# Aufbau von Wireless LANs (802.11b) mit besonderer Bedachtnahme auf Absicherung mittels IPSEC/SSH

**WLAN Forum**
marcus evans conferences
Hotel Inter-Continental Berlin
2002-01-17

**Jodok Sutterlüty**
**Mayr-Melnhof Karton, Wien**

email: jodok.sutterluety@mm-karton.com
tel: +43 1 50136 0

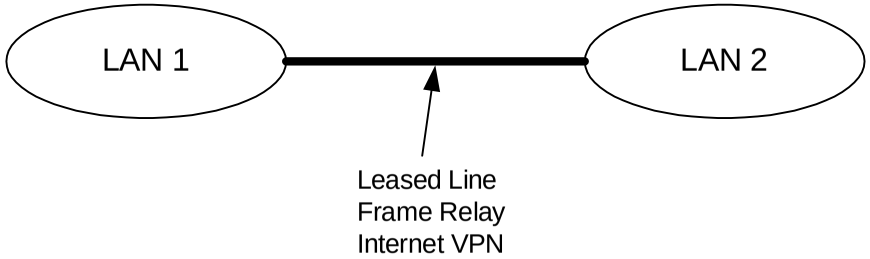
http://www.mm-karton.com/wlan

# INHALT

- WLAN im Einsatz
  - Koppelung von LAN Segmenten
  - Local Area Networks (LAN) basierend auf WLANs
  - Sicherheitsrisiken
- Herkömmliche Sicherheitskonzepte
  - Trafficfiltering
  - MAC-Filtering
  - WEP
  - Verschlüsselung auf Applikationsebene
- Fortgeschrittene Sicherheitskonzepte mittels IPSEC
  - Idee
  - Implementierung
- Demonstration eines mittels IPSEC abgesicherten WLANs
- Zusammenfassung

# WLAN im Einsaz - Koppelung von LAN Segmenten

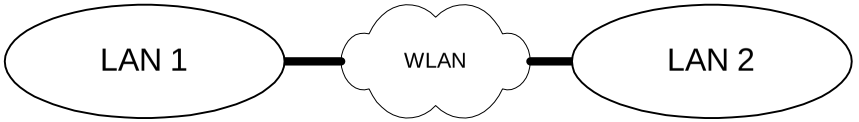
## Kabelbasierend (Kupfer, Fiber)




**Vorteile:**
Relativ sicher
Abhören schwierig
Wetterunabhängig

**Nachteile:**
Verzögerungen bei Inbetriebnahme
Teuer (Bandbreite, Einrichtung, Erhaltung)
Gefahr durch Leitungsbrüche (Bagger!)

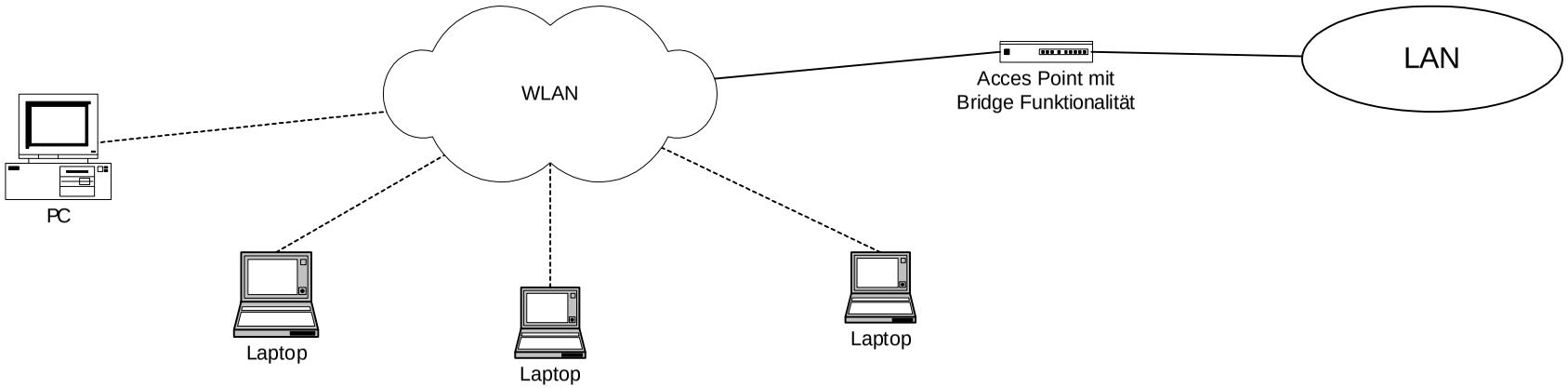
## Wireless




**Vorteile:**
Implementierung einfach
Billig (sowohl Anschaffung als im Betrieb)
Hohe Bandbreite

**Nachteile:**
Teilweise wetterabhängig
OFFEN !! - Mithören relativ leicht möglich
nur beschränkte Distanzen möglich

# Local Area Networks (LAN) basierend auf WLANs



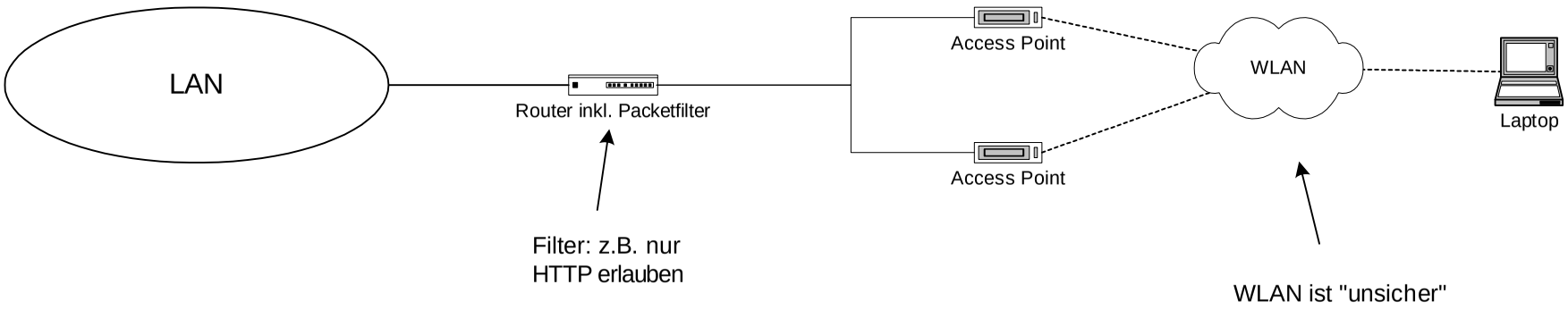

- Mehrere WLAN Clients sind mittels WLAN in ein LAN integriert
- Leicht zu Implementieren
- Kabelnetze haben jedoch einen besseren Durchsatz
- Funkwellen breiten sich "unkontrolliert" aus: Mithören ist relativ leicht möglich

# Herkömmliche Sicherheitskonzepte zur Absicherung von Funknetzen nach 802.11b

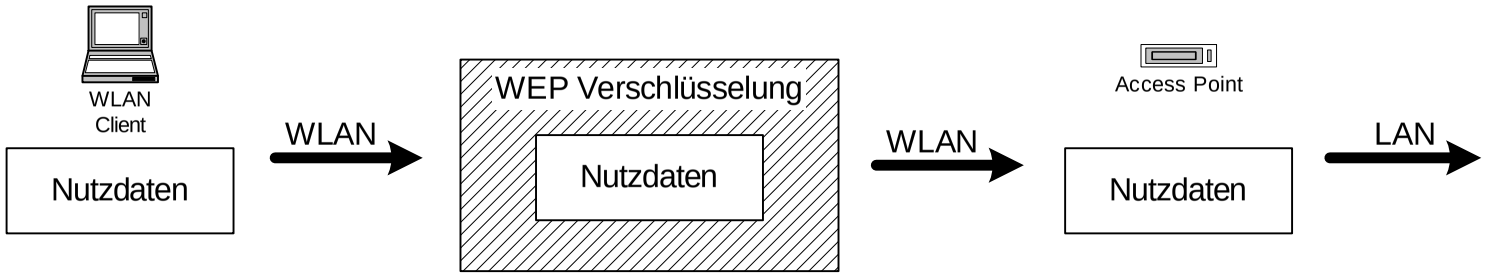
- **Netzwerknamen**
  Nur wer den Namen kennt, kann am WLAN teilnehmen. Der eigentliche Netzwerkverkehr wird aber nicht verschlüsselt

- **MAC Filtering**
  In den Access Points wird festegelegt, welche WLAN Karten am WLAN teilnehmen dürfen (MAC Adresse einer Karte)
  Es ist aber möglich, MAC Adressen vorzutäuschen und somit diesen Schutzmechanismus zu umgehen

- **Segmentierung von WLAN Netzen und Einsatz von Packet Filtern**
  Das WLAN wird mittels Router vom eigentlichen LAN getrennt. An der Übergangsstelle vom WLAN zum LAN kontrolliert ein Packetfilter den Verkehr vom und zum WLAN:



- **WEP (Wireless Equivalent Privacy)**
  - Verschlüsselung durch 40Bit bzw. 128Bit Schlüssel
  - "Shared Secret" bildet den Schlüssel: Nur wer das "Shared Secret" kennt, kann am WLAN teilnehmen




**Probleme von WEP**

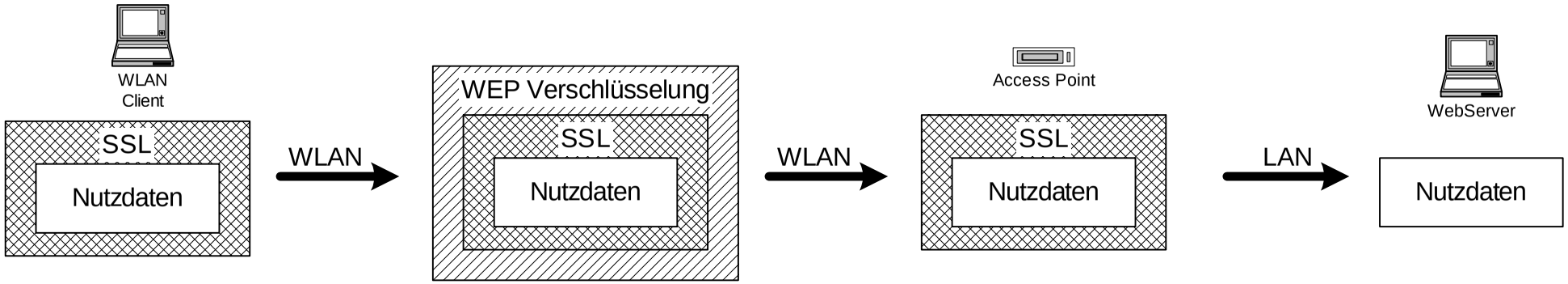
Jeder, der das "Shared Secret" kennt, kann am WLAN teilnehmen. Was ist zu tun, wenn z.B. ein Mitarbeiter das Unternehmen verlässt?

Mitte 2001 wurde bekannt, dass WEP unsicher (RC4 Verschlüsselung) ist. Mittels passiven Angriff kann das "Shared Secret" innerhalb sehr kurzer Zeit rekonstruiert werden (siehe dazu: http://www.cs.rice.edu/~astubble/wpe/ ).

*"Fatal für WEP an der neuen Methode ist, dass der Angriff auf Schlüssel jeder Länge - selbst mit dem RC4-Maximum von 2048 Bit -und IVs jeder Größe anwendbar ist, wobei der Rechenaufwand näherungsweise linear, nicht exponentiell, mit der Schlüssellänge steigt. Damit haben Fluhrer, Mantin und Shamir auch schon ein Loch in den Entwurf WEP2 gerissen, der unter anderem IVs von 128 Bit vorsieht. Schätzungen zufolge soll das Brechen eines 40-Bit-WEP-Schlüssels in einer Viertelstunde möglich sein. Die etwas bessere WEP128-Variante mit 104 Bit langen Schlüsseln würde einen Angreifer dann auch nur etwa 40 Minuten aufhalten."*

**Quelle: http://www.heise.de/newsticker/data/ea-06.08.01-000/**

- **Verschlüsselung auf Applikationsebene**




Ein Client verschlüsselt auf Applikationsebene die Daten. Diese sind nun bis zum Zielserver verschlüsselt.

**Nachteil**

Die Verschlüsselung muss von allen Applikationen, deren Datenverkehr verschlüsselt sein sollte, unterstützt werden.
Dies ist für viele bestehende Applikationen nur sehr schwer bzw. gar nicht möglich, da z.B. proprietäre Programme im Normalfall nicht umgeschrieben werden können.

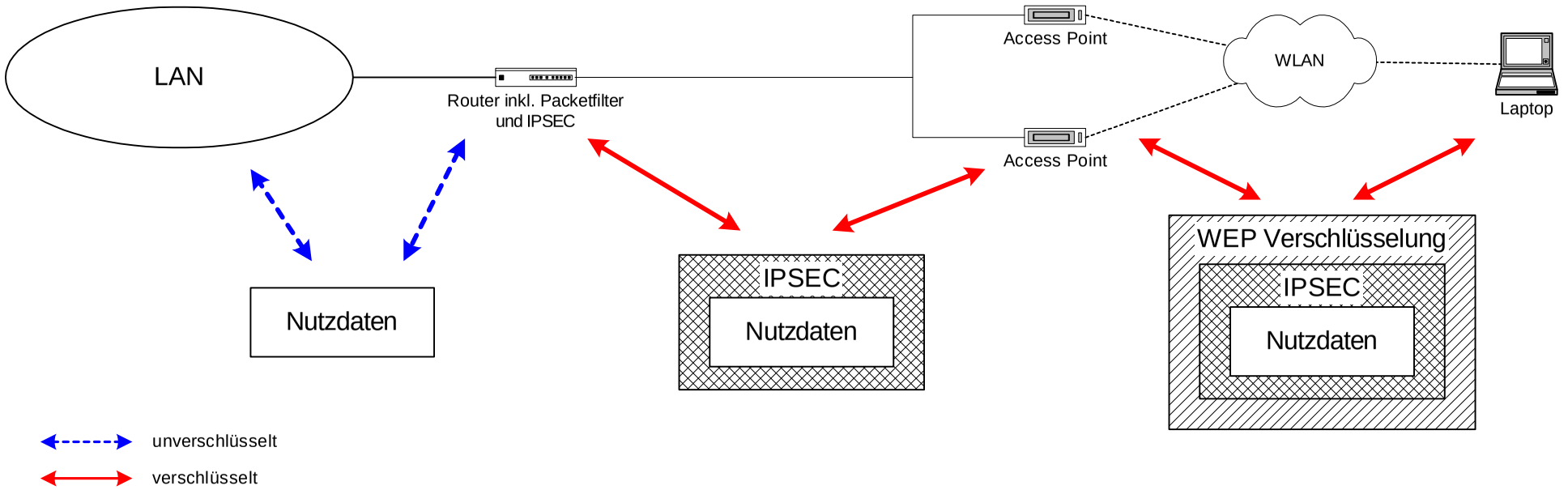
**Lösung**

Ein allgemeinerer Ansatz, der die Verschlüsselung ohne Unterstützung der Applikationen erlaubt, sollte gefunden werden!

→ **IPSEC**

# Absicherung von WLANs mittels IPSEC

Bei IPSEC findet die Verschlüsselung zwischen Applikationsebene und Transportebene statt (Layer 2). Damit können alle Applikationen, die auf TCP/IP basieren, verschlüsselt in einem WLAN ausgeführt werden. Eine Änderung an den Applikationen ist nicht notwendig!

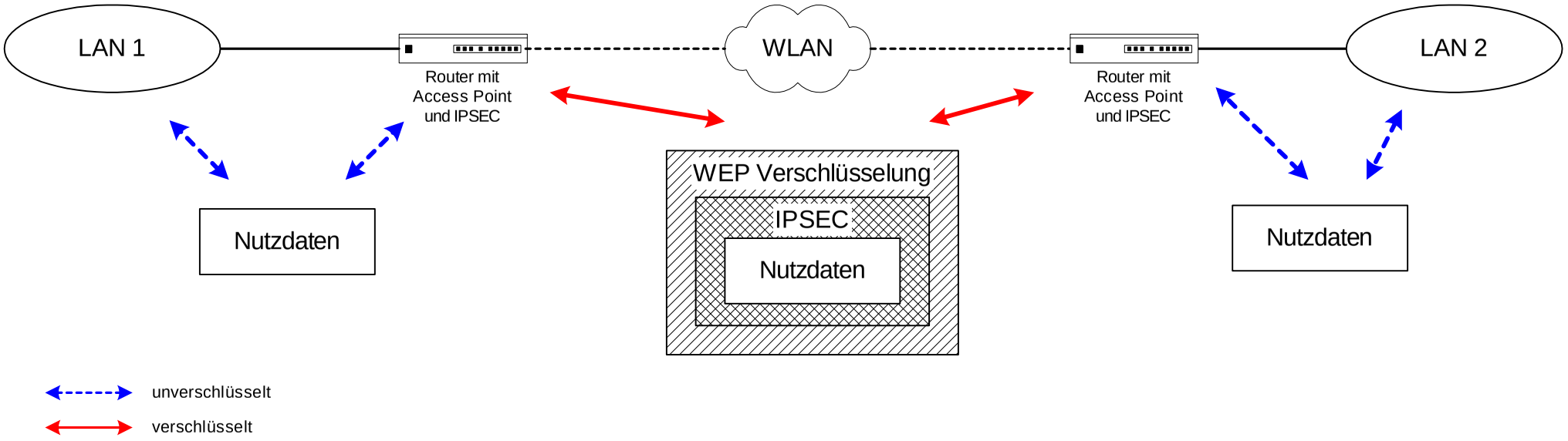



IPSEC gilt als sicher. Dadurch ist es einem Angreifer unmöglich, in ein durch IPSEC abgesichertes WLAN einzudringen.

# Implementierung von IPSEC zur Absicherung von WLANs
# Koppelung von LAN Segmenten

Implementierung ist relativ einfach, da die Teilnehmer des IPSEC/WLAN genau bekannt sind (Router)

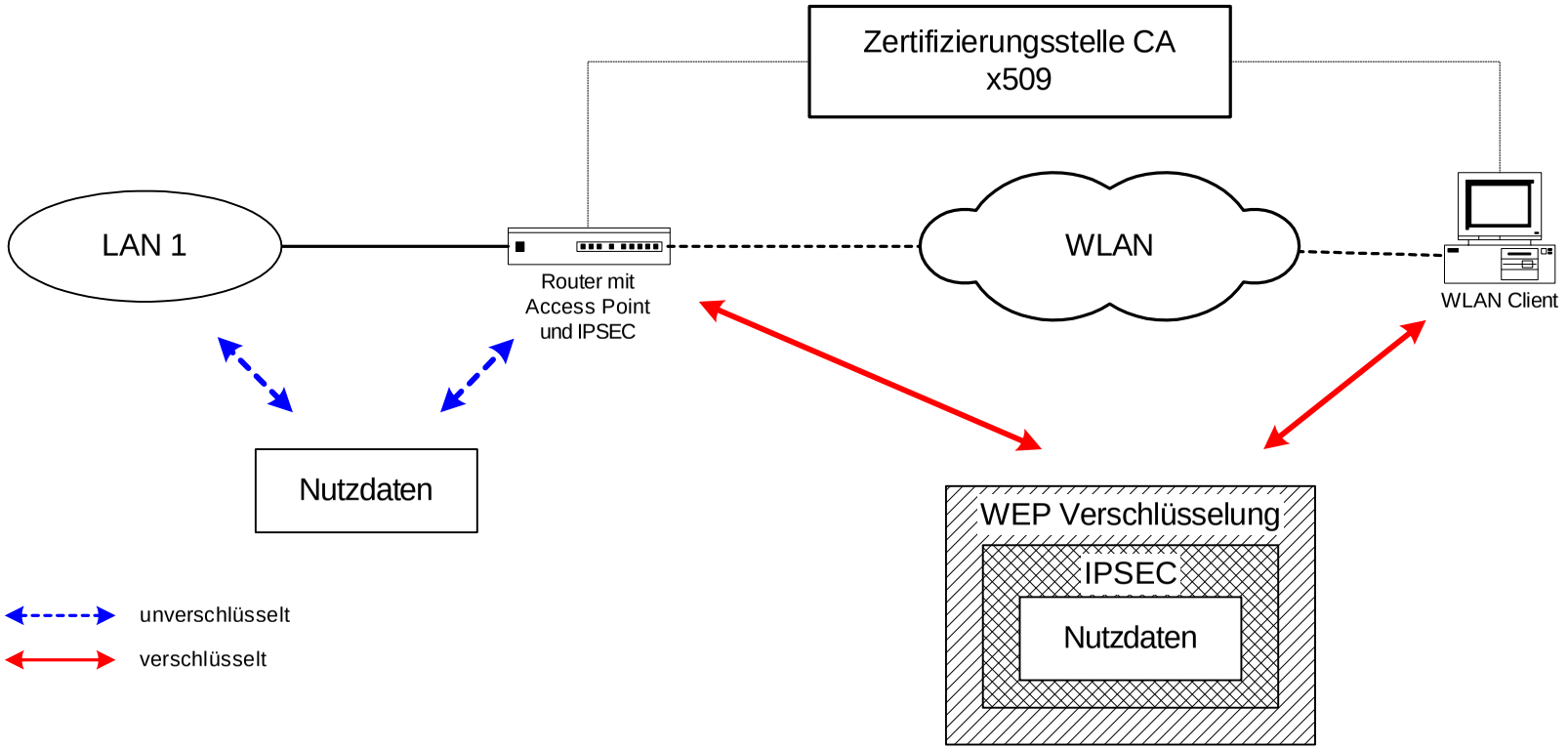

Access Point und Router können in einem Gerät kombiniert sein (z.B. mit Linux sehr einfach und kostengünstig realisierbar)



# Implementierung von IPSEC zur Absicherung von WLANs
# LANs basierend auf WLANs

Implementierung nicht trivial, da der IPSEC Router die WLAN Clients nicht zwingend kennen muss (z.B. öffentliche WLANs wie Flughafen, Hotel, ... )

**Lösung**
Verwendung einer Zertifizierungsstelle (CA) nach x509: Clients, die am WLAN teilnehmen dürfen, erhalten ein Zertifikat der CA. Der IPSEC Router "vertraut" der CA, somit sind alle Clients mit einem gültigen Zertifikat in der Lage, dem WLAN beizutreten.
Mittels CRLs (Certificate Revoke List) können Zertifikate deaktiviert werden.



# IPSEC Clients

IPv4 sieht keine Sicherheit mittels IPSEC vor (erst in IPv6 Standard). Für IPv4 gibt es aber Erweiterungen des TCP/IP Stacks, sodass sichere Kommunikation mittels IPSEC möglich ist:

**Linux**
Freeswan (kostenlos): http://www.freeswan.org

**Windows 2000/XP**
IPSEC implementiert (mind. SP2 bzw. High Encryption Pack verwenden! - 3DES Verschlüsselung)

**WIN9x/ME/NT4.0**
Diverse, teilweise kostenpflichtige Produkte sind erhältlich:

F-Secure VPN+: http://www.datafellows.com/products/vpnplus

Checkpoint SecureRemote VPN:  http://www.checkpoint.com/techsupport/freedownloads.html

PGPNet: http://www.pgpi.org

SSH Sentinel: http://www.ssh.com/products/sentinel

**MAC**

PGPNet: http://www.pgpi.org

# Live Vorführung eines mittels IPSEC abgesicherten WLANs, basierend auf Linux Technologie

**Ausgangssituation**

Anfang 2001 hat Mayr-Melnhof Karton mittels WLAN ein externes Büro an das LAN angebunden. Da die Funkstrecke über öffentlich zugängliches Gelände führt, wurde WEP mit 128Bit Schlüssel eingesetzt. Nach Bekanntwerden der Sicherheitslücke in WEP mußte eine Lösung, die die sichere Anbindung garantiert, gefunden werden.

**Lösung/Implementierung**

Als Sicherungsmechanismus wurde IPSEC gewählt. Als Alternative wäre aber auch eine Absicherung mittels SSH-Tunnel möglich. Da IPSEC jedoch weniger Ressourcen verbraucht (Kernelerweiterung) und somit besser skaliert, wurde es einer SSH Lösung vorgezogen.
Die eigentliche Implementierung war sehr einfach und unkompliziert, da sowohl Linux als auch die IPSEC Erweiterung FREESWAN frei erhältlich sind (keine Lizenzen notwendig, innerhalb von zwei Tagen wurde auf IPSEC umgestellt).

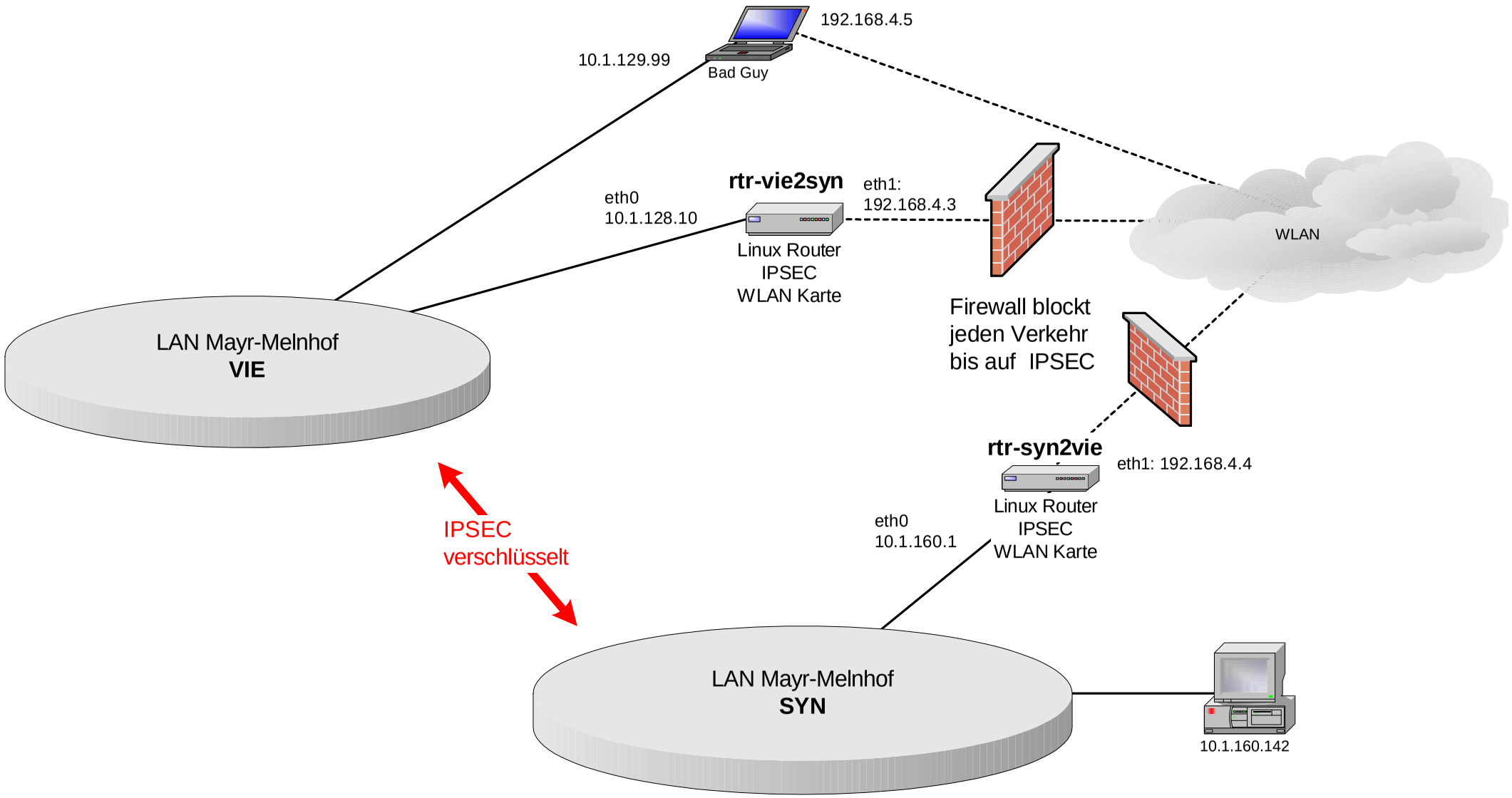
**Kosten**

2 IPSEC Router: Alt PCs, Pentium 200MMX, 64MB RAM, Buchwert: ca. 0 EUR
2 Orinoco Gold WLAN Karten, 2 Antennen, 2 PCI/PCMCIA Karten: ca. 580 EUR

**Stabilität**

Seit der Implementierung (August 2001) gab es noch keinen Ausfall, 24x7 Betrieb

# Die Installation



# Der Einbruch - Netz nur mit WEP gesichert

Der Angreifer **BadGuy** versucht mittels Laptop in das Mayr-Melnhof Netz einzubrechen

**Vorgangsweise**

Schritt 1: Rekonstruieren des "Shared Secrets" mittels Airsnort (Passives Mitprotokollieren des WEP verschlüsselten WLAN Verkehrs und anschliessendes Knacken des Schlüssels)

Schritt 2: Eintragen des "Shared Secrets" in die eigene WLAN Konfiguration

Schritt 3: Herausfinden der verwendeten IP Adressen (= IP Netz) mittels TCPDUMP

```
01:00:51.569585 192.168.4.3.32783 > 192.168.4.4.23: . ack 10577 win 8576
01:00:51.570275 192.168.4.4.23 > 192.168.4.3.32783: P 10577:10834(257) ack 1 win 32120
01:00:51.575725 192.168.4.3.32783 > 192.168.4.4.23: . ack 10834 win 8576
01:00:51.576415 192.168.4.4.23 > 192.168.4.3.32783: P 10834:11091(257) ack 1 win 32120
```

Schritt 4: Konfiguration WLAN Karte mit einer IP Adresse aus dem IP Netz, das in Schritt 3 ausgeforscht wurde: 192.168.4.5

Ab jetzt ist **BadGuy** voll im Netz integriert!

Schritt 5a: Sniffer starten (Passwörter werden ausspioniert)

Schritt 5b: Denial of Service gegen Router starten (z.b. Synflood .. ) - Netz wird unbrauchbar

# Der Einbruch - Netz mit WEP und IPSEC gesichert

Der Angreifer **BadGuy** versucht mittels Laptop in das Mayr-Melnhof Netz einzubrechen

**Vorgangsweise**

Schritt 1: Rekonstruieren des "Shared Secrets" mittels Airsnort (Passives Mitprotokollieren des WEP verschlüsselten WLAN Verkehrs und anschliessendes Knacken des Schlüssels)

Schritt 2: Eintragen des "Shared Secrets" in die eigene WLAN Konfiguration

Schritt 3: Herausfinden der verwendeten IP Adressen (= IP Netz) mittels TCPDUMP:

```
00:58:16.226894 192.168.4.4 > 192.168.4.3: ip-proto-50 204
00:58:16.230705 192.168.4.3 > 192.168.4.4: ip-proto-50 84
00:58:16.232154 192.168.4.4 > 192.168.4.3: ip-proto-50 204
00:58:16.235981 192.168.4.3 > 192.168.4.4: ip-proto-50 84
00:58:16.237424 192.168.4.4 > 192.168.4.3: ip-proto-50 204
00:58:16.241250 192.168.4.3 > 192.168.4.4: ip-proto-50 84
00:58:16.242737 192.168.4.4 > 192.168.4.3: ip-proto-50 204
```

**Hier scheitert BadGuy, da er nur noch IPSEC Verkehr mitprotokollieren kann und dessen Entschlüsselung nicht möglich ist!**

# Zusammenfassung

WLANs nach 802.11b, deren Sicherheit auf WEP basiert, sind als nicht sicher anzusehen!

Es ist einem Angreifer relativ leicht möglich, in ein WEP "geschütztes" WLAN einzubrechen

Absicherung durch IPSEC schließt dieses Sicherheitsloch. Die Art der Implementierung von IPSEC hängt stark von der Art des WLANs ab (Gekoppelte LAN Segmente, LANs basierend auf WLANs, Art der WLAN Clients)

Enorme Kosteneinsparungen (Anschaffung und TCO) durch den Einsatz von Linux