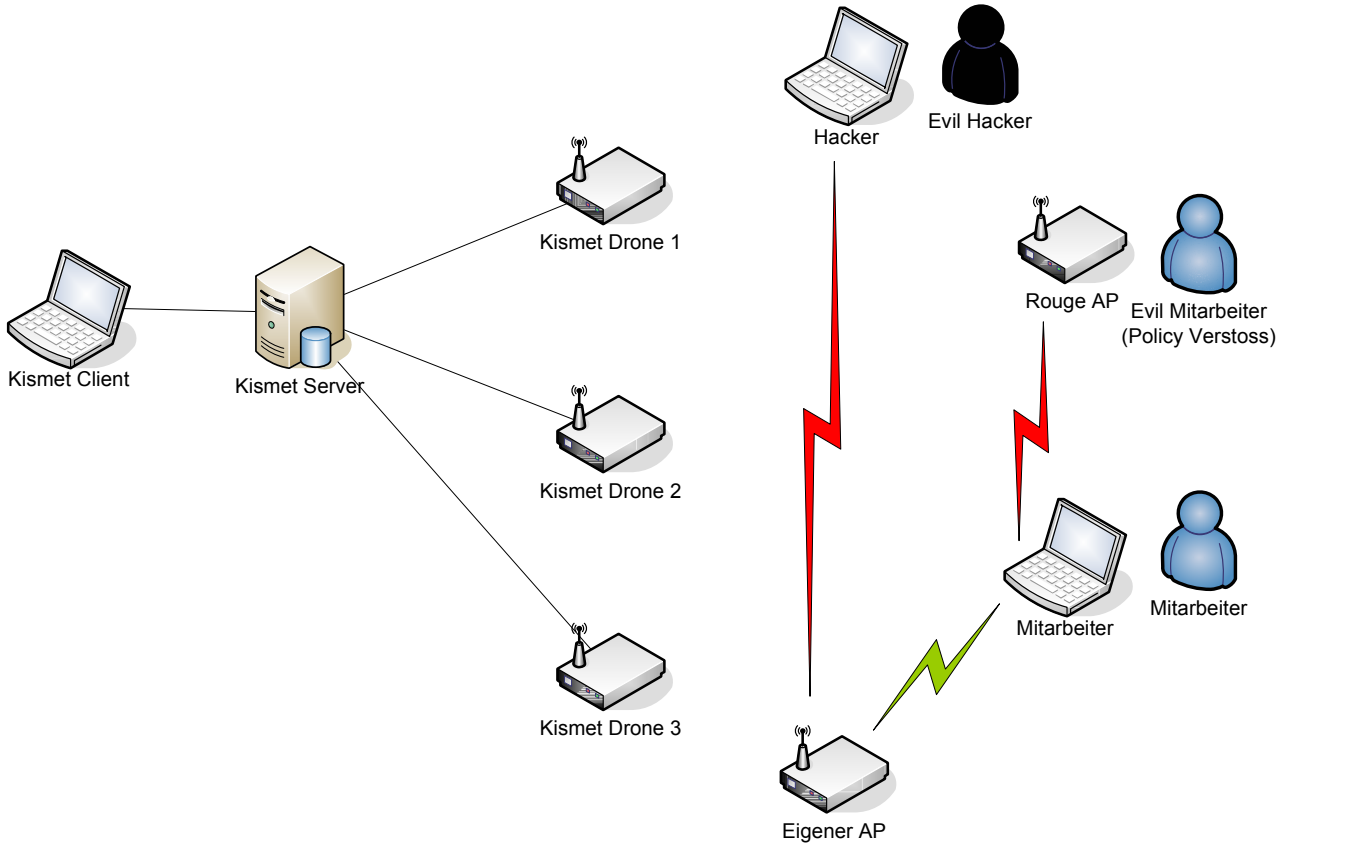
MAC zu AP Zuordnung



Kismet Drone

- Kontrolle der Wireless Aktivitäten in einem Definierten Bereich. (Firmen-Gebäude)
- „Out of the (Kismet) Box“ Unterstützung
- Datenaufzeichnung von Wireless Datenverkehr.
- Individuell den Bedürfnissen anpassbar.

Kismet Dronen



Kismet Drone	Projekt	skymaster
	Author:	chw
	Version:	0.7
	Updated	18.4.2006
© 2006 bychw/wardriving.ch	Vertraulich	

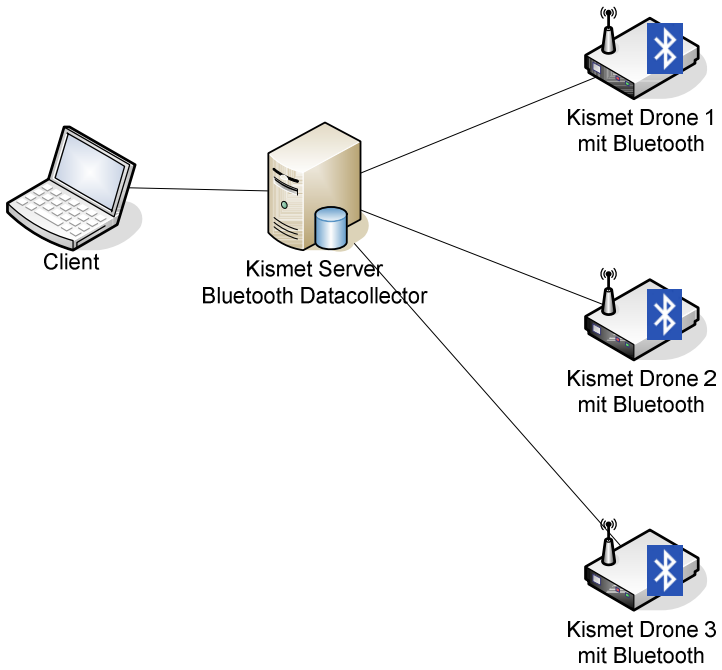
Nachteile Kismet Drone

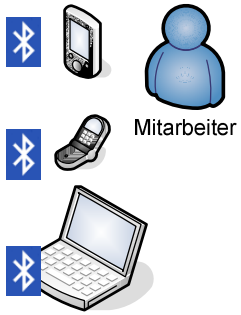
- Keine verschlüsselte Datenübertragung von der Drone zum Server und vom Server zum Client.
- Entwicklung noch nicht abgeschlossen
- Low-Cost Überwachung
- Eigene Entwicklung Notwendig !

Bluetooth Überwachung

- Ausbau der Funküberwachung
- Policy Überprüfung
- Anwesenheitskontrolle
  Locationtracking ?
- Nur Bluetooth Geräte mit Sichtbarer ID werden gesehen.

Bluetooth Überwachung

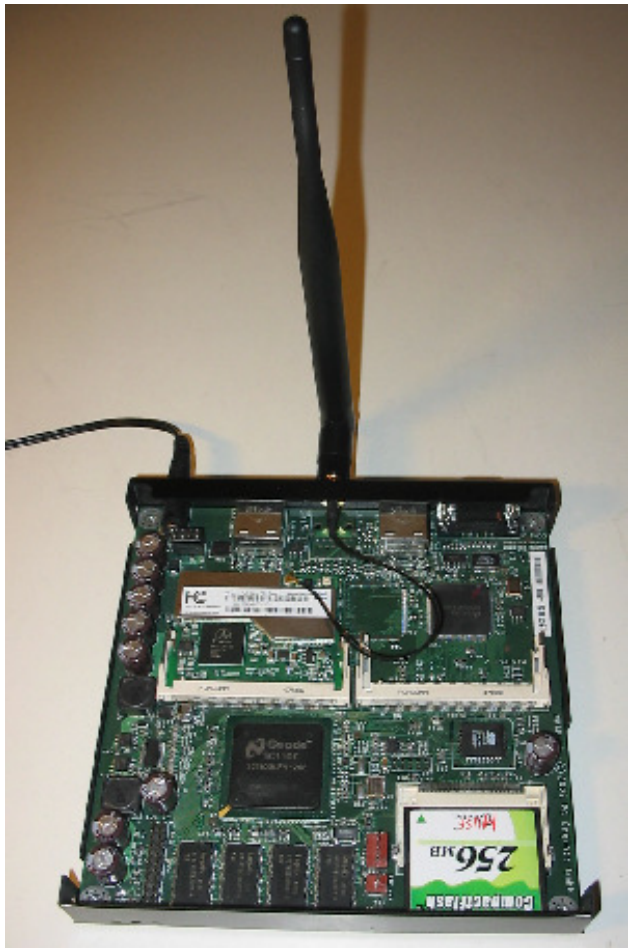




Bluetooth Dronen	Projekt	Bluetooth
	Author:	chw
	Version:	0.3
	Updated	18.4.2006
© 2006 bychw/wardriving.ch	Vertraulich	

Wireless Honeypot

- Standalone Honeypot (www.honeyd.org) ohne Internet Anschluss.
- Simuliert Open AP und Verbindung ins Internet, mit einigen lokalen Server.
- Testinstallation in Betrieb. („just for fun“)



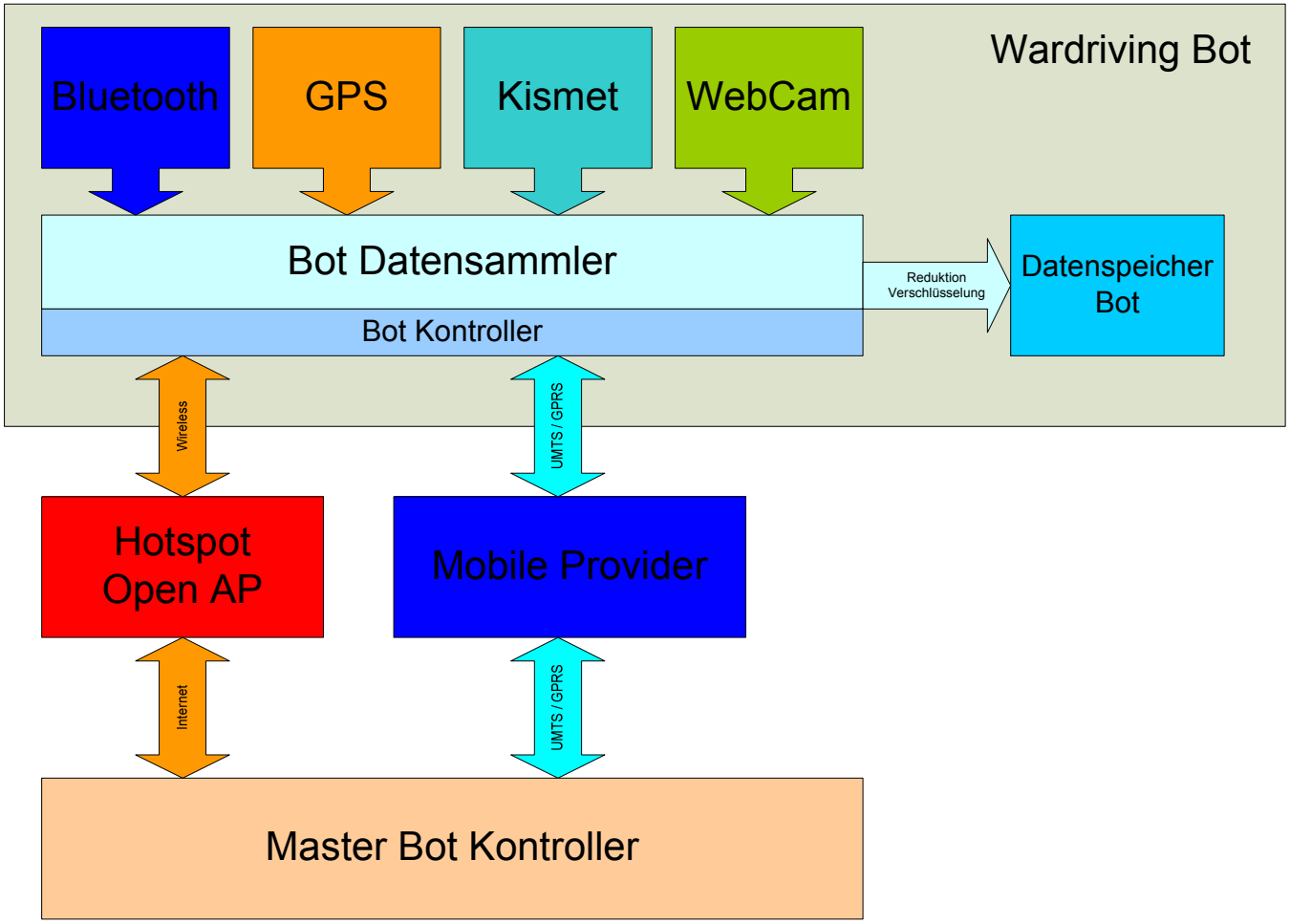
Wardriving Bots

- Wardriving Next Generation
- Die Wardriving Bots sollen sich selber melden und Autonom Handeln.
- Wir basteln uns ein Wardriving Bot Netz.

Bot Controlling

- Kommunikationsweg Wireless
  - Open AP
  - Free Hotspots
  - Closed Hotspots (MOBILE / MONZOON)
- Kommunikationsweg UMTS / GPRS
  - Datenkommunikation via UMTS oder GPRS denkbar, verursacht aber laufend Kosten.

Wardriving Bot Overview



Allgemeiner Ablauf

1. Suche SSID
2. Verbinde zur SSID
3. IP Adresse / DNS / Default Gateway via DHCP
4. Entscheide Anhand der SSID, welche Kommunikation möglich ist.
   Bsp.
   SSID tsunami -> privater (Open) AP
   SSID bluewin-netopia -> privater (Open) AP
   SSID linksys -> privater (Open) AP
   SSID MOBILE -> Swisscom Mobile Hotspot
   SSID MONZOON -> monzoon networks Hotspot
5. Sende SSID+MAC vom AP
6. Sende weitere gesammelte Daten
7. Empfange neue Konfigurationen
   - neue kismet konfiguration
   - Zeitsynchronisation
8. Sende Umgebungs Infos
   (Bsp. Bild Webcam / Bluetoothinfos)

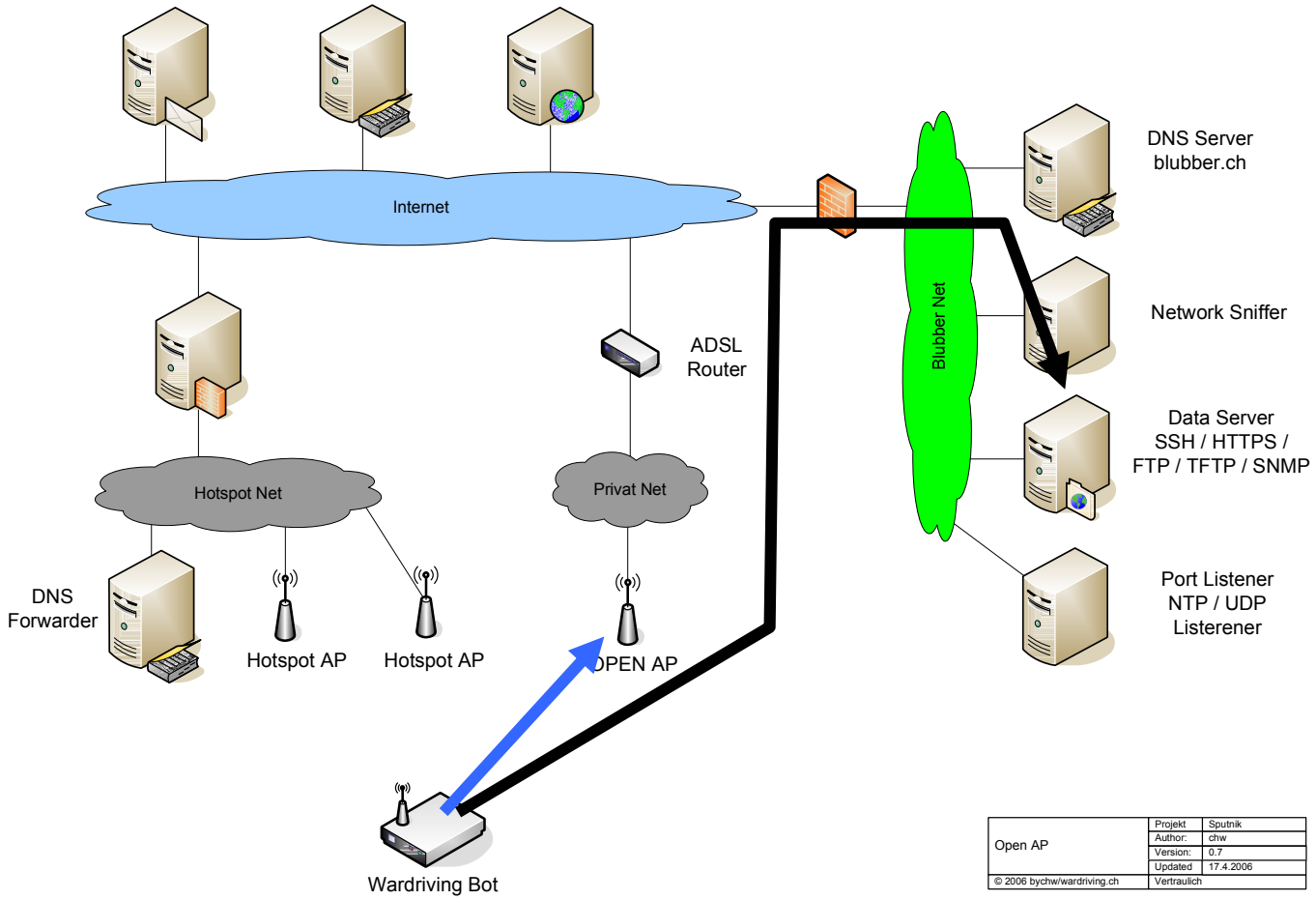
Bekannte Probleme

- Kurze Verbindungszeit, wenn Bot in Bewegung ist.
- Signalschwankungen
- Entscheidung, welche Übertragungswege genutzt werden können.
- IP Adressierung
- Signalabbruch während der Datenübertragung
- Sicherstellung der Datenübertragung
- Mithören beim AP
- Empfangen von Befehlen hinter NAT
- Legalität ?!

Open AP

- Einfacher Verbindungsaufbau
  No WEP
- DHCP Server (meistens)
- Normalerweise keine Einschränkungen Richtung Internet
- Keine Schutzmassnahmen
- Keine IDS Systeme bei Privat Usern
- Legal ???

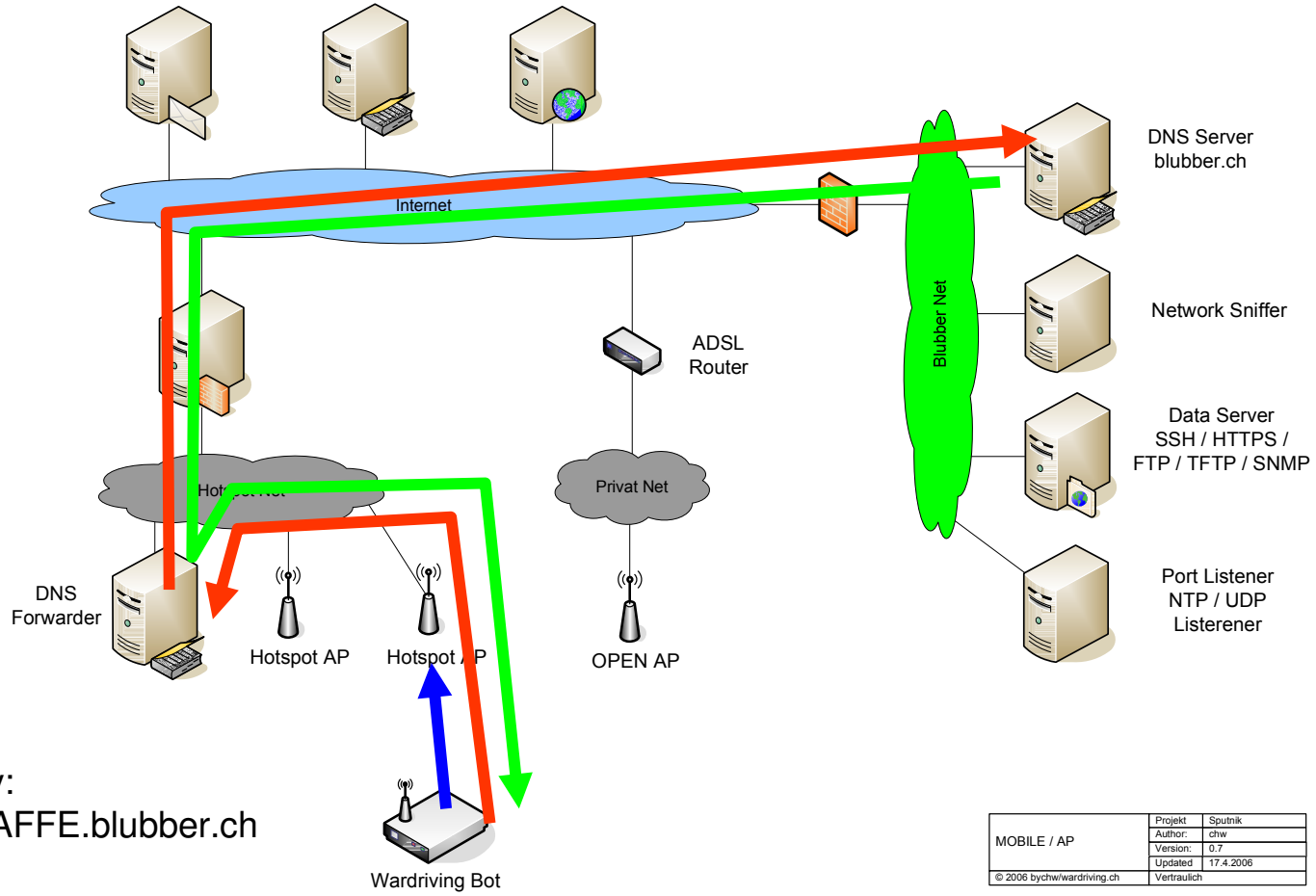
Open AP


Internet
ADSL
Router
Blubber Net
DNS Server
blubber.ch
Network Sniffer
Data Server
SSH / HTTPS /
FTP / TFTP / SNMP
Port Listener
NTP / UDP
Listerener
Hotspot Net
Privat Net
DNS
Forwarder
Hotspot AP
Hotspot AP
OPEN AP
Wardriving Bot
Open AP
Projekt
Sputnik
Author:
chw
Version:
0.7
Updated
17.4.2006
© 2006 bychw/wardriving.ch
Vertraulich

Hotspot (Bsp. MOBILE)

- Einfacher Verbindungsaufbau SSID MOBILE
- DHCP
- Keine Normale Datenübertragung via TCP/IP möglich.
- Tunneling via DNS
- Legal ?

HotSpot (Bsp. MOBILE)



DNS Querry:
01DEAD00AFFE.blubber.ch

DNS Answer: 127.0.0.1

MOBILE / AP	Projekt	Sputnik
	Author:	chw
	Version:	0.7
	Updated	17.4.2006
© 2006 bychw/wardriving.ch	Vertraulich	

Weitere Tricks

- Tunneling via UDP
  - NTP (123)
  - DNS (53)
  - SNMP (161)
  - TFTP (69)
  - VPN Ports
- Tunneling via ICMP
  - ICMP Request/Reply
  - ICMP Port Unreachable
- Individuell aufgebaute Datenpakete
  Bsp.
  RST Pakete mit Daten
- gespoofte Datenpakete
- Übernehmen einer bestehenden Verbindung (MAC Adresse)
- Infoversand via Mail
- …….

- Einfach alle Tricks, mit denen man Daten oder Datenpakete durch eine Firewall senden kann.

Bad Things / Missbrauch

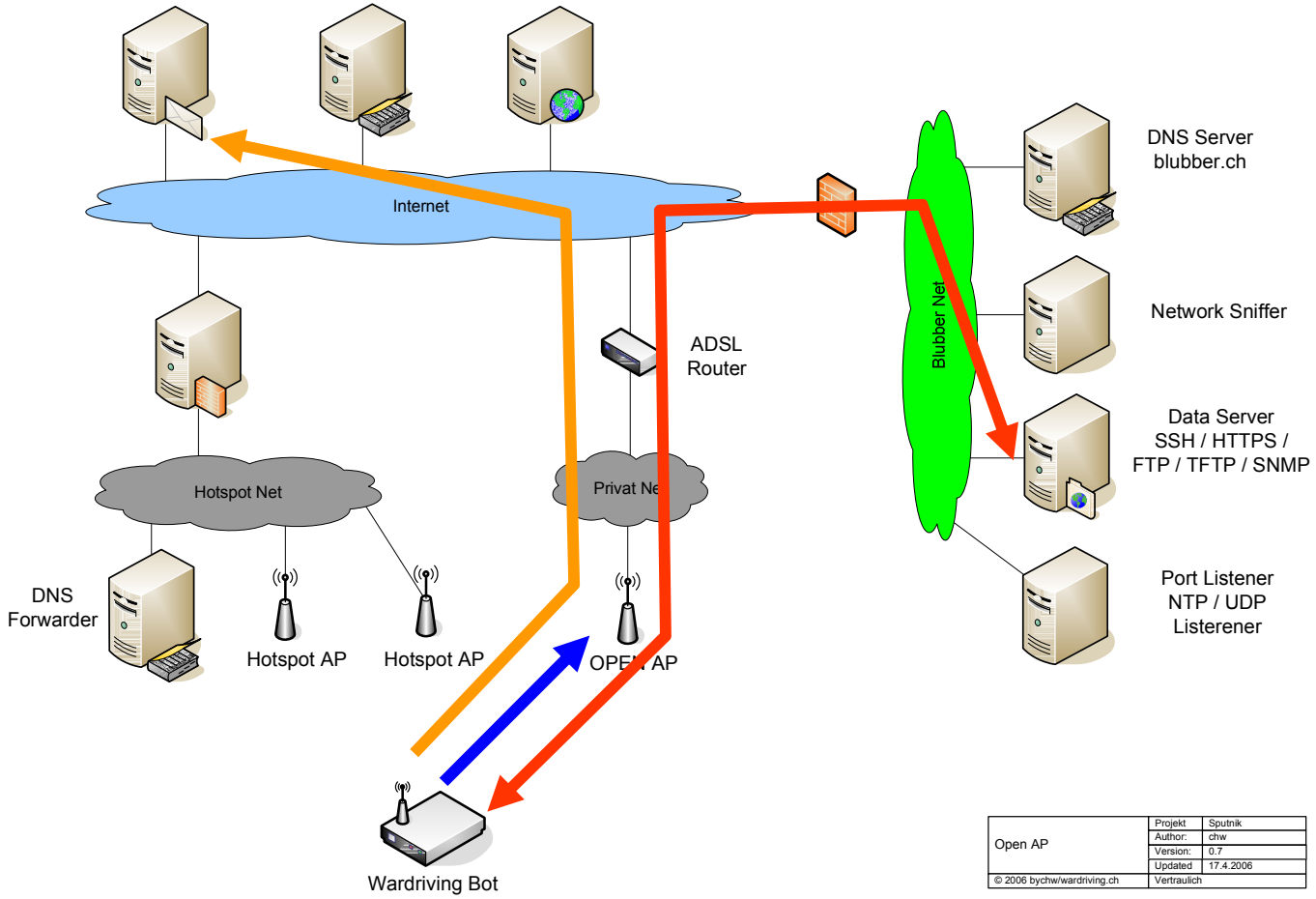
- Spam Bot
- Werkspionage
- Störsender
- WIFI Sniffer
- Scannen via Open AP

- Einfach alles, was man mit einem normalen BOT auch machen kann.

Alle Punkte sind als „Proof of Concept“ zu sehen !

Von der Nachahmung und Umsetzung wird dringend abgeraten !

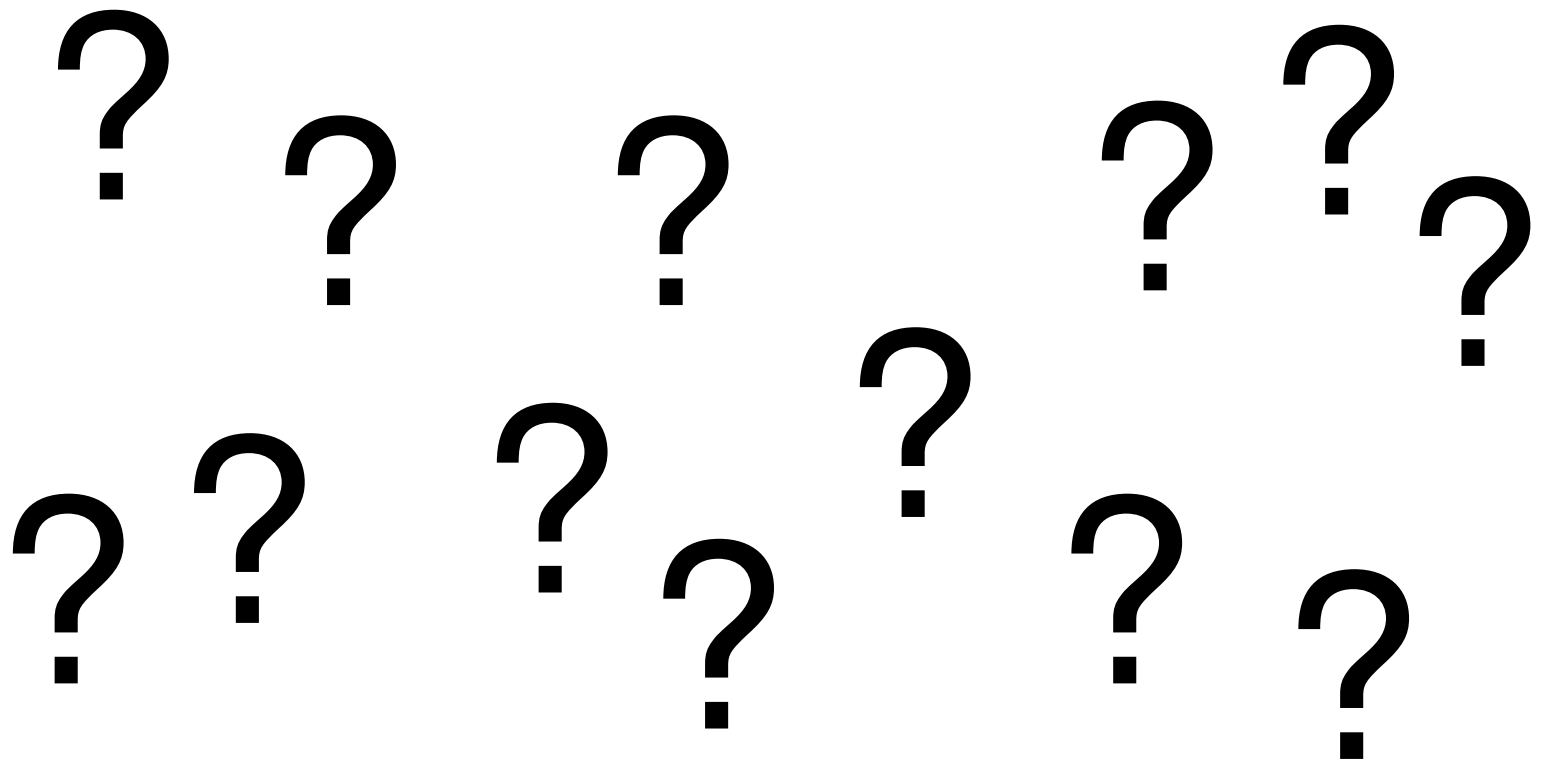
SPAM Bot


Internet
ADSL
Router
Blubber Net
DNS Server
blubber.ch
Network Sniffer
Data Server
SSH / HTTPS /
FTP / TFTP / SNMP
Port Listener
NTP / UDP
Listerener
Hotspot Net
Privat Ne
DNS
Forwarder
Hotspot AP
Hotspot AP
OPEN AP
Wardriving Bot
Open AP
Projekt
Sputnik
Author:
chw
Version:
0.7
Updated
17.4.2006
© 2006 bychw/wardriving.ch
Vertraulich

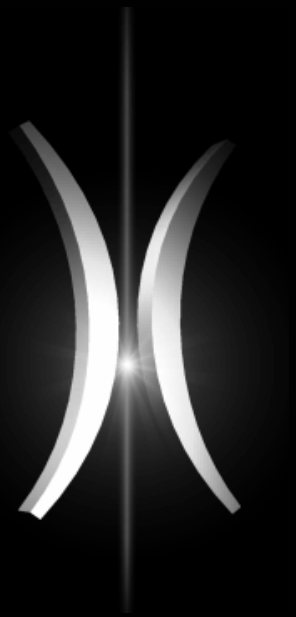
Weitere Ideen

- Einbindung von RFID Scannern
- Erschütterungs-Sensor für Stromsparfunktion (nur Daten Aufzeichnung, wenn das Gerät in Bewegung ist.)
- Wir werden noch weitere Ideen haben….
  …….Garantiert!

Fragen ?



www.wardriving.ch
wardriver@wardriving.ch



here at wardriving labs where the future is being made today!