WLAN Sicherheit

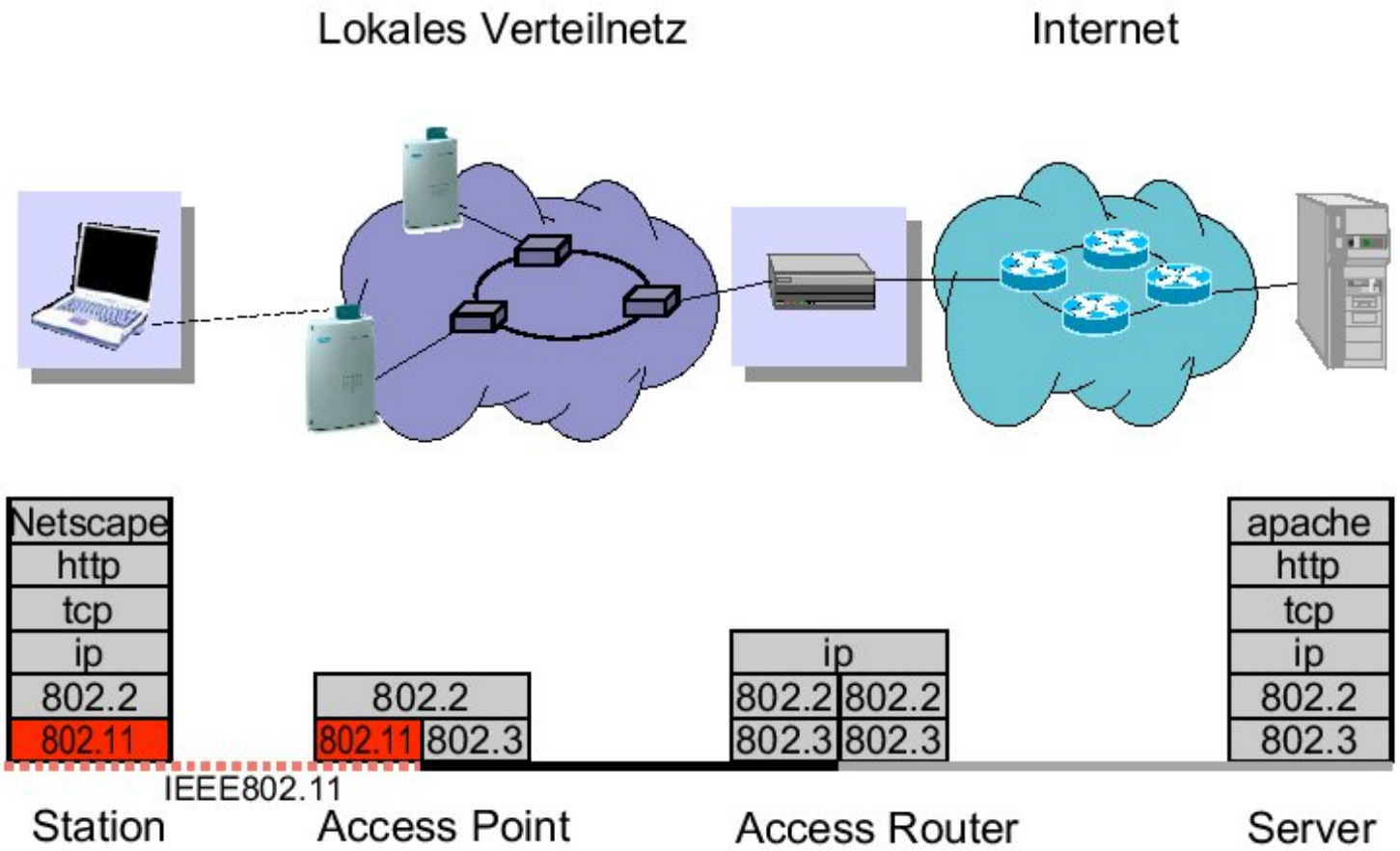
Karl Unterkalmsteiner, Matthias Heimbeck

Universität Salzburg, WAP Präsentation, 2005

Gliederung

Gliederung

Wireless LAN IEEE802.11 Architektur



IEEE 802.11 im Überblick	
Arbeitsgruppe	Arbeitsgebiet
802.11a	54-MBit/s-WLAN im 5-GHz-Band
802.11b	11-MBit/s-WLAN im 2,4-GHz-Band
802.11c	Wireless Bridging, Netzkopplung über WLAN
802.11d	"World Mode", Anpassung an regionsspezifische Regulatoren
802.11e	QoS- und Streaming-Erweiterung für 802.11a/g/h
802.11f	Roaming für 802.11a/g/h (Inter Access Point Protocol IAPP)
802.11g	54-MBit/s-WLAN im 2,4-GHz-Band
802.11h	802.11a mit DFS und TPC, "11a-Europe"
802.11i	Authentifizierung und Verschlüsselung (AES, 802.1x)
802.11j	802.11a mit Zusatzkanälen ab 4,9 GHz, "11a-Japan"
802.11k	Austausch von Leistungsdaten zwischen Client und Access Port
802.11l	unbenutzt wegen typografischer Verwechselungsgefahr
802.11m	maintenance", Veröffentlichung von Standard-Updates
802.11n	Next-Generation-WLAN mit mindestens 100 MBit/s netto

- Unter 802.11: Standard für Übertragungsprotokoll
- Unter WEP, WPA, WPA2: Standard für Sicherheitslösungen basierend auf 802.11

Gliederung

- Nutzung der Infrastruktur durch Unbefugte
- Abhören der Kommunikation
  - Sensitive Daten an Dritte
  - Entschlüsselung durch Unbefugte
- Manipulation der Kommunikation
- Beeinträchtigung der Verfügbarkeit

Gliederung

- Studie Hewlett Packard Ges.m.b.H., Juni 2004
  - Untersuchung von rund 3000 Access Points (AP) in Wien
  - WEP bei 48% aller APs
  - Default SSIDs bei 37% aller APs
  - Default SSIDs mit WEP 29% aller APs

Gliederung

Funktionsweise

- WEP soll Sicherstellen:
  - Vertraulichkeit: RC4 Stromchiffre
  - Integrität: durch CRC (Cyclic Redundancy Check)-Summe geschützt
  - Authentizität: Challenge Response Verfahren

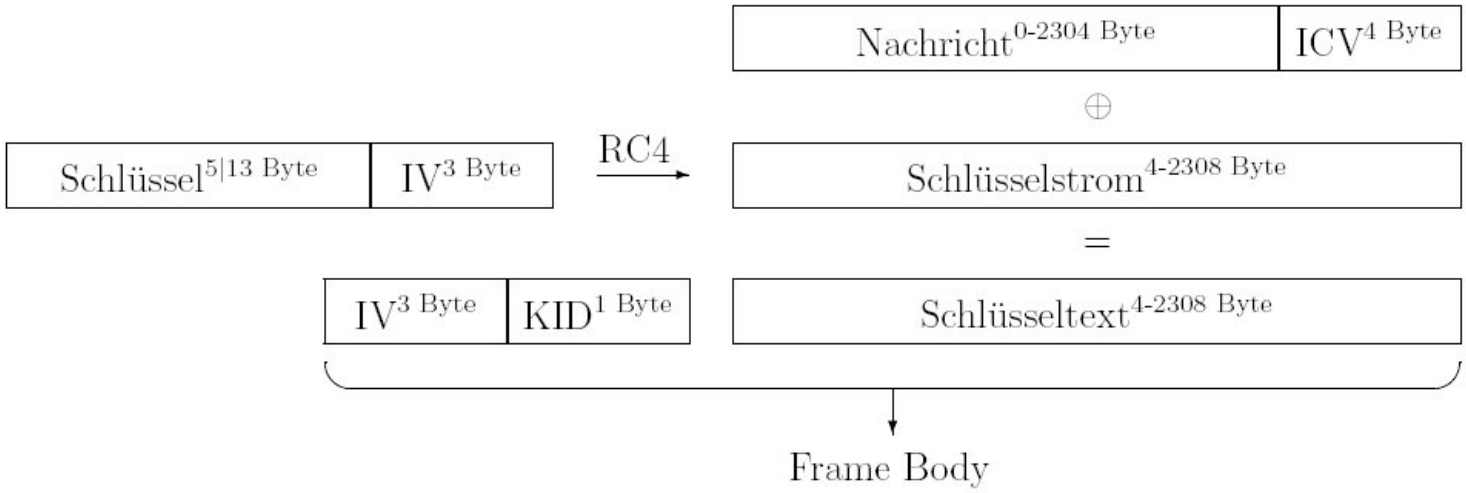
Vertraulichkeit

- Verschlüsselung
  - 40 oder 104 Bits Schlüssel (24 Bits für Initialisierungsvektor)
  - Shared Key, Schlüssel bei Verschlüsselung und Entschlüsselung

Vertraulichkeit

- Schritte:
  - Nachricht (Message M) mit 32 Bits langen CRC-Prüfsumme (CRC-32),dem ICV (Integrity Check Value)
    eigentliches Datenpaket: (M||ICV).
  - 24 Bit langer zufälliger Initialisierungsvektor (IV)
    verkettet mit geheimen Key: (K||IV)
    Länge(K||IV) = 64 oder 128 Bits
    RC4(K||IV) erzeugt Schlüsselstrom
  - (M||ICV) $\oplus$ RC4(K||IV) = C (Ciphertext)

Vertraulichkeit



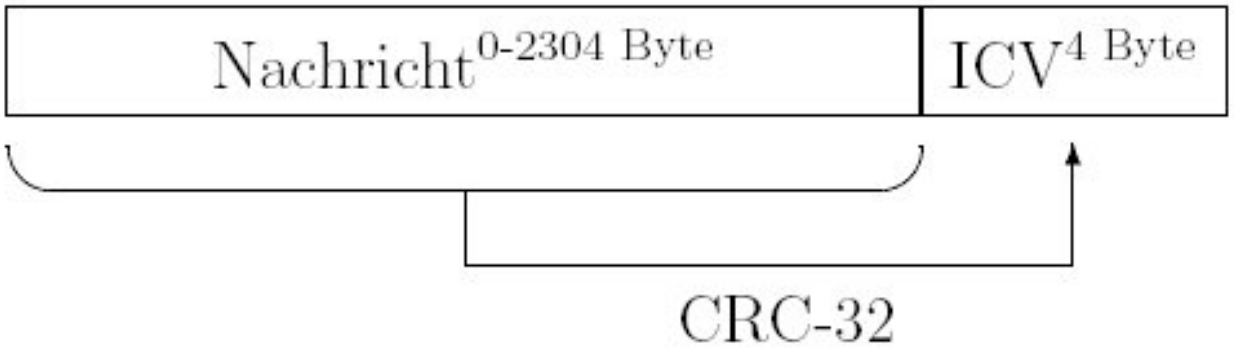
- Eventuell wird Nachricht vor Verschlüsselung fragmentiert
  Bei WEP keinen Einfluss auf Sicherheit und Ablauf der Verschlüsselung

Vertraulichkeit

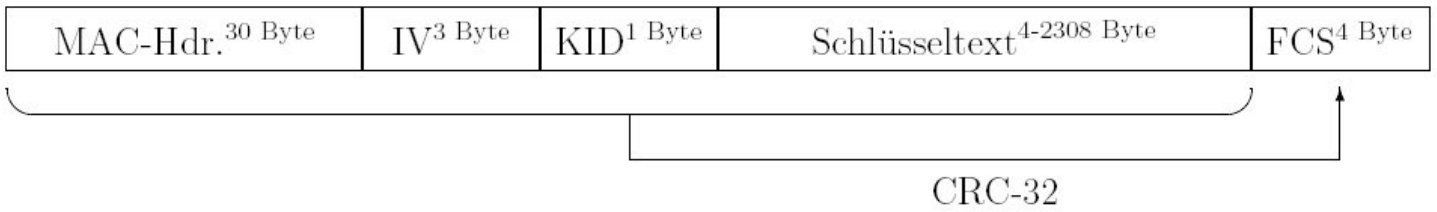
- Entschlüsselung
  - Empfänger: erhält unverschlüsselte IV und Schlüssel-ID
  - Mit Key-ID und Key und IVs kann der selbe Schlüsselstrom RC4(K||IV) wie der des Senders erzeugt werden.
  - Mit C = (M||ICV) $\oplus$ (RC4(K||IV) der Verschlüsselung folgt: (M||ICV) = C $\oplus$ RC4(K||IV)
  - Substitution:
    m = (M||ICV) r = RC4(K||IV)
  - C $\oplus$ r = (m $\oplus$ r) $\oplus$ r = m $\oplus$ (r $\oplus$ r) = m
  - Letzter Schritt: Vergleich des berechneten ICV mit dem erhaltenen ICV.
    Nur bei Übereinstimmung der Prüfsummen wird Nachricht Akzeptiert.

Integrität

- CRC-32 Checksumme normalerweise nur zur Absicherung zufälliger Übertragungsfehler
- Nachricht mit Checksumme vor Verschlüsselung (hilft nicht zur höheren Sicherheit !)



- Passenderer Einsatz: FCS (Frame Check Sequenz)
- WEP Frame Body besteht aus: IV, Schlüssel-ID, RC4(M||ICV)
- CRC-32 wird für WEP Frame Body berechnet (FCS)



Authentizität

- IEEE 802.11-Standard erlaubt zwei Betriebsmodi:
  - Open System:
    Keine Authentifizierung, jeder Client kann sich am AP anmelden
  - Shared Key:
    Anmeldung der Clients in einem Challenge Response Verfahren mit dem aus der Verschlüsselung gemeinsam bekannten Schlüssel

Schwachstellen

Achtung:

Schwachstelle von WLAN Komponenten durch Deaktivierung der Sicherheitsmechanismen der WEP Sicherheitsarchitektur im Auslieferungszustand.

Schwachstellen

- Passive Angriffe: Inhalt des Datentransfers ermitteln (Vertraulichkeit aus hebeln)
  - Brute Force Attacke (alle Möglichkeiten probieren)
  - Known Plaintext Attacke (Angreifer besitzt schon Klartext/Schlüsseltext Paare)
- Aktive Angriffe: Bedrohen Integrität und Authentizität der übermittelten Daten.
  Fremde oder manipulierte Daten einschleusen oder Datenverkehr verhindern.
  - Spoofing: Mit eigenem AP die Benutzer eines WLANs von dem eigentlichen AP abziehen
  - Replay Attacke: Bereits verwendete Datenpakete bestimmten Inhalts in den Datenverkehr einschleusen.

Gliederung

WPA Nachfolger von WEP

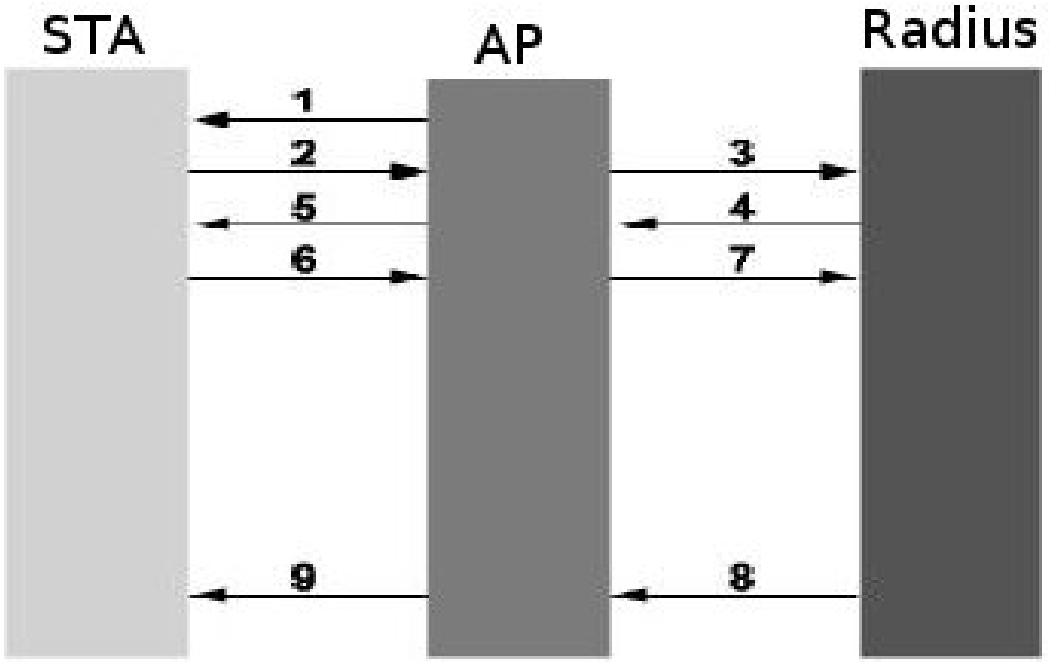
- Wireless Fidelity (Wi-Fi)
- Software Implementierung
- Teile des IEEE Standards 802.11i
- erweitert WEP um ein Schlüsselmanagement

Verschlüsselung - Integrität

- TKIP (Temporal Key Integrity Protocol)
  - Kapselung des WEP
  - Per Packet Key mit MAC Adresse, IV und K
  - kein identischer Bitstrom
  - Verschlüsselung selbst weiterhin RC4
  - temporäre Keys für Datenverschlüsselung
- MICs (Message Integrity Code) Michael
  - kryptographische Einweg-Hashfunktion

Authentizität

- (EAP) Extensible Authentication Protocol
  - Radius / Kerberos



PSK (Pre-shared key) Mode

- Ablauf
  - wie bei WEP vorher ausgetauschter geheimer Key
  - PMK (Pairwise Master Key) generiert durch Pre Shared Passphrase und SSID
  - Verteilung des PMK auf Station und AP
  - erzeugen des PTK (Pairwise Transient Key)
  - Integritäts Check
  - TKIP in PSK Mode

Schwachstelle

Durch die gesendeten Informationen zum erstellen des PTK besteht die Möglichkeit einer offline Wörterbuchattacke "WPA Cracker"

Gliederung

Nachfolger von WPA

- WPA2 - Kennzeichnung der Wi-Fi
- Juli 2004 - 802.11i Standard der TGI (Task Group) des IEEE
- RSN (Robust Security Network)

Ausblick WPA2

- Schlüsselmanagement
- Verschlüsselung
  - TKIP (Temporal Key Integrity Protocol)
  - CCMP (Counter Mode Encryption mit CBC-Mac)
    - AES Verschlüsselung
- Authentifizierung
  - EAP
  - Radius

ENDE

Wir Danken für Ihre Aufmerksamkeit.