The Final Nail in WEP`s Coffin

Alexander Lichti

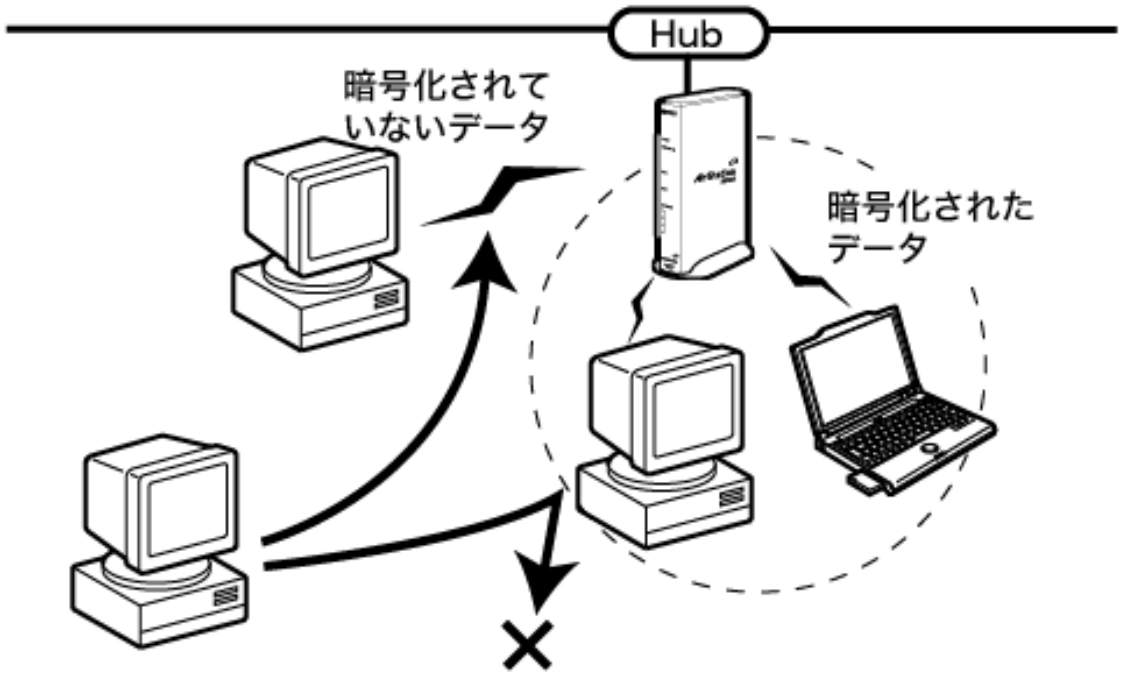
Literatur

- Bittau, Handley, Lackey: „The Final Nail in WEP`s Coffin“
- „Sicherheit im WLAN“, http://www.uni-koblenz.de/~steigner/seminar-net-sec/sem8.pdf
- „RC4“, http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html

Übersicht

- Grundlagen WEP
- Basisverfahren gegen WEP
- Erweiterte Verfahren

Grundlagen WEP



Grundlagen WEP

- WEP:
  Wired Equivalent Privacy
- Ziel:
  Sicherheit wie in kabelgebundenen Netzwerken
- Einsatz:
  Bis vor kurzem der Standard für die Verschlüsselung von Heimnetzwerken

Grundlagen WEP

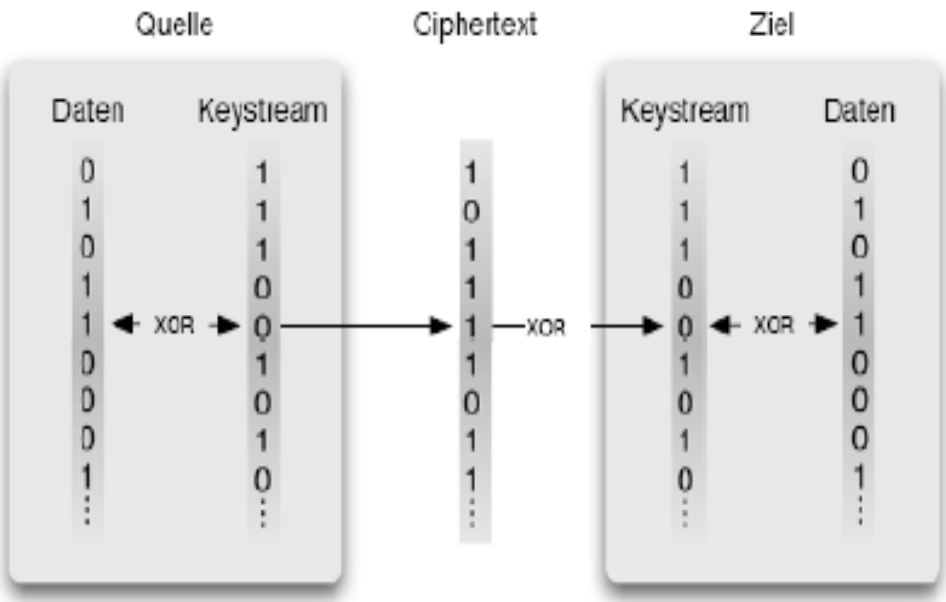
- Anforderungen:
  - Vertraulichkeit
  - Authentifizierung
  - Datenintegrität

Grundlagen WEP

- Funktionsumfang:
  - Paketverschlüsselung
  - Authentifizierung

Grundlagen WEP

- Datenübertragung:

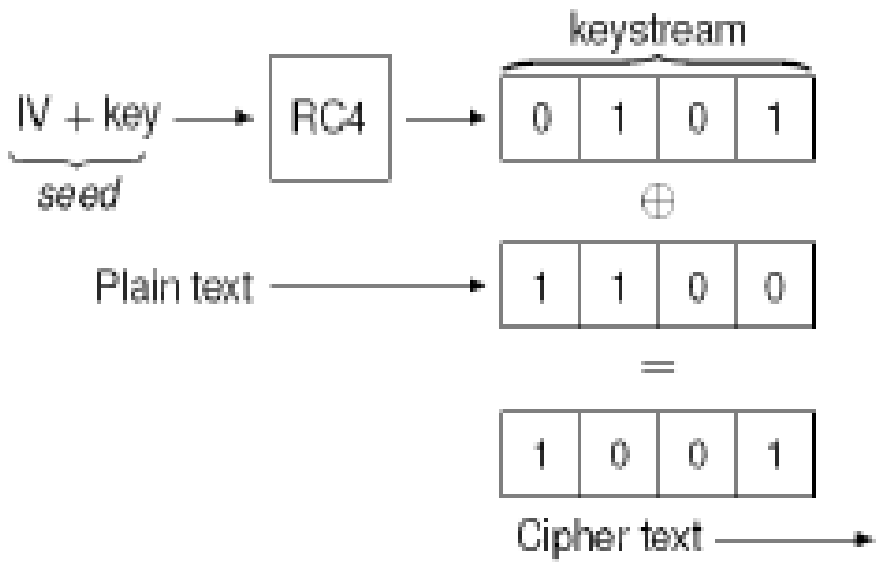


Grundlagen WEP

- Keystream:
  - Pre-shared-key (key)
  - Initialsierungsvektor (IV)
  - RC4

Grundlagen WEP

- RC4:



Basisverfahren gegen WEP

"Somebody has hacked into our computer, sir."

Basisverfahren gegen WEP

- Brute-Force-Attacke
- Authentifizierung (Keystream re-use)
- Weak-IV-Attacks

Brute-Force-Attacke

- Ziel: key

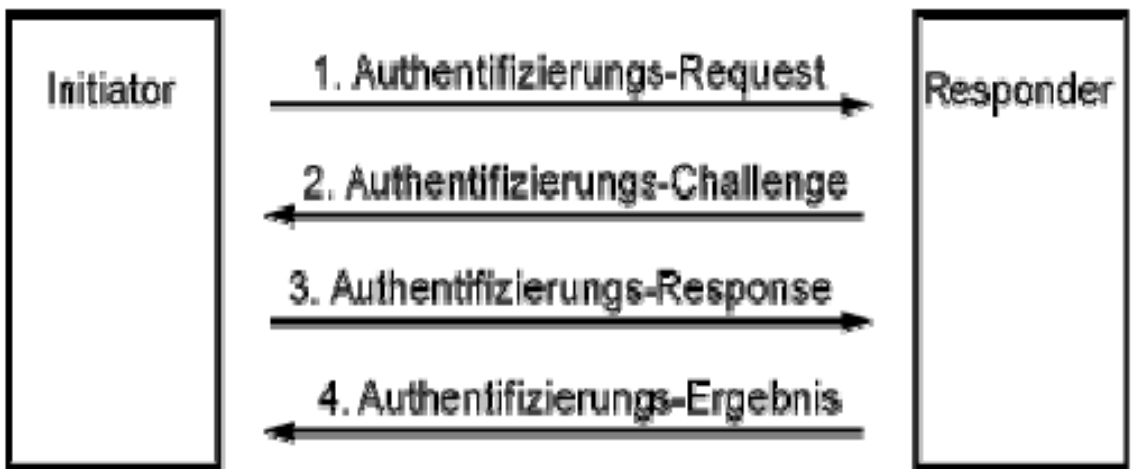
- Bekannt: Klartext (P), Ciphertext (C)
- RC(IV,key) = P $\oplus$ C
- Jetzt: Pure Rechenleistung entscheidet

Authentifizierung

- Ziel: Authentifizierung
- Voraussetzung: Shared Key Authentification aktiviert
- Keystream re-use
- Ausnutzen der Challenge-Response Authentifizierung

Authentifizierung

- Challenge-Response

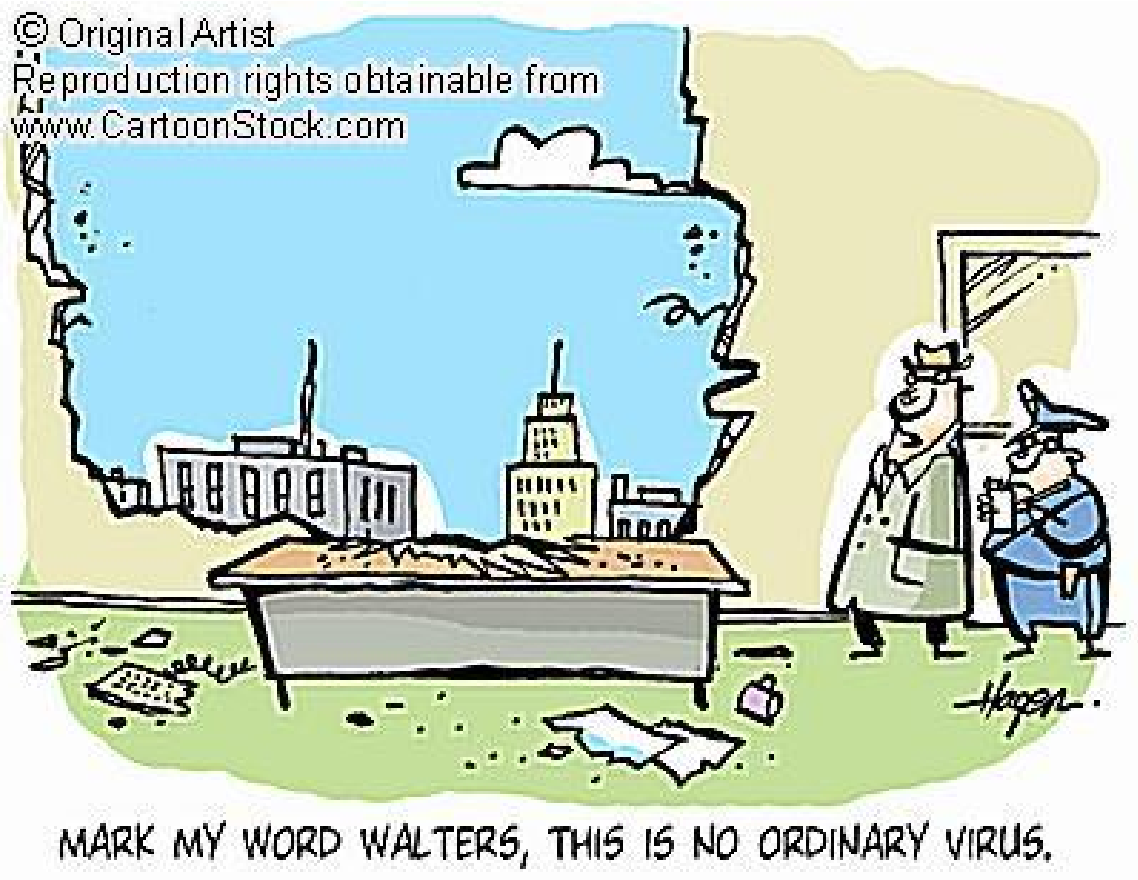


Weak-IV-Attacks

- Ziel: key

- Voraussetzung: (sehr) spezielles Setup
- statistisch-mathematischer Angriff
- Hohe Anzahl von IVs ermöglichen statistische Bestimmung des korrekten Schlüssels

Erweiterte Verfahren



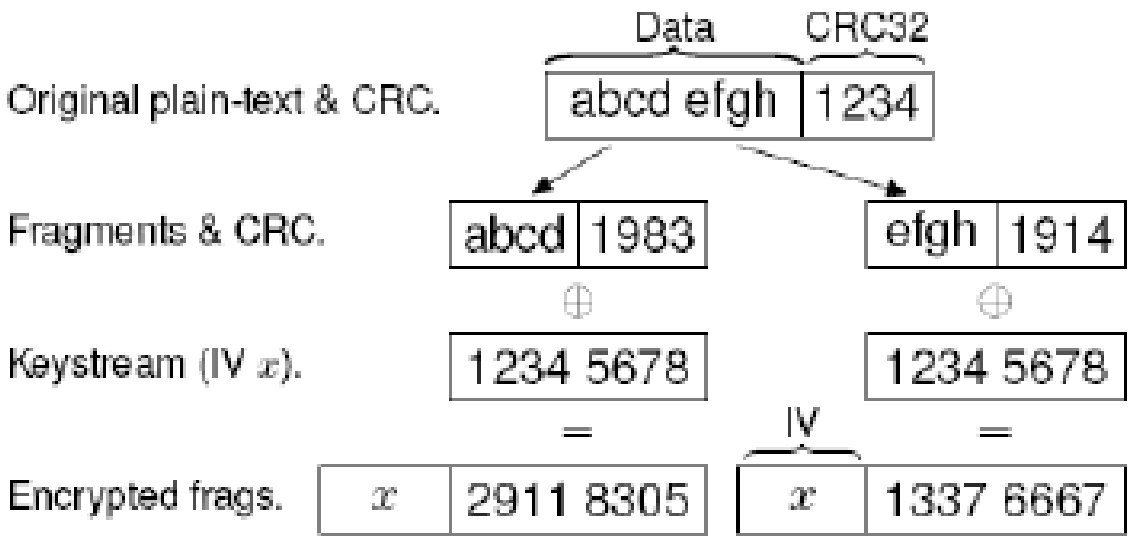
Erweiterte Verfahren

- Layer 2 Fragmentation Attacks
  - Fragmentierung
  - Known Plain-text
- Kernaussage:
  „IEEE 802.11 kann gegen WEP genutzt werden“

Fragmentierung in 802.11

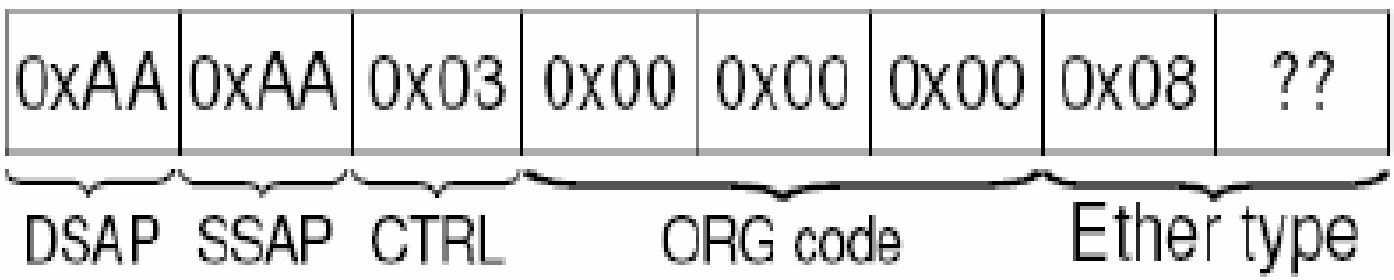
- Fragmentierung (MAC-Layer):
  - Datenpakete können in kleinere Datenpakete (Fragmente) zerlegt werden
  - Unabhängige Verschlüsselung
  - WEP: Bis zu 16 Fragmente mit demselben Keystream

Fragmentierung in 802.11



Known Plain-text in Packets

- 802.11 data frames haben folgenden bekannten, 8 Byte langen LLC/SNAP Header (ARP oder IP):



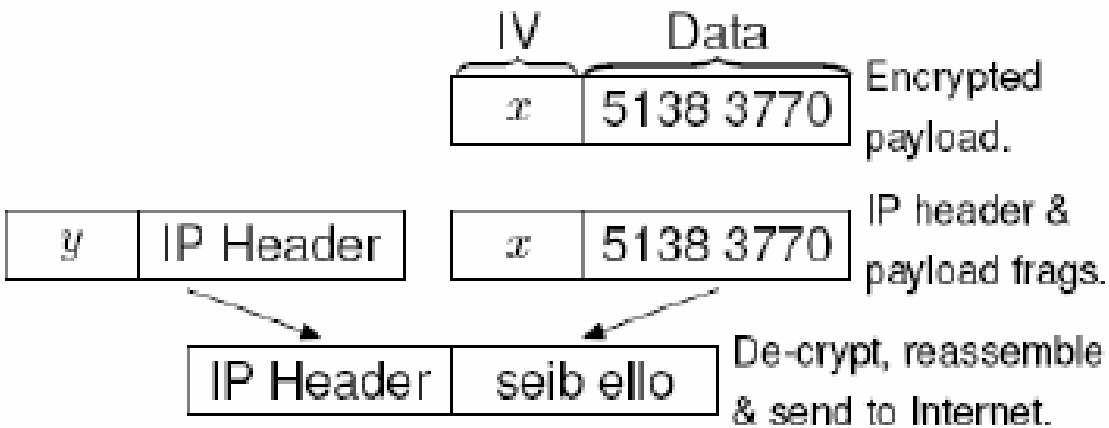
Pure Fragmentation Attack

- Ziel: Echtzeitdekodierung verschlüsselter Pakete
- Voraussetzung: Internetzugang des Zielnetzes
- Prinzip: Datenpakete umleiten

Pure Fragmentation Attack

- Erstellung von 4 Byte großen IP-Header Paketen
- Headerpakete senden
- Abgehörtes Datenpaket senden
- Datenpaket am Ziel in Klartext lesen…

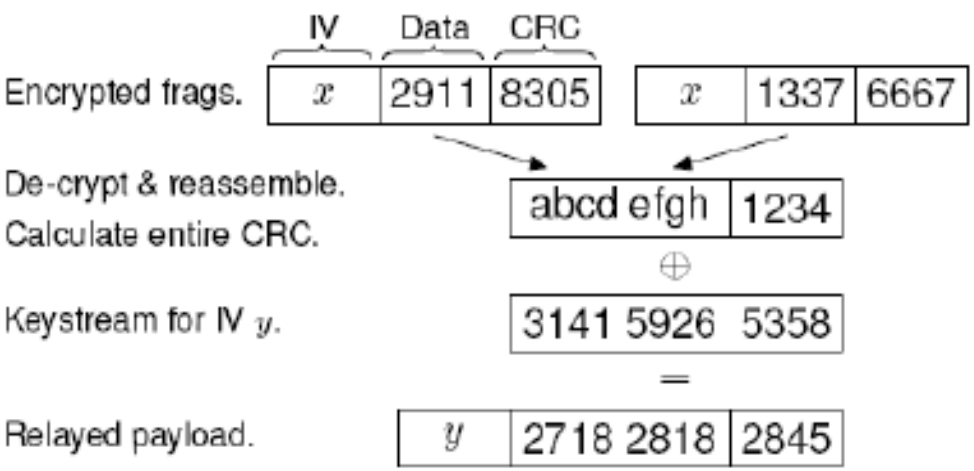
Pure Fragmentation Attack



Discovering Keystreams

- Ziel: IV Dictionary
- Prinzip: Senden von *Broadcast Frames* in kleinen Fragmenten

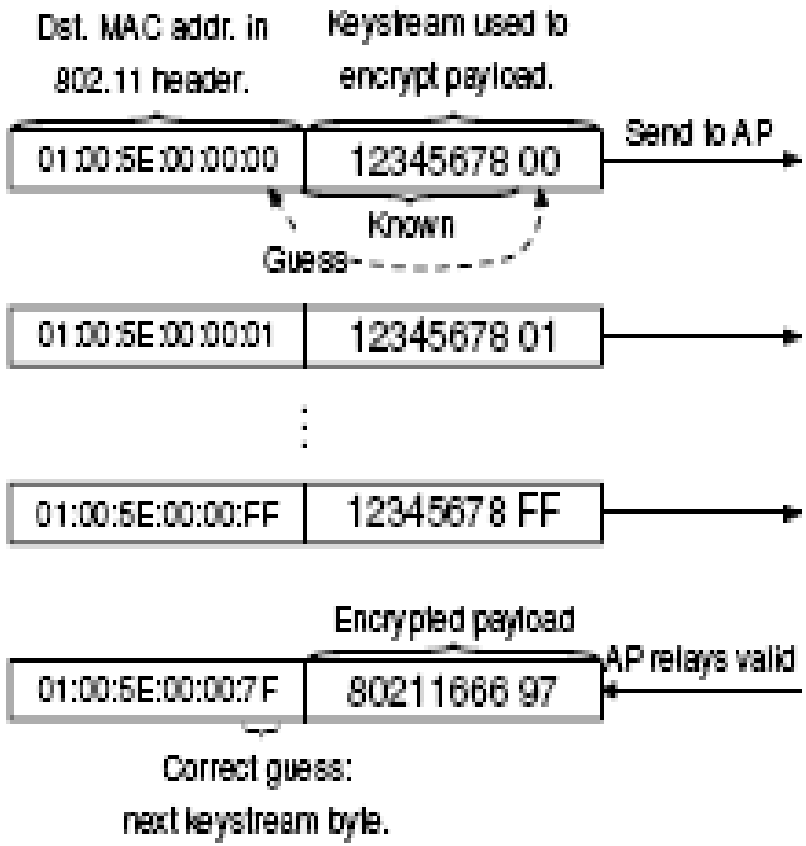
Discovering Keystreams



Discovering specific Keystreams

- Ziel: Entdecken eines speziellen Keystreams
- Prinzip: Senden von IP Multicasts

Discovering specific Keystreams



Zusammenfassung

- WEP ist unsicher!
- Keine der Anforderungen wird erfüllt (Vertraulichkeit, Authentifizierung, Datenintegrität)
- Besser: WPA, WPA2 (802.11i) oder VPN

Questions ??