WLAN-Sicherheit mit WPA(2)

Andreas Dittrich
dittrich@informatik.hu-berlin.de

Institut für Informatik
Humboldt-Universität zu Berlin

10. Januar 2006

Übersicht

Einleitung

- Sommer 2004 verabschiedet IEEE endlich denn Standard 802.11i
- Grundforderungen
  - Zugangsschutz per Authentifizierung
  - Vertraulichkeit durch Verschlüsselung
  - Integrität

Behandelte Verfahren

- WEP
- WPA/TKIP
- WPA2 a.k.a. 802.11i

Warum ich WEP noch behandle

- Grundlage von WPA
- WPA Antwort auf kritische Schwachstellen in WEP
- WPA2 ist noch nicht sehr weit verbreitet
  - ausser in ausgewählten Wohnungen (meiner)

Nur am Rande erwähnt wird

- 802.1x
- Enterprise Authentifizierungs-Systeme
  - EAP in allen Varianten
  - Radius-Server
- nicht relevant für den AP
  - out of scope
  - geringer Mehraufwand

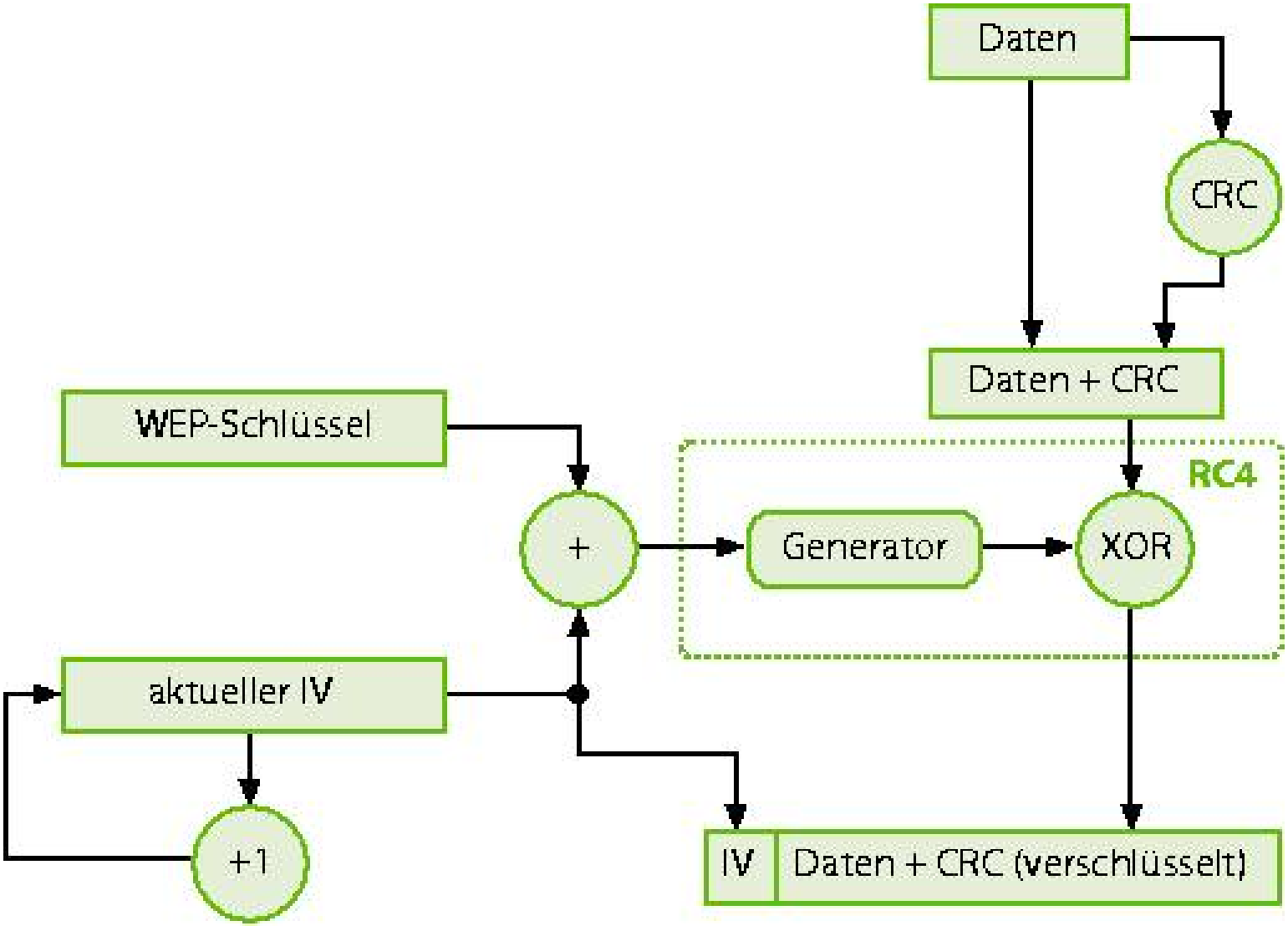
WEP - Übersicht

- 1999 zusammen mit 802.11 definiert
- „Wired Equivalent Privacy“
  - „Weak Encryption Protocol“
  - „What on Earth is Privacy?“
- es wurde wohl an Hubs gedacht ;-)

Authentifizierung

- Client sendet Request mit IV
- AP schickt Challenge zurück
- Client antwortet mit Response
- AP bestätigt
- ab jetzt verschlüsselte Kommunikation ...

Schema


Daten
CRC
Daten + CRC
WEP-Schlüssel
RC4
+
Generator
XOR
aktueller IV
+1
IV
Daten + CRC (verschlüsselt)

Schwachstellen

- kurzer IV (24 Bit)
- Schwache effektive Schlüssel
- jede Menge known-Plaintext Attacken
- normalerweise schwache Authentifizierung
- und und und ...

Bitte nicht mehr benutzen!!

- geeignete Tools knacken WEP-Schlüssel in wenigen Minuten
  - airodump
  - void11
  - aireplay
  - aircrack
  - kismet, kismac
  - insert favorite tool here

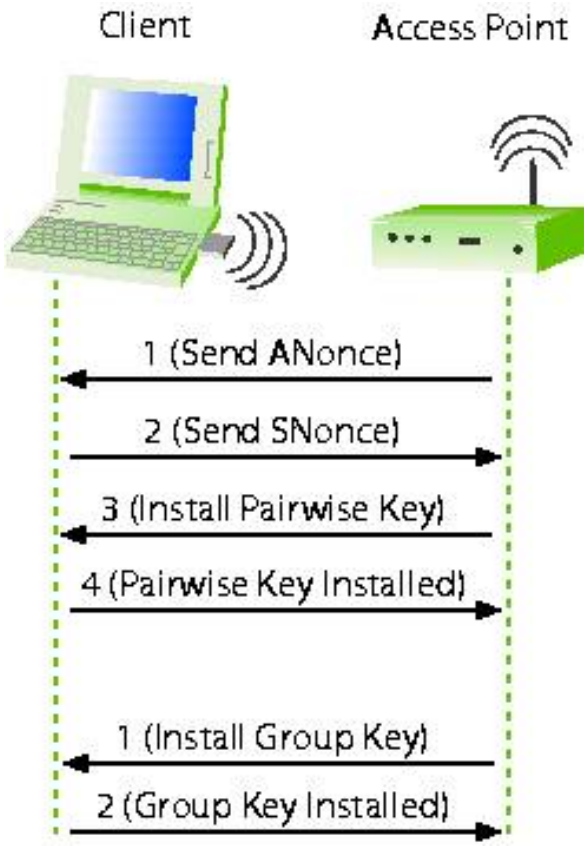
WPA - Übersicht

- WLAN-Boom machte WEP untragbar
- Standards brauchen lange
- Backport aus 802.11i durch Wi-Fi Alliance
- adressiert dringende Schwachstellen in WEP

Ansatzpunkte

- TKIP ergaenzt RC4-Verschlüsselung
- Michael ergänzt CRC
- sichere Authentifizierung
- PSK zusätzlich zu EAP/802.1x zur Ermittlung des Master Secret möglich
  - Sicherheit hängt am Geheimnis des PSK

Authentifizierung

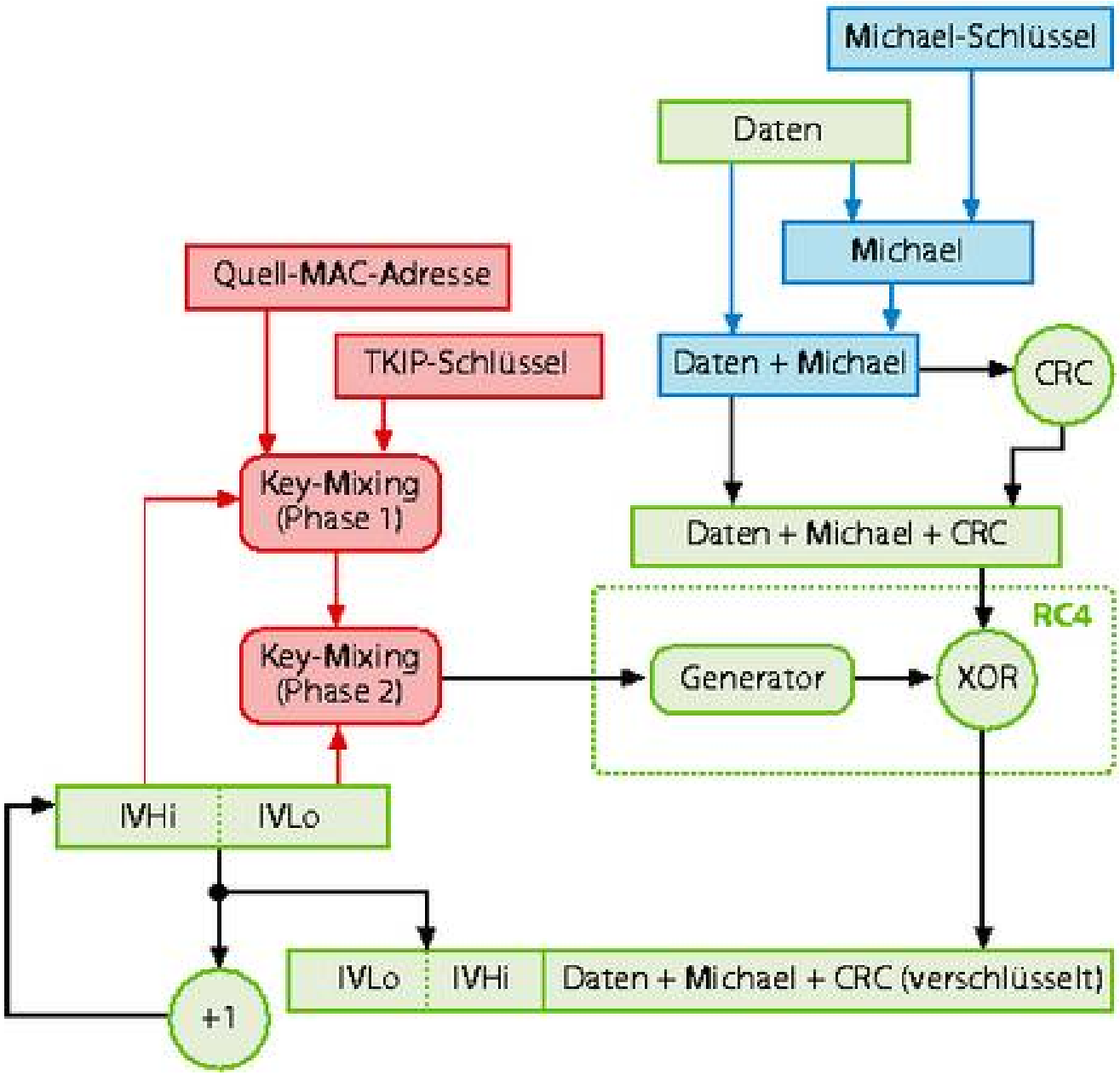


- re-keying genauso möglich

Authentifizierung II

- Aushandlung verschiedener Kryptoverfahren
  - WEP sah das nicht vor
- unterstützt Aushandlung verschiedener Parameter
  - Kryptoverfahren für Broad-/Multicasts
  - Kryptoverfahren für Pairwise Key
  - Authentifizierungsverfahren
- AP gibt diese Info zusammen mit seinen Beacons aus

Verschlüsselung - Schema



TKIP

- nur abgeleiteter temporärer Schlüssel wird für RC4 benutzt
- Zwei Key-Mixing Stufen
  - aus dem IV kann nicht mehr direkt der RC4-Key berechnet werden
  - Phase 1: rechenintensiv aber selten
  - Phase 2: für jedes Paket zu berechnen

Michael

- zusätzlich zum bisherigen CRC
- schneller Hash-Algorithmus
  - zwecks Optimierung leider mit kurzem Schlüssel
- arbeitet mit eigenem Schlüssel

Kompatibilität

- die meisten WEP-fähigen Geraete brauchten nur FW-Update
- jedes WPA-Gerät spricht auch WEP
- Probleme
  - Roaming dauert über 802.1x länger
  - schlecht für Echtzeitanwendungen

WPA2 - Übersicht

- wichtigste Änderung: AES-CCM statt TKIP/RC4/Michael
- Verbesserungen bei der (De-)Authentifizierung
- geschützter Ad-Hoc Modus
- dank geprüftem Entwicklungsprozess kein Disaster wie bei WEP zu erwarten

Standardisierung

- nennt sich markttauglich jetzt RSN (robust security network)
- zertifizierte Clients können trotzdem noch alte Methoden benutzen
  - AES Pflicht, TKIP/RC4/Michael optional
  - mit Einschränkungen
- WEP ausdrücklich NICHT erwünscht
- leider kostet die genaue Spezifikation zur Zertifizierung 25$

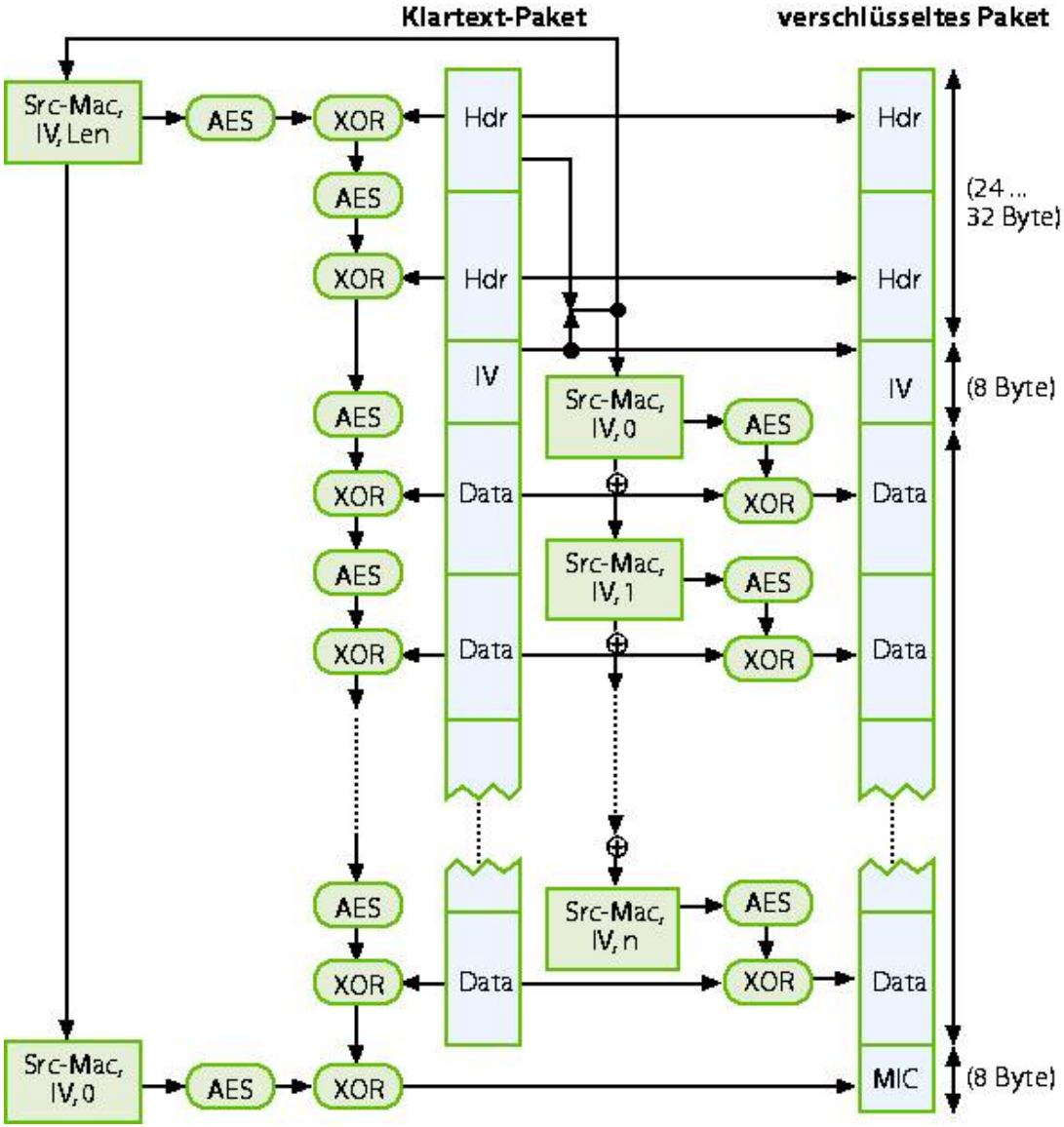
Authentifizierung

- wie schon bei WPA erklärt
  - fast ...
- Verbesserungen für 802.1x
  - PMK-Caching
  - Preauthentication

Verschlüsselung - AES-CCM

- CCM = Counter with CBC-MAC
  - CTR fuer Verschlüsselung
  - CBC fuer Prüfsumme
  - genaueres siehe RFC 3610
- nur noch ein 128 Bit Schlüssel nötig für Verschlüsselung und Prüfsumme
- IV bleibt 48 Bit lang
- wie AES funktioniert ist ja jedem klar ;-)

Verschlüsselung - Schema



Implementierungen

- Windows
  - WPA ab XP SP1 (plus Patch)
  - WPA2 ab XP SP2 (plus Patch)
  - für 98,2000 muss der Treiber die Funktionalität liefern
- Linux, FreeBSD, NetBSD
  - wpasupplicant
- OS X
  - Unterstützung für WPA und WPA2 ab 10.3
- OpenBSD noch nicht so weit :'-(

Demo?

```
State:  DISCONNECTED -> SCANNING
State:  SCANNING -> ASSOCIATING
State:  ASSOCIATING -> ASSOCIATED
State:  4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
State:  4WAY_HANDSHAKE -> GROUP_HANDSHAKE
State:  GROUP_HANDSHAKE -> COMPLETED
```


Literatur

http://www.wi-fi.org
http://www.wirelessdefence.org
http://www.cs.umd.edu/ waa/wireless.html
http://www.phptr.com/
http://standards.ieee.org/
Wikipedia
RFC 3610
Lars Richter, Untersuchung und Bewertung von Netzzugangssteuerungen auf Basis des Standards 802.1x
Claudia Eckert, IT-Sicherheit (Studienausgabe)
Heise Verlag:
c't 15/01 S.186ff
c't 04/02 S.178ff
c't 18/04 S.192ff
c't 21/04 S.214ff
c't 24/05 S.196ff
Alle Abbildungen aus c't 21/04 S.214ff