Wired Equivalent Privacy - WEP

Dr. Axel Wachtler

Dresden, 12.03.2004

Einleitung

- Was ist WEP ?
- Arten von Wireless Netzen

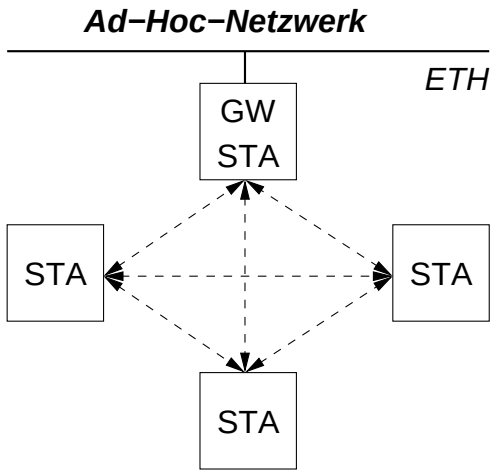
Was ist WEP ?

- optionale Sicherheitsergänzung für WLAN's nach IEEE 802.11
- Implementierung im MAC, Verschlüsselung der Daten auf der Luftschnittstelle
- Ziele bei der Definition des WEP-Standards:
  - äquivalente Sicherheit eines Kabelnetzes
  - einfache Nachrüstung bestehender Systeme (Softwareimplementierung)
  - Ressourceneffizienz (Mobilsysteme, Akku, Speicher, Rechenleistung)

Arten von Wireless Netzen

Ad-Hoc Netzwerke

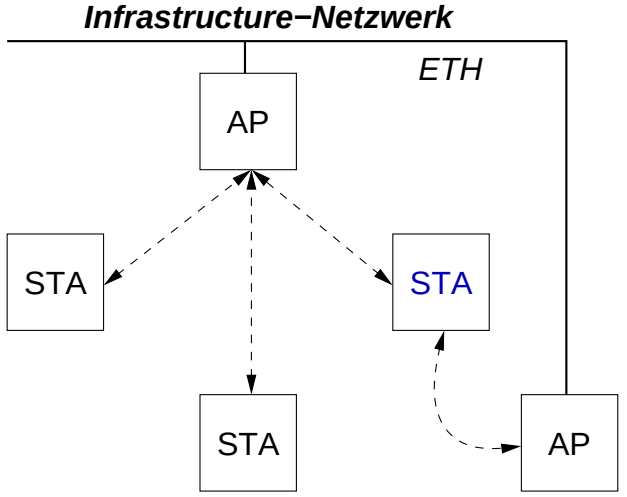
- Stationen haben Verbindung untereinander
- keine zentrale Zugangskontrolle
- geringerer Durchsatz (Collissions)



STA: Independent Basic Service Set (IBSS)

Infrastruktur Netzwerke

- Stationen Verbinden sich mit AP
- zentrale Zugangskontrolle
- AP steuert den Zugriff der Stationen zum Medium (weniger Collissions, RTS/CTS)
- Netzzugang auf Basis der MAC-Adressen



STA: Basic Service Set (BSS)

STA: Extended Service Set (ESS)

Das 802.11-Protokoll

Einleitung

802.11-Protokoll

- Verbindungsaufbau
- Authentifizierung

Verschlüsselung

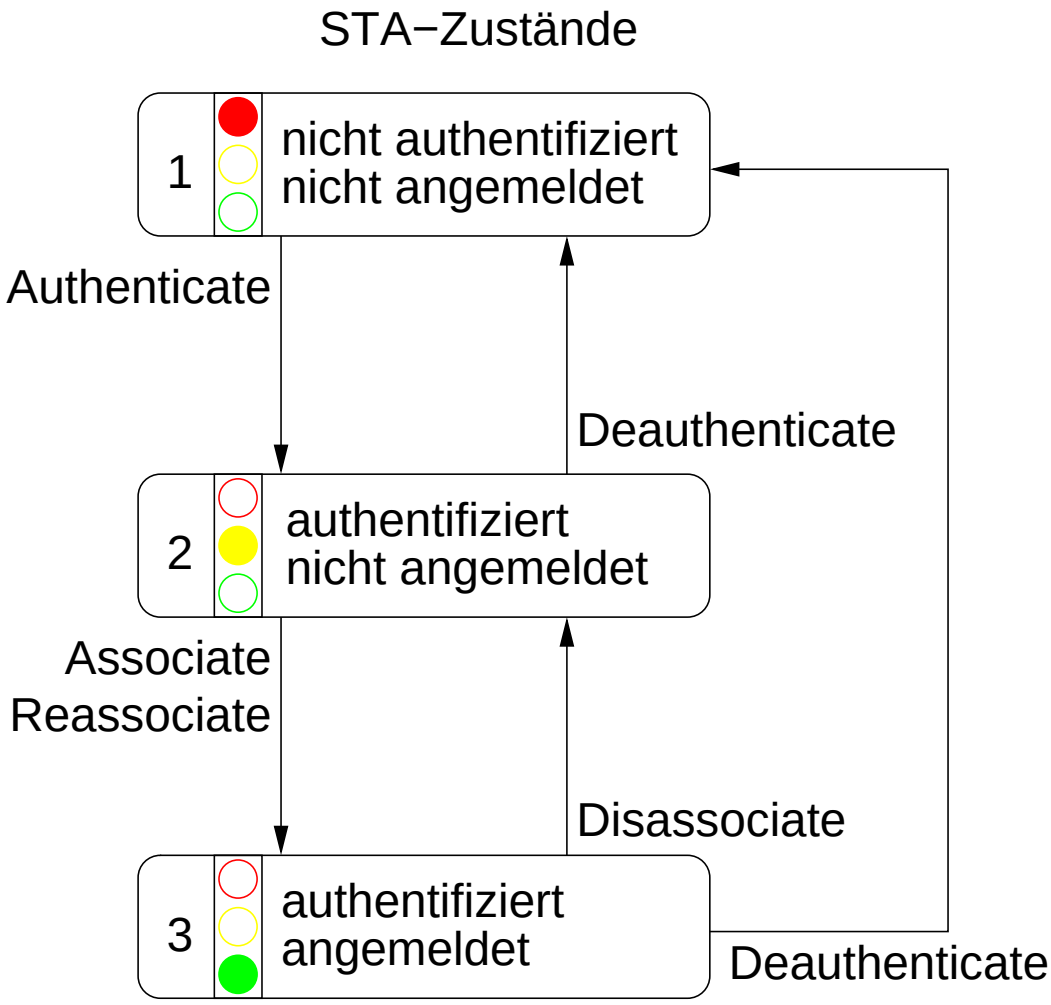
Ausblick

Verbindungsaufbau

- *Zustand 1:*
  Netzparam. werden gesendet (Beacon, Probe-Req./Resp.)

- *Zustand 2:*
  STA sendet Auth.-Req. (Varianten Open-System- oder Shared-Key-Authentication

- *Zustand 3:*
  STA sendet (Re)Assoc-Req., nur bei Ergebnis “successful” ist Datenübertragung möglich.



Authentifizierung

- nur die STA muß sich beim AP authentifizieren (Problem Fake-AP)
- zwei Arten zur Authentifizierung:
  - **Open-System-Authentification**:
    formale Authentizierung,
    AP authentifiziert anhand seiner MAC-Adresstabelle
  - **Shared-Key-Authentification**:
    AP sendet Challenge-Text im Klartext, STA antwortet mit encryptetem Challenge-Text, beide Rahmen sind On-Air beobachtbar und der Angreifer kann daraus den Key ermitteln (z.B. Wörterbuchangriff, AP gibt Auskunft, ob Key korrekt oder falsch "geraten" wurde).

Verschlüsselung

Einleitung

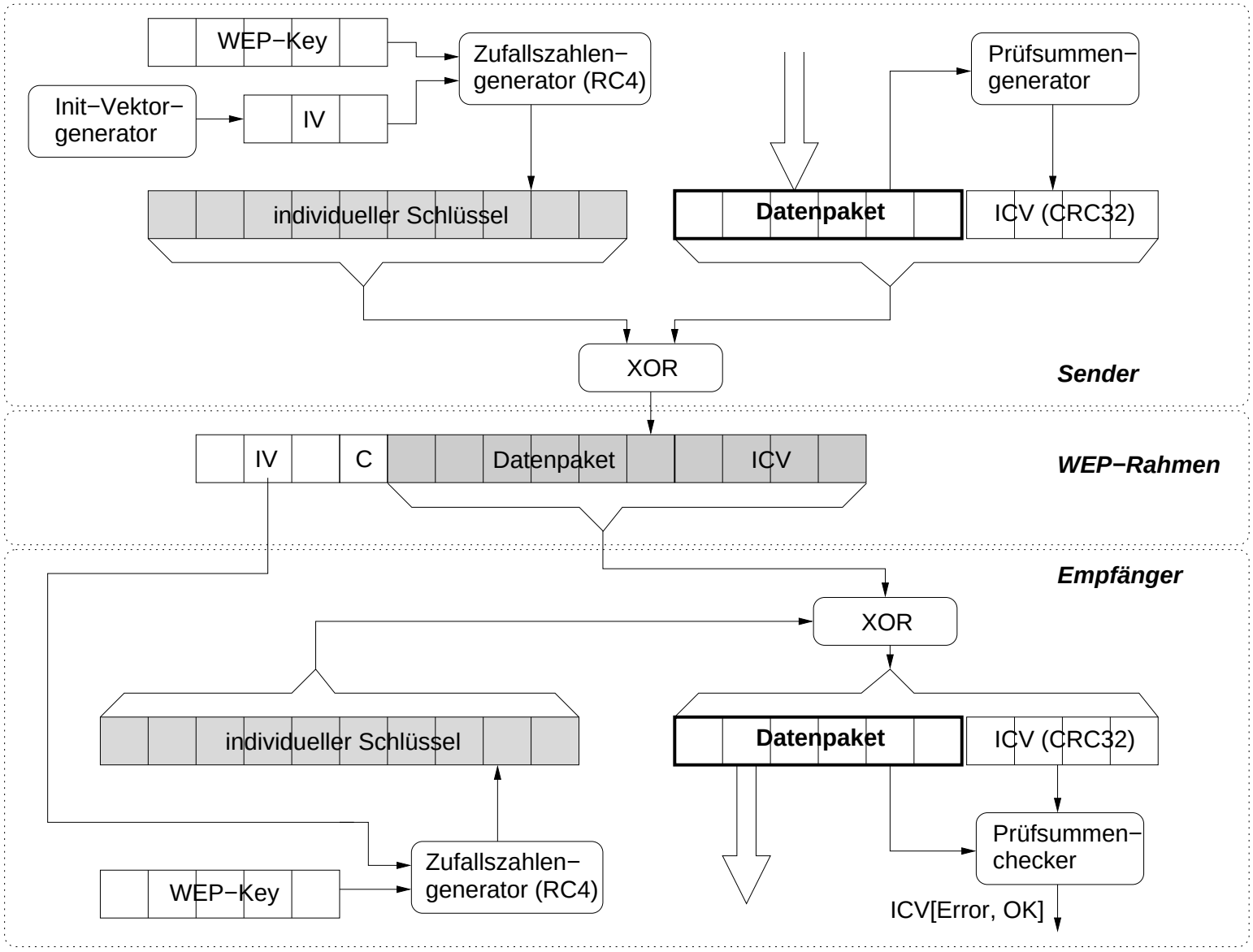
802.11-Protokoll

Verschlüsselung

Ausblick

- Datenverschlüsselung
- RC4-Verfahren
- WEP-Key und Init-Vektor
- Integritätsprüfung

Datenverschlüsselung



RC4-Verfahren

- Stromchiffirierung entwickelt von Ron Rivest, 1987, bis 1994 geheim, einfach in SW zu implementieren

- ausgehend von einem Schlüssel beliebiger Länge wird eine Bytefolge erzeugt, die als individueller Schlüssel (One Time Pad) bezeichnet wird.

- Ciphertext entsteht aus Exor-Verknüpfung von individuellem Schlüssel und Klartext

- die Größe des internen Schlüsselraumes bei RC4 beträgt $2^{1700} = 256^2 \cdot 256!$

- Problem bei RC4: es existieren kryptografisch schwache Schlüssel, bei denen Klar- und Ciphertext stärker korreliert sind.

- Bei WEP wird der RC4-Algorithmus mit jedem Datenpaket neu gestartet.

Init-Vektor

- Problem: Nach der Initialisierung mit dem WEP-Key würde der RC4-Generator immer die gleiche Bytefolge als individueller Schlüssel emitieren. Identische Klartexte ergeben somit identische Geheimtexte (Klartextangriff, IP-Protokoll enthält viel Klarext).

- Lösung: Hinzufügen einer Zufallskomponente (Initvektor) zum WEP-Key

- WEP verwendet einen 24-Bit Initialvektor, damit sind 16 777 216 Startwerte bei gleichem WEP-Key möglich, davon sind 9000 krypt. schwach.

- Theoretischer Verbrauch des IV-Raumes: Pakete mit 1500 Byte, eine Station, ca. 5 Mbyte/s: 84 min, praktisch treten IV-Kollisionen bereits nach 5000 Paketen auf

- Warum nur 3 Byte IV ? Design zugunsten der Maximimierung des Durchsatz. (Minimierung des Protokoll-Overheads)

Integritätsprüfung

- Ziel Prüfung der Authentizität einer Nachricht (Signatur) und Erkennung von modifizierten Rahmen (Replay-Angriff)
- Integrity Check Value (ICV) wird mit CRC32-Algorithmus berechnet (4 Byte Prüfsumme)
- CRC32 ist ein Algorithmus zur Erkennung von Übertragungsfehlern und kein kryptographischer Hash wie MD5 oder HMAC-SHA1.
- CRC32 ist ein lineares Verfahren, daher kann der ICV auch im Ciphertext ohne Kenntniss des Schlüssels korrigiert werden.

Ausblick

- Schwachstellen von 802.11 und WEP
- Aktuelle Lösungsmöglichkeiten
- Wifi Protected Access - WPA

Schwachstellen von WEP

- bei Shared-Key-Authentification ist Klartext und encrypteter Text beobachtbar
- kleiner Werteraum des IV und grosser Anteil an bekannten Daten bei TCP-IP
- krypt. schwache Schlüssel werden nur z.T. bei der IV-Generierung ausgefiltert.
- statische Schlüssel, viele Benutzer verwenden den gleichen Key über Wochen und Monate
- fehlende Definition zur Wahl des IV im Standard: Implementationsschwächen, z.B. Nullinitialisierung, Zähler mit 16 Bit Wraparound, kein Ausfiltern von schwachen IV's
- CRC32 ist ungeeignet für Integritätsschutz der Pakete - somit kein Schutz vor Replay-Attacken

Aktuelle Lösungsmöglichkeiten

- keine Shared-Key-Authentification, SSID löschen
- Standardeinstellungen der Hersteller ändern (SSID, Passwort)
- 104 Bit-Keys anstelle 40 Bit-Keys verwenden
- WEP-Keys öfter wechseln
- WLAN-Segmente zusätzlich sichern
  - End-zu-Endverschlüsselung (ssh, ssl, VPN)
  - Firewalls
  - wo möglich, dynamischer Schlüsseltausch nach 802.1X (Radius)

Wifi Protected Access - WPA

- neuer Standard 802.11i behebt die Schwächen von WEP
- Unterstützung von 802.1X Key Exchange (Radius, Benutzerauthentifizierung)
- dynamischer Sessionkey für Unicast and Multicast Traffic
- Message Integrity Code (MIC) ersetzt CRC32-ICV
- Replay-Detection beim Empfänger, mitgeführte Sendefolgenummer
- Auswahl aus zwei Verschlüsslungsverfahren: RC4 (TKIP) und AES (AES-CCMP)

Zusammenfassung

- für ein sicheres WLAN ist erheblicher Aufwand nötig
- Standardeinstellungen von Herstellern ändern
- End-zu-End-Verschlüsselung einsetzen
- WEP ist unsicher, es macht jedoch Eindringlingen das Leben schwerer.
- mit WPA werden die Schwächen von WEP behoben

Literatur

[1] Axel Sikora. *Wireless LAN - Protokolle und Anwendungen*. Addison-Wesley München, Boston, 2001.

[2] Cyrus Peikary and Seth Fogie. *Maximum Wireless Security*. Sams Publishing, 2002.

[3] R. Wobst. *Abenteuer Kryptologie: Methoden, Risiken und Nutzen der Datenverschlüsselung*. Addison-Wesley-Longman Bonn, 1998.

[4] The InteropNet Labs (iLabs). What is wrong with WEP ?
`http://www.ilabs.interop.net/WLAN_Sec/What_is_wrong_with_WEP-lv03.pdf`, 2003.