

WirelessLAN

Universitatea “Transilvania” din Brasov

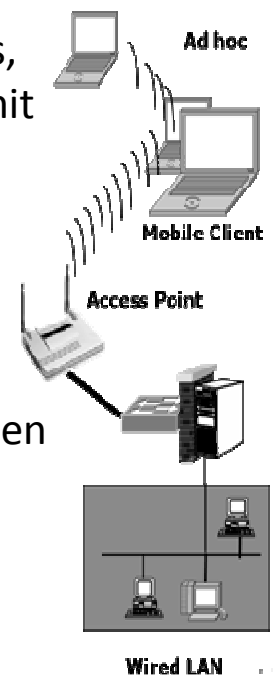
1 Einführung

Wireless LAN

Wireless LAN

- ☐ Wireless LAN wird über die Luft mittels Funkwellen übertragen
- ☐ Komponenten von einem Subnetz: mobile drahtlose Clients (Laptops, Notebooks, Personal Digital Assistants), Access Point (das Gerät, das WLAN-Clients verbindet mit dem drahtgebundenen LAN oder an andere Stationen)
- ☐ **Ad-hoc-Netzwerk:** Verfassen von mehreren WLAN-Stationen sich gegenseitig die Kommunikation über die Luft (Mobile Ad-hoc-Netz, **MANET**)
- ☐ **Infrastruktur-Netzwerk:** Wireless LAN-Stationen kommunizieren über einen Zugangspunkt (funktioniert als Hub) mit anderen Netzwerktechnologien
- ☐ **Wireless Access** von mobilen Geräten (Notebook, PDA, etc.), um kabelgebundenen LANs, um ihre Ressourcen zu nutzen, die auch Zugang zum Internet bekommen
- ☐ **WLAN Standard:** IEEE 802.11b, 1999

➡ WLAN-Sicherheit wie im Wireline-LANs, ist, dass Vertraulichkeit, Datenintegrität und Zugriffskontrolle



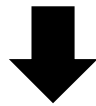
1 Einführung

WLAN-Sicherheit

Sicherheitsaspekte

Funkwellen überall und so kann es sein
von einer gut ausgestatteten Person erhalten

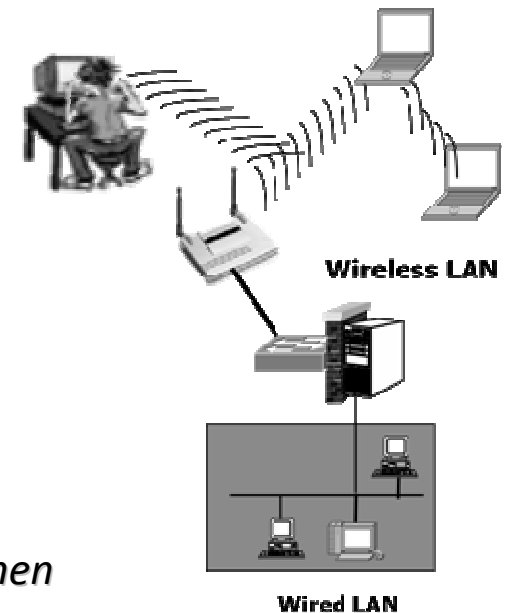
Eavesdropper können alle übertragenen Daten schnüffeln
zwischen mobilen Client und Access Point



Verschlüsselung, um die Vertraulichkeit zu bekommen
Eavesdropper können Pakete oder Ort fälschen
ein Schelm Zugangspunkt (Maskerade)



Die gegenseitige Authentifizierung den Zugang Kontrolle zu bekommen



IEEE 802.11b Standard

- ❑ Im Jahr 1999 als Erweiterung des bisherigen Standards IEEE 802.11- Standard für die Definition Wireless- LAN-Produkte
- ❑ beschreibt den Schutz der Funkübertragung auf der Datenübertragungsschicht des Netzes
- ❑ theoretische Datenübertragungsrate von 11 Mbps , Frequenz 2,4 GHz
- ❑ bietet Vertraulichkeit durch das symmetrische Verschlüsselungsverfahren RC4(Stromchiffre)
- ❑ gibt zwei Typen von Authentifizierungsmechanismen , wo nur der Zugangspunkt entscheidet welches mobile Client kann mit ihr assoziieren (ein Wege-Authentifizierung)
 - *Offene Authentifizierung* : Client und Access Point Austausch uncodierte Informationen
zum Beispiel : Der Kunde muss den Service Set Identifier (Netzwerkname des wissen
Zugangspunkt des drahtlosen Netzwerks) des Zugangspunkts ;
Media Access Control -Adresse des Clients (MAC) des drahtlosen Netzwerkkarte gespeichert
wird die MAC- Zugriffssteuerungsliste (ACL) auf dem Access Point
 - *Shared -Key-Authentifizierung* : Der Access Point sendet eine Herausforderung und hat der
Kunde schickt die verschlüsselte Herausforderung, den richtigen Schlüssel , der Schlüssel muss
von Hand, bevor konfiguriert



WLAN 802.11b

Wireless LAN

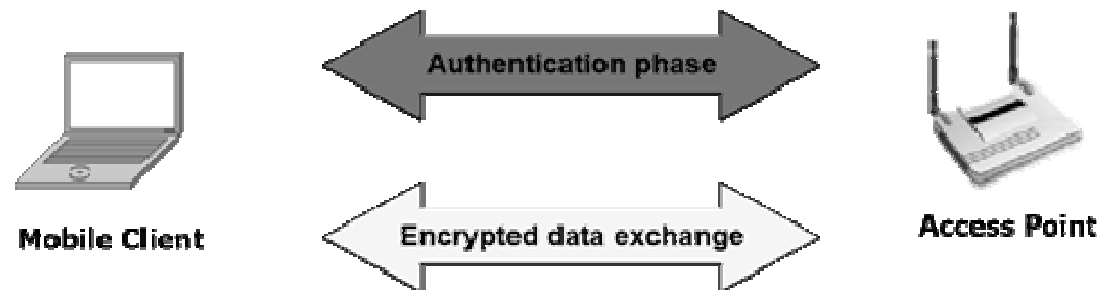
IEEE 802.11b Standard

❑ **Schlüsselverwaltung:** 4 Pre-Shared-statische Schlüssel zwischen Mobilstationen und einem Zugangs zeigen, keinen Mechanismus für die Schlüsselverhandlung und Schlüsselverteilung

❑ **Sicherheitsziele**

- Vertraulichkeit: verhindern, dass die Decodierung von verschlüsselten WLAN-Verkehr durch Lauscher
- Datenintegrität: Manipulationen verhindern der gesendeten Nachricht
- Zugangskontrolle: deny Zugriff auf das drahtlose Netzwerk durch nicht autorisierte Benutzer

❑ **Datenübertragung in zwei Phasen:**

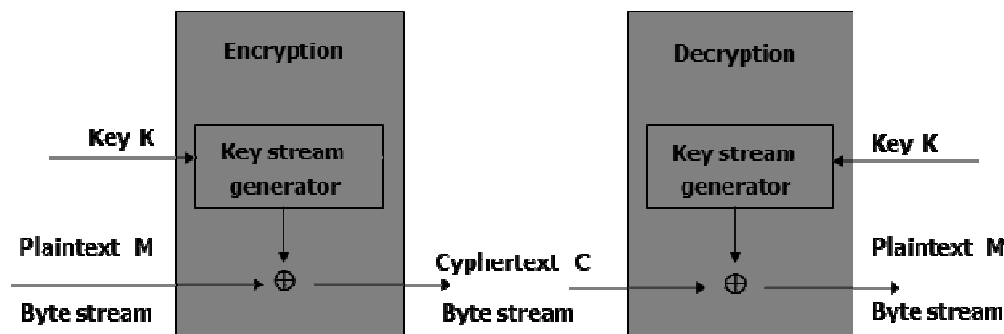


WLAN 802.11b

WEP Protocol

Wired Equivalent Privacy (WEP)

- ❑ Sollte die Privatsphäre von WLAN-Datenströme wie in kabelgebundenen Netzwerken bieten
- ❑ WEP verwendet die symmetrische Stromchiffre RC4 mit einer variablen geheimen Schlüssel für die Verschlüsselung
- ❑ Schlüsselverwaltung: 4 Pre-Shared Keys zwischen Mobilstationen und einem Zugangspunkt, das Feld von 4 Schlüssel müssen auf jedem Gerät von Hand konfiguriert werden, keine zentrale Punkt der Verwaltung und Wartung
- ❑ "klassischen" WEP spezifiziert die Verwendung von 40-Bit-Schlüssel (ehemaliger US-Regierung Beschränkung), jetzt 128-Bit-Schlüssel (mit 24-Bit-Anfangsvektor und 104 Bit auf jedem Gerät vorinstalliert) sind üblich im Moment
- ❑ **Symmetrische Stromchiffre RC4:**



WLAN 802.11b

WEP Protocol

WEP Protocol by the Sender (Mobile Station)

- ☐ Global-Shared-Array mit 4 Tasten, eine Schlüssel-ID-Feld in jeder Nachricht geben Sie den Schlüssel verwendet
- ☐ Echt geheimen Schlüssel k ist mit einer Länge von 104 Bit, da 24 Bit sind öffentlich bekannten Verschlüsselung
- ☐ eine Zufallszahl als Startvektor iv (24 Bit) wählen und nutzen Sie die Eingabe-Taste K für das Stromchiffre durch Verkettung mit dem geheimen Schlüssel:
- ☐ eine Integritäts-Prüfsumme $ics(m)$ aus der Nachricht m berechnen und zu verketten, um sowohl der Klartext (ICs: Cyclic Redundancy Codes sind eine Klasse von linearen Fehlerkorrekturcodes)
- ☐ Chiffre mit der XOR-Operation und der durch einen Algorithmus von RC4 erzeugte Schlüsselstrom:
 - (a) Initialisierung eines 256-Byte-Zustandsvektor S mit den Werten von K (K ist abhängig von der Länge wiederholt)
 - (b) Permutation von S und Auswahl einer Komponente von S als ein Byte des Schlüsselstrom



WEP Protocol by the Receiver (Access Point)

Übertragung über die Funkverbindung \underline{iv} (unverschlüsselt), \underline{c} (Geheimtext)

Die Entschlüsselung

- ☐ den Empfänger kehrt einfach den Verschlüsselungsprozess
- ☐ mit dem empfangenen Wert \underline{iv} und die gemeinsamen geheimen Schlüssel \underline{k} erhält man den Schlüsselstrom K
- ☐ Rechen $c \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus 0 = M$
- ☐ in die Nachricht \underline{m} und die Prüfsumme \underline{ics} spalten den Klartext M

Überprüfung der Prüfsumme

- ☐ Berechnen der Prüfsumme $ics' = ics(m)$ der empfangenen Nachricht \underline{m}
- ☐ den Rahmen mit der Nachricht anzunehmen, wenn $ics = ics'$



Die Integrität der Daten sicherzustellen

WEP Prüfsummenfehler, um die Datenintegrität

- ❑ CRC-Prüfsumme ist eine spezielle lineare Fehlerkorrekturcode, es bietet nur Schutz gegen Übertragungsfehler und es ist nicht ausreichend, um die Datenintegrität sicherzustellen
- ❑ Wir verwenden die Tatsache, dass jede Prüfsumme ist eine lineare Funktion
- ❑ **Man-in-the-Middle-Angriff:** Angreifer abfangen Chiffre \underline{c} zu erreichen, bevor es die Ziel, ersetzen durch einen anderen Chiffretext \underline{c} und übertragen sie durch Spoofing der Quelle
- ❑ Annahme: $m' = m \oplus d$ and $c' = c \oplus (d, ics(d))$

$$\begin{aligned} c' &= c \oplus (d \mid ics(d)) = (M \oplus Kstream) \oplus (d \mid ics(d)) \\ &= (m \oplus d \mid ics(m) \oplus ics(d)) \oplus Kstream \\ &= ((m \mid ics(m)) \oplus Kstream) \oplus (d \mid ics(d)) \\ &= (m + d \mid ics(m + d)) \oplus Kstream = (m' \mid ics(m')) \oplus Kstream \end{aligned}$$

Dies zeigt, dass die neuen verschlüsselten Text an eine andere Nachricht mit der entschlüsselt werden entsprechende Prüfsumme und der Angreifer kann die Nachricht ohne ändern Erkennung durch Überprüfung der Prüfsumme



Vertraulichkeit

WEP-Verschlüsselung nicht durch das Risiko der Schlüsselstrom Wiederverwendung

- ❑ WEP verwendet den öffentlichen Anfangsvektor iv zu den Schlüsselstrom-Erzeugungsprozess für jede variieren Rahmen, da der geheime Schlüssel für alle Pakete
- ❑ der Berechnung des iv nicht in der Norm festgelegte
- ❑ Die Anfangsvektor sollte nach jedem Paket geändert werden, aber der Standard nicht sagen, wie: so einige Karten erhöhen den Wert um eine für jedes Paket übertragen
- ❑ Keystream-Wiederverwendung-Angriff: Angreifer versuchen, zwei verschlüsselte Pakete, verwenden entdecken das gleiche iv (Länge von 24 Bit gibt 16.277.216 verschiedene Möglichkeiten!), seit vielen Felder der Pakete sind vorhersagbar ist es möglich, den Klartext zurückzugewinnen
- ❑ Es ist eine Eigenschaft des Stromchiffren von Angreifern verwendet, um eine Nachricht zu entschlüsseln, wenn zwei Nachrichten wurden mit derselben Schlüsselzeichenfolge verschlüsselt: $c1 = M1 \oplus Kstream$, $c2 = M2 \oplus Kstream$

$$\begin{aligned} c1 \oplus c2 &= (M1 \oplus Kstream) \oplus (M2 \oplus Kstream) \\ &= (M1 \oplus M2) \oplus (Kstream \oplus Kstream) = M1 \oplus M2 \end{aligned}$$

Somit wird, wenn der Klartext von einer dieser Nachrichten ist bekannt oder sogar einige Abschnitte der andere. Das ist einfach erhältlich.



Access Control

nicht autorisierte Benutzer Zugriff auf das Netzwerk erhalten

☐ Authentifizierung von mobilen Clients mit MAC-Access Control Lists (ACL) für die gespeicherte Zugangspunkt berücksichtigt nicht die Identität des Benutzers, trotz der Tatsache, dass MAC-Adressen von Geräten können gefälscht werden??

☐ Ein Weg Authentifizierung ermöglicht die Platzierung von Rogue Access Points

☐ WEP Integritäts-Prüfsumme ist eine Funktion ohne Schlüssel

☐ Darüber der WEP-Standard ermöglicht die Wiederverwendung von Anfangsvektoren iv

☐ Die Kenntnis des Klartextes von jedem beliebigen Chiffretext-Paket ermöglicht es einem Angreifer, Wiederherstellung der Schlüsselstrom:

$$M \oplus c = M \oplus (M \oplus K stream) = (M \oplus M) \oplus K stream = K stream$$

☐ Somit kann der Angreifer die Prüfsumme berechnen und verschlüsselt seine Nachricht :

$$ca = (ma \mid ics(ma)) \oplus Kstream$$

Durch das Abfangen der ursprünglichen Nachricht und Spoofing die Quelle kann er nun seine spritzen Geheimtext mit dem gleichen Anfangsvektor iv.



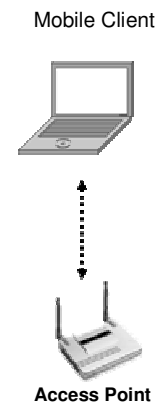
Schlussfolgerungen aus Sicherheitsbedrohungen

- ❑ Mit MAC-Filter ist eine wirklich schwache Sicherheitsproblem, Hardware-Diebstahl
- ❑ Verschlüsselung mit statischen WEP-128-Bit-Schlüssel ist ein Risiko, auch ohne Brute-Force Angriff auf den geheimen Schlüssel kann ein Angreifer den Klartext zu entdecken
- ❑ Da die Prüfsumme ist kein Schlüssel Hashfunktion ein Angreifer spritzen kann seine Nachrichten ohne Nachweis durch den Empfänger
- ❑ Wiederverwendung sowohl der Anfangsvektor und den geheimen Schlüssel ist Realität und gefährden den Schlüssel
- ❑ Aktuelle Implementierung des Algorithmus RC4 System verursacht Fehler

➔ Der WEP-Standard 802.11 bietet keiner der drei Sicherheitsziele!

Wir brauchen: Geräteunabhängige zentrale Benutzer-Authentifizierung, Schlüsselverteilung.

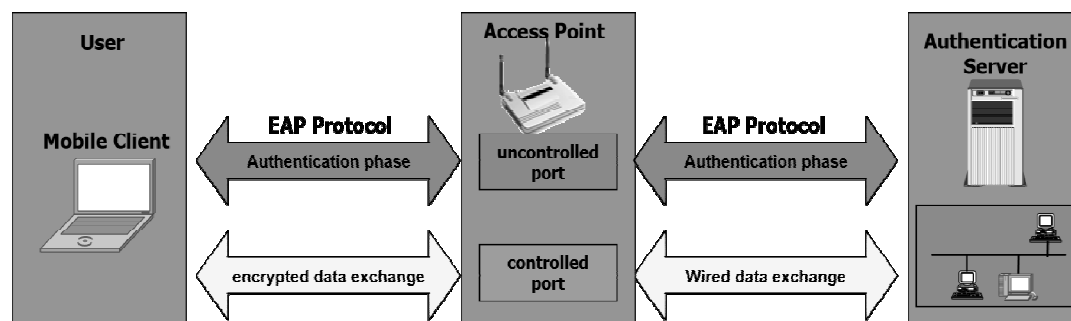
Die gegenseitige Authentifizierung zwischen Client und Access Point, Session-basierte dynamische Schlüssel, Schlüssel Hashfunktion, pro-Paket-Authentifizierung



Verbesserungen von Sicherheitsbedenken

Standard IEEE 802.1x-Authentifizierung

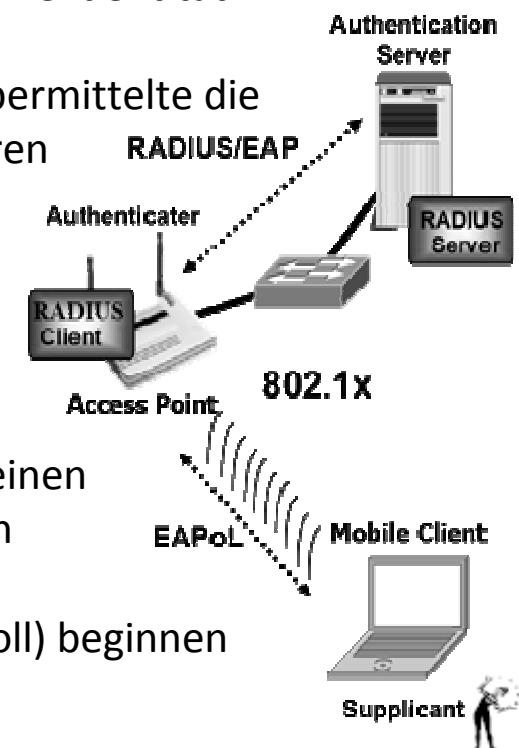
- ❑ Ist ein vorgeschlagener Standard für die zentrale Wireless LAN-Authentifizierung auf geräteunabhängige Elemente wie Benutzername, Benutzer-ID und Passwort (Benutzerauthentifizierung)
- ❑ Bietet eine Authentifizierungsdiallog zwischen dem mobilen Client, der Access Point mit Port-basierte Network Access Control (ungeregelten und geregelten Slots) und einen Authentifizierungsserver
- ❑ Principe: ein WLAN-Client erhalten Zugang zu dem Zugangspunkt und damit auf die Netzwerkressourcen nur nach erfolgreicher Authentifizierung von dem Authentifizierungsserver (basierend auf Benutzerdaten wie Benutzername und Passwort), eindeutige Port für die einzelnen Verbände an dem Zugangspunkt



Verbesserungen von Sicherheitsbedenken

WLAN-Sicherheit mit 802.11b und 802.1x/EAP

1. Mobile Client (MC) assoziierte mit dem Access Point (AP)
2. AP blockiert den Zugang zu den Netzwerkressourcen und fordert eine Identität (Benutzernamen, ...) von der Benutzer
3. Anmeldeinformationen des Benutzers werden von der AP (über übermittelte die unkontrollierten Port) an den Authentifizierungsserver (AS) zu initiieren die Authentifizierungsdiallog zwischen MC und AS
4. AS (RADIUS) und MC führen eine EAP-Authentifizierung Dialog (mehrere Anfragen und angemessene Reaktionen) durch die AP (EAP Nachrichten zwischen MC und AP sind gekapselt in LAN-Rahmen und zwischen AP und AS in RADIUS-Pakete)
5. Im Falle einer erfolgreichen Authentifizierung ermöglicht der AP seinen Port gesteuert, um die einzigartige Verbindung mit der MC etablieren (nur der MC authentifiziert - ein Weg-Authentifizierung)
6. Verschlüsselte Datenaustausch zwischen MC und AP (WEP-Protokoll) beginnen können




Verbesserungen von Sicherheitsbedenken

Das System ist bereits gefährdet:

- ❑ 802.1x-Standard erfordert nur die Authentifizierung des mobilen Client; gegenseitige Authentifizierung optional, so dass Rogue Access Points können in das WLAN infiltriert werden
- ❑ Der Authentifizierungsdialog ist unsicher: Benutzername und andere Authentifizierungsinformationen werden übergeben werden in der klaren, mit EAP-MD5 ein Angreifer die Authentifizierung Herausforderung und analysieren die entsprechenden Hash-Antwort, um die Benutzer-Anmeldeinformationen erkennen (Benutzerpasswort)
- ❑ Das System bietet keine Schlüsselverteilungsanlagen
- ❑ Schlüssel nicht in kurzen Abständen erneuert; Angreifer versuchen, zwei verschlüsselte Pakete, die das verwenden entdecken elbe *iv* und da viele Felder der Pakete sind vorhersagbar ist es möglich, den Klartext zurückzugewinnen (Keystream-Wiederverwendung-Attack)
- ❑ Der Standard bietet keine pro Paket Authentifizierung, nur pro-Paketverschlüsselung

Der WEP-Standard 802.11 mit 802.1x-Authentifizierung mildert die Sicherheitslücken, sondern bietet nicht genügend Sicherheit!

Wird durch  *dynamische Sitzungsschlüssel und schnell Sitzungsschlüssel Erneuerung, gegenseitige Authentifizierung, pro Paket Verschlüsselungsschlüssel, Keyed Hash-Funktion für pro Paket-Authentifizierung*



Verbesserungen von Sicherheitsbedenken

Herstellerspezifische Implementationen

- ❑ Es gibt eine Menge von herstellerspezifischen erweiterten Sicherheitsfunktionen (MS, Cisco Systems und andere)
- ❑ EAP-TLS : eine starke Authentifizierungsmethode auf Basis von Public -Key-Zertifikate (Benutzer und Maschine) TLS (Transport Layer Security) ist ein Sicherheitsprotokoll auf TCP (ähnlich SSLv3) und stellt ein vertrauliche Authentifizierungsdialog mit der Datenintegrität und gegenseitige Authentifizierung auf der Basis von Zertifikate , derzeit nur unter Windows XP unterstützt PKI notwendig ist : öffentliche und private Schlüssel, ein eindeutiges Zertifikat (CA) für jeden Netzwerkbenutzer und die Anwendungsserver , auch Smartcard- basierte Authentifizierungssysteme mit Benutzeridentifikation zwischen der Benutzer und der mobile Client (Wissen und Besitz)
- ❑ EAP-TTLS : Tunnel TLS eine sichere Verbindung zwischen dem mobilen Client und dem Authentifizierungs-Server , als Benutzeranmeldeinformationen sicher ausgetauscht werden und so gibt es keine Notwendigkeit für Kunden Zertifikate
- ❑ Protected EAP (PEAP) : verwendet TLS , Zertifikat basierte Authentifizierung , konkurriert mit EAP –TTLS



Verbesserungen von Sicherheitsbedenken

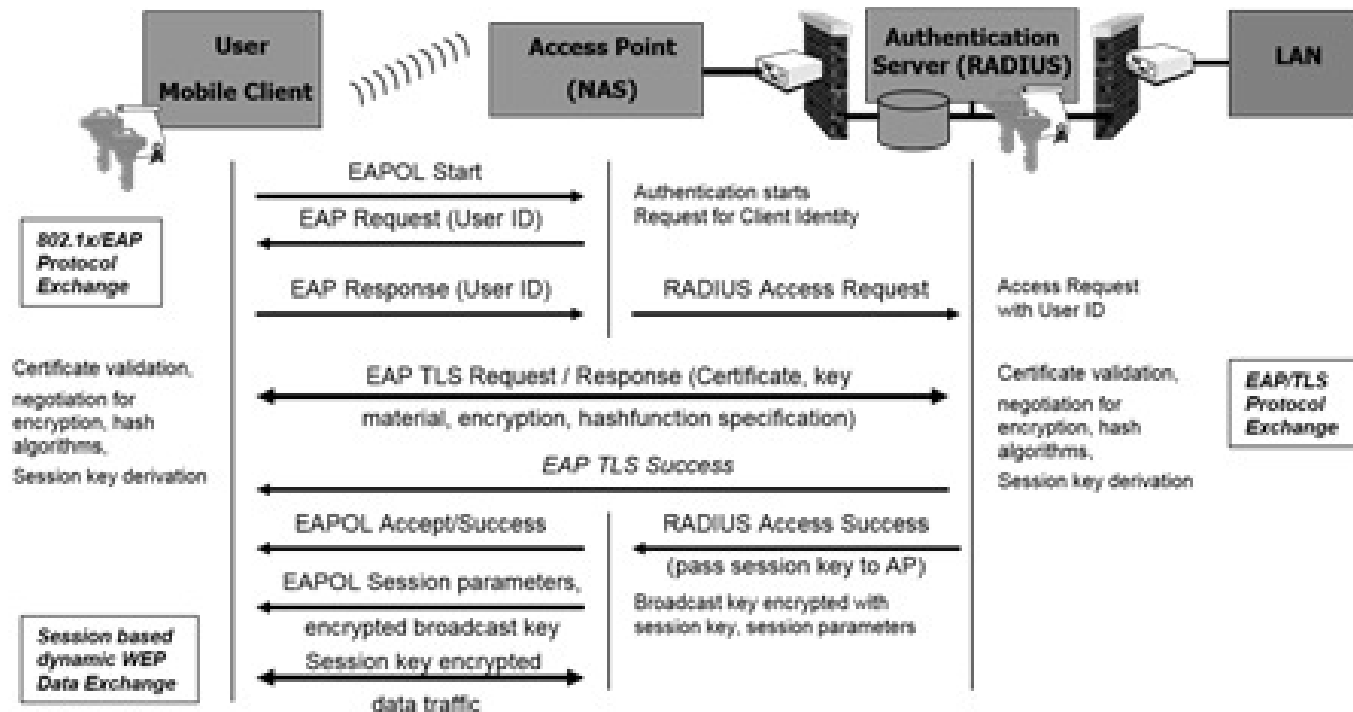
Herstellerspezifische Implementationen...

- ☐ EAP- SRP : Secure Remote Password (SRP) ist eine kryptographisch starke Authentifizierungsmechanismus ohne dass eine CA , es bietet auch einen gemeinsamen Schlüssel
- ☐ Temporal Key Integrity Protocol (TKIP) : leiten eine pro - Paket Schlüssel für die Verschlüsselung
- ☐ Virtual Private Network (VPN) : L2TP , IPsec oder L2TP-IPsec



Verbesserungen von Sicherheitsbedenken

WLAN Authentifizierung / Key Exchange mit EAP / TLS



Verbesserungen von Sicherheitsbedenken

Herstellerspezifische Implementationen ...

- ☐ Protected EAP (PEAP): verwendet TLS, Zertifikat basierte Authentifizierung, konkurriert mit EAP-TTLS
- ☐ EAP-SRP: Secure Remote Password (SRP) ist eine kryptographisch starke Authentifizierung Mechanismus ohne ein CA erfordern, es bietet auch einen gemeinsamen Schlüssel
- ☐ Temporal Key Integrity Protocol (TKIP): leiten eine pro-Paket Schlüssel für die Verschlüsselung in zwei Phasen, eine Mischung aus dem Sitzungsschlüssel mit MAC-Adresse und der Anfangsvektor iv geben dem perpacket Schlüssel für den Verschlüsselungsstrom RC4
- ☐ Gesamt Ersatz WEP/RC4 durch den Advanced Encryption Standard (AES, Rijndael Algorithmus, symmetrische Blockchiffre mit Schlüssellänge von 128, 256 Bits und mehr), aber die Bereitstellung erfordert Hardware-Beschleunigung, im Moment Geräte nicht unterstützt
- ☐ Es gibt andere in Arbeit!

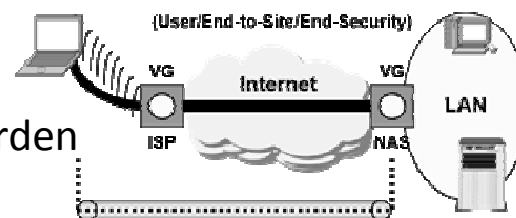
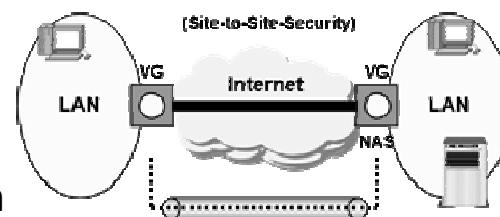
Die neue Wireless-Standard IEEE 802.11i (Task Group i) hoffentlich lösen alle Sicherheitslücken der "klassischen" WEP-Standard und bietet Sicherheit in WLAN als in drahtgebundenen Netzen!



WLAN-Sicherheit mit VPN-Tunneling

VPN Tunneling

- ☐ Kapselung: Frames oder Pakete eines Protokolls zu sein über eine Brücke net sicher übertragen sind gekapselt in einem zusätzlichen Header (Tunnel-Header) an der Tunnel Startpunkt (VPN-Client, VPN-Gateway)
- ☐ Routing: Der Tunnel Routing-Header enthält und Sicherheitsinformationen (Verschlüsselung, Authentifizierung Parameter) wie etwa die IP-Adressen der Tunnelstart und Endpunkt
- ☐ Decapsulation: Erreichen der Tunnel-Endpunkt (VPN Server) die Rahmen decapsulated und weitergeleitet seiner Endziel
- ☐ Tunneling-Technologie kann auf Layer 2 (Data-Link verwendet werden Schicht mit Rahmen) und / oder Schicht 3 (Netzwerkschicht mit Pakete) des OSI-Referenzmodells
- ☐ Netzwerksicherheitsprotokolle bieten verschiedene Funktionen und kategorisiert werden in:
Schicht-2-Tunnelprotokoll: PPTP, L2TP (basierend auf PPP, die zwischen einem DFÜ-Client und einem NAS verwendet wird) Layer-3-Tunneling-Protokoll: IPSec mit IKE



Zusammenfassung

Wireless LAN – Mobilität zu Lasten der Sicherheit !!!

☐ Standard 802.11 b bietet nur Grundschutz für “Hausgebrauch” !

- WEP mit RC4 und statischen 128-bit-Schlüssel
- Statische Schlüssel häufig wechseln
- AP in geschützten Bereich

☐ Herstellerspezifische Verbesserungen anwenden

- RC4 mit dynamischen Schlüsselmanagement
- Paketweise Schlüsselwechsel mit Temporal Key Integrity Protocol (TKIP)

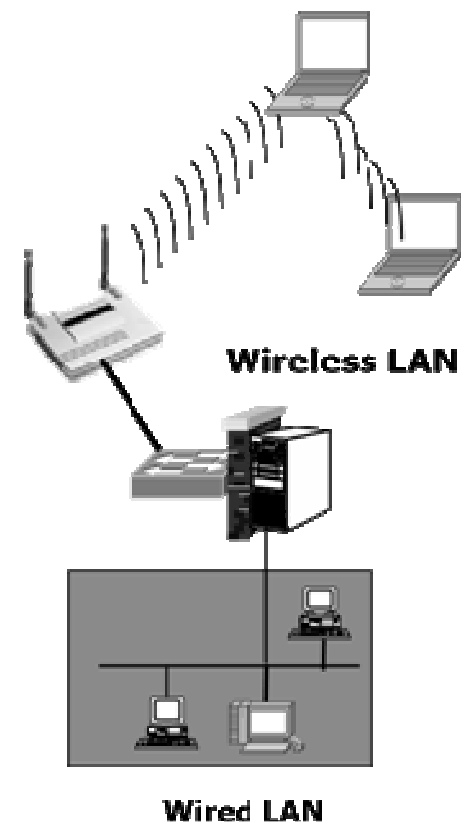
- Zentralisierte Authentifizierung mit RADIUS/802.1X

- Gegenseitige Authentifizierung von User und AP mit EAP-TLS

☐ Neuer Standard IEEE 802.11i ist “Hoffnungsträger”

- Verschlüsselung mit AES
- Paketweise Authentifizierung
- Dynamisches Schlüsselmanagement

☐ VPN ist sichere Alternative, aber aufwendig



WLAN Kriminalität

Warchalking / Wardriving

= Kennzeichnung von ungesicherten Wireless-LANStandorten in öffentlichen und privaten Bereichen

- ❑ Erstmalig in London aufgetreten!
- ❑ Explosionsartige Verbreitung einer Subkultur!



WLAN Kriminalität

Offener Kreis:
Geschlossener Kreis mit „W“:
Jetzt auch: Warflying

freier Internetzugang
WLAN mit WEP Protokoll

