IT-Sicherheit

- Sicherheit vernetzter Systeme -

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

Inhalt

- WLAN kurze Einführung
- WLAN Sicherheitsanforderungen und Mechanismen
- Wired Equivalent Privacy (WEP)
  - Authentisierung
  - Vertraulichkeit
  - Integrität
  - Autorisierung
  - WEP 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)

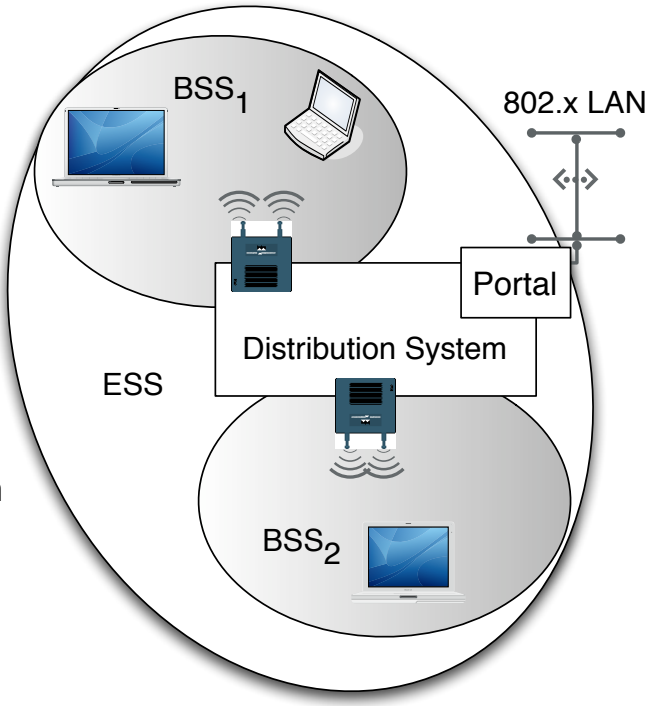
- WLAN standardisiert in IEEE 802.11x

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 (noch nicht verabschiedet)	2,4 5	600

- Alle Geräte teilen sich Bandbreite
- Maximaler Durchsatz kaum erreichbar (i.d.R. wird die Hälfte erreicht)

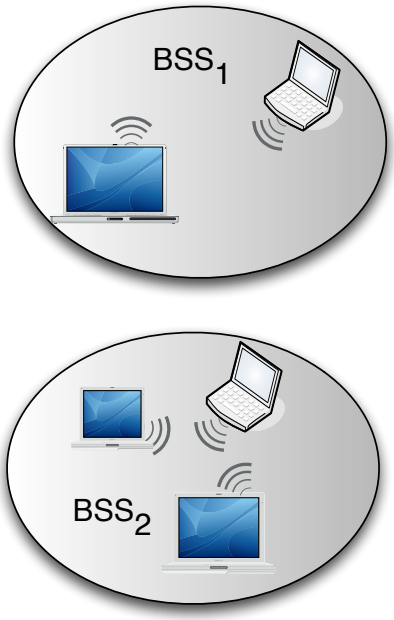
WLAN: Infrastruktur Modus

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



WLAN: AD-Hoc Modus

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

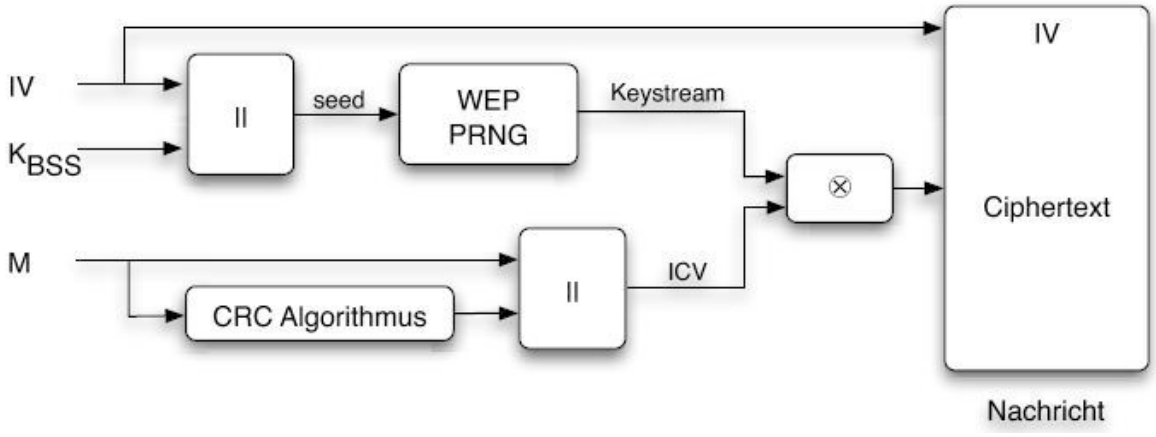


WLAN Sicherheitsmechanismen

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

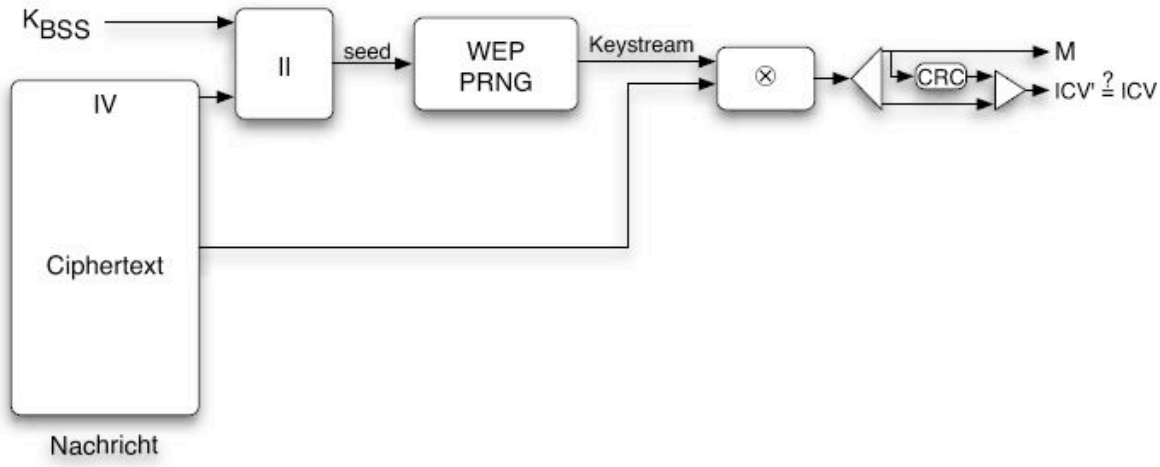
Vertraulichkeit: Wired Equivalent Privacy (WEP)

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



WEP Entschlüsselung

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



WEP: Integritätssicherung

- Cyclic Redundancy Code (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) geteileilt; M(x) mod G(x)
  - Teilungsrest ist CRC und wird mit M konkateniert
  - Empfänger berechnet (M(x)|CRC) modulo G(x)
    = 0; Nachricht wurde nicht verändert (außer Äderung ist Vielfaches von G(x))
    ≠ 0; Nachricht wurde verändert

WEP Authentisierung

- Open System Authentication
  - keine Authentisierung
  - Bei aktivierter WEP Verschlüsselung; Wer Schlüssel kennt, kann Daten übertragen
- Shared Key Authentication
  - Challange Response Protocol
  - 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 Authenticiation 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 definierte MAC Adressen dürfen senden
  - MAC kann einfach mitgelesen werden
  - MAC kann einfach gefälscht werden

WEP Bewertung

- WEP erfüllt KEINE der Sicherheitsanforderungen
- Vertraulichkeit:
  - Schlüsselmanagement und Schlüssel sind ein Problem
  - WEP ist einfach zu brechen
- Integrität
  - WEP CRC kein geeignetes Verfahren zur Integritätssicherung
- Authentisierung
  - basiert auf WEP
  - Fehler in der Umsetzung
- Zugriffskontrolle
  - keine wirkliche Zugriffskontrolle

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 und keine Verschlüsselung aktiviert
- Schlüssellängen
  - WEP-40; 40 Bit Schlüssel (wegen Exportrestriktionen)
  - WEP-104; 104 Bit Schlüssel
- Aber selbst mit ausreichend langen Schlüsseln: WEP ist 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 sind deutlich zu kurz
- Wiederverwendung des Keystream
  - 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, d.h. M_2 berechnen ohne K_{BSS} zu kennen (Known-Plaintext Angriff)

WEP Schwäche: Wiederverwendung Key Stream

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

- Wissen über verwendete höherliegende Protokolle erleichtert 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 erzeugt gefälschte Nachricht X
  - Mallet wählt beliebige Nachricht M´ mit derselben Länge
  - $C' = C \oplus (M', CRC(M')) =$
    $RC4(IV, K_{BSS}) \oplus (M,CRC(M)) \oplus (M',CRC(M')) =$
    $RC4(IV, K_{BSS}) \oplus (M \oplus M', CRC(M) \oplus CRC(M')) =$
    $RC4(IV, K_{BSS}) \oplus (M \oplus M', CRC(M \oplus M')) =$
    $RC4(IV, K_{BSS}) \oplus (X, CRC(X))$
  - Mallet kennt 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

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 Mio Packete mithöhren
    - Dies kann weniger als 15 Minuten dauern
    - Abhängigkeit von der Schlüssellänge (40 oder 104 Bit) ist nur linear
- Klein zeigt 2005 dass es größere Korrelationen zwischen Keystream und Schlüssel gibt und verbessert den Angriff aus 2001

Breaking 104 bit WEP in less than 60 Seconds

- Papier von Tews, Weinmann, Pyshkin, Uni Darmstadt, 2007
- Aktiver Angriff
- Nutzt ARP Request und Reply Packete
  - Feste Länge der Pakete
  - Über Länge der Frames sind verschlüsselte ARP Packete erkennbar
  - die ersten 16 Byte des ARP Packetes 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 Packete mit dieser Bytefolge liefert die ersten 16 Byte des Keystream
  - Widereinspielen abgehörter ARP Requests beschleunigt den Angriff
  - Erfolgsrate bei 40.000 Frames > 50 %
  - Erfolgsrate bei 85.000 Frames > 85 %

Schlussfolgerung

- WEP ist **NICHT** sicher
- WEP sollte **NICHT** verwendet werden

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 Wechsel 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
  - nutzt 802.1X

WPA Authentisierung

- Nutzt Preshared Keys oder 802.1X
- 802.1X EAP; aus [IEEE 802.1i-2004]

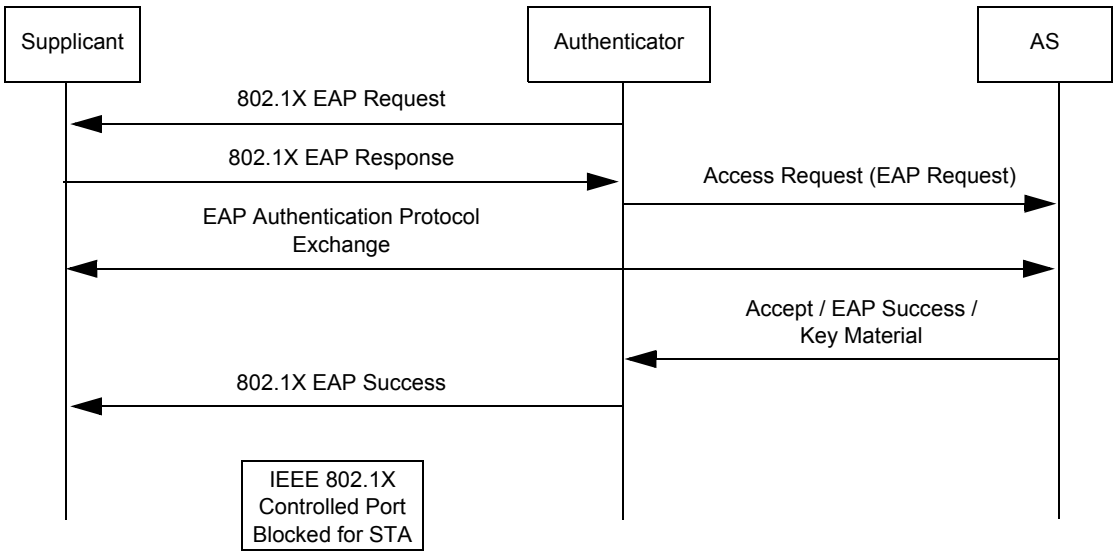


Figure 11b—IEEE 802.1X EAP authentication

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
   - Hinweis: 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

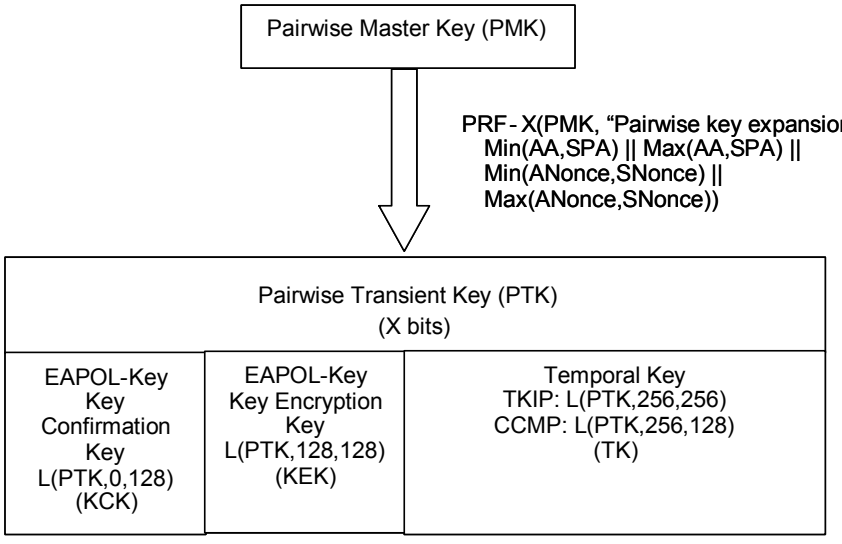


Figure 43s—Pairwise key hierarchy

- **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

TKIP Verschlüsselung: Block Diagramm

- Aus IEEE 802.1i-2004

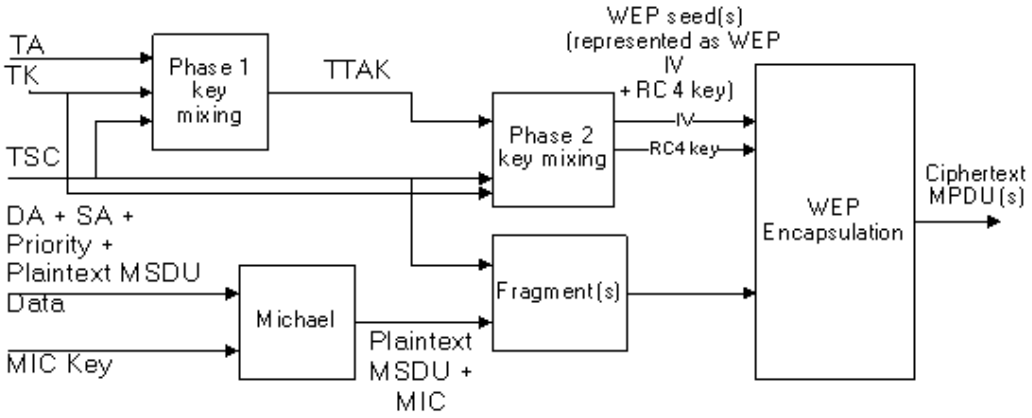
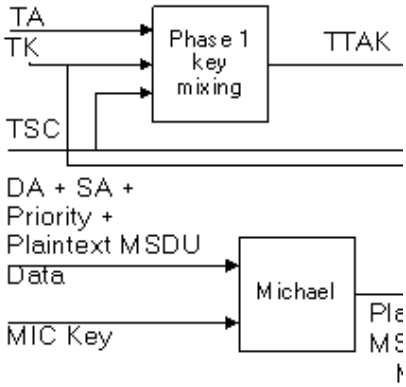


Figure 43c—TKIP encapsulation block diagram

- TA Transmitter Adress
- 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

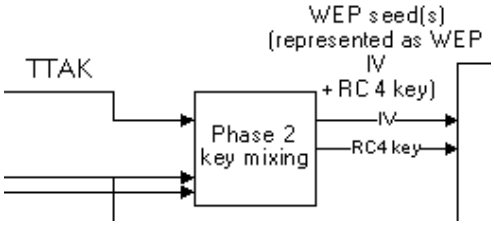


- TA Transmitter Adress
- TK Temporal Key
- TSC TKIP Sequence Counter
- DA Destination Address
- SA Source Address

- Kein wirklich neues Verfahren; soll nur Schwäche 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 das zwei STAs selben Schlüssel erhalten
  - TSC als Sequenznummer für MPDUs

TKIP Verschlüsselung: Phase 2

- Aus [IEEE 802.1i-2004]

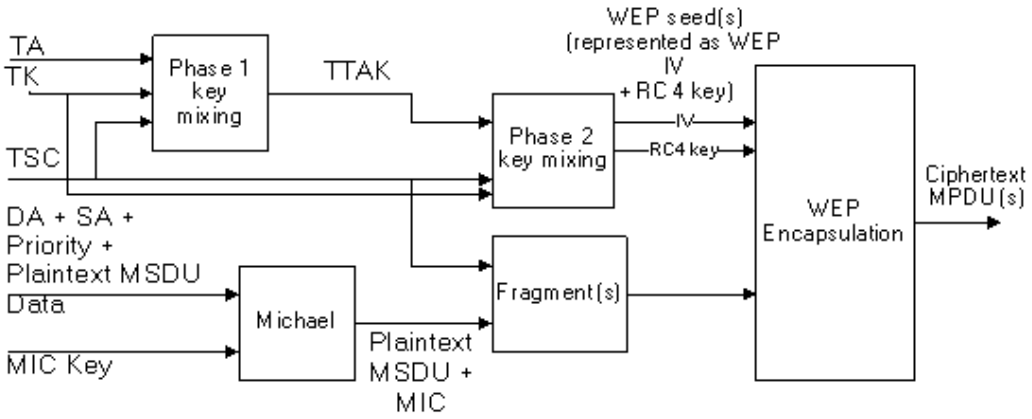


- **TTAK** TKIP Mixed Address and Key

- 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 Initialisierunsvektor
    - 104 Bit RC4 Schlüssel

TKIP Verschlüsselung: Zusammenfassung

- Aus IEEE 802.1i-2004



- Für jeden Frame (MSDU) wird eigener Schlüssel generiert
- Hardware „Abwärtskompatibilität“; d.h. Verwendung von RC4 problematisch

WPA und TKIP Sicherheit

- Bei Verwendung von Pre Shared Keys (PSK) hängt Sicherheit essentiell von Stärke des Passwortes ab
- Angriff mit Rainbow-Tables (seit 2004)
- Angriff auf PRF Funktion der Schlüsselverteilung (August 2008)
  - nutzt GPUs (Grafik 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 ohne Kenntnis des Schlüssels möglich
  - Schlüssel ist damit nicht zu brechen

CERN School of Computing

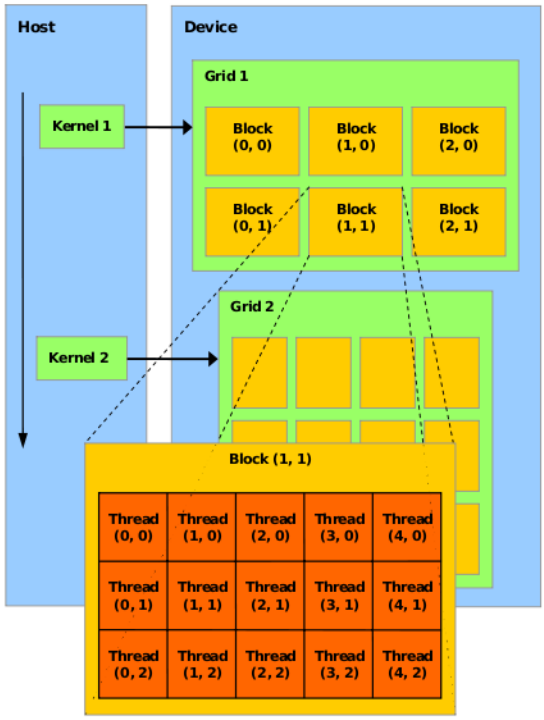
Multi-core architectures – NVIDIA G80

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

CERN School of Computing

Multi-core architectures – NVIDIA G80

- **Moved away from traditional GPU design**
- **128 stream processors**
- **330 GFLOPS peak**
- **Second generation: G92**



Einschub: Rainbow-Tabellen

- Bei allen Crypto-Angriffen ist Rechenzeit- und Speicherplatzkomplexität zu betrachten
- Rainbow-Tabellen versuchen optimalen time-memory tradeoff zu nutzen
- Idee: optimale Speicherung einer Klartext:Hash Tabelle
- Kompakte Speicherung von sog. Chains (Ketten)
  - Kette startet mit initialem Klartext-Wort, dieses wird Hash unterworfen
  - resultierender Hash wird Reduktionsfunktion unterworfen
  - Reduktionsfunktion liefert weiteres potentielles Klartext-Wort
  - Dieser Vorgang wird n-mal wiederholt
  - gespeichert wird 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
  - gespeichert werden alle resultierenden Ketten (1. Klartext: letzter Hash)

Einschub: Rainbow-Tabellen; Anwendung

- Rainbow-Tabelle mit w Einträgen und Ketten der Länge n
- MD5 Hash: `4a871ebe4f9adda5c5819cbb846ea02a` („IT-Sec“)
- Suche in Tabelle auf rechter Seite

1. Hash-Wert ist steht in Zeile 17
   - Kette aus Zeile 17 komplett durchlaufen Reduktionsfunktion n-1 liefert Klartext
2. Hash-Wert steht nicht in Rainbow-Table
   - Reduktion des Hashes (vereinfachtes Bsp. erste 6 Zeichen): `4a871e`
   - MD5(`4a871e`) liefert `e3e1c76024e25d8145069afa79049ae4`
   - Suche diesen Hash in Tabelle

- In der Praxis werden verschiedene Reduktionsfunktionen genutzt

Angriff auf TKIP Verschlüsselung

- Beck, TU-Dresden, Tewes, TU-Darmstadt; publ. 8.11.2008
- Erstes Verfahren dass keine Pre Shared Keys voraussetzt
- Basiert auf chopchop 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
  - Packet wird an AP gesendet:
    - Inkorrekt: Paket wird verworfen
    - Korrekt: Client erzeugt MIC Failure Report Frame; Angreifer muss vor nächstem Versuch 60 Sekunden warten sonst Verbindungsabbau durch Client
  - 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 Sendekanal sondern an anderen Kanal
- Entschlüsselung des ARP Packetes ermöglicht:
  - Schlüsselstrom vom AP zu STA kann ermittelt werden
  - Eigene verschlüsselte Packete können an STA gesendet werden; z.B. zum Umleiten von ARP Anfragen
- Grenzen des Angriffs
  - Rekeying Intervall muss ≥ 3600 Sekunden 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
- Änderung: AES ersetzt verpflichtend RC4
- Verfahren gilt derzeit als sicher