Willkommen...

26. DECUS Symposium in Bonn 08. April 2003

DECUS München e.V.

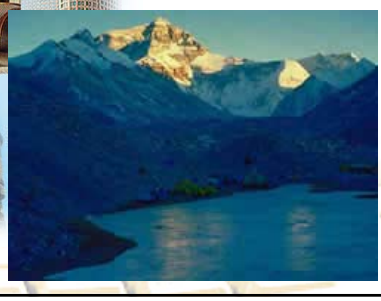
Sicherheit in Wireless Netzwerken

Thorsten Kocher
t.kocher@drachenfels.de

Agenda

- **Sicherheit bei 802.11a und 802.11b**
- **Ausblick auf Verbesserungen**
- **Tools zum Ausnutzen der Sicherheitslöcher**
- **Vorgehen zum Auffinden von illegal betriebenen Access Points**

Einsatzgebiete



http://ltsu.net/europe.htm

http://mobileaccess.de/wlan/

http://www.hotspot-locations.com

iPass

IEEE 802.11 Standard Aktivitäten

- 802.11a – 54 Mbps, 5GHz, verabschiedet 1999
- 802.11b - 11 Mbps, 2.4 GHz, verabschiedet 1999
- 802.11d - World Mode, verabschiedet
- 802.11e - Quality of Service
- 802.11g - Higher Data rate (>20 Mbps) 2.4GHz
- 802.11h - Dynamic Frequency Selection und Transmit Power Control Mechanismus
- 802.11i - Authentication und Sicherheit

Wireless LAN Security


THE WALL STREET JOURNAL.

MONDAY, FEBRUARY 5, 2001 WSJ.com

Hackers Can Penetrate Wireless Network

By James Sandberg
Staff Reporter of The Wall Street Journal
A group of respected security research-

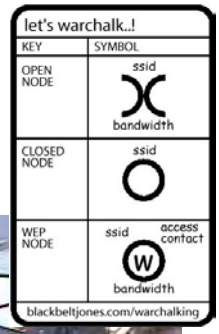
ple, brought to light by network-security specialists around the globe. Mr. Goldberg himself found a significant flaw in the

rel." He adds that the IEEE is working on future versions that won't be vulnerable. But Mr. Ennis says this type of attack

connect to networks using major base antennas in their laptop or desktop PCs. The technology, also called Wi-Fi, is sup- by many vendors but was popularized by Apple Computer Inc. under the name Air-Port and is quickly being deployed in net- works at a growing number of business- college campuses, hotels and airports. By the end of 2001, an estimated 10 million Wi-Fi radios will be deployed, according to research firm Cahners In-Stat. Starbucks Corp., for instance, plans to use the tech- nology to allow latte quaffers to noodle

The weakness is another reminder of the difficulty in implementing effective network security.

chief scientist at Zero Knowledge Systems Inc., a privacy-software firm in Montreal.

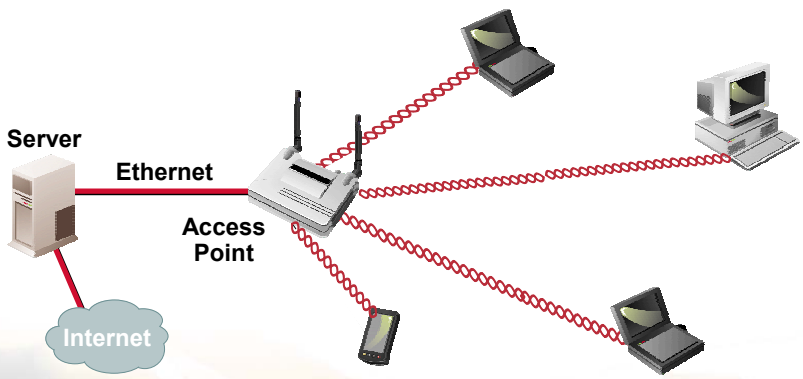


Berichte zu WLAN Security

University of California, Berkeley	University of Maryland	Scott Fluhrer, Itsik Mantin, and Adi Shamir	University of Maryland
Feb. 2001	April 2001	July 2001	Feb. 2002
Focuses on static WEP; discusses need for key management	Focuses on authentication; identifies flaws in one vendor's proprietary scheme	Focuses on inherent weaknesses in RC4; describes pragmatic attacks against RC4/WEP	An Initial Security Analysis of the IEEE 802.1x Standard

* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"
– University of California, Berkeley report on WEP security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Übertragungsmedium von Wireless



Sniffing 802.11 WLAN

www.wildpackets.com

www.sniffer.com

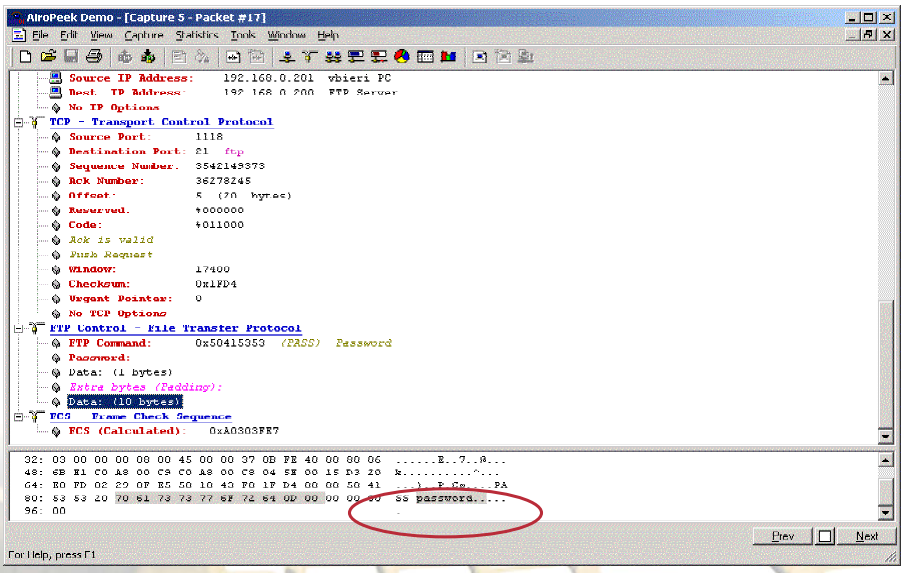
802.11 Sniffers Eigenschaften

- Automatische Channel Auswahl
- Signalstärke wird pro Accesspoint angezeigt (Minimum – Durchschnitt - Maximum).
- Klartext Analyse
- Driver Support und Integration des promiscuous Mode von 802.11b. Treiber für 2 namhafte Hersteller integriert:

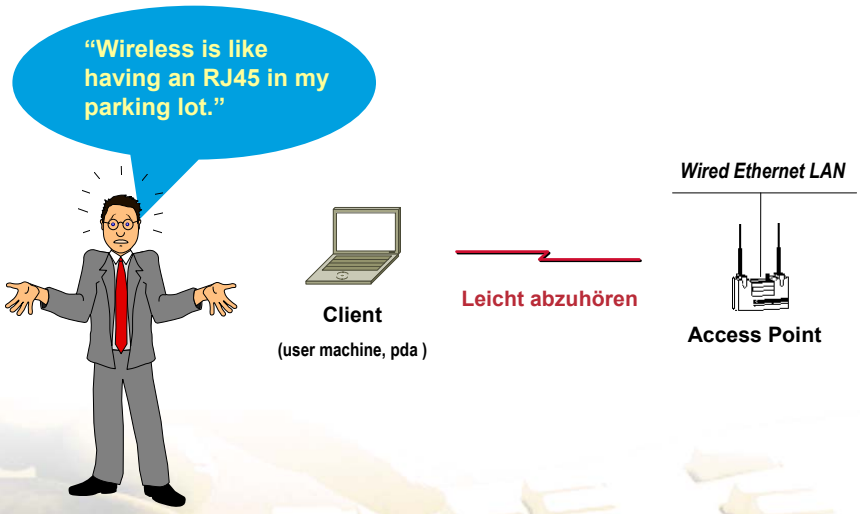
  Symbol Technologies' Spectrum24® Model 4121

  Cisco Systems' Aironet 340/350 client adapters cards

Verkehr im Klartext



Wireless LAN



Wireless LAN
Security Anforderungen

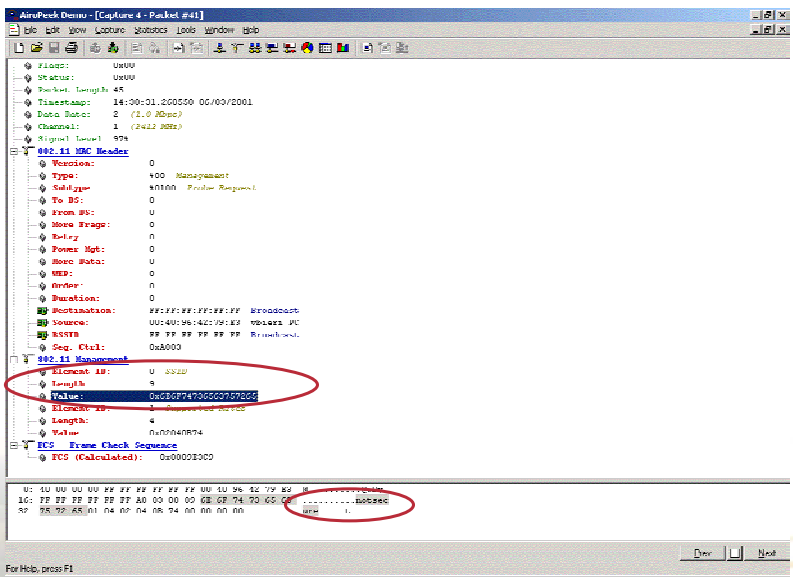
- **Authentifizierung**
  - **User Authentifizierung**
  - **Access Point Authentifizierung**
- **Verschlüsselung**
  - **Schutz der übertragenen Daten**
  - **Out of the Box keine Verschlüsselung**
    - **Problem unbekannter (rouge) Accesspoints**

??? Was bietet der Standard 802.11 ???

SSID : Service Set Identifier

- Netzauswahl über SSID → kein Security Feature
- Logische Segmentierung der Bandbreite für User (for management, for load distribution, …)
- Wird von einigen AP sogar mitgeschickt (beacon frame)
- Oder manuell am Client konfiguriert.

SSID is Sent in the Clear



SSID problem

- 32 ASCII characters string
- Wird unverschlüsselt gesendet
  (AP beacon und Client probe frames)
- Bei 802.11, kann jeder Client sich zu jedem AP assoziieren ohne Beachtung der SSID
- Unter XP werden alle verfügbaren AP (unterschieden durch SSIDs) angezeigt

➔ KEIN SECURITY FEATURE

Wired Equivalent Privacy - WEP

- Soll Abhören der “Leitung” verhindern
  → Keine Ende-zu-Ende Security
- Authentifizierung durch den WEP Schlüssel
  → Keine sinnvolle Authentifizierungsmethode
- Stromverschlüsselung RC4 wird verwendet
- kein Keymanagement definiert

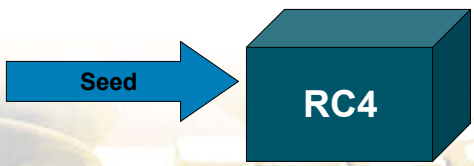
WEP (Cont.)

- IEEE hat nur 40-Bit Schlüssel im Standard vorgeschrieben
- Die meisten Hersteller unterstützen 104 (128) Bits
- Jedes Paket hat einen Integrity Check Value (ICV)
  Die CRC-32 Checksumme wird bei WEP mitverschlüsselt
- Adressierung durch MAC Adressen
  → werden im Klartext gesendet

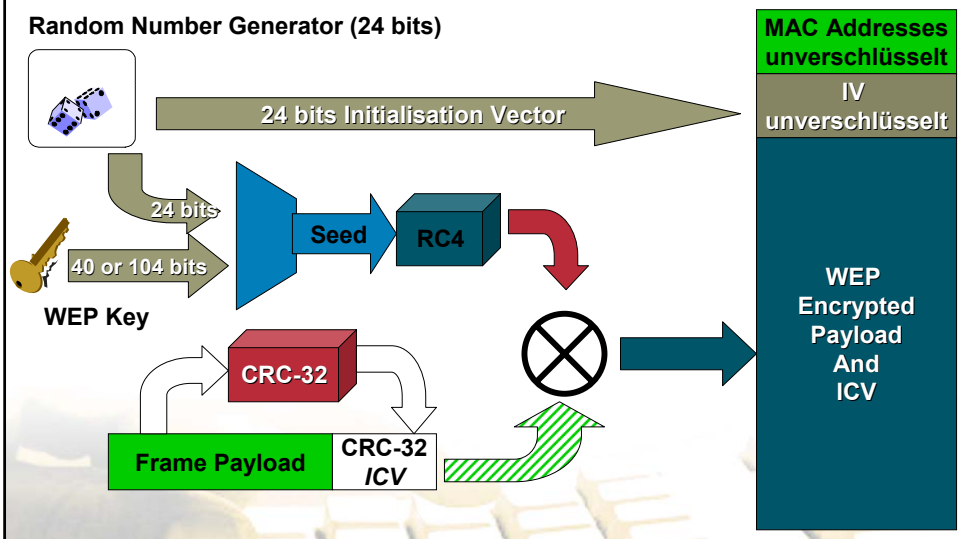
RC4 Stromverschlüsselung

- RC4 ist eine Stromverschlüsselung
  (vgl: DES, 3DES, AES Blockverschlüsselung)
- Anhand eines Seeds wird eine Pseudozufallszahl erzeugt
- Es existieren schwache Schlüssel (Seeds)

Schlüssellänge	Anzahl schwache IV's
40Bit	1280
104Bit	3328
128Bit	4096



802.11 WEP Encryption



Assoziation != Authentifizierung

- **Assoziation ist der Prozess bei dem sich ein Client beim AP anmeldet (vgl. RJ45 Stecker in Buchse stecken)**
- **Authentifizierung ist der Prozess, die Assoziation des Clients zu legimitieren**

802.11 Client Authentication

Open Authentication

Authentication request →

← Authentication response

Shared-Key Authentication

Authentication request →

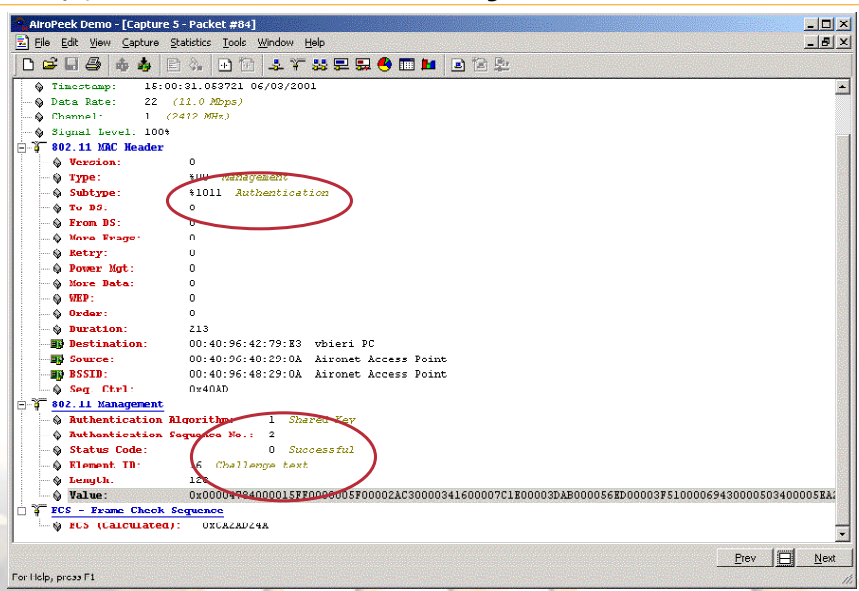
← 128 bits Challenge text packet

WEP Encrypted challenge text packet →

← WEP Encrypt

Klartextanalyse möglich

Shared Key Authentication



Probleme mit WEP

- Verbindungsloses Protokoll
  - → Replay Attack
- Lineare Checksumme (CRC)
  - → Paket Modifikationen möglich (bits flips)
- IV Reuse (Kollision, gleiche IVs)
  - → Schwache IVs für RC4 (airsnort)

Replay Attack

- Ein aufgezeichnetes Paket kann als gültiges Paket immer wieder eingespielt werden
  - mindestens Denial of Service Angriff möglich
- Wiedereingespieltes Paket wird von AP und Client entschlüsselt und verarbeitet
  - z.B. Abmeldung eines Clients kann wieder eingespielt werden
- Extrem gefährlich für verbindungslose Protokolle: UDP: NFS, NTP, …

Linear verschlüsselter ICV

- **Nicht nur Daten können verändert werden, auch der ICV kann entsprechend angepasst werden**
  - **ICV wird linear aus Nutzdaten berechnet**
  - **Kein Hash, wegen automatischer Fehlerkorrektur**
  - **Änderung des Klartextes → Änderung des CRCs (lineare XOR Verschlüsselung)**

IV Wiederholung
Plain Text Attack gegen RC4

- **Wie führt man Klartextangriffe durch?**
  - **IP Verkehr ist weitgehend vorhersagbar (definiertes Protokoll)**
  - **Authentication challenge** *(in shared key authentication)*
  - **Send packets from outside** *(ping to one specific STA)*
- **Wenn Klartext und Geheimtextpaar bekannt sind:**

  Key stream = Cipher Text ⊗ Plain Text = RC4 (IV, WEP Key)
- **Proof:**
  1. **KS ⊗ PT = CT** (Basis of key ciphers)
  2. **KS ⊗ PT ⊗ PT = CT ⊗ PT** (apply ⊗ *PT* on both side)
  3. **KS = CT ⊗ PT** (PT ⊗ PT = 0)

Wiederverwendung des IVs

- **Paketschlüssel sollten nicht wieder verwendet werden**
- **Paketschlüssel besteht aus**

  WEP key *(Geheim)*

  IV *(bekannt)*
- **Um ein WEP Frame entschlüsseln zu können, muss der entsprechende Paketschlüssel bekannt sein.**

➔ **Schlüsselsequenz nur abhängig von IV bei statischem WEP Key**

Wiederverwendung eines IV

- **24 bit IV**

  2^24 unterschiedliche IV = 16.777.216
- **Bei Verwendung von zufälligen IVs**

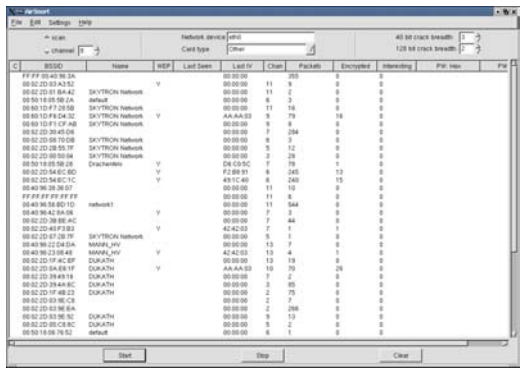
  50% Kollision nach 4.823 frames
  (Geburtstagsproblem, 23 Leute werden benötigt, damit zu 50 % zwei am gleichen Tag Geburtstag haben)

  → **Kollision alle 5s bei 1000 frames/s !**
- **Mit zählendem IV (beste Möglichkeit)**

  → **IV Wiederholung nach 70 Stunden**

Airsnort

WEP Key kann durch passiven Client nach 5-10 Mio mitgeschnittenen Paketen innerhalb von Sekunden entschlüsselt werden



Schlüssellänge	Zeitdauer (Cisco/SMC)	Verschlüsselte Pakete (Cisco/SMC)	Anzahl „interesting“ (Cisco/SMC)
40Bit	10h / 2h	3.4Mio / 0.9Mio	1621 / 821
128Bit	-h / 75h	- / 900 Mio	- / 5600

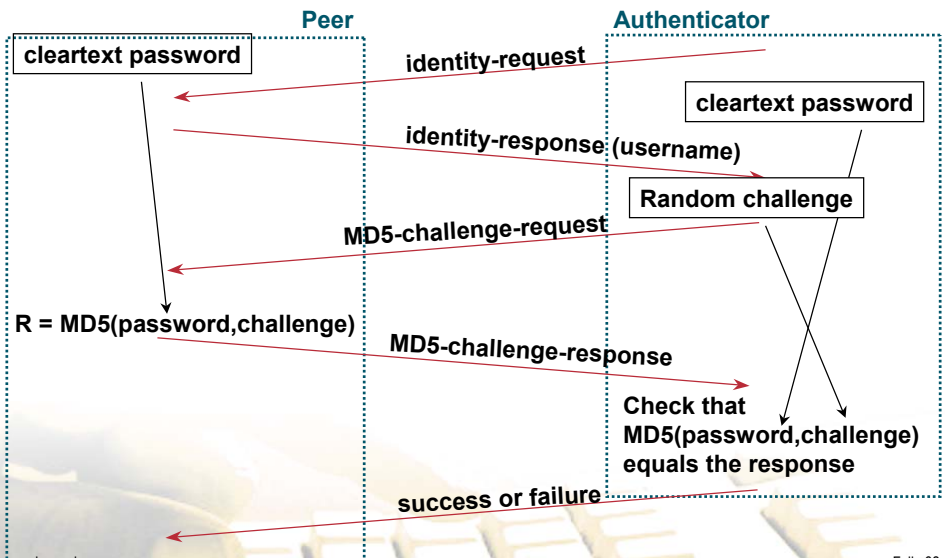
Agenda

- Sicherheit bei 802.11a und 802.11b
- Ausblick auf Verbesserungen
- Tools zum Ausnutzen der Sicherheitslöcher
- Vorgehen zum Auffinden von illegal betriebenen Access Points

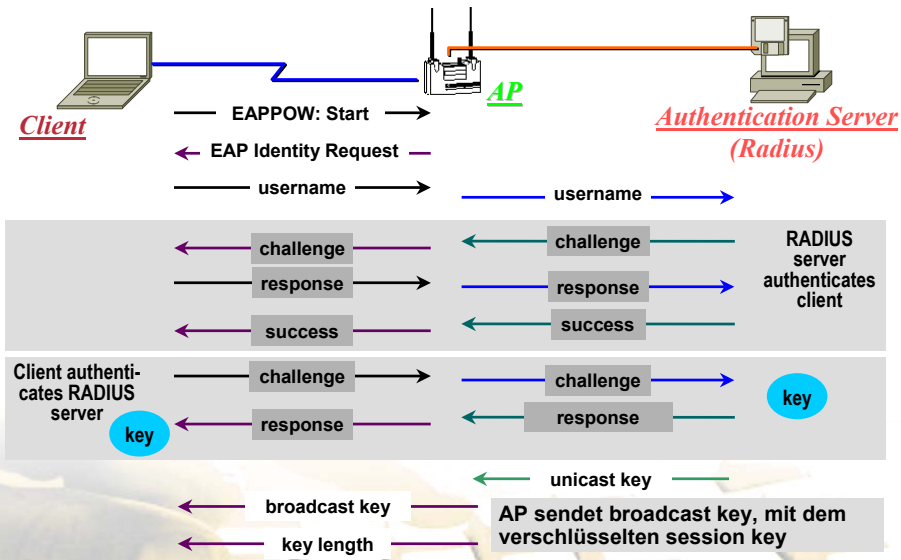
RFC 2284: EAP Defined

- **Extensible Authentication Protocol (EAP) ist eine Erweiterung von CHAP/PAP in PPP**
  - **Support multiple "authentication" schemes:**
    - **plain password hash (MD5)**
    - **token cards**
    - **GSS-API (Kerberos)**
    - **TLS (based on X.509 certificates)**

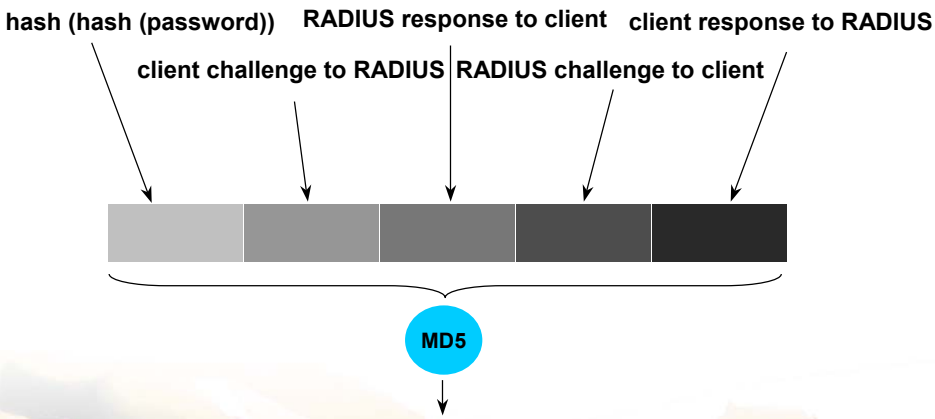
EAP with MD5



LEAP Steps: Mutual Authentication



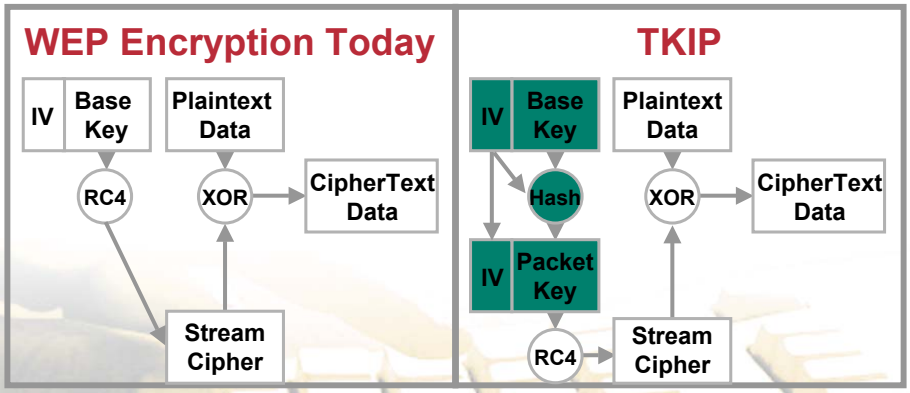
Bildung des Session Schlüssels



128-bit user based key
zeitlich limitieren: Reauthentication nach bestimmter Zeit → Neuer User Key

IV Key Hashing / Temporal Key

- WEP benutzt heute den IV und den Base Key; beinhaltet “schwache” Schlüssel, welche kompromittiert werden können.
- TKIP benutzt den IV und Base key um einen neuen Key zu hashen—daher pro Paket ein neuer Key; schwache Keys werden abgefangen



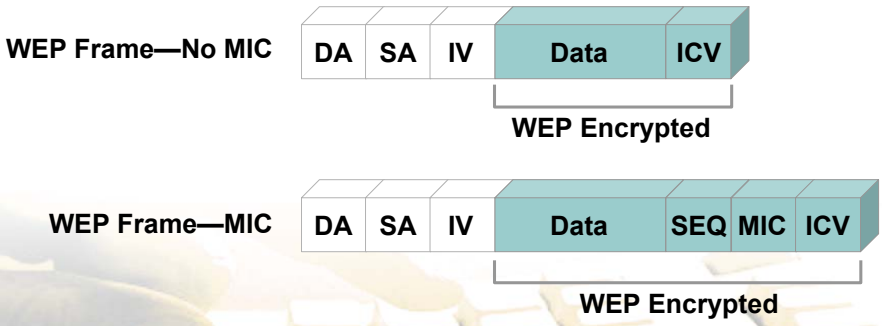
Message Integrity Check (MIC)

- MIC verhindert, dass WEP Frames verändert werden können.
- MIC basiert auf einem Seed Wert, Destination MAC, Source MAC, und Payload.

  Jegliche Änderung bedeutet, dass der MIC Value verändert wird.
- MIC ist in der WEP verschlüsselten Payload enthalten.

Message Integrity Check

- MIC benutzt einen Hashing Algorithmus um einen Frame zu markieren.
- MIC ist noch Pre-Standards, 802.11i Ratifizierung wird erwartet.



Wireless LAN Security: Authentifizierung

- IEEE 802.11 Authentifizierung
  - Open oder shared-key – Nicht sicher !
- Statische WEP Keys (Wired Equivalent Privacy)
  - Ohne korrekten Key kein Senden/Empfangen von Daten
  - Gerätediebstahl. Keys können gecracked werden.
  - Management der Keys
- MAC Address Authentifizierung
  - Geräte-basierend. Adressen können gespoofed werden.
- IEEE 802.1X: EAP Types
  - LEAP, PEAP und EAP-TLS. Komponenten eines neuen Standard für WLAN security. Unterstützt gegenseitige Authentifizierung und dynamische, per-user, per-session definierte WEP keys.

Wireless LAN Security: Verschlüsselung

- **IEEE 802.11 WEP - Standard für Verschlüsselung**
  - **Benutzt RC4 Algorithmus – bekannte Schwachstellen**
  - **Keys sind statisch und für alle User gleich, mit 802.1X, keys können für jeden User dynamisch und einzigartig sein.**

Pre Standards (z.T. noch proprietär):

- **Temporal Key Integrity Protocol (TKIP): Verbesserungen am RC4-basierten WEP**
  - **Key Hashing oder Per-packet keying, Message Integrity Check (MIC), Broadcast Key Rotation**
- **Advanced Encryption Standard (AES)**
  - **Vorgesehen bei 802.11i**

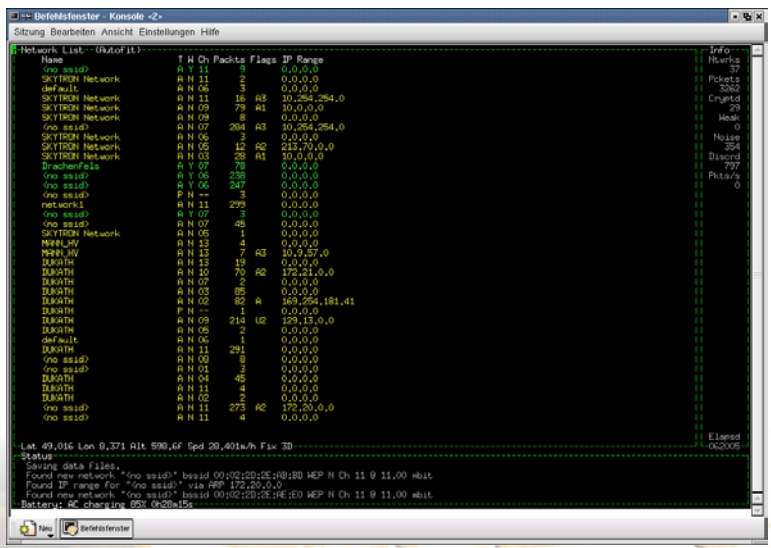
Wireless Security Suite

No Security	Basic Security	Enhanced Security	Specialized Security
No WEP and Broadcast Mode	Wi-Fi 40-bit, 128-bit, and Static WEP	Dynamic Key Management System, Mutual Authentication, and 802.1x via EAP	End-to-end security using VPN
			
Public Access	Telecommuter and Small Business	Mid-Market and Enterprise	Mobile User and Public Access

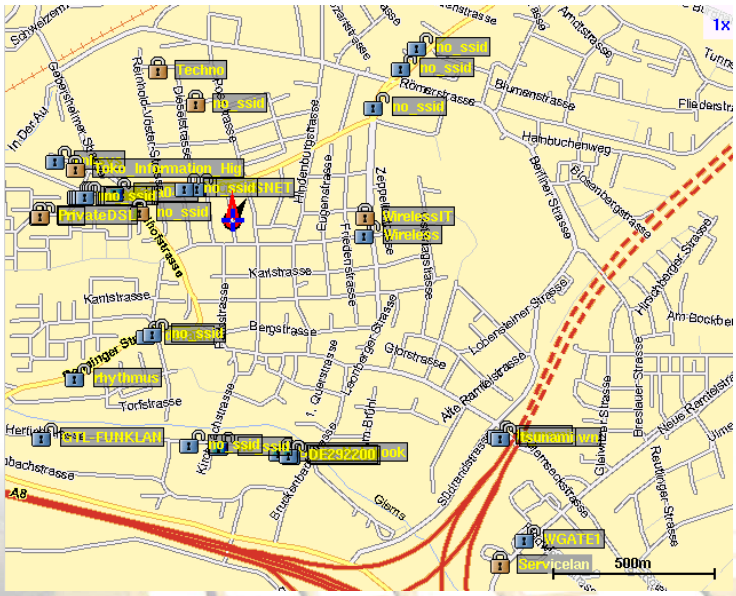
Agenda

- Sicherheit bei 802.11a und 802.11b
- Ausblick auf Verbesserungen
- Tools zum Ausnutzen der Sicherheitslöcher
- Vorgehen zum Auffinden von illegal betriebenen Access Points

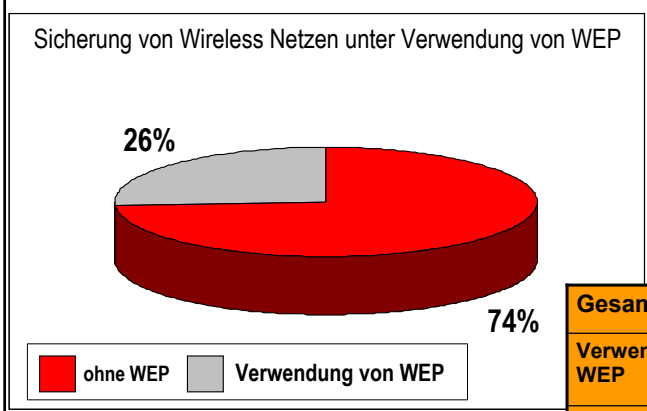
Kismet (GNU Public Lizenz)



GPSDrive mit Kismet Daten



Sicherheitsuntersuchungen - WarDriving



Gesamtanzahl	126
Verwendung von WEP	33 (26%)
Aufgelöste IP-Adressen	37 (29%)
Keine SSID erhalten	37 (29%)

Agenda

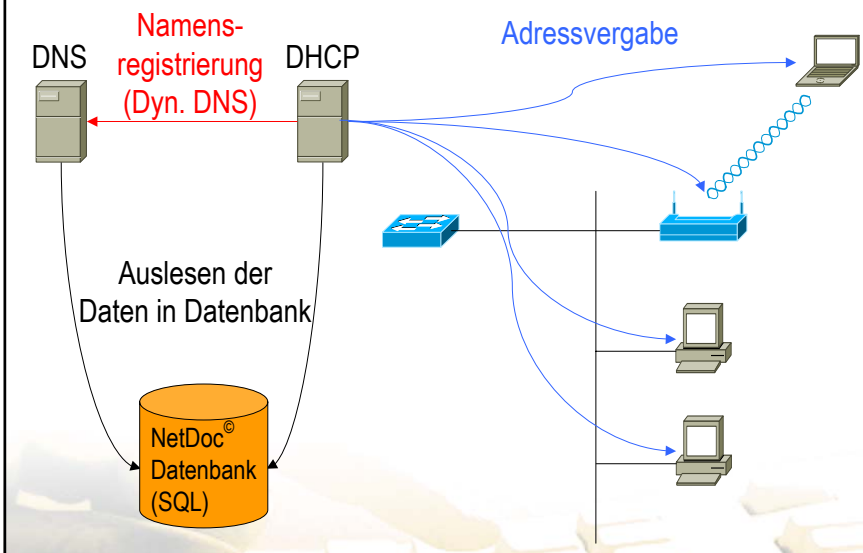
- **Sicherheit bei 802.11a und 802.11b**
- **Ausblick auf Verbesserungen**
- **Tools zum Ausnutzen der Sicherheitslöcher**
- **Vorgehen zum Auffinden von illegal betriebenen Access Points**

Suche nach „illegalen“ Access Points

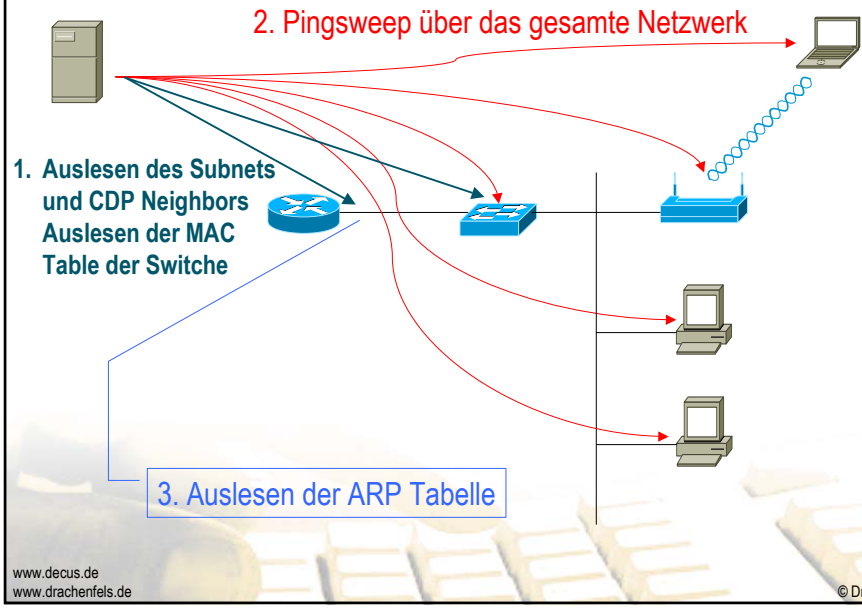
Zielsetzung:
- Auffinden von Access Points, die von Mitarbeitern selbst betrieben werden und deshalb ein Sicherheitsrisiko darstellen
- Auffinden von Access Points, die installiert wurden um illegalen Zugriff auf das Corporate Netzwerk zu bekommen

Vorgehen:
- Automatisches Auslesen der aktiven Netzwerkkomponenten durch NetDoc
- Automatische Erfassung aller MAC Adressen im Unternehmen
- Klassifizierung der MAC Adressen
- Manuelle Überprüfung potentieller Access Points

MacCheck ©



MacCheck ©



MacCheck ©

Prüfen der Daten auf manuell gesetzte MAC Adressen („global / local Bit“)
Prüfen von mehreren MAC Adressen auf einem Switchport (auch um Hubs im Netzwerk zu identifizieren)

Datenbank über MAC Adressen im gesamten Unternehmen erstellen
→ Zuordnung zu den Herstellern
OUI (Organizational Unique Identifier)
→ Namenszuordnung (DNS Hostname)
→ IP Adresszuordnung
→ Abgleich der ARP Tabellen Soll ⇔ Ist

MacCheck ©

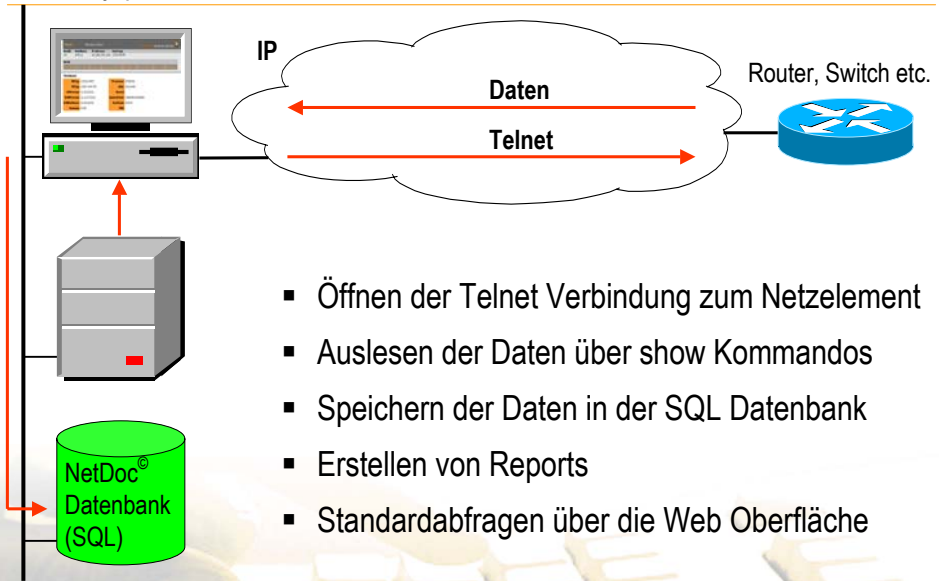
Datenbankabgleich zwischen IST und SOLL Zustand
a) Namenskonventionen der Hostnamen (DNS Eintrag vorhanden ?)
b) bekannten Netzwerkkarten in Unternehmen
c) Daten aus login-Scripten (MAC Adressen auslesen, evt. Wirelesskarten schon klassifizieren, USB Geräte erkennen)
d) CDP Identifikation bei Cisco AP
e) Changereport von Netdoc (Klassifizierung von neuen MAC Adressen hinzu?)

→ manuelle Überprüfung der Restmenge

Datenstruktur

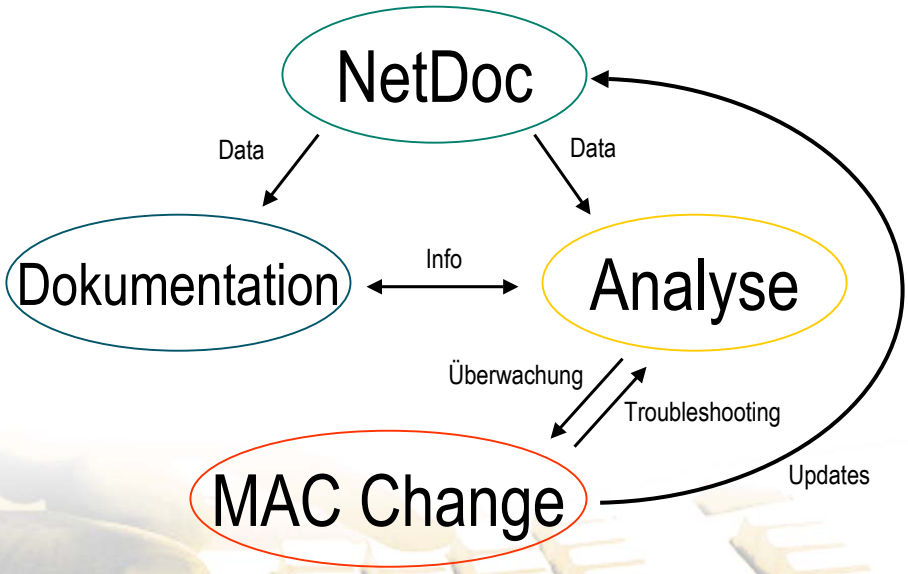
Datum	Mac Adresse	CDP	Global / Local Bit	Hersteller (OUI)	IP Adresse	DHCP (ja / nein)	DNS Host Name	Switch Port	Bekannter Eintrag
...	...	...	...	...	...	...	...	...	...

NetDoc© Übersicht



- Öffnen der Telnet Verbindung zum Netzelement
- Auslesen der Daten über show Kommandos
- Speichern der Daten in der SQL Datenbank
- Erstellen von Reports
- Standardabfragen über die Web Oberfläche

NetDoc© Prozesse



Zusammenfassung

- Wireless Netzwerke sind sicher, wenn über 802.11a/b hinausgehende Sicherheit verwendet wird (802.11i)
  - LEAP
  - TKIP
  - MIC
- Keine „illegal“ betrieben (rouge) Access Points im Unternehmen dulden
  - Mitarbeitern sicheres Wireless zur Verfügung stellen
  - Suche nach diesen Access Points durch MacCheck und anderen Tools

Kontakt

Thorsten Kocher	mobile: +49-160-5820455
Drachenfels GmbH	mail: t.kocher@drachenfels.de
Bleichstr. 56	home: www.drachenfels.de
D-75173 Pforzheim	phone: +49-7231-9223800

Frank Greisiger	mobile: +49-171-5761460
Drachenfels GmbH	mail: frank@drachenfels.de
Bleichstr. 56	home: www.drachenfels.de
D-75173 Pforzheim	phone: +49-7231-9223800

Vielen Dank