# Konzept eines WLAN Gateways unter Benutzung von VPN und Zertifikaten

Labor für Kommunikationstechnik und Datensicherheit
FH Köln - Campus Gummersbach

Mentor: Prof. Karsch

Referenten:
Daniel Jedecke
Manuel Atug
Dennis Engel
Jörg Ebbinghaus

# Inhalt

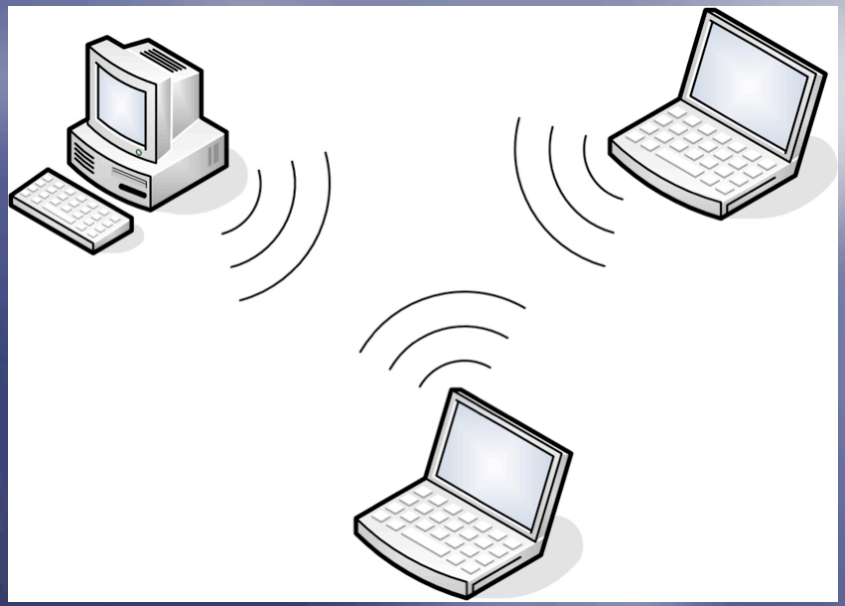
- Einführung zu Wireless LAN
- Probleme mit Wireless LAN und WEP
- Lösungsansatz
- Sicher durch VPN?
- Umsetzung mit Hilfe von FreeS/WAN
- Probleme mit FreeS/WAN
- Ausblick
- Demonstration des IPSec Tunnels

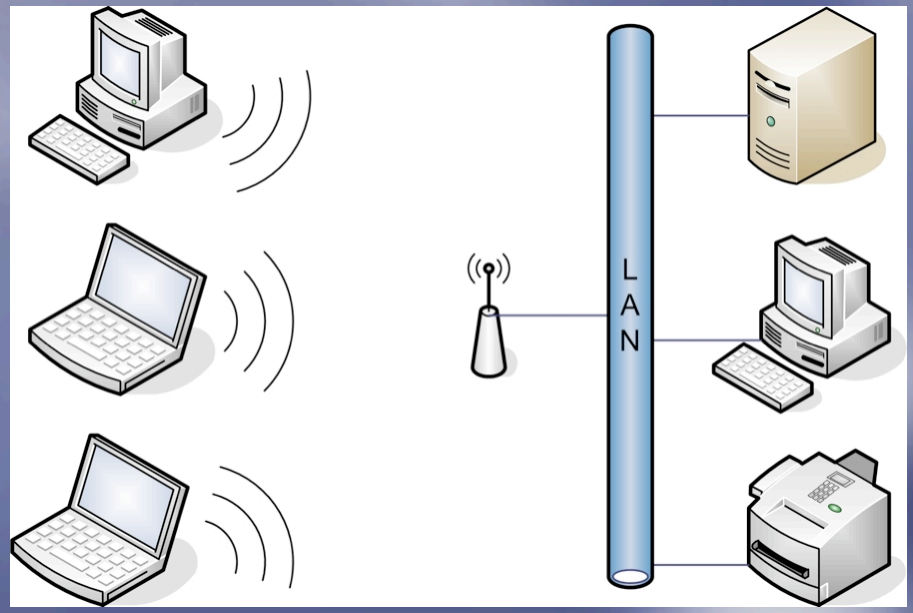
# Einführung zu Wireless LAN

# Einführung Wireless LAN

- Wireless LAN (Wireless Local Area Network)
- 1997 verabschiedeter Standard 802.11
- Aktuell relevante Standards:
  - 802.11b, 11 MBit/sec
  - 802.11.g, 54 MBit/sec
- Große Wachstumsraten, steigende Beliebtheit
- Sorgloser Umgang mit Sicherheit

# Ad-Hoc Modus






# Infrastructure Modus

# Marktrelevanz

- 22,7 Millionen verkaufte Access Points und Wireless LAN Karten im Jahr 2003
- 214% Steigerung gegenüber 2002
- 1,7 Milliarden US-Dollar Umsatz (2003)
- Umsatzsteigerung von 140% gegenüber 2002

Quelle: heise.de

# Sicherheits-Mechanismen

- SSID - Service Set ID
- MAC - Media Access Control
- WEP - Wired Equivalent Privacy

# Inhalt

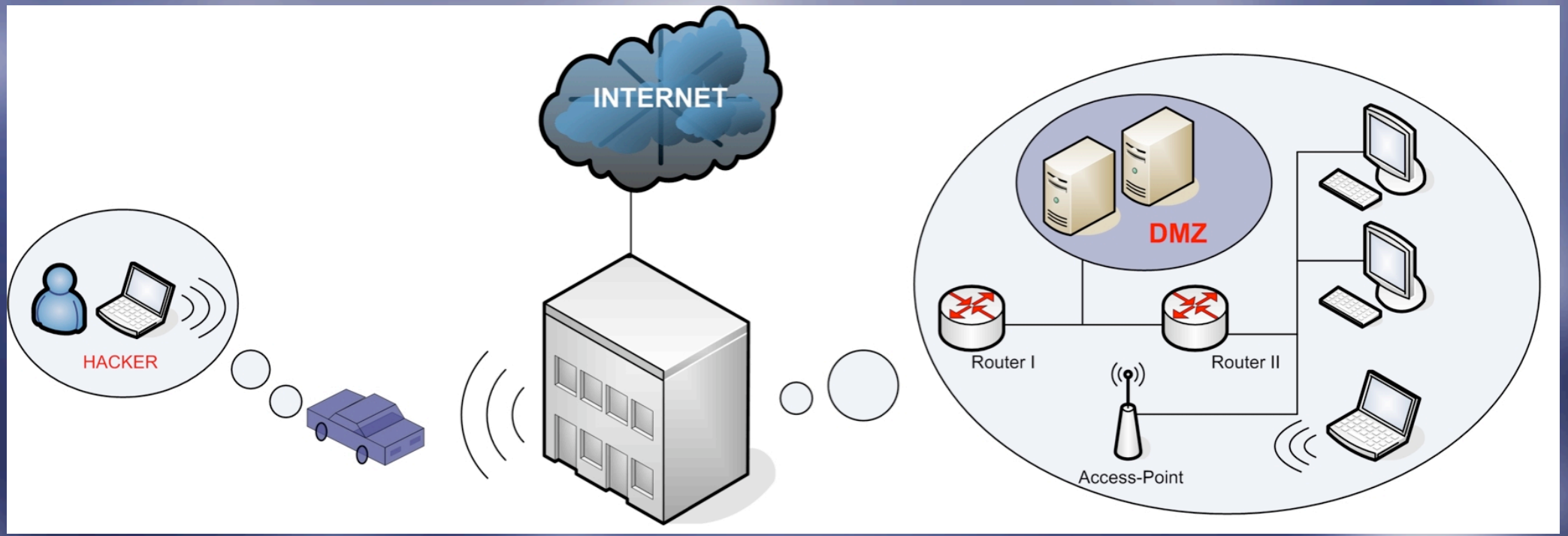
- Einführung zu Wireless LAN
- Probleme mit Wireless LAN und WEP
- Lösungsansatz
- Sicher durch VPN?
- Umsetzung mit Hilfe von FreeS/WAN
- Probleme mit FreeS/WAN
- Ausblick
- Demonstration des IPSec Tunnels

# Probleme mit Wireless Lan und WEP

Von 1000 geprüften Wireless LAN Netzen in München, Berlin und Hannover waren 500 ungeschützt.
(Quelle: www.heise.de)

- Keine Aktivierung der Sicherheits-Mechanismen
- Beibehalten der Standardeinstellungen
- Fehlerhafte und unzureichende Sicherheits-Mechanismen im Wireless-LAN

# Beispielangriff auf ein Unternehmen



# Erste Tipps zur Absicherung (1)

- Standard SSID ändern
- Kryptische SSID Namen wählen
- SSID Broadcast am Access Point abschalten
- Standard Passwörter zur Konfiguration des Access Points ändern
- MAC Adressen-Filterung am Access Point einschalten

# Erste Tipps zur Absicherung (2)

- WEP Verschlüsselung einschalten
- Periodischer Wechsel von WEP Schlüssel, SSID und Zugangspasswörtern
- Aufstellungsort und Antennencharakteristik des Access Points in Bezug auf die Ausbreitung der Funkwellen berücksichtigen
- Sendeleistung am Access Point anpassen, um möglichst nur das gewünschte Gebiet funktechnisch zu versorgen

# Erste Tipps zur Absicherung (3)

- statische IP Adressen vergeben
- Firmware Updates auf den Access Point einspielen
- Wireless LAN bei Nichtbenutzung abschalten
- Konfiguration und Administration des Access Points nur über sichere Kanäle
- Authentisierungsmethode “Open” wählen, anstatt “Shared Key”

# Trotzdem gibt es Sicherheitsmängel (1)

- Sicherheitsmechanismen sind unzureichend
- Schwachstellen im RC4 Design der WEP Verschlüsselung
- Ermittlung des WEP Schlüssels durch passives abhören

# Trotzdem gibt es Sicherheitsmängel (2)

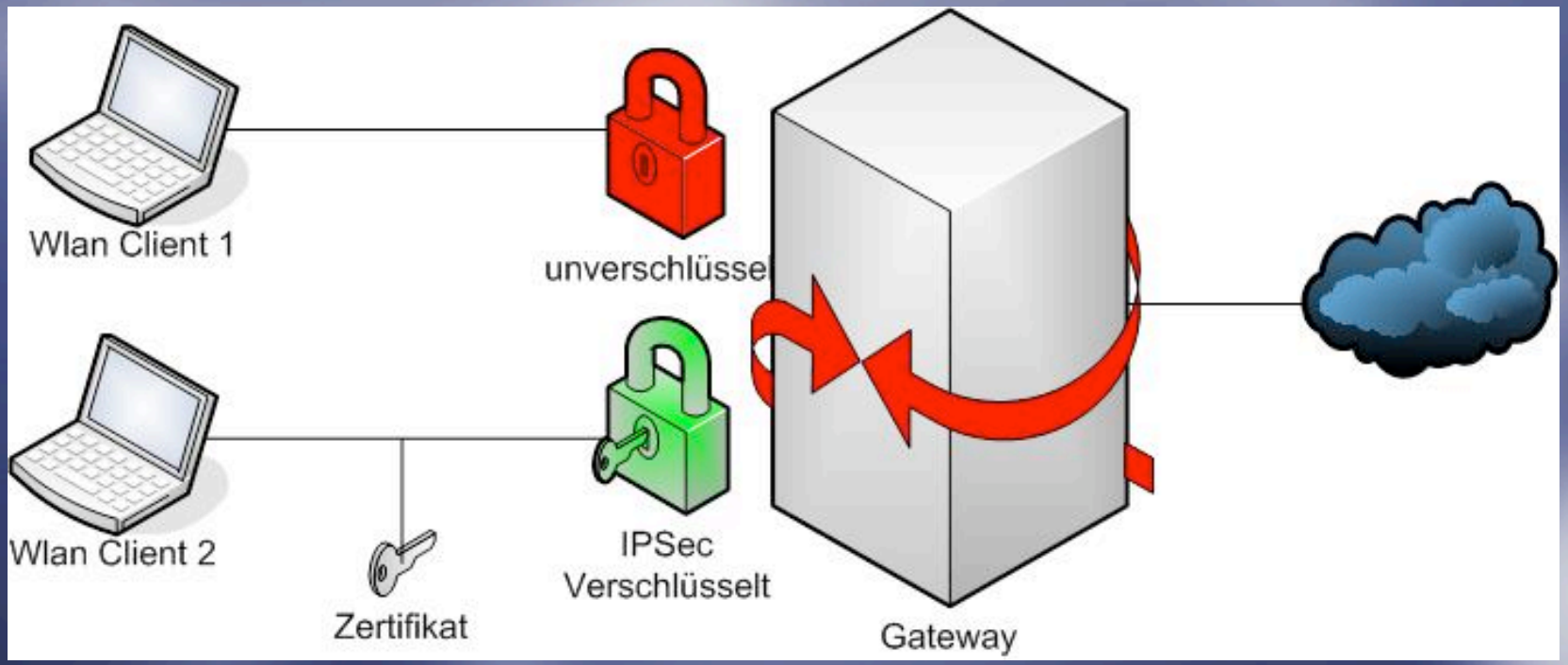
- Bei einer Paketgröße von 1024 Byte sind nur ca. 3.81 GB Daten für einen erfolgversprechenden Angriff auf den RC4 Algorithmus nötig
- Bei einer durchschnittlichen Auslastung von 5 MBit/s könnte ein Angriff nach ca. 1 Stunde und 42 Minuten erfolgreich sein

# Inhalt

- Einführung zu Wireless LAN
- Probleme mit Wireless LAN und WEP
- Lösungsansatz
- Sicher durch VPN?
- Umsetzung mit Hilfe von FreeS/WAN
- Probleme mit FreeS/WAN
- Ausblick
- Demonstration des IPSec Tunnels

# Lösungsansatz

# Beispiel für eine Absicherung



# Wer darf rein?

- Netzwerkzugang nur für bekannte Personen
- Jeder User muss einzeln löschbar sein
- Kein “Shared Key” Verfahren
- User müssen sich sicher authentisieren

# Unsere Idee

- Vergabe von Zertifikaten für jeden User
- Anmeldung am zentralen Gateway über ein VPN (Virtual Private Network)
- Benutzerverwaltung über eine CA (Certification Authority)
- Einfach anzuwenden unter den gängigen Betriebssytemen

# Wie können wir unsere Idee umsetzen?

- Installieren und Konfigurieren eines Gateways
- Einrichten eines VPN Tunnels
- Testbenutzer
- Auswertung der Daten

# Inhalt

- Einführung zu Wireless LAN
- Probleme mit Wireless LAN und WEP
- Lösungsansatz
- Sicher durch VPN?
- Umsetzung mit Hilfe von FreeS/WAN
- Probleme mit FreeS/WAN
- Ausblick
- Demonstration des IPSec Tunnels

# Sicher durch VPN?

# Was ist VPN?

- VPN steht für Virtual Private Network
- VPN dient zum Tunneln privater Daten durch unsichere Netze wie dem Internet
- VPN ist für Anwendungen transparent
- Eine bekannte Implementierung, um Netzwerke durch VPN abzusichern, ist IPSec

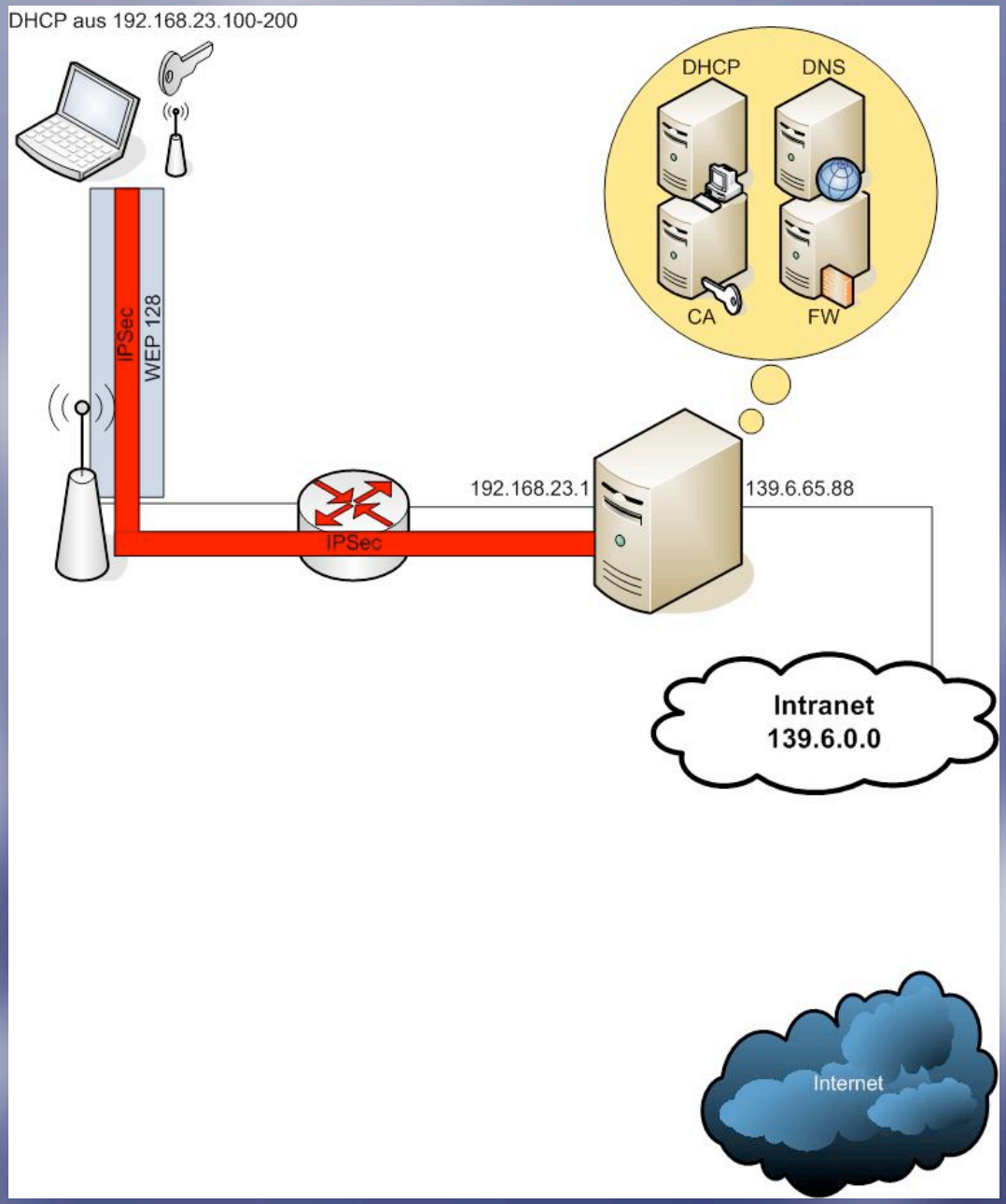
# Wie hilft uns VPN als Lösung?

- Tunneln der Daten durch das unsichere Wireless LAN
- Einfache Konfiguration der Firewall für das VPN
- Durch die Erweiterung mit Zertifikaten vereinfachte User Administration
- VPN unsichtbar für Browser oder E-Mail Programme

# VPN mit IPSec

- IPSec steht für IP Security
- Erweiterung des TCP/IP Protokolls, um sichere Verbindungen zu ermöglichen
- IPSec setzt an der Netzwerk-Ebene an und ist somit transparent für Programme
- Bekannteste OpenSource-Variante ist FreeS/WAN (jetzt Openswan)

# Lösungs-skizze



# Inhalt

- Einführung zu Wireless LAN
- Probleme mit Wireless LAN und WEP
- Lösungsansatz
- Sicher durch VPN?
- Umsetzung mit Hilfe von FreeS/WAN
- Probleme mit FreeS/WAN
- Ausblick
- Demonstration des IPSec Tunnels

# Umsetzung mit Hilfe von FreeS/WAN

# Server-Konfiguration (1)

- OS: Debian 3.0 RC2 “Woody” aka stable
- Kernel: 2.4.24 mit
  - FreeS/WAN 2.04
  - X.509 Patch 1.4.8
- FIAIF Firewall Skriptsystem
- OpenSSL 0.9.7d

# Server-Konfiguration (2)

- ipsec.secrets
  - RSA Key + Keyname + Passphrase
- ipsec.conf
  - conn roadwarrior
    - left / leftsubnet
    - leftrsasigkey / leftcert / leftid
    - right / rightrsasigkey

# Client-Konfiguration

- OS: MS Win 2000 + SP4 / MS Win XP + SP1
- Support Tools von Installations-CD
- Nutzung von E-Bootis VPN Tools
- Einbindung des PK12-Zertifikates

# Inhalt

- Einführung zu Wireless LAN
- Probleme mit Wireless LAN und WEP
- Lösungsansatz
- Sicher durch VPN?
- Umsetzung mit Hilfe von FreeS/WAN
- Probleme mit FreeS/WAN
- Ausblick
- Demonstration des IPSec Tunnels

# Probleme mit FreeS/WAN

# Probleme unter Windows

- Relativ umständliche Installation
- Probleme bei der Fehlerbehandlung
- Windows nicht 100% kompatibel zum IPSec Standard

# Probleme unter Linux

- Bisher nur stabil unter Kernel 2.4
- Kernel 2.6 hat eigene IPSec Unterstützung (Racoon)
- Keine GUI Programme
- Konfiguration nicht trivial

# Inhalt

- Einführung zu Wireless LAN
- Probleme mit Wireless LAN und WEP
- Lösungsansatz
- Sicher durch VPN?
- Umsetzung mit Hilfe von FreeS/WAN
- Probleme mit FreeS/WAN
- Ausblick
- Demonstration des IPSec Tunnels

# Ausblick

# Was ist noch zu tun?

- Webbasierte Benutzerverwaltung
- Anpassung an Openswan
- Vereinfachen des Installationsprozesses
- Auslagern der Zertifizierungstelle auf ein seperates System

# Umsetzung in einem FH-weiten Umfeld

- User könnten über Ihre Benutzerkennung ein Zertifikat beantragen
- Da wir NAT benutzen, muss ein gutes Logging-System auf dem Gateway laufen
- Rechtliche Fragen müßten geklärt werden

# Mögliche Folgeprojekte

- Transparantes Proxy-System
- Automatisierte Zertifikatsvergabe
- Roaming
- Erweiterung auf Racoon (Kernel 2.6)

# Inhalt

- Einführung zu Wireless LAN
- Probleme mit Wireless LAN und WEP
- Lösungsansatz
- Sicher durch VPN?
- Umsetzung mit Hilfe von FreeS/WAN
- Probleme mit FreeS/WAN
- Ausblick
- Demonstration des IPSec Tunnels

# Demonstration des IPSec Tunnels

# Konzept eines WLAN Gateways unter Benutzung von VPN und Zertifikaten

Labor für Kommunikationstechnik und Datensicherheit
FH Köln - Campus Gummersbach

Mentor: Prof. Karsch

Referenten:
Daniel Jedecke
Manuel Atug
Dennis Engel
Jörg Ebbinghaus

Fragen?

E-Mail: ktds@gm.fh-koeln.de