

Sicherheit in Funknetzen

WEP & WPA

Christian Viergutz

18. Dezember 2006

Kryptographische Verfahren WS 2006/07
AG Kombinatorische Algorithmen
Universität Osnabrück



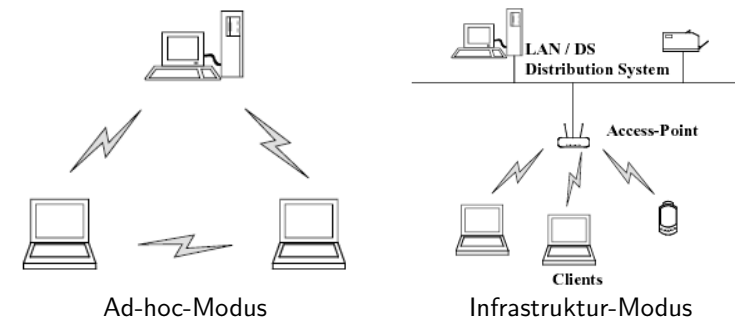
Vortragsübersicht

1. Einleitung
2. Das WEP-Protokoll
 - 2.1 Ansätze von WEP zum Erreichen der kryptographischen Ziele
 - 2.2 Sicherheitsprobleme im WEP-Protokoll
3. Weitere Sicherheitsaspekte in drahtlosen Netzwerken
4. WPA
5. WPA2 und IEEE 802.11i
6. Zusammenfassung

1. Einleitung

- Funknetze (WLANs) sind heute allgegenwärtig z.B. in Universitäten, Flughäfen, Messen, Hotel-Lobbys usw.
- Der de-facto Standard sind Funknetze nach dem IEEE-Standard 802.11, der 1997 definiert wurde. Die meisten verfügbaren Systeme arbeiten nach den Versionen 802.11b (11 Mbit/s) bzw. 802.11g (54 Mbit/s).
- WLANs bieten die Möglichkeit, mit geringem Aufwand drahtlose Netzwerke aufzubauen oder auch bestehende drahtgebundene Netze zu erweitern. Sie werden häufig eingesetzt, um drahtlosen Zugang zum Internet zu ermöglichen oder getrennte Gebäudeteile (z.B. von Firmen) zu koppeln.

- Es gibt 2 Modi, in denen WLANs betrieben werden können:
 - Ad-hoc-Modus (sog. Peer-to-Peer Kommunikation)
 - Infrastruktur-Modus (gebunden an zentrale Funkbrücke (Access Point, AP))



- **Grundlegendes Problem** beim Einsatz von WLANs:

Verkehr (versandte Pakete) im Netzwerk ist für jeden Benutzer mit einem (mobilen) Netzwerk-Empfänger einfach abzufangen und mitzulesen.

⇒ **Sicherheitsmechanismen sind unerlässlich.**

- Die Sicherheitsrisiken beim Einsatz von WLANs im privaten Gebrauch sind oft **unbekannt** oder werden **falsch eingeschätzt**.

⇒ Manche Benutzer setzen z.B. aus Gründen der **Bequemlichkeit** keine Datenverschlüsselung ein.



Abbildung 1: Unverschlüsselte Zugriffspunkte bei einer Rundfahrt durch Berlin

Quelle: c't 13/2004, S.96

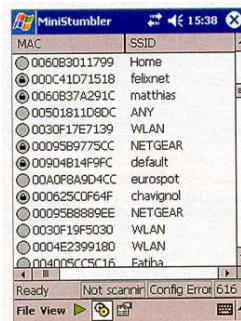


Abbildung 2: MiniStumbler

Mit Programmen wie z.B. „MiniStumbler“ (für PDA) können unverschlüsselte drahtlose Netze „im Vorbeigehen“ entdeckt werden. Einträge in der Abbildung ohne Schloss signalisieren offene Netze. Quelle: c't 13/2004, S.93 – <http://www.stumbler.net>

2. Das WEP-Protokoll

- Das Wired Equivalent Privacy-Protokoll (WEP-Protokoll) wurde innerhalb des IEEE Standards 802.11 mit dem Ziel entwickelt, drei wichtige Sicherheitsanforderungen zu erfüllen:
 - **Vertraulichkeit** (privacy): Unbefugte sollen die übermittelten Daten nicht mitlesen können.
 - **Integrität** (integrity): Versendete Pakete sollen nicht unbemerkt verändert werden können.
 - **Zugriffskontrolle** (access control): Die drahtlose Infrastruktur soll vor unberechtigtem Zugriff geschützt werden.

Daten zu WEP

- WEP basiert auf der Stromchiffre **RC4**. Es ist ein Protokoll auf der Verbindungs- bzw. Sicherungsebene (Schicht 2) des ISO/OSI-Referenzmodells.
- Der Initialisierungsvektor (**IV**) hat eine Länge von 24 Bit und wird stets **unverschlüsselt** übertragen. Die Schlüssellänge selbst beträgt im Standard 40 Bits. Von vielen Herstellern wurde eine Erweiterung mit 104 Bit implementiert.
- Der Initialisierungsvektor sollte für jedes Paket vom Absender **neu gewählt** werden.
- Der Schlüssel muss jedem Kommunikationspartner im Voraus bekannt sein (**symmetrisches Verfahren**). Dieser wird für das gesamte Netzwerk verwendet.

2.1 Ansätze von WEP zum Erreichen der kryptographischen Ziele

- **Vertraulichkeit**: Der RC4-Algorithmus bekommt als Eingabe den (für jedes Paket verschiedenen) IV v und den Schlüssel k . Daraus wird dann der Pseudozufalls-Strom generiert, der mit dem Klartext per XOR verknüpft wird.
- **Integrität**: Für jedes Paket M wird eine CRC-32 Prüfsumme (Cyclic Redundancy Check) berechnet, die an M angehängt wird (und danach als P mitverschlüsselt wird). Diese kann nach Entschlüsselung auch der Empfänger berechnen und vergleichen.

Symbolischer Ablauf des Verfahrens bei Versand von A nach B :

$$A \rightarrow B : \langle v, P \oplus RC4(v, k) \rangle \quad \text{wobei} \quad P = \langle M, CRC(M) \rangle$$

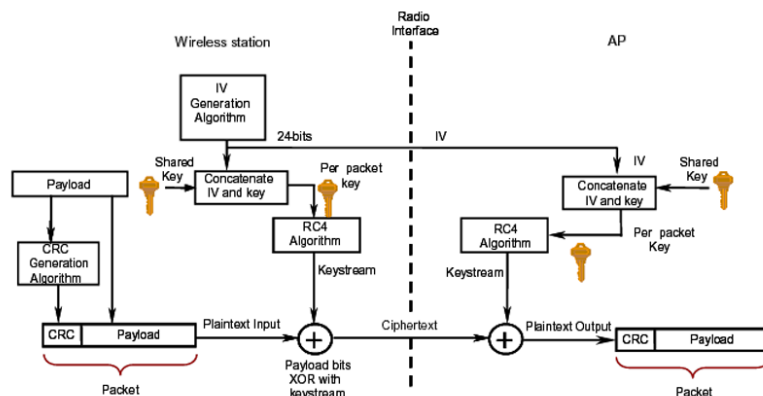


Abbildung 3: Das WEP-Protokoll schematisch

Quelle: Karygiannis, Owens: Wireless Network Security (NIST Special Publication 800-48), November 2002

- **Authentisierung**: 2 Authentisierungs-Modi:

1.) „Open“: keine Authentisierung

2.) „Shared Key“:

- * Protokoll mit Herausforderung und Antwort (engl. challenge-response).
- * Der AP erzeugt 128 Bytes zufällig und sendet sie unverschlüsselt an den Kommunikationspartner (**Herausforderung**).
- * Der Partner verschlüsselt dieses Paket und sendet das Ergebnis an den AP zurück (**Antwort**).
- * Wenn der AP die Antwort korrekt entschlüsseln kann, dann hat sich der Partner erfolgreich authentisiert (**einseitige Authentisierung**).

Zur Authentisierung wird **derselbe Schlüssel** wie zur Verschlüsselung verwendet.

Wireless - Interface	
SSID:	My Network
Channel:	11
Data Rate(Mbps):	Auto
54g Mode:	Auto <input checked="" type="checkbox"/> 54g Protection
Authentication Method:	Open System or Shared Key
Encryption:	WEP-64bits
Passphrase:	*****
WEP Key 1 (10 or 26 hex digits):	F8B0B000C9
WEP Key 2 (10 or 26 hex digits):	AEF33E3B16
WEP Key 3 (10 or 26 hex digits):	C2F8D62C0C
WEP Key 4 (10 or 26 hex digits):	B31A3E79C5
Default Key:	Key1

Abbildung 4: Konfiguration eines APs (Ausschnitt)

2.2 Sicherheitsprobleme im WEP-Protokoll

- Der ursprüngliche Entwurf von WEP erlaubte nur 40 Bit-Schlüssel. Mit aktuellen Computern ist ein Angriff durch erschöpfende Suche (*brute force*) in (relativ) kurzer Zeit möglich. (Erweiterung auf 104 Bit macht solche Angriffe heutzutage unpraktikabel).
- Statische Schlüssel Mangels eines durchdachten Schlüsselmanagements wird der WEP-Schlüssel k i.d.R. selten geändert. Er kann daher für längere Zeit als konstant angesehen werden.
- Die Länge des IVs ist mit 24 Bit viel zu kurz. Dadurch wiederholen sich die erzeugten IVs schon nach kurzer Zeit.

Annahme: Der Angreifer fängt zwei Pakete auf, die mit demselben IV v und Schlüssel k verschlüsselt worden sind. Es gilt dann:

$$\begin{aligned} C_1 &= P_1 \oplus RC4(v, k) \\ \wedge C_2 &= P_2 \oplus RC4(v, k) \\ \Rightarrow C_1 \oplus C_2 &= P_1 \oplus P_2 \end{aligned}$$

Falls einer der Klartexte bekannt ist, kann der andere sofort ermittelt werden.

Wie häufig treffen wir auf Pakete mit gleichem IV, wenn dieser zufällig gewählt wird?

- Es gibt $m := 2^{24} = 16.777.216$ viele verschiedene IVs.
- Die W'keit, dass unter r abgefangenen IVs mind. zwei gleiche auftreten, ist

$$Pr(\text{Mind. 1 Kollision bei } r \text{ Paketen}) = 1 - \frac{m \cdot (m-1) \cdot \dots \cdot (m-r+1)}{m^r}$$

- Der letzte Ausdruck kann (mit Einsetzen) umgeformt werden zu

$$Pr(\text{Mind. 1 Kollision bei } r \text{ Paketen}) = 1 - \prod_{i=0}^{r-1} \left(1 - \frac{i}{2^{24}}\right)$$

- Es lässt sich zeigen: $Pr(\text{Mind. 1 Kollision bei } r \text{ Paketen}) \geq 0,5$ ab dem Wert

$$r \geq 4823 \approx 1,18 \cdot \sqrt{2^{24}}$$

- Wegen $4823 \ll 2^{24}$ und der Anwendung auf Geburtstags-Probleme nennt man diese Tatsache **Geburtstags-Paradoxon**.

Anmerkung: Der IEEE 802.11-Standard schreibt noch nicht einmal vor, dass der IV für jedes Paket geändert wird!

- **Datenpakete können leicht gefälscht werden.**

- Gelangt ein Angreifer in Besitz eines Bitstroms (aus RC4), dann kann er bis zum nächsten Schlüsselwechsel beliebige verschlüsselte Pakete erzeugen und in das Netz einschleusen.

- Pakete besitzen dann alle denselben IV.

- ⇒ Kein Problem, da der Sender allein den IV wählen darf.

- **Einfache Methode, um an einen Bitstrom zu gelangen:** Gültige Authentisierung mitschneiden: Es wird eine Herausforderung M vom AP (unverschlüsselt) gesendet und die mobile Station antwortet mit $R = M \oplus RC4(v, k)$.

$$\Rightarrow RC4(v, k) = M \oplus R$$

- **Die Integritätssicherung ist wirkungslos.** Die in WEP benutzte Prüfsumme CRC-32 ist eine lineare Funktion der Nachricht, d.h.

$$\forall x, y : CRC(x \oplus y) = CRC(x) \oplus CRC(y)$$

Angenommen, A schickt ein verschlüsseltes Paket an B, das der Angreifer zwischendurch abfängt und ändern möchte. Das Paket enthält

$$C = RC4(v, k) \oplus \langle M, CRC(M) \rangle$$

Dann können wir einen neuen, gültigen Chiffretext C' erzeugen, der (unbemerkt vom Empfänger) zu M' entschlüsselt wird, wobei $M' = M \oplus \Delta$. Es ist nämlich

$$C' = C \oplus \langle \Delta, CRC(\Delta) \rangle = E(M', (v, k))$$

Beweis: siehe Tafel

- **Das Authentisierungsprotokoll kann gebrochen werden.**

- Ein Angreifer könnte wiederum eine gültige Authentisierung mithören und daraus den Bitstrom $RC4(v, k)$ rekonstruieren.

- Solange sich der Schlüssel k nicht ändert, kann der Angreifer zukünftig Herausforderungen (Challenges) vom AP verschlüsseln und sich somit authentisieren.

- ⇒ Der Angreifer braucht den Schlüssel nicht zu kennen, um verschlüsselte Pakete (einer gewissen Länge) zu erzeugen.

Meist wird derselbe Schlüssel von allen Mobilstationen verwendet, was zur Vereinfachung des Angriffs beiträgt.

- **Angriff auf RC4:** Veröffentlicht von Fluhrer, Mantin und Shamir (2001)

- ⇒ Es gibt frei verfügbare Programme (z.B. „WEPCrack“ und „AirSnort“), die diesen Angriff ausführen können.

3. Weitere Sicherheitsaspekte im drahtlosen Netz

- **Problematische Grundeinstellung der Komponenten:**

- ⇒ Auslieferungszustand: Konfiguration von Komponenten für reibungslosen Betrieb, zumeist auf Kosten der Sicherheit.

- **SSID Broadcast (Rundsendung des Netzwerk-Namens):**

- ⇒ Wiederholte Rundsendung des Netznamens (Service Set Identifier, SSID) kann oft unterbunden werden (nicht standardkonform).

- ⇒ SSID kann in vielen Fällen trotzdem aus Steuersignalen und mitgehörtem Netzwerkverkehr ermittelt werden.

- ⇒ Empfehlung: Rundsendung nicht ausschalten, aber SSID sollte keinen Zusammenhang zum Funknetzbetreiber haben.

- **Manipulierbare MAC-Adressen (Media Access Control):**

- ⇒ MAC-Adressfilter (White-/Blacklists) können mit einfachen Mitteln umgangen werden (MS Windows: Schlüssel in Registry).
- ⇒ Aus gültigen Paketen können gültige MAC-Adressen ermittelt und die eigene Adresse dementsprechend angepasst werden.

- **Fehlendes Schlüsselmanagement:**

Schlüssel muss von Hand in alle Komponenten eingetragen werden.

- ⇒ Beträchtliche logistische Aufgabe in mittleren bis großen Netzwerken.
- ⇒ Schlüssel wird effektiv nur sehr selten oder gar nicht geändert.
- ⇒ Wird der Schlüssel bekannt, ist die Sicherheit des ganzen Netzes kompromittiert.

4. WPA und der IEEE 802.11i-Standard

- WPA (Wi-Fi Protected Access) gedacht als Antwort der WLAN-Industrie auf die Schwächen von WEP.
- Die Methode sollte eine **Zwischenlösung** darstellen, um mehr Zeit für die Entwicklung des IEEE 802.11i-Standards zu schaffen

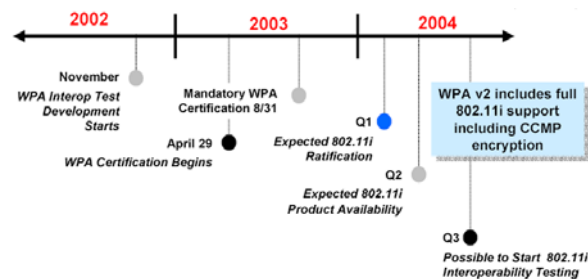


- Es gibt zwei Modi:

Enterprise-Modus: Benutzt Authentisierung und Schlüsselmanagement mittels RADIUS-Servern (vorwiegend in größeren Netzwerken).

PSK-Modus: Ein an alle Anwender verteilter geheimer Passwort-Satz dient zur Authentisierung (eher für Privatanwender gedacht).

- WPA erfordert ein Software/Firmware-Update auf beteiligten Komponenten, ist aber auf vorhandener Hardware lauffähig (Nutzerakzeptanz!)
- Die Methoden in WPA sind eine vorgezogene Teilmenge des Entwurfs für 802.11i. WPA ist zu 802.11i aufwärtskompatibel (Juni 2004 ratifiziert).



Quelle: Michael Disabato, Vortrag: „WPA: Locking Down the Link“, Burton Group

Wie geht WPA die Schwächen von WEP an?

WPA bildet eine Hülle (Wrapper) um das RC4-Verfahren:

1. Der **IV** wird auf **48 Bit** verlängert. Dazu festgelegte Regeln, wie neue IVs ausgewählt werden.
2. Ein **Nachrichten-Integritätscode (MIC)**, genannt „Michael“, wird statt des CRC-Verfahrens eingeführt (krypt. Einweg-Hashfunktion, MAC).
3. Es wird ein Verfahren zur **Schlüssel-Erzeugung** (Ableitung) und zur automatischen **Verteilung** im Netz verwendet.
4. Das **TKIP (Temporal Key Integrity Protocol)** generiert aus dem **Master Key** neue Schlüssel für jedes Paket.

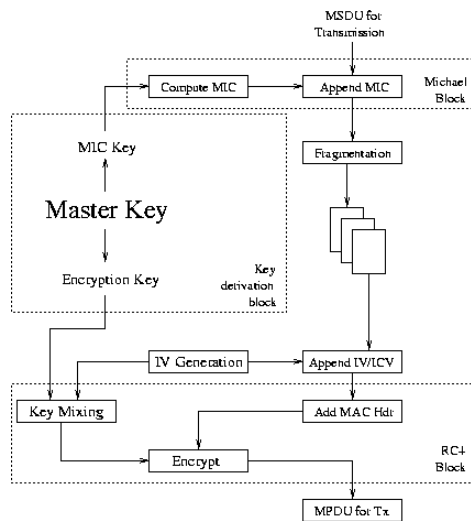


Abbildung 5: Vorgehen von TKIP bei der Verschlüsselung

5. WPA2 - IEEE 802.11i

- WPA2 zertifizierte Produkte halten IEEE 802.11i Standard ein und sind auf Interoperabilität überprüft.
- WPA2 ist abwärtskompatibel zu WPA.
- WPA2 ersetzt TKIP (mit RC4) durch AES (Erfüllung formaler Anforderungen einiger Behörden und Organisationen).
- AES benötigt neue Hardware für APs, da rechenintensiver als TKIP.
- **CCMP**: Einsatz von AES im Rahmen des „Counter (CTR) Mode mit CBC-MAC Protokolls“

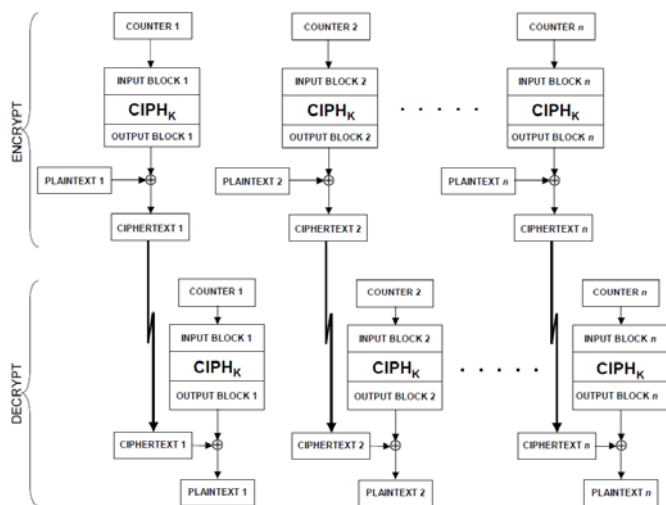
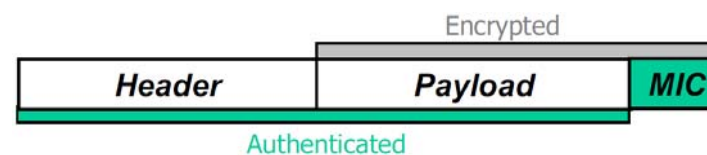


Abbildung 6: Counter-Modus für Blockchiffren

Quelle: M. Dworkin, Recommendation for Block Cipher Modes of Operation (NIST SP 800-38a), 2001

Übersicht zu CCMP



Das CCMP-Verfahren ist Paket-basiert:

- Benutze CBC-MAC-Verfahren, um den MIC zu Header und Payload (Daten) zu berechnen
- Benutze Counter-Modus zur Verschlüsselung des Payloads (Zähler=1, 2, 3, ...) und des MICs (Zähler=0)
- Verfahren wurde speziell für IEEE 802.11i entworfen

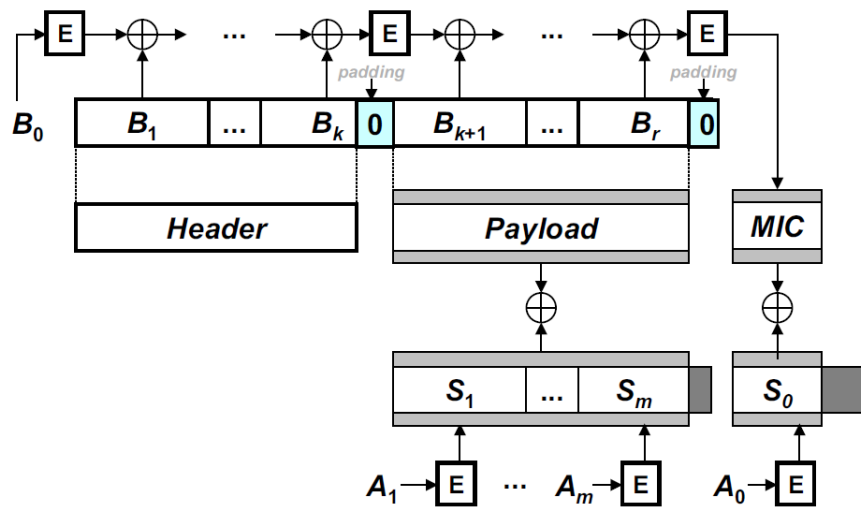


Abbildung 7: Ablauf von Verschlüsselung und MIC bei CCMP

Quelle: N. Cam-Winget, T. Moore, D. Stanley, J. Walker: IEEE 802.11i Overview, 2002

CCM Eigenschaften

- Das CCM Protokoll bietet **Authentizität** und **Vertraulichkeit**.
 - An den Paketklartext wird ein MIC (durch AES im CBC-Modus ermittelt) angehängt.
 - Aus Klartext und MAC wird der Chiffretext durch Anwendung von AES im CTR-Modus bestimmt.
- CCM ist **paketerorientiert**, Ströme (Streams) sind nicht vorgesehen.
- CCM bietet im Gegensatz zu einigen anderen Verfahren **beweisbare Sicherheit**.
- Bisher keine Angriffe bekannt.

Übersicht der Verfahren

	WEP	WPA	802.11i
Chiffre	RC4	RC4/TKIP	CCMP/AES
Schlüssellänge	40 Bits	128 Bit Verschl. 64 Bit Authentisierung	128 Bits
IV-Länge	24 Bits	48 Bits	48 Bits
Paketschlüssel	konkateniert	Mischfunktion	nicht nötig
Integrität	CRC-32	Michael	CCM
Header-Integrität	Keine	Michael	CCM
Wiederholungs-Angriff	Kein Schutz	IV Sequenz	IV Sequenz
Schlüsselmanagement	Kein	EAP-basiert	EAP-basiert

CCM ⇒ Counter mode encryption with Cipher block chaining MAC

EAP ⇒ Extensible Authentication Protocol

6. Zusammenfassung

- **WEP**
 - ist ungeeignet, um Datensicherheit zu gewährleisten. Es kann mit einfachen Mitteln gebrochen werden.
 - sollte auch in SoHo-Umgebungen nicht mehr eingesetzt werden
- **WPA**
 - beseitigt alle von WEP bekannten Schwächen.
 - ist als Interimslösung bis zum Erscheinen von 802.11i-kompatiblen Komponenten zu empfehlen (bis heute noch ungebrochen!)
- **WPA2/IEEE 802.11i mit CCMP (AES)** bringt eine erweiterbare Sicherheitsarchitektur, die WPA überlegen ist. Der Wechsel zu WPA2 wird einige Zeit dauern, da neue Hardware erforderlich.