http://ks.fernuni-hagen.de/

Sicherheitsaspekte in IEEE 802.11

Thorsten Kisner

Gliederung

- Einleitung: IEEE 802.11
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Robust Security Network (RSN)
- Zusammenfassung

Übersicht IEEE 802.11

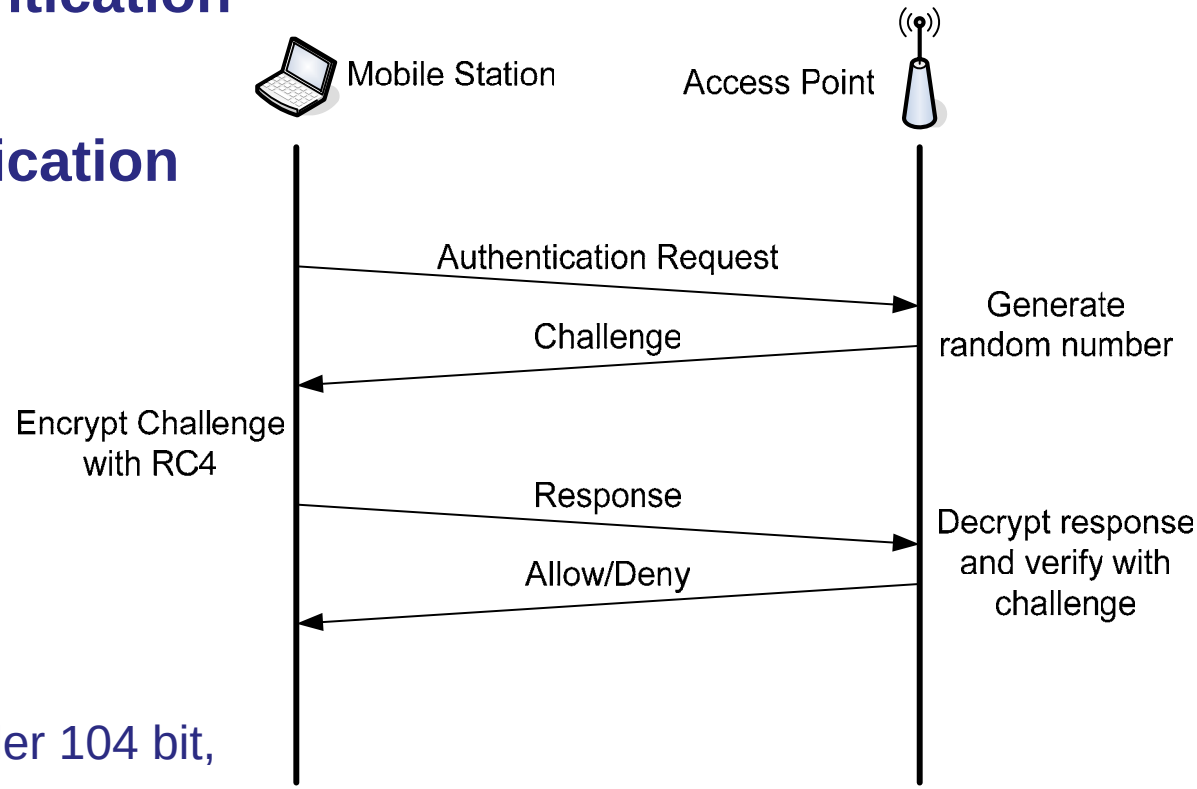
- **1997** Spezifikation physikalische Schicht und Mediumzugriff (2MBit/s im 2,4 GHz ISM-Band)
- **1999** Alternativen in der physikalischen Schicht
  802.11a: 5 GHz mit bis zu 54 MBit/s
  802.11b: 2,4 GHz mit bis zu 11 MBit/s
  Berücksichtigung von Sicherheitsaspekten (WEP)
- **2003** 802.11g: 2,4 GHz mit bis zu 54 MBit/s
- **2004** 802.11i: Erweitertes Sicherheitsprotokoll (Teile bereits vorher als WPA vorweggenommen)
- **2006** 802.11n: MIMO-Technologie mit bis zu 600 MBit/s

Gliederung

- Einleitung: IEEE 802.11
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Robust Security Network (RSN)
- Zusammenfassung

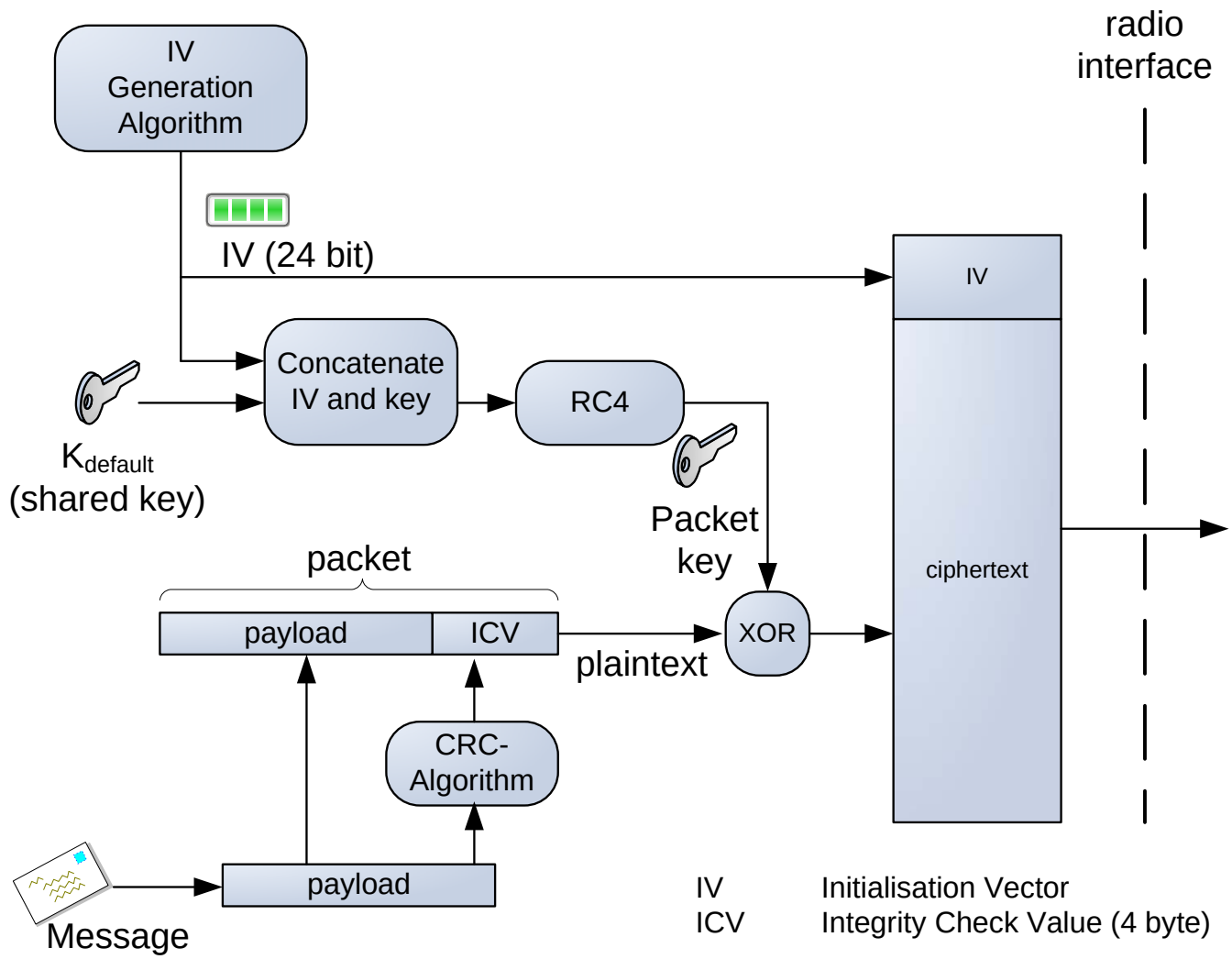
Authentifizierung in WEP

- **Open System Authentication**
- **Shared Key Authentication**



- **Schlüssel**
  - haben die Länge 40 oder 104 bit,
  - sind statisch, gemeinsam verwendet und symmetrisch.

Verschlüsselung in WEP



Passive Angriffe auf WEP

- **Wörterbuchangriffe**
  - Viele Access-Points (und Betriebssteme) stellen Methoden zur Verfügung aus einem Kennwort einen WEP-Schlüssel zu generieren (z.B. MD5)
  - Ein generierter Schlüssel wird mit dem bekannten IV bei einem bekannten Paket ausprobiert
- **Schwache Initialisierungsvektoren (FMS-Angriff)**
  - Schwache IV führen zu einer hohen Korrelation zwischen der Ausgabe und dem verwendeten Schlüssel
  - ca. 10 Mio. verschlüsselte Pakete notwendig
  - Schwache IV werden von neuerer Hardware gemieden
- **KoreK-Angriff**
  - Schwache IV nicht mehr notwendig
  - Statistische Kryptoanalyse
  - ca. 200.000 bis 600.000 verschlüsselte Pakete notwendig

Aktive Angriffe auf WEP

- **Wiederholungsangriffe**
  - Zur Generierung von Datenverkehr.
  - Z.B. Finden von ARP-Requests (Broadcast FF:FF:FF:FF:FF:FF).
  - Pakte mit immer dem gleichen IV sind in WEP erlaubt.
- **Entschlüsselung einzelner Pakete**
  - Bekannt unter „chopchop“ (ebenfalls von „KoreK“).
  - Das jeweils letzte Byte *n* wird sukzessive abgeschnitten.
  - Angenommen wird das letzte Byte *n* im Klartext [0-255].
  - ICV wird berechnet. Überpfüfung ob der Access Point das Paket verwirft.
- **Paket Injection**
  - Mit einem bekannten RC4-Schlüsselstrom und dem jeweiligen IV kann jedes Paket eingespielt werden ohne den aktuellen WEP-Schlüssel zu kennen.

Gliederung

- Einleitung: IEEE 802.11
- Wired Equivalent Privacy (WEP)
- **Wi-Fi Protected Access (WPA)**
- Robust Security Network (RSN)
- Zusammenfassung

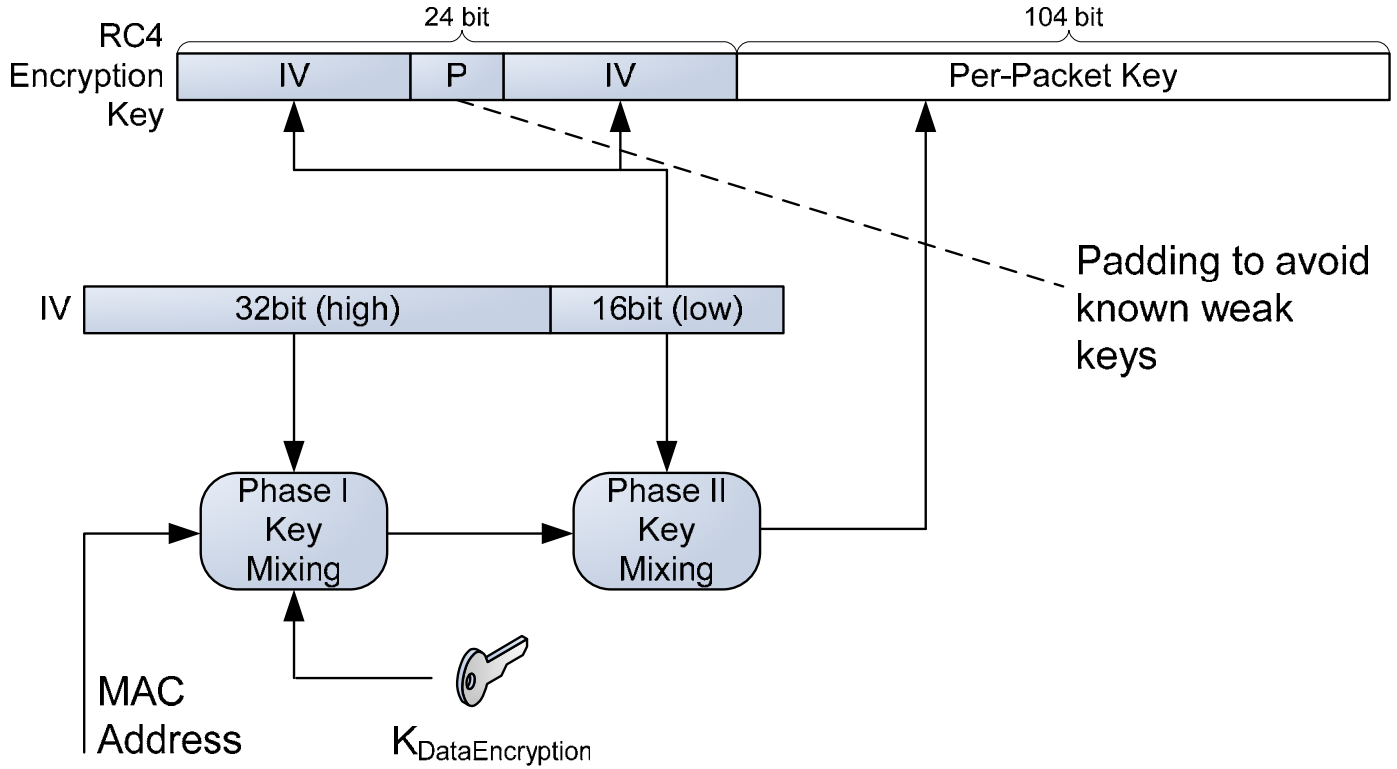
Verbesserungen in WPA

- **WiFi Protected Access**
  - Übergangslösung / Quasistandard der WiFi Alliance
  - Nebenbedingung: Die Erweiterungen müssen auf „alter“ Hardware (durch Firmware Upgrade) lauffähig sein!

Schwächen in WEP	Verbesserungen in TKIP
IV zu kurz, mehrfache Verwendung gleicher Werte	IV von 24 auf 48bit vergrößert
IV nicht auf einzelne Stationen bezogen, mehrere Stationen können gleichen IV verwenden	IV fungiert als Sequenznummernzähler
„Schwache IV“ (FMS-Angriff)	Schwache IV werden vermieden
Prüfsumme nur durch CRC32	Prüfsumme durch MIC bestimmt.

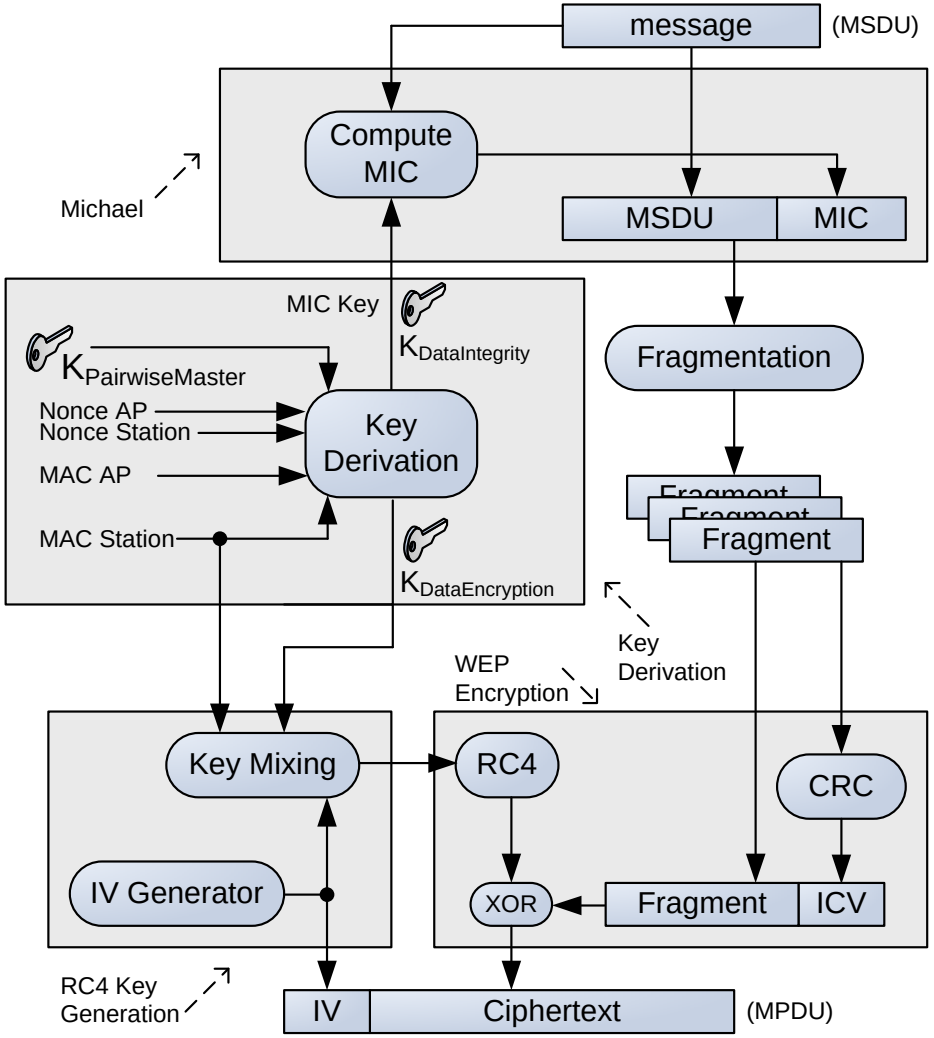
Initialisierungsvektor in TKIP

- Temporal Key Integrity Protocol
- Verlängerung des IV von 24 bit auf 48 bit



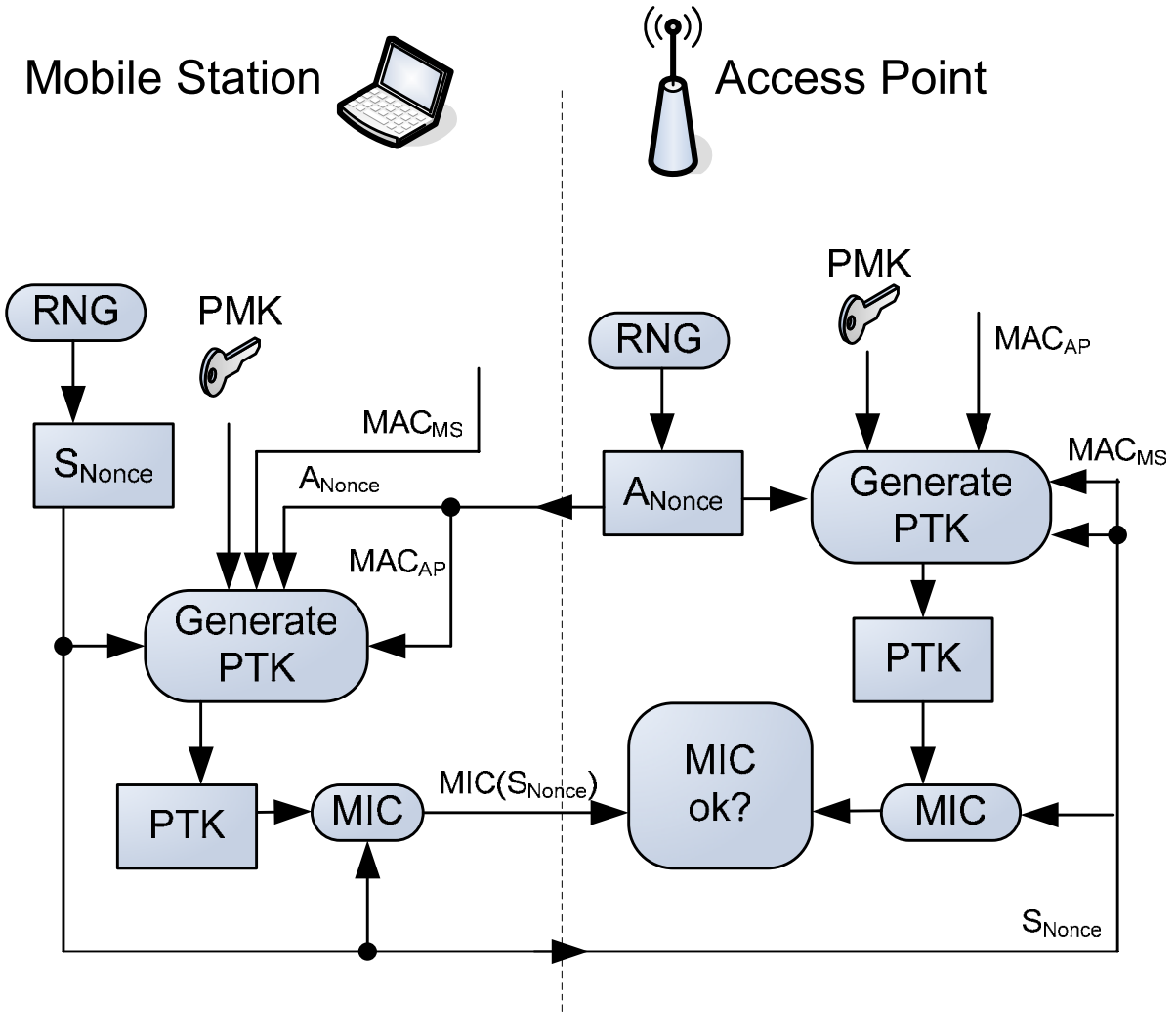
Verschlüsselung in WPA

- **Michael**
  - SHA-1 oder RIPEMD-160 nicht lauffähig
  - Nur Shift/Add Operationen
  - Gegenmaßnahmen!
- **Schlüsselerzeugung**
  - PMK während Auth.-Phase
  - Verschlüsselung, Integrität
  - Authentifizierung
  - Re-Keying alle 2^{16} Pakete
- **RC4 Schlüsselerzeugung**
  - Key Mixing I + II
- **WEP Verschlüsselung**
  - Identisch zu WEP



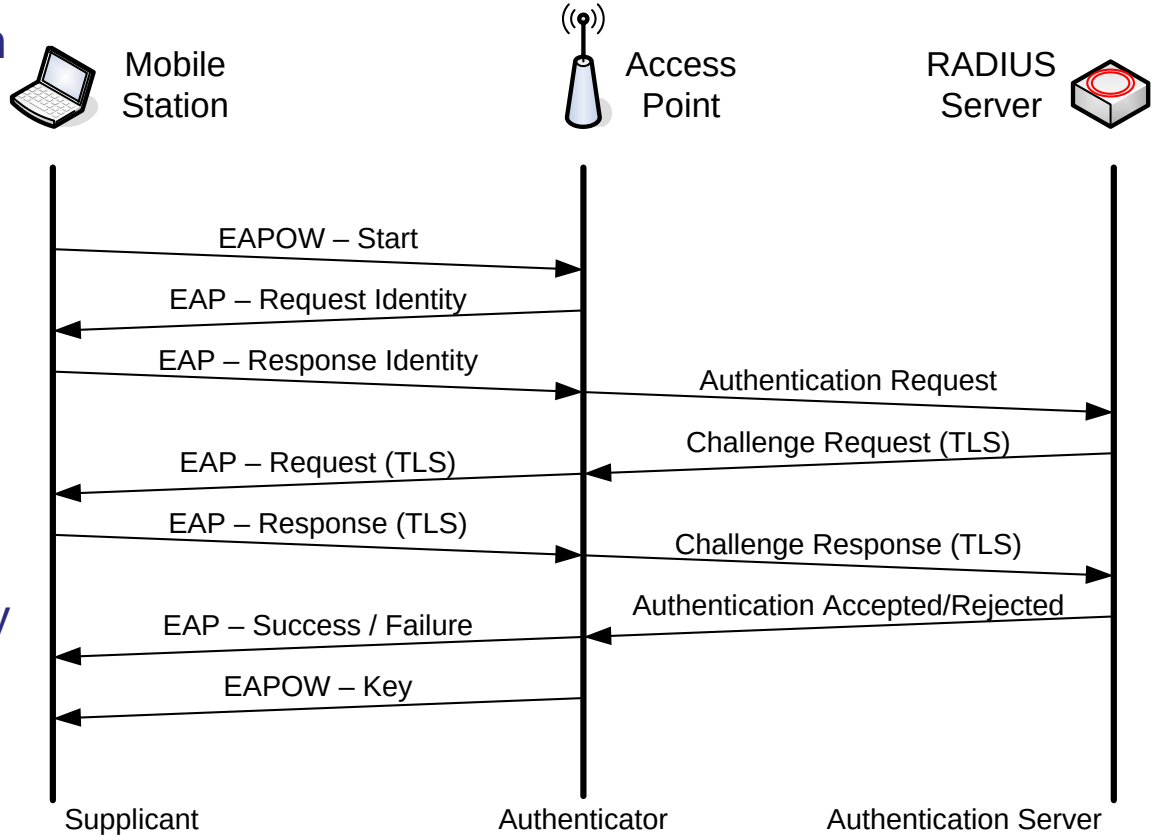
Authentifizierung mit Pre-Shared Keys

- Einsatz im SOHO-Bereich
- 4-Wege Handshake (2 sind dargestellt)
- Pre-Shared Key identisch mit dem Pairwise Master Key (PMK)
- Ziel: Erzeugung des Pairwise Transient Keys (PTK)



Authentifizierung über IEEE 802.1x

- **Basiert auf EAP (Extensible Authentication Protocol)**
- **Authentifizierungs-server**
  - RADIUS
- **Verschiedene Möglichkeiten**
  - Message-Digest 5
  - Transport Layer Security
  - Protected EAP
  - Lightweigt EAP



Gliederung

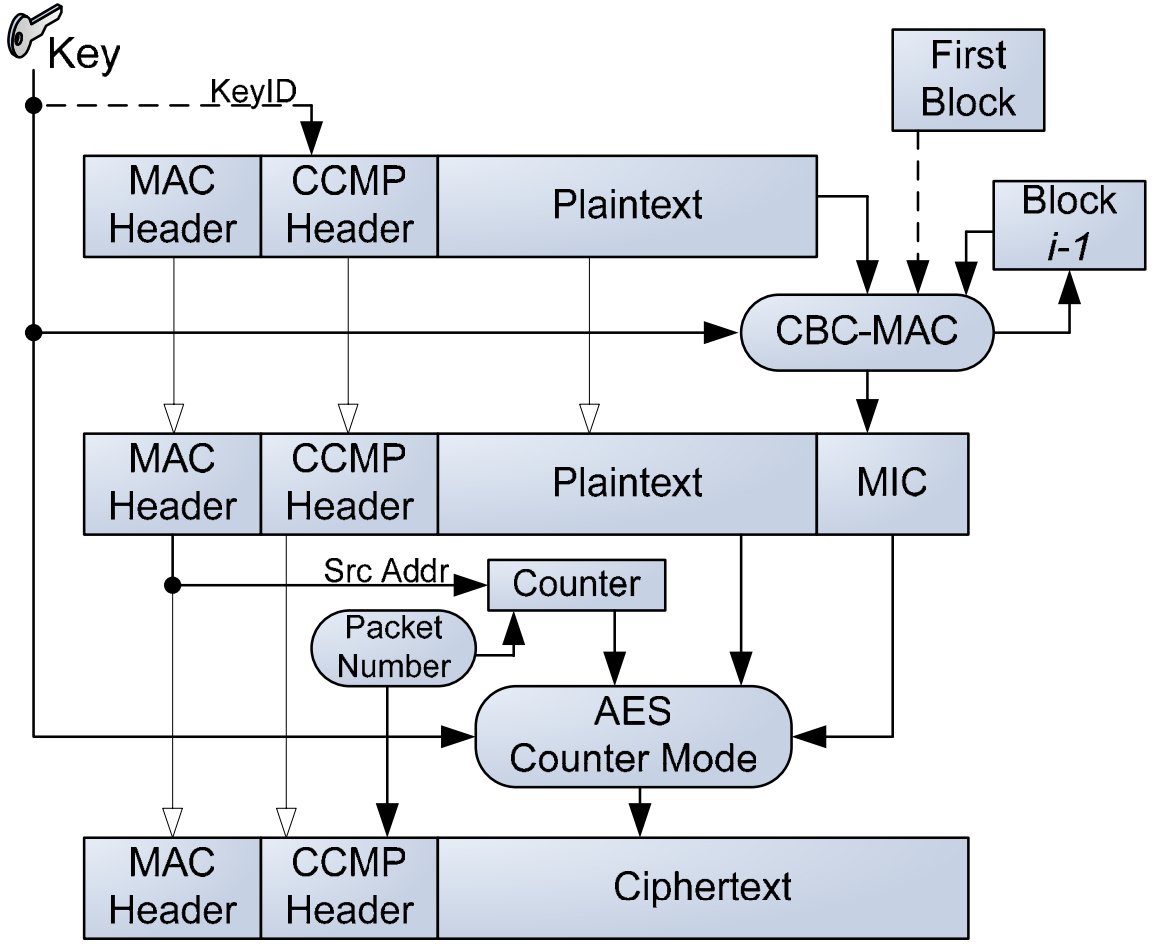
- Einleitung: IEEE 802.11
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- **Robust Security Network (RSN, 802.11i)**
- Zusammenfassung

Robust Security Network

- **IEEE 802.11i**
- **Von der Wi-Fi Alliance als WPA2 vermarktet und im März 2006 für alle Wi-Fi zertifizierten Produkte vorgeschrieben**
- **Neben TKIP kann auch AES (Advanced Encryption Standard) verwendet werden**
- **Betriebsmodus für AES notwendig:**
  - Betriebsmodus OCM von der IEEE 802.11i Arbeitsgruppe verworfen
  - Neuentwicklung: CCMP
    Counter Mode with CBC Message Authentication Code Protocol

Verwendung von CCMP

- **CCMP-Header**
  - 48bit Packet Number
  - KeyID für Multicast oder in Mischumgebungen
- **Counter**
  - Source Address
  - Packet Number
  - Interner Counter



Angriffe auf WPA/RSN

- **Angriffspunkt: Pre-Shard Keys (PSKs)**
  - Durch KDF2 (Key Derivation Function 2 aus PKCS#5) wird aus einem Kennwort und dem Service Set Identifier (SSID) in 4096 Iterationen der PSK (256 bit) gebildet.
- **Interne Angriffe**
  - Mitschneiden des 4-Way-Handshake
  - Berechnung der Pairwise Transient Keys (PTKs)
  - Abhören und Entschlüsseln des Datenverkehrs
- **Externe Angriffe**
  - Mitschneiden des 4-Way-Handshake
  - Wörterbuchangriff auf MIC

Gliederung

- Einleitung: IEEE 802.11
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Robust Security Network (RSN)
- **Zusammenfassung**

Zusammenfassung

	WEP	WPA	WPA2
Verschlüsselung	RC4	RC4	AES/CM
Schlüssellänge	40/104 bit	128 bit	128 bit
Integrität	CRC-32	Michael	CBC-MAC
Authentifizierung	Shared Key	802.1x	802.1x
Schlüsselverwaltung	-	802.1x	802.1x
IV Länge	24 bit	48 bit	48 bit
Replay Attack	-	TSC	PN

Ende

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?