



Oli Schacher
Cédric Wider

Warsurfer

When Connection Matters

Diplomanden	Oli Schacher, Cédric Wider
Examinator	Prof. Dr. Andreas Steffen
Themengebiet	Wireless, Wardriving



Arbeitskleidung von Thinkgeek

Aufgabenstellung: Unter Wardriving versteht man die systematische Suche nach Drahtlosnetzwerken während einer Autofahrt. Sobald ein geeignetes Netz gefunden wurde, wird versucht, eine Verbindung ins Internet herzustellen. Mittlerweile ist die Dichte von ungeschützten Netzen so hoch, dass es möglich sein sollte, während einer Busfahrt eine mehr oder weniger konstante Verbindung ins Internet herzustellen.

Ziel der Arbeit: Es soll eine Software entwickelt werden, die es ermöglicht, automatisiert auf Wireless LANs zuzugreifen, welche während ei-

ner Busfahrt in Reichweite gelangen. Es soll nach Realisierungsmöglichkeiten gesucht werden, eine Internetverbindung auf der logischen Ebene aufrechtzuerhalten, auch wenn diese auf der physikalischen Schicht oft unterbrochen wird. Das heisst, laufende Applikationen sollen durch die Unterbrüche und den ständigen Wechsel der IP-Adresse nicht beeinträchtigt werden. Eine Proof-of-Concept Implementation soll zumindest das automatisierte Herunterladen von E-Mail-Nachrichten erlauben.

```

root@wgwhr: /home/gryphius - Shell - Konsole
Session Edit View Bookmarks Settings Help
Network List—(Autofit)
Name      T W Ch  Packts  Flags  IP Range
! MONKEYISLAND  A Y 006  1430   0.0.0.0
! default      A N 006   807   T4  192.168.0.102
! linksys      A N 006   780   0.0.0.0
! warzone_public_wireless  A N 011   295   A4  192.168.1.1

Info
Ntwrks      4
Pckets     3322
Cryptd      96
Weak         0
Noise        0
Discrd      43
Elapsd     00:02:18

Status
Ch 11 @ 11.00 mbit
Found new network "linksys" bssid 00:13:10:3F:A1:09 Crypt N Ch 6 @ 54.00 mbi
Found IP 192.168.0.64 for default::00:04:23:6B:B8:B5 via TCP
Found IP 192.168.1.1 for warzone_public_wireless::00:06:25:67:29:C6 via ARP
Battery: AC 100%

```

Wireless Sniffer „Kismet“ in Aktion

Lösung: Mit Hilfe eines für Drahtlosnetzwerke optimierten Sniffers („Kismet“) werden die verfügbaren Netze erkannt und nach diversen Kriterien kategorisiert:

- Verschlüsselung
- Hersteller
- Standardeinstellungen
- Signalstärke
- Verfügbarkeit

Basierend auf diesen Daten versucht die Applikation, die geeigneten Netzwerkeinstellungen zu erraten, um möglichst schnell auf einen Accesspoint zu verbinden. Sämtliche Informationen werden in einer Datenbank gespeichert, um bei einem späteren Testlauf bessere Resultate zu erzielen. Das Roaming wird mittels einer VPN („Virtual Private Network“) Software realisiert.