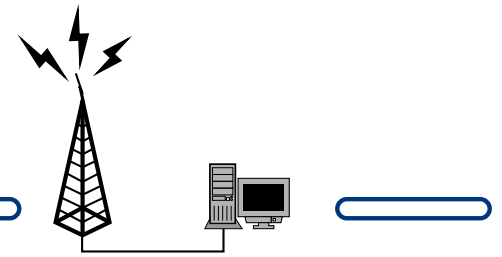
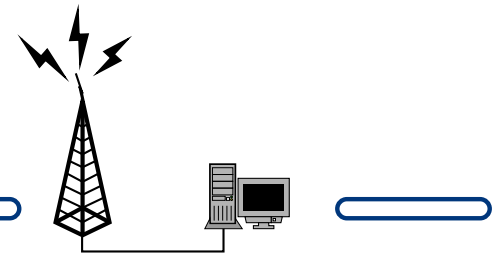


# Datensicherheit und Datenschutz in Funknetzen am Beispiel WLAN nach 802.11b

Markus Brückner (vortrag@slash-me.net)



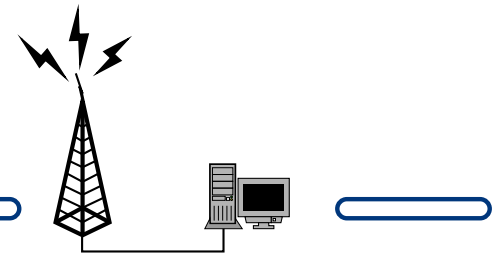
- Sicherungsmöglichkeiten klassischer kabelgebundener Netze
- Veränderte Bedingungen im Funknetz
- VPN-Techniken und ihre Eignung für Funknetze
- Die Realität - Projekt WHIRL



# Sicherungsmöglichkeiten klassischer kabelgebundener Netze

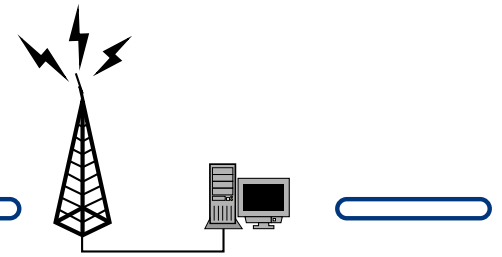
## Sicherungsmöglichkeiten ... ⇒ physikalisch

---



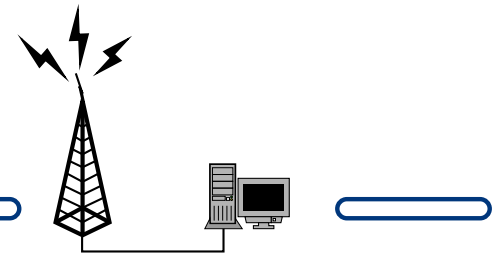
Sicherung gegen physikalischen Zugriff:

- Kabelverlegung in Wänden oder unter der Erde
- abschließbare Schränke für aktive Technik
- Rechenzentren mit Zugangskontrollen und Bewachung
- Schranküberwachungssysteme, Alarmanlagen
- ...



### Sicherung gegen logischen Zugriff:

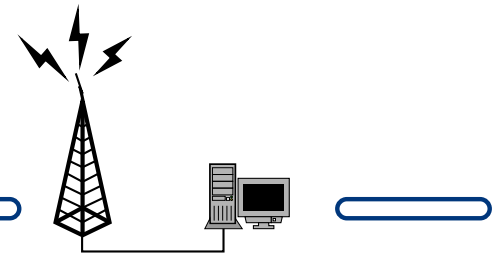
- Port Security
- Paketfilter
- Application Level Gateways
- Virens Scanner
- Intrusion Detection Systems
- (NAT)
- . . . .



# Veränderte Bedingungen im Funknetz

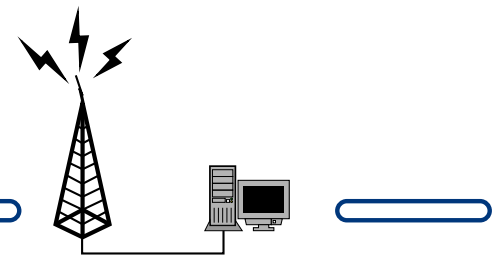
# Veränderte Bedingungen im Funknetz

---



## Gliederung:

- Allgemeines
- Technische Grundlagen Wireless LAN nach 802.11b
- Neue Probleme
- Lösungsmöglichkeiten

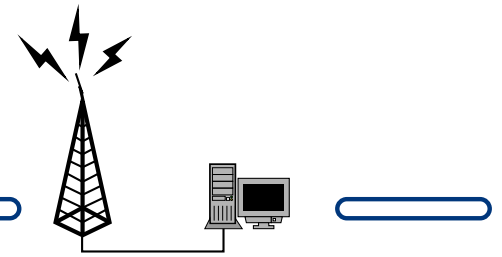


Durch die physikalischen Eigenschaften von Funknetzen ergeben sich veränderte Bedingungen bei deren Sicherung:

### **Wellenausbreitung stoppt nicht an Grundstücksgrenze oder Wänden**

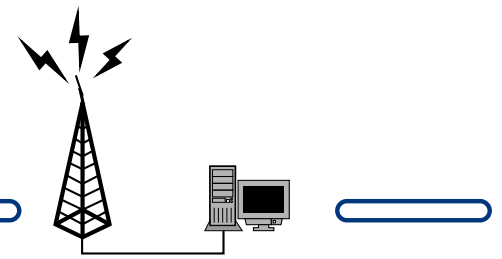
Durch die freie Ausbreitung der Trägerwellen des Funknetzes ist keine Einschränkung auf einzelne Räume oder Gebäude möglich.

**Begrenzte Anzahl an Frequenzen** Aufgrund der begrenzten Anzahl an vorhandenen Trägerfrequenzen sind Überlappungen von verschiedenen Funkzellen mit gleichen Trägerfrequenzen möglich → Störungen (Beispiel: 2 Funktastaturen auf dem selben Kanal in angrenzenden Räumen sorgen für „Buchstabensalat“)



### Funknetze nach IEEE 802.11b

- Standardisierung seit 1999 in IEEE 802.11b mit einer Geschwindigkeit von 11MBit/s netto
- 13 (Europa) bzw. 11 (weltweit) Kanäle im ISM-Band (Industrial, Scientific & Medical, 2.4 GHz)
- typische Sendeleistung 35 mW, damit Reichweiten zwischen 30m (innerhalb von Gebäuden) und 500m (absolut freies Gelände)
- Benutzung eines Service Set Identifier (SSID) zur Trennung verschiedener logischer Netze

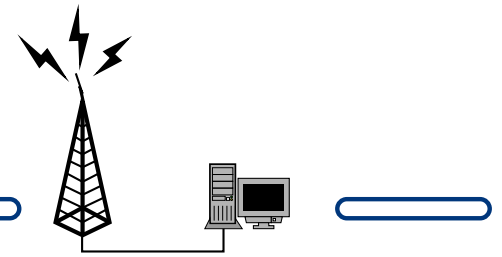


3 mögliche Vernetzungsstrategien:

**IBSS - Independant Basic Service Set** auch Adhoc-Netzwerk  
genannte Möglichkeit, eine beliebige Anzahl von Clients  
innerhalb einer Reichweite direkt zu vernetzen

**BSS - Basic Service Set** selten gebräuchliche Konstruktion,  
mit der die Größe eines IBSS mit Hilfe eines  
Accesspointes als Repeater verdoppelt wird

**ESS - Extended Service Set** Netzwerk mit mehreren  
Accesspoints, zwischen denen ein Client frei wechseln  
kann (Roaming)



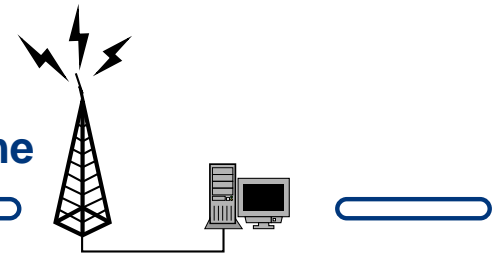
### Hardware:

- aufgrund der kurzen Wellenlänge der Trägerfrequenzen (13 cm) sehr kleine Antennen → WLAN-Ausrüstung ist platzsparend zu bauen
- moderne Fertigungstechnologien ermöglichen kostengünstige Produktion

⇒ WLAN ist mittlerweile weit verbreitet

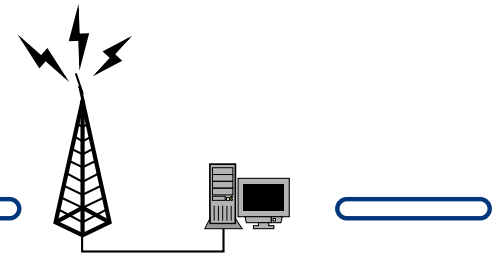
## Veränderte Bedingungen im Funknetz → Neue Probleme

---



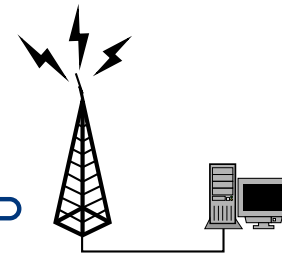
Aufgrund der veränderten Bedingungen in Funknetzen ergeben sich gegenüber kabelgebundenen Netzen neue Probleme. Einige der klassischen Sicherheitsstrategien greifen im WLAN nicht mehr und müssen ergänzt oder ersetzt werden.

- Physische Trennung zwischen „innen“ und „außen“ nur noch bedingt möglich
- Lokalisierung von Clients teilweise schwierig (besonders bei großen Installationen wie z.B. dem WILNET)
- Keinerlei Kontrolle über Empfänger von Paketen



### Neue Lösungsmöglichkeiten:

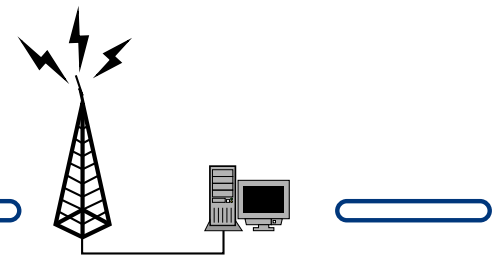
- Reichweitenbeschränkung durch bauliche Maßnahmen  
⇒ meist nicht möglich
- Beschränkung aller Dienste auf bestimmte Adressbereiche ⇒ leichte Umgehbarkeit
- Authentifizierung aller Netzwerkteilnehmer (z.B. über RADIUS)
- Verschlüsselung des Netzwerkverkehrs als Basis für ein VPN



# VPN-Techniken und ihre Eignung für Funknetze

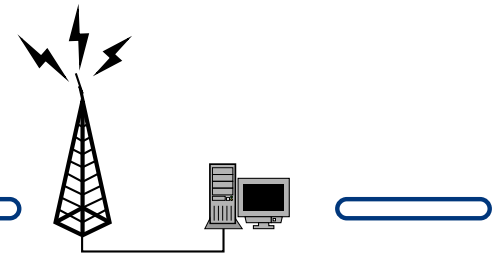
# VPN-Techniken und ihre Eignung für Funknetze

---



## Gliederung:

- Definition VPN
- Eigenschaften von Transportprotokollen
  - Source Routing
  - Label Switch Path von MPLS
- VPN-Protokolle
  - WEP
  - PPTP
  - IPSec
  - andere (CIPE, vtund,...)
- Eignung zur Sicherung von Funknetzen



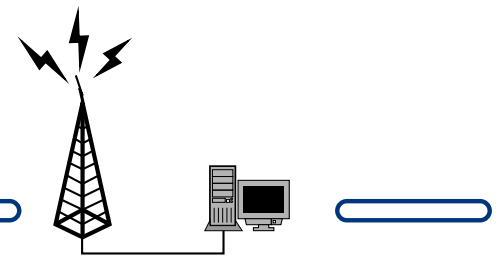
VPN:

„[...]any network built upon a public network and partitioned for use by individual customers.“

Cisco Enterprise: Virtual Private Network Design

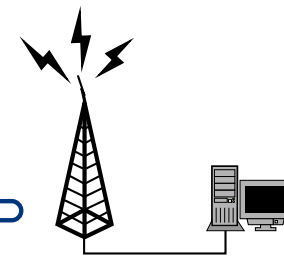
Eigenschaften:

- Nutzung eines öffentlichen Netzes
- Abschottung des Datenverkehrs gegenüber anderen Nutzern
- Transparenz gegenüber Anwendungen zur Schaffung eines virtuellen Netzes „im Netz“



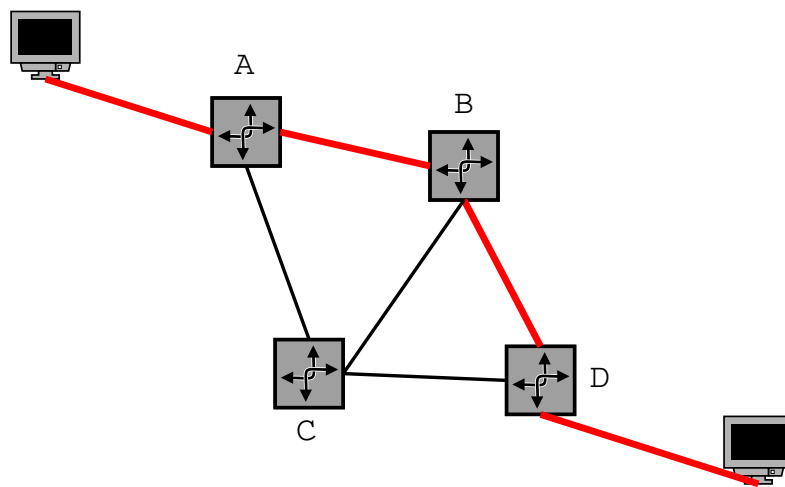
## Source Routing

- im IPv4-Header definierte Option
- Unterscheidung zwischen Strict und Loose Source Routing
- Absender gibt Weg des Paketes durch das Netz vollständig (Strict SR) oder teilweise (Loose SR) an
- maximal 9 Einträge in der Routing-Tabelle möglich
- bei den meisten Providern deaktiviert

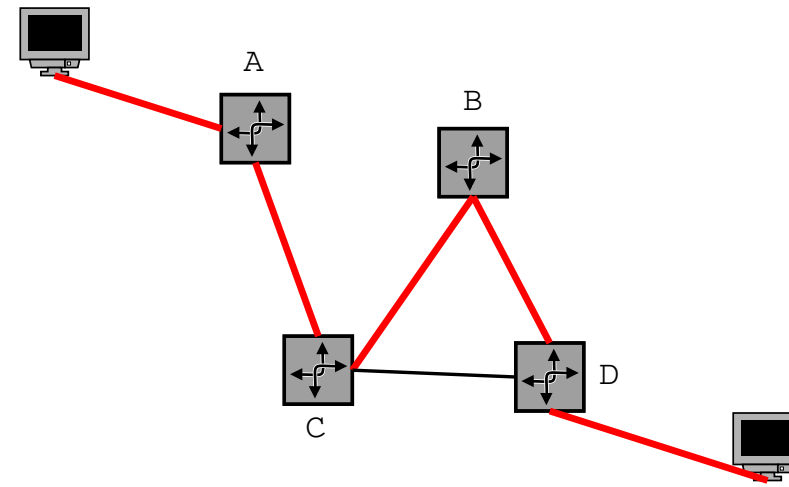


## Beispiel Strict & Loose SR

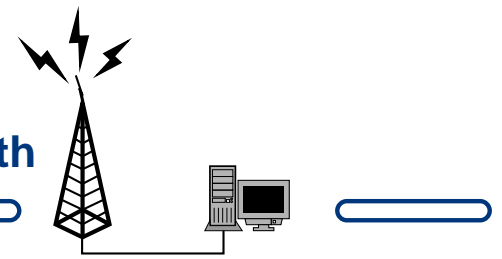
(Routing-Informationen enthalten jeweils A, B und D als zu durchlaufende Router)



Strict SR

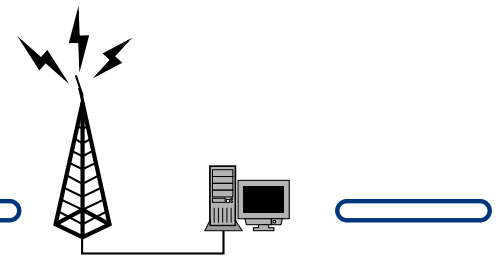


Loose SR



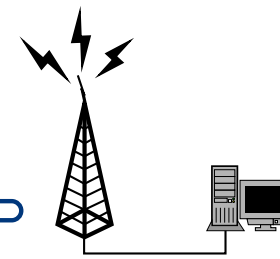
## Label Switch Path in MPLS-Netzen

- Pakete werden in MPLS-Netzen anhand eines sog. Labels weitergeleitet
- nach dem Aufbau der Verbindung (mit Vergabe der Labels) laufen alle Pakete im Normalfall den selben Weg ⇒ Label Switch Path
- unter Mithilfe des Carriers ist so eine festgelegte Route für die Pakete möglich

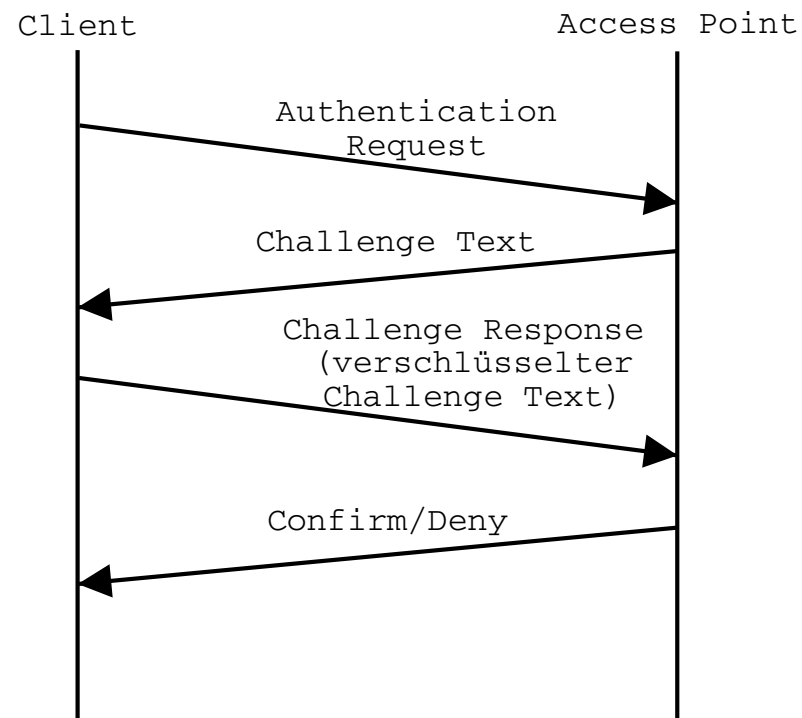


## WEP

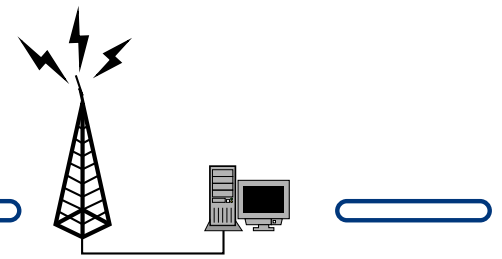
- Wired Equivalent Privacy
- in IEEE 802.11 spezifizierte Architektur zur Verschlüsselung und optional Authentifizierung im WLAN
- Authentifizierung und Verschlüsselung über gemeinsame Passwörter
- Verwendung eines Stromchiffrierers mit 40 (bzw. 128) Bit Schlüssellänge



Authentifizierung bei WEP geschieht über ein einfaches Challenge-Response-Verfahren mit gemeinsamem Passwort.

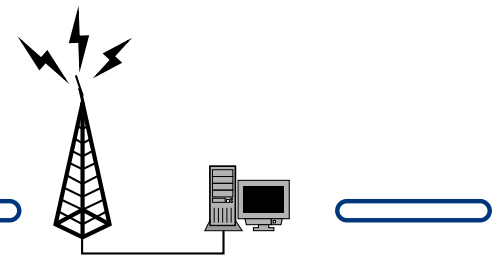


Challenge-Response-Authentifizierung bei WEP



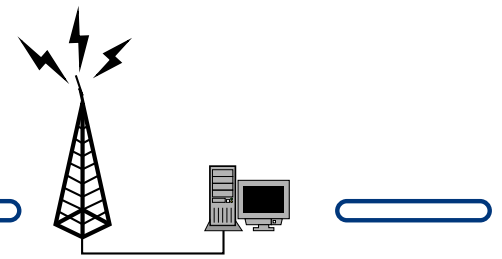
### Details des Verschlüsselungsalgorithmus von WEP:

- RC4 als Pseudozufallszahlengenerator, Ausgaben mittels XOR mit Klartext verknüpft
- Schlüssel wird gebildet aus 24 Bit Initialisierungsvektor (zufällig) und dem gemeinsamen Passwort (fest)
- lineare CRC-Prüfsumme zur Sicherung der Datenintegrität



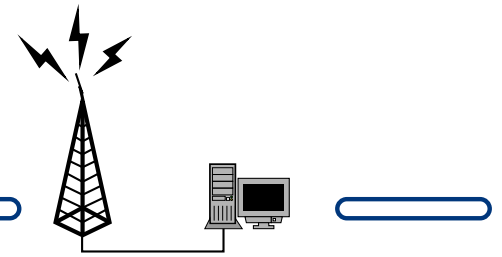
### Schwächen von WEP:

- IEEE 802.11 macht keinerlei Aussagen über Schlüsselmanagement  $\Rightarrow$  meist nur ein Passwort für das gesamte Netz
- 24 Bit Initialisierungsvektor zu klein  $\Rightarrow$  Wiederholung eines identischen Schlüssels bereits nach einigen Stunden
- Schwäche im verwendeten Betriebsmodus von RC4 ermöglicht Brechen des Schlüssels relativ schnell (5-6 Mio. Pakete)
- Kombination aus RC4 und CRC-Prüfsumme ermöglicht unentdeckte Manipulation der Daten



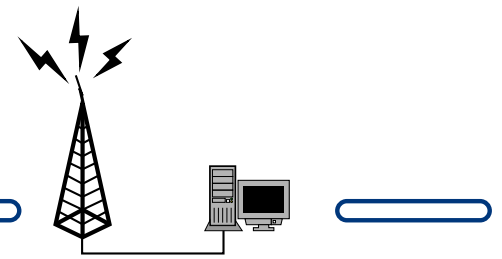
### PPTP

- Point-to-Point Tunneling Protokoll (RFC 2637)
- von Microsoft entwickelte Erweiterung zu PPP
- Protokoll zum Auf-/Abbau von virtuellen Verbindungen
- modifizierte Version von IP GRE zum Transport von PPP-Paketen über IP-Netze
- keine eigene Verschlüsselungsfunktionalität, daher meist in Zusammenhang mit MPPE (RFC 3078) verwendet



### PPTP Verschlüsselung/Authentifizierung:

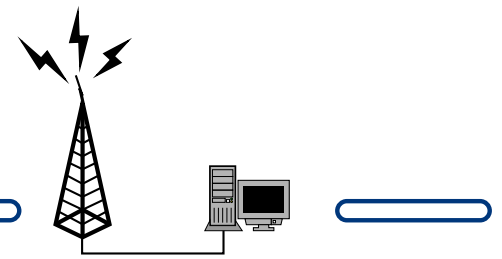
- Authentifizierung mittels gemeinsamem Passwort über ein Challenge-Response-Verfahren (MS-CHAPv2)
- Serverauthentifizierung findet statt
- Verschlüsselung bei MPPE erfolgt mittels RC4
- Unterschiedliche Schlüssel für beide Richtungen eines Tunnels aus dem Passwort berechnet



### Kritik an PPTP/MPPE:

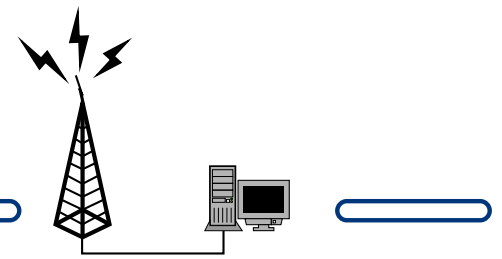
- erste Version des Protokolls vollkommen unbrauchbar
- neue Versionen können unter bestimmten Umständen veranlaßt werden, auf das Verhalten der ersten Protokollversion zurückzufallen
- Offline-Attacke gegen das verwendete Passwort ist möglich

⇒ Sicherheit des Systems steht und fällt mit der Einstellung des Servers und der Stärke der Nutzerpasswörter.



### IPSec

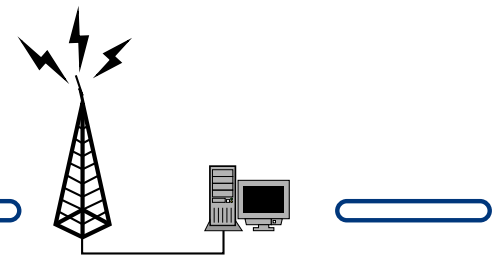
- Security Architecture for the Internet Protocol (RFC 2401ff.)
- optionaler Bestandteil von IPv4, vorgeschriebener von IPv6
- komplexe Architektur aus zwei zusätzlichen IP-Protokollen (ESP und AH), sowie einem Schlüsselaustauschprotokoll (IKE)
- Sicherung der Datenintegrität über kryptographisch starke Hash-Funktionen



- Angebot verschiedener Verschlüsselungsalgorithmen (z.B. DES, 3DES, IDEA, ...) und Hash-Funktionen (MD5, SHA-1, ...)
- Möglichkeit der Nutzung einer PKI zur Schlüsselverwaltung
- zwei Betriebsmodi

**Transport mode** direkte Manipulation der IP-Pakete und versenden an den Empfänger

**Tunneling mode** Einpacken der IP-Pakete in den Datenteil eines weiteren IP-Paketes

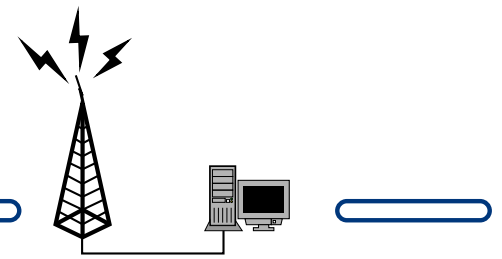


Schlussfolgerung:

⇒ IPSec bietet alle notwendigen Eigenschaften zur  
Wahrung von Integrität, Vertraulichkeit und Authentizität von  
Daten und Kommunikationspartnern.

*aber...*

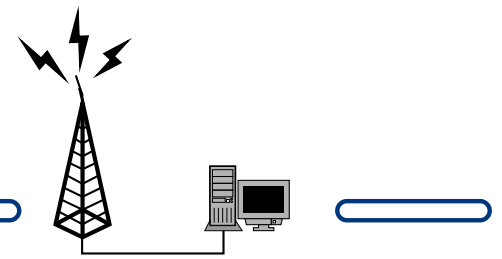
- kompliziertes Protokoll
- aufgrund hoher Flexibilität ständig Inkompatibilitäten  
zwischen verschiedenen Anbietern von IPSec-Software
- Probleme mit bestimmten Netzinstallationen (NAT)



Es existieren noch andere Möglichkeiten, VPNs aufzubauen, bspw. CIPE, vtund etc., die alle an einem oder mehreren der folgenden Punkte Probleme aufweisen:

- mangelnde Standardisierung oder Unterstützung durch große Hersteller
- Verfügbarkeit nur auf wenigen Betriebssystemen
- unsichere oder ineffiziente Protokollentwürfe

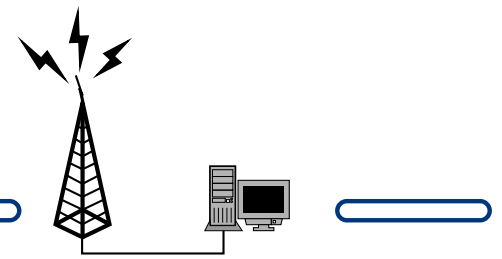
⇒ können in bestimmten Fällen einfache und wirkungsvolle Lösungen darstellen, sind jedoch für allgemeine Anwendungen zu unflexibel.



Eignung der verschiedenen VPN-Techniken zur Sicherung von Funknetzen

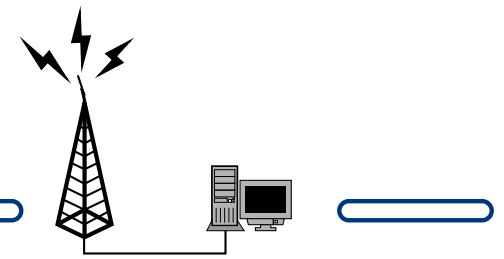
Zwei Beispiele für typische WLAN-Netze:

- Studenten-WG mit einem Accesspoint und 4 Client-Rechnern, die sich einen DSL-Anschluss teilen
- WILNET - Campus WLAN der TU Ilmenau



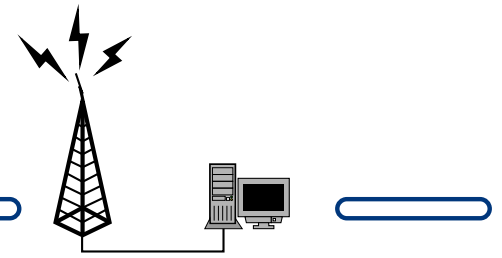
**Source Routing & Label Switch Path** ungeeignet zur Sicherung von Funknetzen, da diese Protokollbestandteile sich auf die Trennung verschiedener Netzwerkströme innerhalb eines öffentlichen Netzes konzentrieren und keinerlei Fähigkeiten wie Authentifizierung oder Verschlüsselung beherrschen

**WEP** Die Studenten-WG ist durch WEP vorm dem zufälligen Mithören ihrer Daten geschützt und kann bei regelmäßigem Passwortwechsel auch den Zugang zu ihrem Accesspoint kontrollieren. Im WILNET wäre eine Authentifizierung mittels WEP durch das gemeinsame Passwort aller Clients, sowie das regelmäßige Wechseln dessen, unmöglich.

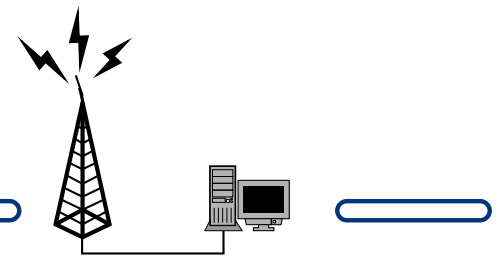


**PPTP** Durch den Einsatz eines zentralen Knotens, auf dem alle PPTP-Tunnel terminiert werden wäre eine Sicherung sowohl des Netzes der Studenten-WG, als auch des WILNET möglich. Eine direkte Kommunikation der Clients untereinander ist nur möglich, wenn diese wiederum ein gemeinsames Passwort besitzen.

**IPSec** Bei Einsatz einer PKI wäre die Sicherung sowohl des Netzzugangs, als auch der Kommunikation der Clients untereinander in der WG und dem WILNET problemlos möglich. Für große Installationen wie das WILNET ist IPSec die einzige umfassende und benutzbare Sicherungsvariante.

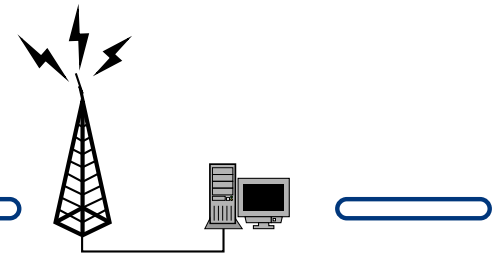


# Die Realität - Projekt WHIRL



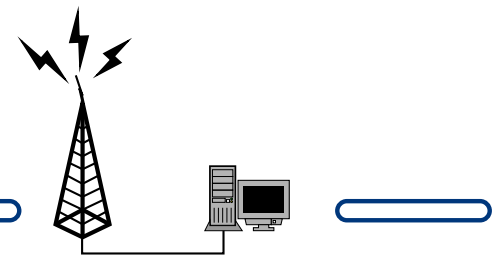
## Projekt WHIRL

- begleitendes Projekt zur Vorlesung „Sicherheit in Rechnernetzen“ im WS 2002/2003
- Ziele:
  - Zählung/Schätzung vorhandener Funknetze
  - Statistiken über die Absicherung der Netze
- Vorgehensweise
  - Aufteilung von Teams aus mehreren Personen auf verschiedene Gegenden in Erfurt und Aufspüren von WLAN-Signalen mit Hilfe von Laptops und einfachen WLAN-Karten
  - statistische Erfassung bestimmter Netzparameter (hauptsächlich der verwendeten Verschlüsselung)



### Ergebnisse:

- erschreckend hohe Anzahl ungesicherter Netze (34 Netze insgesamt, davon 10 mittels WEP gesichert, 1 mittels IPSec)
- relativ hohe Anzahl an Netzen (12) mit Standard-SSID des Herstellers  $\Rightarrow$  vermutlich gänzlich unkonfiguriert
- einziges Netz mit IPSec als Sicherung war die TU Ilmenau  $\Rightarrow$  Aufsetzen von IPSec für kleinere Installationen zu aufwändig

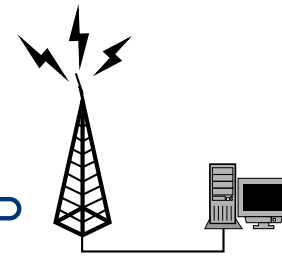


## Schlussfolgerungen:

- Trotz Verfügbarkeit von Sicherungsmöglichkeiten werden diese kaum eingesetzt
- Wahrscheinlich aufgrund mangelhafter Dokumentation seitens der Hersteller werden Accesspoints oft vollkommen unkonfiguriert und offen aufgestellt
- Selbst wenn genügend Dokumentation/Fachkenntnis vorhanden ist, bspw. die SSID des Accesspoints zu konfigurieren, so scheint doch oft kein wirkliches Problembewußtsein bzgl. der Sicherheitsrisiken im WLAN vorhanden zu sein.

Fragen? Anregungen? Öffentliche Hinrichtung?

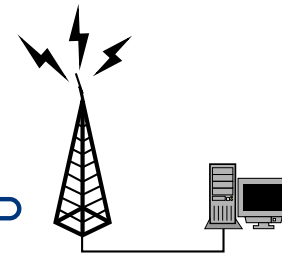
---



Fragen? Anregungen?  
Öffentliche Hinrichtung?

Danke

---



# Danke für die Aufmerksamkeit

Folien: <http://work.slash-me.net/vortrag-wlan-sicherheit/folien.pdf>

Kontakt: Markus Brückner <[vortrag@slash-me.net](mailto:vortrag@slash-me.net)>