IT-Sicherheit

- Sicherheit vernetzter Systeme -

Kapitel 10: Netzsicherheit - WLAN-Sicherheit (Schicht 2)

Inhalt

- WLAN: Eine kurze Einführung
- WLAN-Sicherheitsanforderungen und Mechanismen
- Wired Equivalent Privacy (WEP)
  - Authentisierung
  - Vertraulichkeit
  - Integrität
  - Autorisierung
  - Schwächen und Angriffe
- WiFi Protected Access (WPA)
  - Authentisierung mit 802.1X oder Preshared Keys (PSK)
  - Vertraulichkeit (TKIP)
  - TKIP-Schlüsselhierarchie
  - WPA- und TKIP-Sicherheit
- WPA 2

Wireless Local Area Network (WLAN)

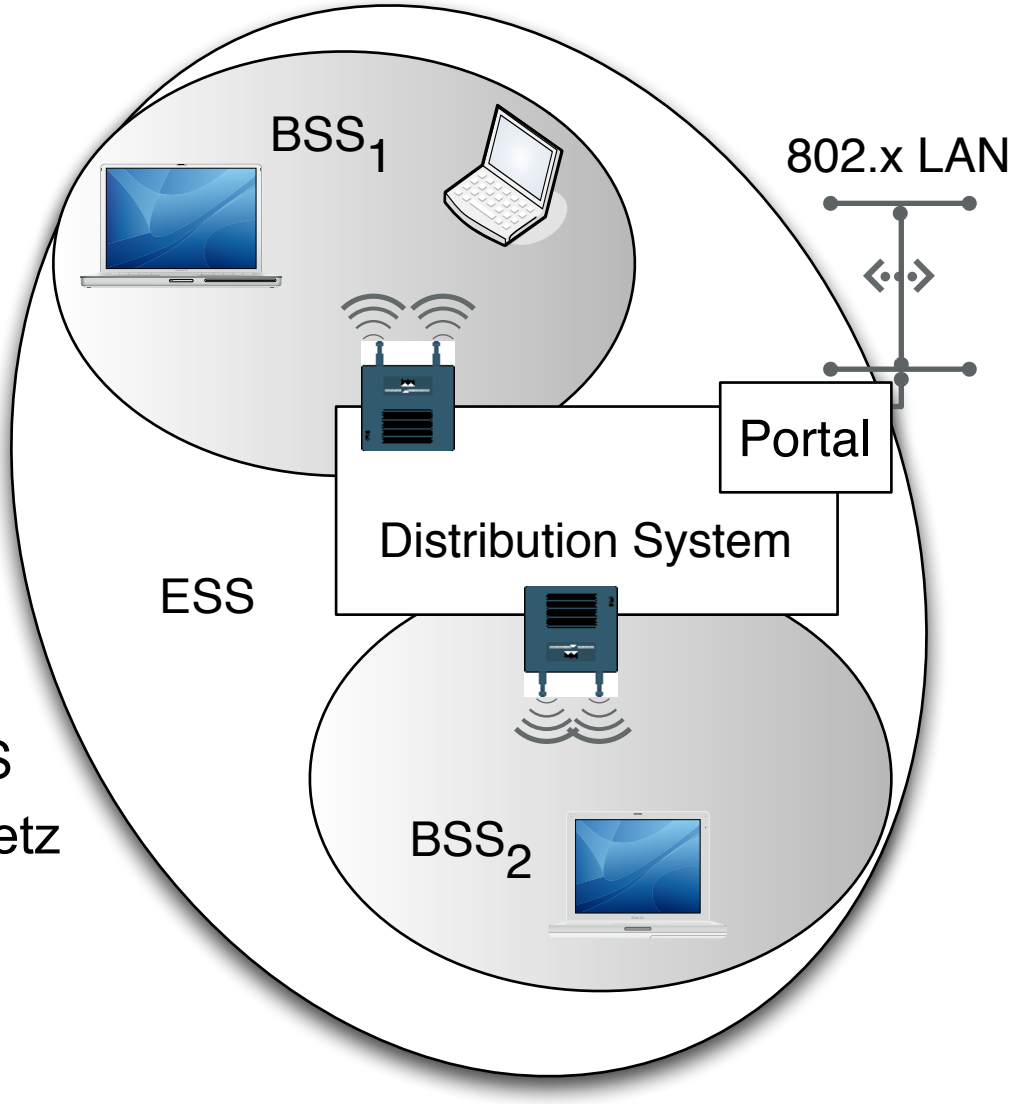
- WLAN standardisiert in IEEE 802.11x:

Standard	Frequenz [GHz]	maximaler Durchsatz [Mbit/s]
802.11	2,4	2
802.11a	5	54
802.11b	2,4	11
802.11g	2,4	54
802.11n (verabschiedet 09/2009)	2,4 5	600

- Alle Geräte teilen sich die Bandbreite
- Maximaler Durchsatz praktisch nicht erreichbar (netto wird i.d.R. weniger als die Hälfte erreicht, z.B. 120 Mbit/s bei 802.11n)

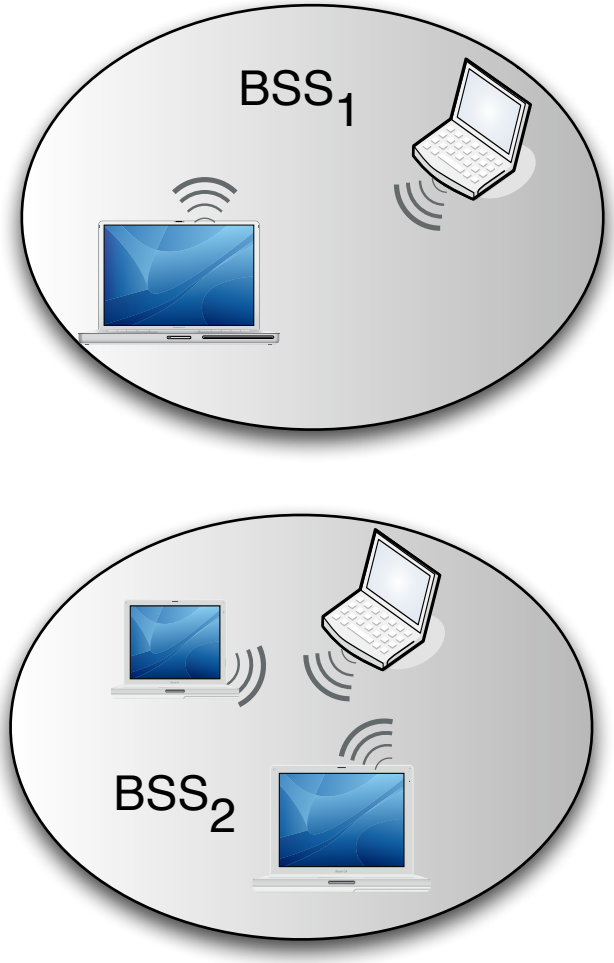
WLAN: Infrastruktur-Modus

- Access Point (AP): Zugangsknoten zum WLAN
- Station (STA)
  - Gerät mit WLAN-Ausstattung
  - (Intelligenter) Client
- Basic Service Set (BSS)
  - Gruppe von STAs, die selbe Frequenz nutzen
- Extended Service Set (ESS)
  - logisches Netz aus mehreren BSS
  - wird gebildet durch Verbindungsnetz (Distribution System (DSS))
  - ESS wird durch SSID identifiziert
- Portal: Verbindung zu anderen Netzen



WLAN: Ad-Hoc Modus

- Kein Access Point (AP) erforderlich
- Alle Stationen sind gleichberechtigt
- Basic Service Set (BSS)
  - Gruppe von STAs, die dieselbe Frequenz nutzen
  - Keine Kommunikation zwischen BSS möglich

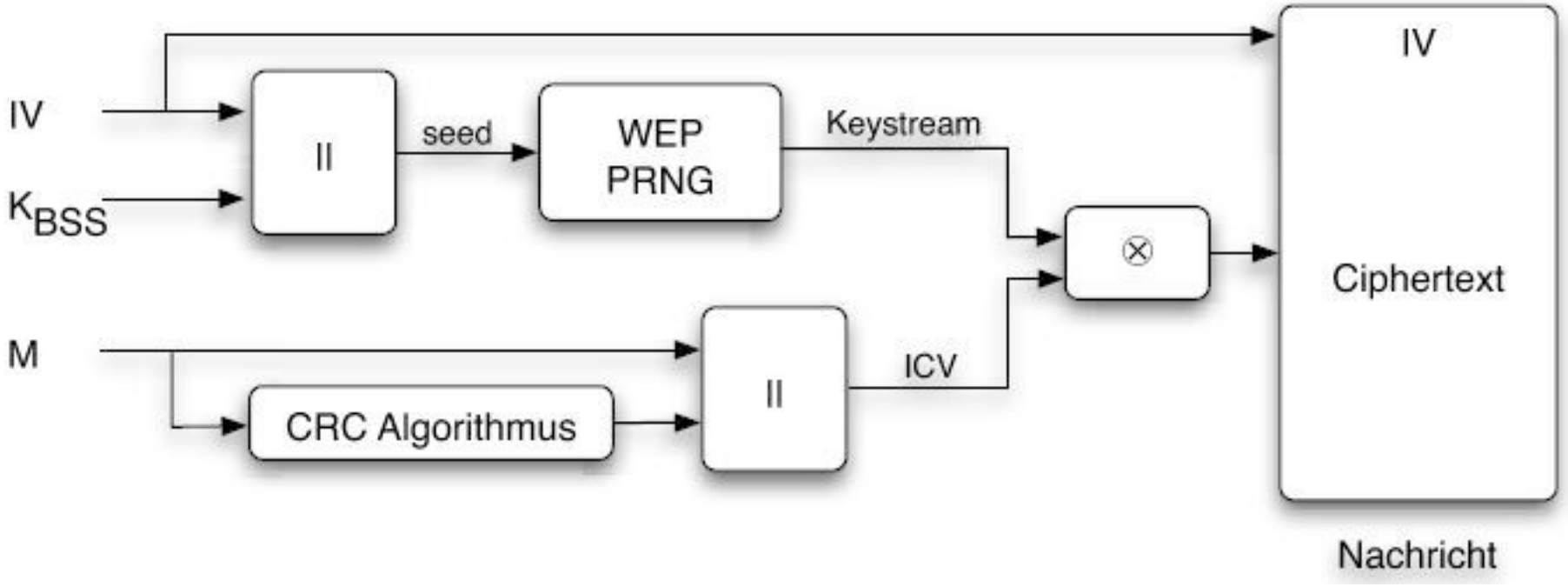


WLAN Sicherheitsmechanismen

- Mallet und Eve haben es im WLAN (wg. Funk) noch einfacher als in kabelgebundenen Netzen
- Sicherheitsanforderungen
  - Authentisierung
  - Zugangskontrolle zum Netz
  - Vertraulichkeit
  - Integrität
- Sicherheitsmechanismen
  - Wired Equivalent Privacy (WEP)
  - WiFi Protected Access (WPA)
  - WiFi Protected Access 2 (WPA2)
  - IEEE 802.11i (Standard, wegen Verspätung etablierte die Wi-Fi Alliance (Herstellerkonsortium) bereits WPA)
    - IEEE 802.11i D3.0 ist äquivalent zu WPA
    - IEEE 802.11i D9.0 ist äquivalent zu WPA2

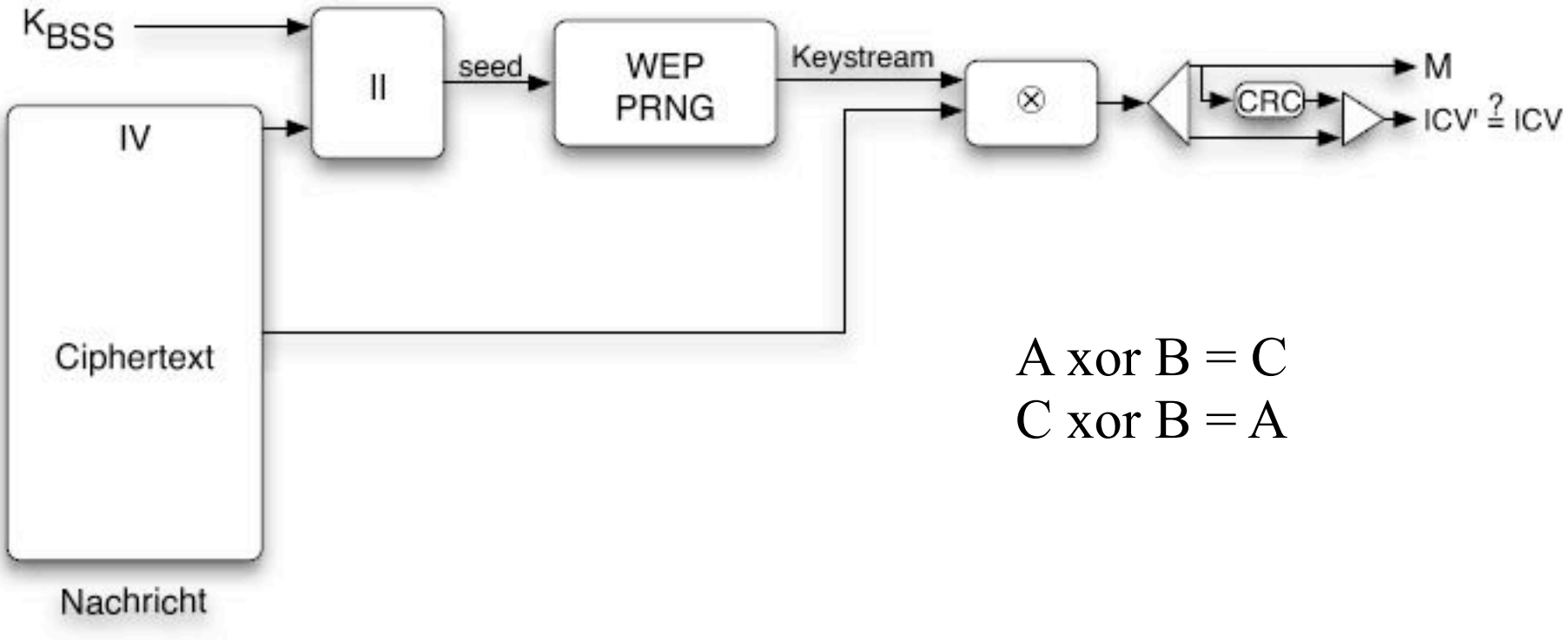
Vertraulichkeit: Wired Equivalent Privacy (WEP)

- Klartext wird mit Bitstrom XOR-verknüpft
- Bitstrom wird mit RC4 als Pseudozufallszahlengenerator (WEP PRNG) erzeugt
  - Für jede Nachricht 24-bit Initialisierungsvektor (IV) konkateniert mit 40-bit WEP-Schlüssel als 64-bit Seed für PRNG
  - Nachricht konkateniert mit CRC wird XOR verknüpft



WEP: Entschlüsselung

- IV wird im Klartext mit jedem Chiffretext übertragen
  - Jeder, der K_{BSS} kennt, kann Keystream erzeugen und Nachricht entschlüsseln
  - Selbstsynchronisierung von WEP
- Entschlüsselung ist inverser Vorgang zur Verschlüsselung



A xor B = C
C xor B = A

WEP: Integritätssicherung mit CRC-32

- Cyclic Redundancy Check (CRC) ist ein Fehlererkennungcode
- Entwickelt, um Übertragungsfehler in Netzen zu erkennen
- Mathematische Grundlagen:
  - Bit-String wird als Polynom mit Koeffizienten 0 und 1 aufgefasst
  - Nachricht M wird interpretiert als Polynom M(x)
  - Polynomberechnung modulo 2; d.h. Addition und Subtraktion identisch mit XOR
- Berechnung des CRC von M(x) zur Integritätssicherung:
  - Einigung auf Generatorpolynom G(x) (i.d.R. standardisiert)
  - Sei n der Grad von G(x), dann ist n+1 die Länge von G(x)
  - M(x) wird durch G(x) geteilt; M(x) mod G(x)
  - Teilungsrest ist CRC und wird mit M konkateniert
  - Empfänger berechnet Gesamtnachricht (M(x)|CRC) modulo G(x)
    = 0; Nachricht wurde nicht verändert (außer Änderung ist Vielfaches von G(x))
    ≠ 0; Nachricht wurde verändert

Anwendungen und Grenzen von CRC

- Einfach und billig in Hardware umzusetzen (32-bit Schieberegister)
- Gut geeignet für die Erkennung von „zufälligen“ Fehlern (z.B. bei Rauschen)
  - Ethernet
  - Festplatten-Datenübertragung
  - ...
- Aber: Keine kryptographische Hashfunktion!
  - Andere (sinnvolle) Nachrichten mit selbem CRC-Wert können einfach erzeugt werden
- Nur Fehlererkennung, keine Fehlerkorrektur möglich

WEP Authentisierung

- Open System Authentication
  - Entweder AP verschlüsselt nicht: Dann keine Authentifizierung, jeder kann AP nutzen
  - Oder bei aktivierter WEP-Verschlüsselung: Wer den Schlüssel kennt, kann Daten übertragen

- Shared Key Authentication
  - Challenge-Response-Protokoll
  - Basiert auf WEP-Verschlüsselung:

1. STA sendet Authentication Request an AP
2. AP sendet Challenge r im Klartext zurück
3. STA verschlüsselt r und sendet WEP(r) zurück
4. AP verifiziert

WEP Zugangskontrolle

- Bei Open System Authentication kann jeder senden
- Falls WEP aktiviert ist, kann nur senden, wer K_{BSS} kennt
- Viele APs bieten zusätzlich MAC-basierte Access Control Listen (ACLs)
  - Nur bekannte/freigeschaltete MAC Adressen dürfen senden
  - MAC kann einfach mitgelesen werden
  - MAC kann einfach gefälscht werden

WEP-Schwächen: Überblick

- WEP erfüllt KEINE der Sicherheitsanforderungen
- Vertraulichkeit:
  - Schlüsselmanagement und Schlüssel sind ein Problem
  - WEP ist einfach zu brechen
- Integrität
  - CRC kein geeignetes Verfahren zur Integritätssicherung bei absichtlicher Manipulation
- Authentisierung
  - basiert auf WEP
  - Fehler in der Umsetzung
- Zugriffskontrolle
  - Keine individuelle Authentifizierung, somit generell nur rudimentäre Zugriffskontrolle möglich

WEP Schwäche: Schlüsselmanagement

- Standard legt kein Schlüsselmanagement fest
- „Out-of-Band“ Schlüsselverteilung erforderlich
  - Manuelles Schlüsselmanagement oft fehlerbehaftet
  - Schlüssel werden sehr selten gewechselt
  - Oft wurde Open System Authentication ganz ohne Verschlüsselung aktiviert
- Schlüssellängen
  - WEP-40; 40 Bit Schlüssel (wegen Exportrestriktionen)
  - WEP-104; 104 Bit Schlüssel
    - Vom Benutzer z.B. in Form von 26 Hexziffern einzugeben
    - Somit mühsam/fehleranfällig und deshalb häufig sehr einfach gewählt
  - Aber selbst mit ausreichend langen Schlüsseln wäre WEP nicht sicher

WEP Schwäche: Verschlüsselung

- RC4 ist Stromchiffre, d.h. der selbe Schlüssel sollte nie wiederholt werden
  - IV soll dies verhindern
  - IV wird im Klartext übertragen
  - 24 Bit für den IV sind deutlich zu kurz
- Wiederverwendung des Keystream (bei gleichem IV)
  - Zwei Klartextnachrichten M_1 und M_2 mit $P_i = (M_i|CRC_i)$
  - $C_1 = P_1 \oplus RC4(IV_1, K_{BSS})$
  - $C_2 = P_2 \oplus RC4(IV_1, K_{BSS})$
  - dann gilt
  - $C_1 \oplus C_2 = (P_1 \oplus RC4(IV_1, K_{BSS})) \oplus (P_2 \oplus RC4(IV_1, K_{BSS})) = P_1 \oplus P_2$
  - d.h. falls Angreifer M_1 und C_1 kennt, kann er P_2 (somit M_2) aus dem mitgehörten C_2 berechnen, ohne K_{BSS} zu kennen (Known-Plaintext Angriff)
  - Known-Plaintext ist einfach zu erzeugen (Daten von außen schicken)

WEP Schwäche: Traffic Injection

- Known-Plaintext Angriff: Mallet kennt M und C:
  $C = RC4(IV,K_{BSS}) \oplus (M,CRC(M))$
- Damit kann Mallet den Key Stream berechnen:
  $RC4(IV,K_{BSS}) = C \oplus (M, CRC(M))$
- Absichtliche Wiederverwendung alter IVs möglich:
  Mallet berechnet
  $C' = RC4(IV, K_{BSS}) \oplus (M',CRC(M'))$
  und schickt (IV, C´) an Bob
- Bob hält dies für ein gültiges Paket

- Wissen über verwendete höherliegende Protokolle erleichtert rein passiven Known-Plaintext Angriff
  - Protokoll-Header, Adressen, Protokollprimitive sind Teile von M

WEP Schwäche: Integritätssicherung

- CRC und RC4 sind linear
- Mallet fängt Nachricht von Alice an Bob ab: (IV, C) mit
  $C = RC4(IV, K_{BSS}) \oplus (M, CRC(M))$
- Mallet verfälscht die Nachricht M zu Nachricht X
  - Mallet wählt beliebige Nachricht M´ mit derselben Länge
  - Mallet sendet Ciphertext $C' = C \oplus (M', CRC(M')) =$
    $RC4(IV, K_{BSS}) \oplus (M,CRC(M)) \oplus (M',CRC(M')) =$
    $RC4(IV, K_{BSS}) \oplus (M \oplus M', CRC(M) \oplus CRC(M')) =$
    $RC4(IV, K_{BSS}) \oplus (M \oplus M', CRC(M \oplus M')) =$
    $RC4(IV, K_{BSS}) \oplus (X, CRC(X))$
  - Mallet kennt Inhalt von X nicht, da er M nicht kennt
  - ABER: Eine „1“ an Position n in M´ führt zu gekipptem Bit an Position n in X; Mallet kann kontrollierte Änderungen in M durchführen. Beispiel: Zieladresse von IP-Paketen ändern

Weakness in Key Scheduling of RC4

- Papier von Fluhrer, Mantin und Shamir; 2001:
  - Grosse Zahl unsicherer Schlüssel wurden identifiziert, kleine Zahl von Bits reicht, um die meisten Output-Bits zu berechnen
  - Schwäche: IV wird mit K_{BSS} konkateniert; IV im Klartext übertragen
  - K_{BSS} bleibt relativ lange konstant, IV wechselt
  - Passive Ciphertext-Only Attack:
    - Eve muss 4 bis 6 Millionen Pakete mithören
    - Dies dauert nur wenige Minuten (ggf. Traffic stimulieren)
    - Abhängigkeit von der Schlüssellänge (40 oder 104 Bit) ist nur linear
- Klein zeigt 2005, dass es stärkere Korrelationen zwischen Keystream und Schlüssel gibt und verbessert den Angriff aus 2001

Breaking 104-bit WEP in less than 60 seconds

- Artikel von Tews, Weinmann, Pyshkin, Uni Darmstadt, 2007
- Aktiver Angriff
- Nutzt ARP-Request- und ARP-Reply-Pakete
  - Feste Länge der Pakete
  - Über Länge der Frames sind die verschlüsselten ARP Pakete erkennbar
  - Die ersten 16 Byte des ARP Paketes sind vorhersagbar
    - 8 Byte LLC Header (AA AA 03 00 00 00 08 06) gefolgt von
    - 8 Byte ARP Header:
      - 00 01 08 00 06 04 00 01 für ARP Request
      - 00 01 08 00 06 04 00 02 für ARP Response
  - XOR Verknüpfung abgehörter Pakete mit dieser Bytefolge liefert die ersten 16 Byte des Keystream
  - Wiedereinspielen abgehörter ARP Requests beschleunigt den Angriff
  - Erfolgsrate bei nur 40.000 Frames schon > 50 %
  - Erfolgsrate bei 85.000 Frames rund 95 %

Schlussfolgerung

- WEP ist **NICHT** sicher
- WEP sollte **NICHT** verwendet werden
- Das 2008er Update des Data Security Standards (DSS) der Payment Card Industry (PCI) verbietet die Nutzung von WEP im Rahmen jeglicher Kreditkarten-Datenverarbeitung ab Juli 2010

WiFi Protected Access

- WPA zur Verbesserung der Sicherheit eingeführt
- WEP-Hardware sollte weiter benutzbar bleiben
- Vertraulichkeit:
  - Temporal Key Integrity Protocol (TKIP)
  - Rekeying-Mechanismus zum automatischen Wechseln der Schlüssel
  - Hierarchie von Schlüsseln
- Integritätssicherung
  - TKIP Message Integrity - MIC (genannt „Michael“);
    zur Unterscheidung von MAC (Media Access Control)
  - Mit Schlüssel parametrisierte kryptographische Hash-Funktion
  - Verbessert ungeeigneten CRC-Mechanismus von WEP
- Authentisierung
  - Nach wie vor Möglichkeit für Pre-Shared Key (PSK)
  - Bietet aber auch 802.1X (insb. in großen IT-Infrastrukturen genutzt)

Temporal Key Integrity Protocol (TKIP)

- TKIP verwendet Schlüsselhierarchie, um kurzlebige Schlüssel zu erzeugen
- Drei Hierarchiestufen:

1. Temporäre Schlüssel (Temporal Key, TK)
   - In jede Richtung eigene Schlüssel
     - Zur Verschlüsselung (128 Bit)
     - Zur Integritätssicherung (64 Bit)
   - Erneuerung des Schlüsselmaterials durch `rekey key` Nachricht
   - `rekey key` Nachricht enthält Material, damit STA und AP neue Sitzungsschlüssel ableiten können; Nachricht verschlüsselt mit
2. Pairwise Transient Key (PTK)
   - Sichern die Übertragung temporärer Schlüssel
   - 1 Schlüssel zur Sicherung des Schlüsselmaterials
   - 1 Schlüssel zur Sicherung der `rekey key` Nachricht

TKIP Schlüsselhierarchie

3. Pairwise Master Key (PMK)
   - Höchster Schlüssel innerhalb der Hierarchie
   - Erzeugt vom 802.1X Authentication Server und vom AP an STA weitergereicht
   - Falls 802.1X Setup „zu komplex“; Preshared Keys möglich (d.h. in der Praxis: Passwörter)
   - Master Key wird zur Sicherung der key-encryption Keys genutzt
   - Damit Aufbau einer Sitzungsstruktur möglich; von der Authentisierung über 802.1X bis
     - Widerruf des Schlüssels
     - Ablauf des Schlüssels
     - STA verliert Kontakt zum AP
   - Klar: Kompromittierung des Master Key führt zur Kompromittierung der gesamten Hierarchie!

TKIP Schlüsselhierarchie Zusammenfassung

- Aus IEEE 802.11i-2004 (geht über reines TKIP hinaus)
- hier Verwendung von 802.1X

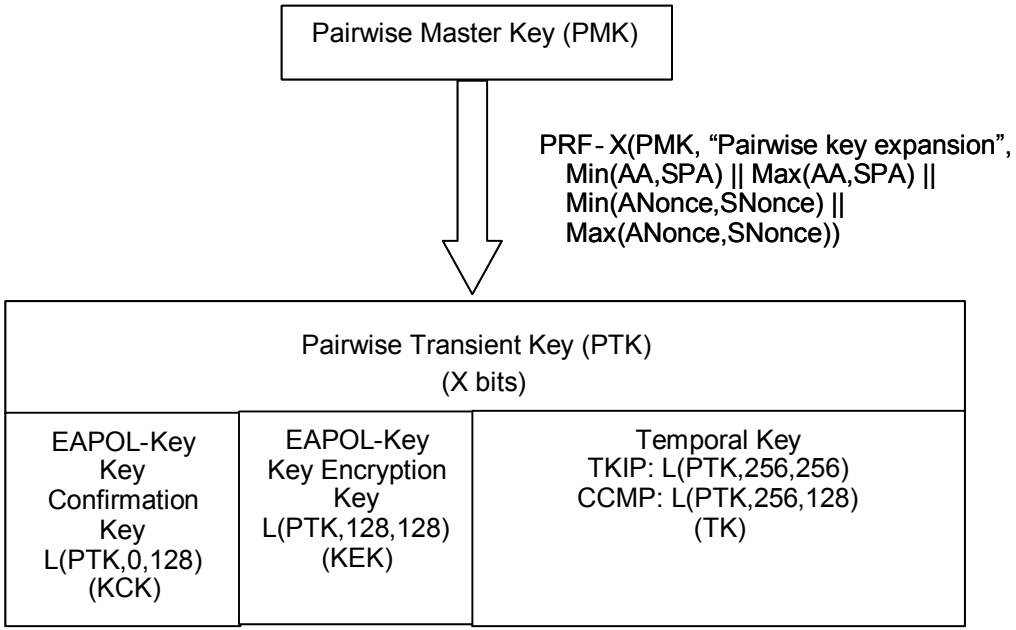


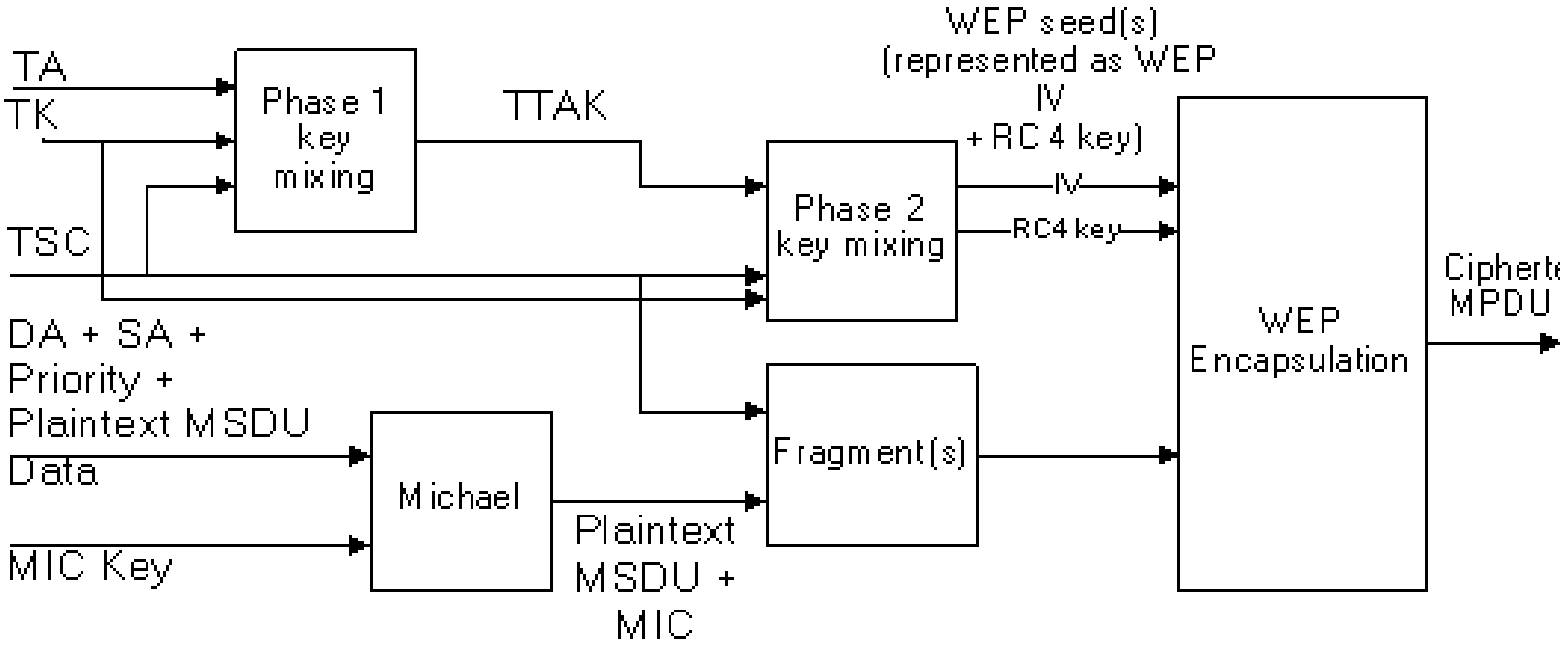
Figure 43s—Pairwise key hierarchy

- **PRF** Pseudo Random Function
- **AA** Authenticator Address
- **SPA** Supplicant Address
- **EAPOL** EAP over LAN
- **KCK** Key Confirmation Key (Integritätssicherung)
- **KEK** Key Encryption Key
- **L(x,0,128)** Teilstring ab Bit 0 mit Länge von 128

CCMP ist Bestandteil von WPA2 (später)

TKIP Verschlüsselung: Blockdiagramm

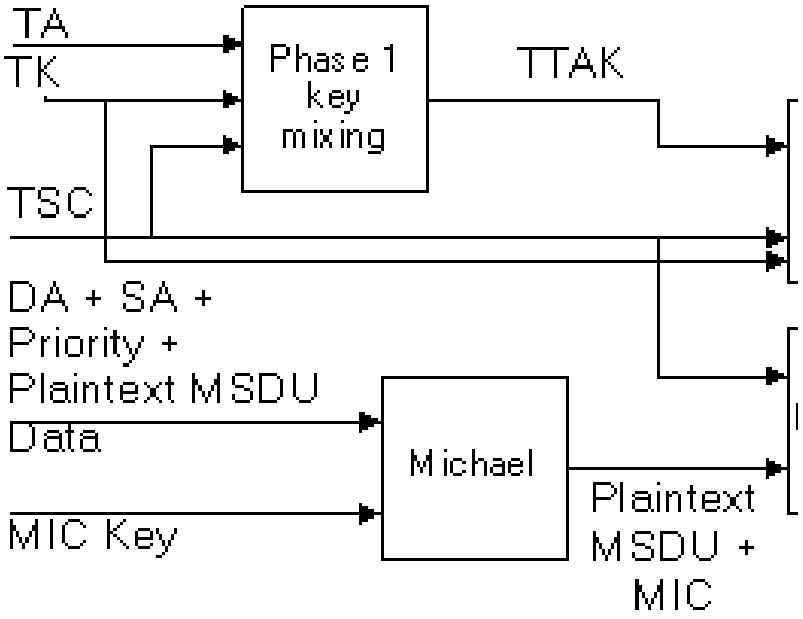
- Aus IEEE 802.1i-2004



- TA Transmitter Address
- TK Temporal Key
- TSC TKIP Sequence Counter
- DA Destination Address
- SA Source Address
- MSDU MAC Service Data Unit
- MPDU Message Protocol Data Unit
- TTAK TKIP Mixed Address and Key
- MIC Message Integrity Code

TKIP Verschlüsselung

- Aus IEEE 802.1i-2004

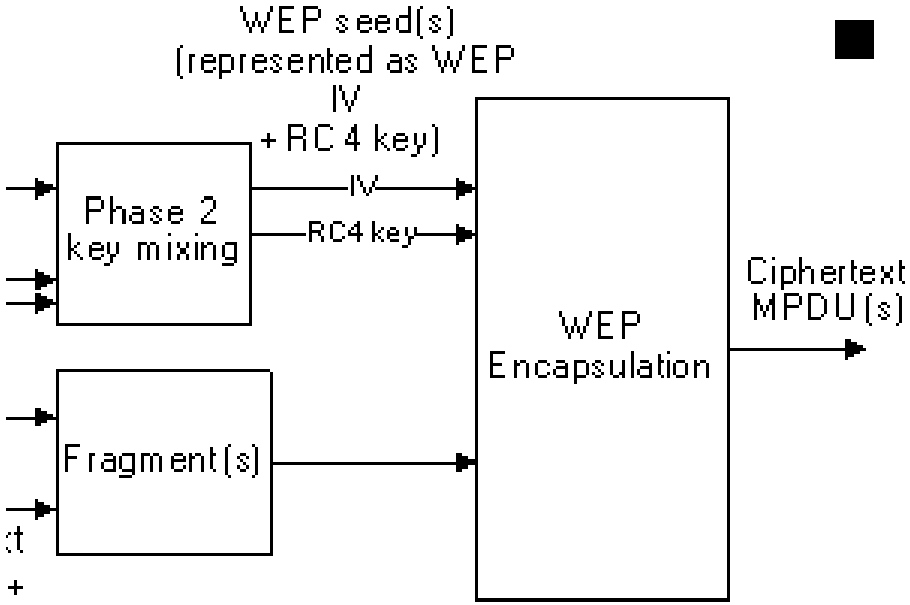


- TA Transmitter Address
- TK Temporal Key
- TSC TKIP Sequence Counter
- DA Destination Address
- SA Source Address

- Kein wirklich neues Verfahren; soll nur Schwächen beseitigen
- Phase 1 Key Mixing
  - TTAK = Phase1(TA,TK, TSC)
  - Phase1 ist nichtlineare Funktion mit XOR-Operationen, bitweiser UND-Operation sowie einer Verkürzungsfunktion
  - TA verhindert, dass zwei STAs denselben Schlüssel erhalten
  - TSC als Sequenznummer für MPDUs

TKIP Verschlüsselung: Phase 2

- Aus [IEEE 802.1i-2004]

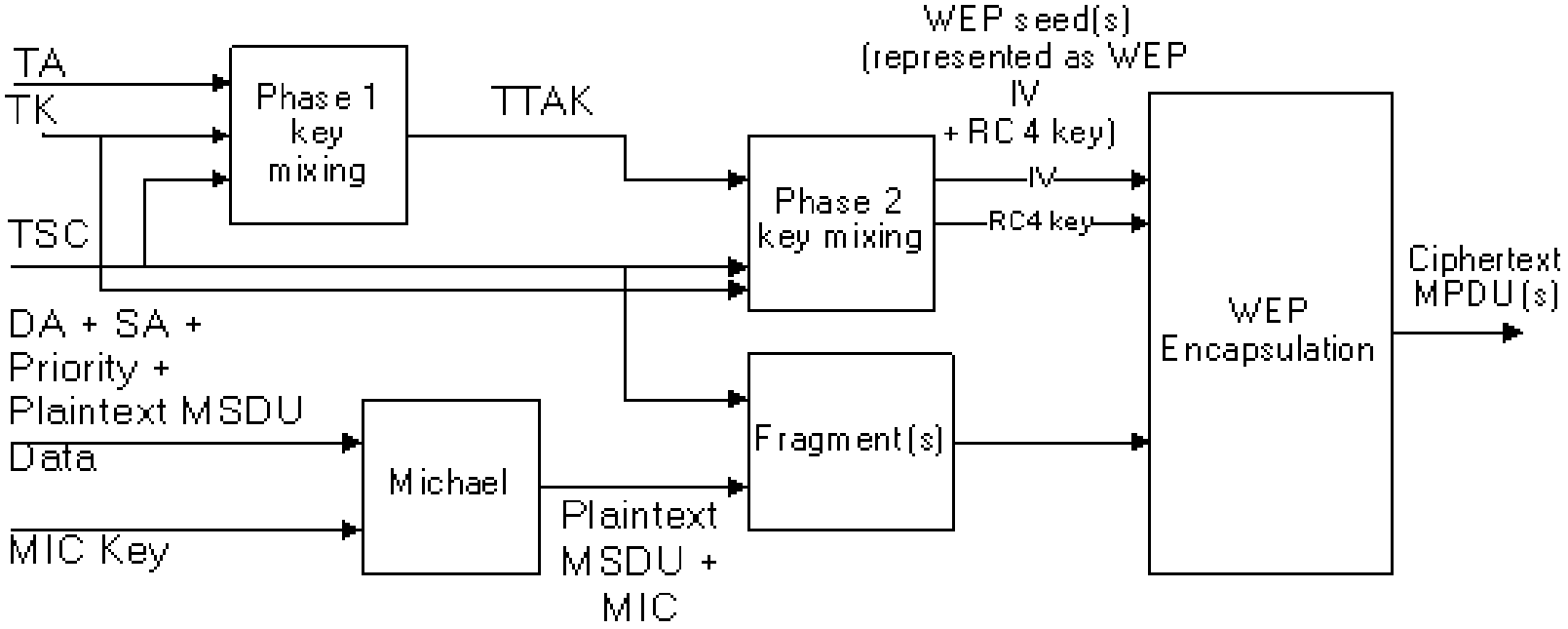


- **TTAK** TKIP Mixed Address and Key

- Phase 2 Key Mixing
  - TTAK = Phase1(TA, TK, TSC)
  - Phase2(TTAK, TK, TSC)
  - Phase2 ist Feistel-Chiffre:
  - Einfache Operationen für „schwache“ AP-Hardware
    - XOR, UND, ODER, >>
    - S-Box
  - Erzeugt 128 Bit WEP Schlüssel
    - 24 Bit Initialisierungsvektor
    - 104 Bit RC4 Schlüssel

TKIP Verschlüsselung: Zusammenfassung

- Aus IEEE 802.1i-2004



- Für jedes Frame (MSDU) wird eigener Schlüssel generiert
- Hardware-Abwärtskompatibilität; d.h. Verwendung von RC4 nach wie vor problematisch

WPA und TKIP: Sicherheit

- Bei Verwendung von Pre Shared Keys (PSK) hängt die Sicherheit stark von der Stärke des Passworts ab
- Angriff mit Rainbow-Tables (seit 2004)
- Angriff auf PRF Funktion der Schlüsselverteilung (August 2008)
  - nutzt GPUs (Graphics Processing Units) anstatt CPUs
  - Entwickelt auf NVIDIA-CUDA (Compute Unified Device Architecture)
    - Compiler und Entwicklungsumgebung
    - nativer Zugriff auf GPUs auf Grafikkarten
    - dadurch massive Parallelisierung möglich
    - damit Speedup von Faktor 30 und mehr möglich
    - Zeit für „Raten“ eines Passwortes reduziert sich auf 2-3 Tage
- Angriff auf TKIP Verschlüsselung (November 2008)
  - Entschlüsselung von Paketen mit teilweise bekanntem Inhalt ohne Kenntnis des Schlüssels möglich
  - Schlüssel ist damit nicht zu brechen

CERN School of Computing

Multi-core architectures – NVIDIA G80

- **128 stream processors**
- **330 GFlops (today's general purpose CPUs have ~10)**
- **150W**
- **Top of the line graphics hardware (along with the G92)**

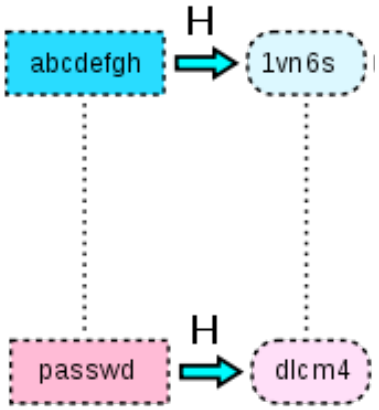
damals

Einschub: Rainbow Tables

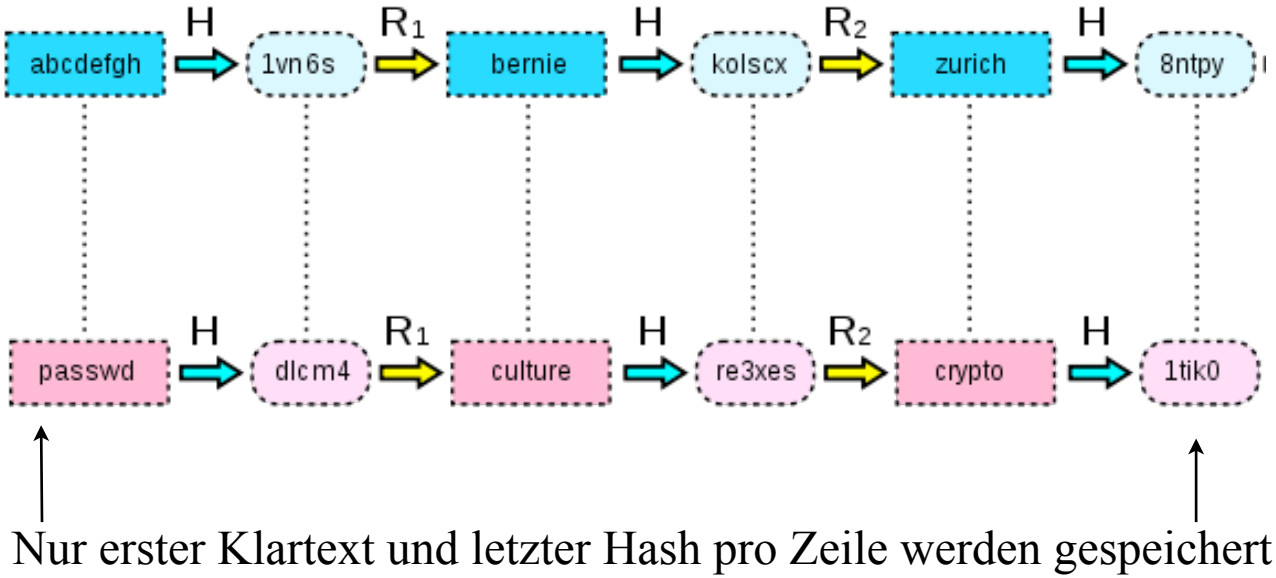
- Bei allen Krypto-Angriffen ist Rechenzeit- und Speicherplatzkomplexität zu betrachten
- Rainbow-Tables versuchen, optimalen time-memory tradeoff zu nutzen, um vollständigen Brute-Force-Angriff zu sparen
- Idee: Optimale Speicherung einer Klartext-zu-Hash Tabelle
- Kompakte Speicherung von sog. Chains (Ketten/PW-Sequenzen)
  - Kette startet mit initialem Klartext-Wort, dieses wird gehasht
  - resultierender Hash wird Reduktionsfunktion unterworfen
  - Reduktionsfunktion liefert weiteres potentielles Klartext-Wort
  - Dieser Vorgang wird n-mal wiederholt
  - relevant sind nur erstes Klartext-Wort und letzter Hash-Wert
  - Vorgang wird einmal für alle Wörter eines Wörterbuchs wiederholt
  - Kollisionen vermeiden: internes Klartext-Wort darf nicht Startwert einer anderen Kette sein
  - Rainbow Table speichert alle resultierenden Ketten (1. Klartext : letzter Hash)

Einschub: Rainbow Tables; Beispiele

- Trivialfall: Nur 1 Iteration
  - Speichert zu jedem Klartext seine Hashsumme
  - Rainbow-Tabelle wird sehr lang und damit zu groß



- 3 Iterationen:



Einschub: Rainbow Tables; Anwendung

- Rainbow-Tabelle mit w Einträgen und Ketten der Länge n
- MD5 Hash: `bca6a2aed3edc8e22f68ed65e39682c6` („IT-Sec“)
- Suche in Tabelle auf rechter Seite. Fallunterscheidung:

1. Hash-Wert gefunden, steht z.B. in Zeile 17
   - Kette aus Zeile 17 komplett durchlaufen Reduktionsfunktion n-1 liefert den gesuchten Klartext
2. Hash-Wert steht nicht in Rainbow-Table
   - Reduktion des Hashes (vereinfachtes Bsp. erste 6 Zeichen): `bca6a2`
   - MD5(`bca6a2`) liefert `3c41c8c8c5d27647d3f64937a801c90a`
   - Suche diesen Hash in Tabelle

- In der Praxis werden verschiedene Reduktionsfunktionen kombiniert
  - Ziel: Kollisionen / Wiederholungen vermeiden, um möglichst viele Klartexte abzudecken

Angriff auf TKIP Verschlüsselung

- Beck, TU-Dresden, Tewes, TU-Darmstadt; publ. 08.11.2008
- Erstes Verfahren, das keine Pre Shared Keys voraussetzt
- Basiert auf chop-chop Angriff (bekannt seit 2005)
- Funktionsweise:
  - Angreifer schneidet Verkehr mit, bis er verschlüsseltes ARP Packet findet (vgl. Folien „Breaking WEP in less than 60 seconds“)
  - letztes Byte wird entfernt
  - Annahme: Byte war 0; mit XOR-Verknüpfung mit bestimmten Wert wird versucht gültige Checksumme zu erzeugen
  - Paket wird an AP gesendet:
    - Inkorrekt: Paket wird verworfen
    - Korrekt: Client erzeugt MIC Failure Report Frame; Angreifer muss dann vor nächstem Versuch 60 Sekunden warten, sonst erzwungener Verbindungsabbau
  - Worst Case: 256 Tests für 1 Byte erforderlich. Praktisch: In 12 Minuten mindestens 12 Byte entschlüsselbar

Beck, Tewes Angriff (Forts.)

- Sicherheitsmaßnahmen von WPA
  - Anti-chopchop: zwei falsche MICs in 1 Minute ➪ Verbindungsabbau
  - TSC verhindert Wiedereinspielen
- Gegenmaßnahmen:
  - 60 Sekunden warten (vgl. Folie vorher)
  - Replay nicht an verwendeten, sondern an anderen Sendekanal
- Entschlüsselung des ARP Paketes ermöglicht:
  - Schlüsselstrom vom AP zu STA und MIC Code können ermittelt werden
  - Eigene verschlüsselte Pakete können an STA gesendet werden; z.B. zum Manipulieren von ARP-Paketen
- Grenzen des Angriffs
  - Rekeying Intervall muss ausreichend groß sein
  - QoS muss aktiviert sein, sonst stehen keine 8 Kanäle zur Verfügung
  - nur eine Richtung: AP zu STA

WPA 2

- Empfehlung: Verwendung von WPA 2 anstelle von WPA
- Änderungen:
  - AES ersetzt verpflichtend RC4
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) als Ersatz für TKIP
- Verfahren gilt derzeit als sicher
  - Verpflichtend für Geräte mit Wi-Fi Logo
- Aber: Verschlüsselung schützt nicht ewig
  - Mitgehörte Daten können evtl. später entschlüsselt werden