

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



1. Motivation
2. Der Weg ins Internet
3. Überblick

4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung



Wireless LAN

Wireless LAN (WLAN) IEEE 802.11

- private Nutzung
- Nutzung in der Internet-Infrastruktur (WLAN-Hotspots)
- **Zugangskontrolle besonders wichtig**
→ kein physischer Kontakt zur Kommunikation notwendig

- **WEP**
 - Sicherheitsmechanismen für LAN-äquivalente Sicherheit
- **WPA, WPA2, 802.11i**
 - Verbesserung der Sicherheit und Behebung der Probleme von WEP
- **EAP-TLS, PEAP, EAP-TTLS**
 - Beidseitige Authentifizierung mit EAP
- **802.11w**
 - Sicherung von Management Rahmen

1

Wired Equivalent Privacy (WEP)

- Klassen von Authentifizierungsdiensten
 - *Open System*: keine Authentifizierung, nur Handshake
 - *Shared Key*: alle Benutzer verwenden gleichen Schlüssel
- Schlüssel
 - Verschlüsselung mit Stromchiffre RC4
 - Statischer 40 Bit Schlüssel, mit zufällig gewähltem 24 Bit IV als Eingabe für Schlüsselerzeugung
 - Key-Management und Erneuerung aufwendig
- Probleme
 - kurzer und statischer Schlüssel
 - kurzer IV, Rollover und erneute Nutzung möglich
 - Tools wie *AirSnort* und *WEPCrack* knacken WEP-Schlüssel

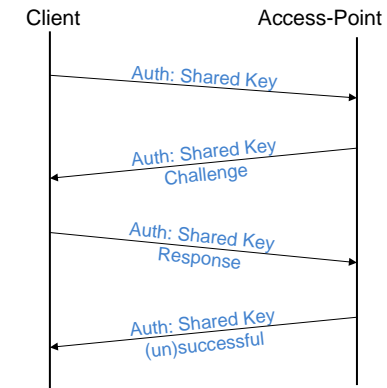
2

•Shared Key Verfahren

- Authentifizierung via Verschlüsselung
- Authentifizierung der Gruppenzugehörigkeit, nicht der Identität

•IV steht für Initialisierungsvektor

- Klassisches Challenge-Response-Verfahren
- Challenge wird mit Schlüssel via WEP verschlüsselt



3

1. Client generiert IV1, berechnet Schlüsselzeichen

Secret Key (40 Bit) → RC4 → Key1
IV1 (24 Bit) →

2. Client berechnet

Response1 = Challenge1 XOR Key1

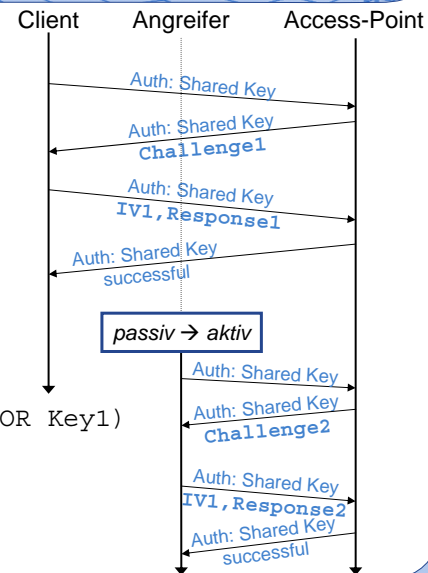
3. Angreifer erlauscht

Challenge1, IV1, Response1

4. Angreifer berechnet

Challenge1 XOR Response1
= Challenge1 XOR (Challenge1 XOR Key1)
= Key1

→ IV1 und Key1 sind gültige Kombination
Response2 = Challenge2 XOR Key1



4

• Vielzahl von Angriffen gegen WEP

- RC4 als Pseudozufallszahlengenerator mit schwachen IVs ungeeignet → viele **schwache Schlüssel**
- Kontrollnachrichten nicht authentifiziert → **DoS** möglich
- **Known-Plaintext-Angriffe** möglich (ARP, IP- und TCP-Header)

• Verbesserungen in WEP2

- Verlängerung des Schlüssels
 - ▶ WEP 40 (+24=64) Bit, WEP2 104 (+24=128) Bit
- Nutzung von 802.1x zur Authentifizierung
- Austausch von Session-Keys via 802.1x-Key-Nachrichten
- Kerberos-5-Support ist verpflichtend

• Verbleibende Probleme

- Kontrollnachrichten immer noch nicht authentifiziert
 - weiterhin Verwendung von RC4
- **WEP2 ebenfalls schon gebrochen**, da Probleme mit RC4 und schwachen IVs weiterhin bestehen

5

- Lang andauerndes Problem
 - Standardisierungsprozess von 802.11i sehr langwierig
 - Kernfunktionalität fix und WEP inzwischen vollständig gebrochen
- Lösung
 - WiFi-Allianz definiert **WiFi Protected Access** (WPA) Profil
 - Nutzung neuer, verbesserter Algorithmen von 802.11i
 - ▶ Verbesserte Verschlüsselung: **Temporal Key Integrity Protocol** (TKIP)
 - ▶ Verbesserter Authentizitätsschutz: **Michael**
 - anwendbar auf herkömmlicher WEP-Hardware!
- Inzwischen
 - 802.11i verabschiedet und deutlich sicherer als WPA und WEP
 - ▶ TU Darmstadt: *Breaking 104 bit WEP in less than 60 seconds*, 2007
 - WPA2 ist Profil für volle Sicherheit (z.B. Nutzung von AES-CCM verpflichtend)

6

•Erik Tews and Ralf-Philipp Weinmann and Andrei Pyshkin : „Breaking 104 bit WEP in less than 60 seconds“, 2007

•<http://eprint.iacr.org/2007/120.pdf>

•<http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>

•<http://www.heise.de/newsticker/meldung/87874>

- **Authentifizierung**: Handshake über EAPoL/802.1x mit beidseitiger Authentifikation (z.B. EAP-TLS)
- Neues Modell zum Schlüsselmanagement
 1. **Client und AS** erzeugen Hauptschlüssel (**Master Key**)
 2. Individueller Hauptschlüssel (**Pairwise Master Key, PMK**) für **Client** und **AP**. Transport zum **AP** via RADIUS
 3. **Client, AP**: 4-teiliger EAPoL-Key-Austausch erzeugt aus **PMK** temporären Schlüssel (**Pairwise Transient Key, PTK**)
 4. Aufspaltung des **PTK** in Unterschlüssel
 - ▶ **Data Encryption Key, Data MIC Key**
 - ▶ **EAPoL Encryption Key**
 5. **AP** sendet Client einen mit **EAPoL Encryption Key** verschlüsselten temporären Gruppenschlüssel (**Group Transient Key, GTK**)
 - ▶ **Group Encryption Key**
 - ▶ **Group Integrity Key**

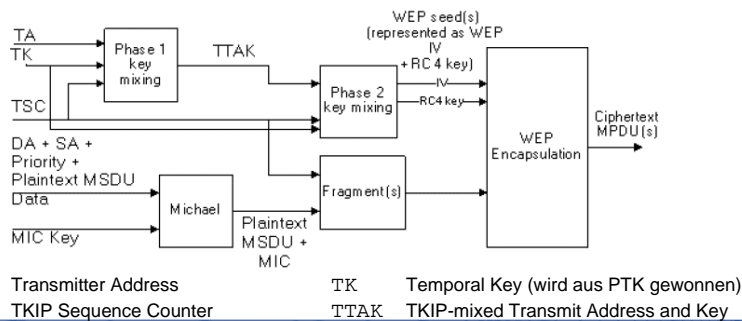
7

•Die Gruppenschlüssel werden für Broadcast und Multicast benötigt.

•EAPoL MIC Key dient zum Schutz des Austauschs neuer Schlüssel

802.11i Draft 3 / WPA

- Temporal Key Integrity Protocol
 - verwendet MAC-Adresse und zusätzlichen Schlüssel um per Mixing weiteren Zufall in RC4-Eingabe zu Erzeugen
- Michael
 - sehr einfaches Verfahren zur Integritätssicherung von Daten
 - kann ohne Änderungen auf WEP-Hardware laufen



8

Netzicherheit – Architekturen und Protokolle

Infrastruktursicherheit

•Ablauf WPA:

•Key-Mixing:

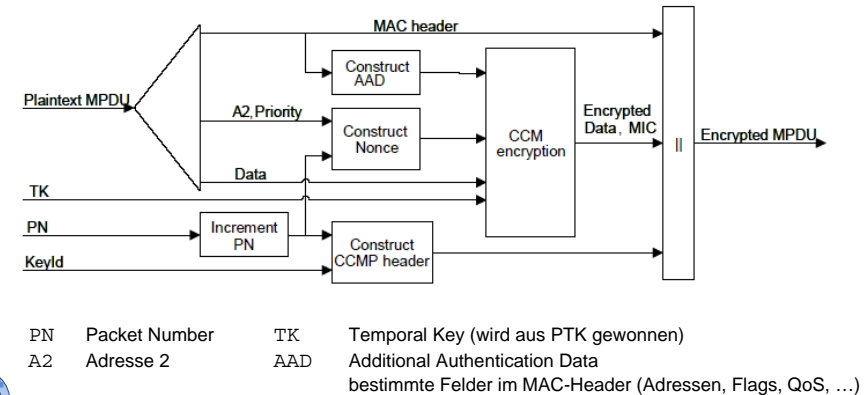
- Aus Transmitter Adresse (TA), Schlüssel (TK) und TKIP Sequenznummer (TSC) werden mit Phase 1 „gemischt“. Das Ergebnis nennt man TTAk.
- Aus TTAk, Schlüssel (TK) und TKIP Sequenznummer (TSC) wird nun ein Initialisierungsvektor und RC4-Schlüssel für WEP generiert.

•Integritätsschutz:

- Parallel hierzu wurden Zieladresse (DA), Quelladresse (SA), Priorität, MSDU und Daten mittels „Michael“ (MIC Key als Schlüssel) geschützt.
- Die Ausgabe von Michael (Plaintext, MSDU und Message Integrity Code (MIC)) werden nur mit der TKIP Sequenznummer verbunden und an das ursprüngliche WEP übermittelt.
- Michael ist ein sehr einfaches Verfahren. Es soll auch auf alter WEP-Hardware ohne Änderungen funktionieren und kann auf einem sehr einfachen Prozessor ausgeführt werden.
- WPA wurde in 802.11i Draft 3 (einem sehr frühen Draft) standardisiert.

802.11i final / WPA2

- zusätzlich AES-CCM
- Verschlüsselung und Authentifizierung mit AES



9

Netzicherheit – Architekturen und Protokolle

Infrastruktursicherheit

•Ablauf 802.11i

- Der MAC-Header wird durchgereicht, get aber in die Konstruktion des Additional Authentication Data (AAD) ein
- 802.11i Paketnummer (PN) und Paketfelder (A2, Priority) ergeben eine Nonce
- AAD, Nonce, Daten und dem Temporal Key (TK) werden an
- WPA2 (oder auch RSN) wurde im endgültigen Standard festgeschrieben und ist somit empfehlenswerter als WPA (802.11 Draft 3).

	WPA PSK Modus	WPA (Enterprise) Modus	WPA2 Personal Mode	WPA2 Enterprise Mode
Optionale Algorithmen	AES-CCM	AES-CCM	TKIP + Michael	TKIP + Michael
Verpflichtende Algorithmen	TKIP + Michael	TKIP + Michael	AES-CCM	AES-CCM
Authentifikation	Passwort	802.1x	Passwort	802.1x

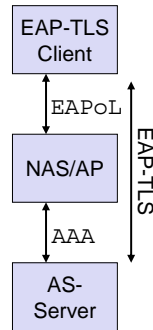
•PSK: Pre Shared Key

Probleme von EAPoL/802.1x bei Nutzung in WLAN

- **Passive Angriffe** einfacher möglich
 - Identitäten beim initialen Austausch können mitgehört werden
- **Aktive Angriffe** einfach möglich
 - Man-in-the-Middle-Angriff während Authentifikation, da Server nicht authentifiziert wird
 - Spoofen von Frames möglich, z.B. End-of-Session bei EAPoL
 - EAP-Success/Failure-Nachrichten ungeschützt
- daher
 - **Authentifizierung und Verschlüsselung von EAP notwendig**
 - Schlüsselmaterial für Authentifizierung/Verschlüsselung der Nutzdaten auf Link-Layer notwendig
 - häufiges Wechseln von NASen führt zu häufigem Authentifizieren
 - Mechanismus für schnelle Re-Authentifizierung notwendig

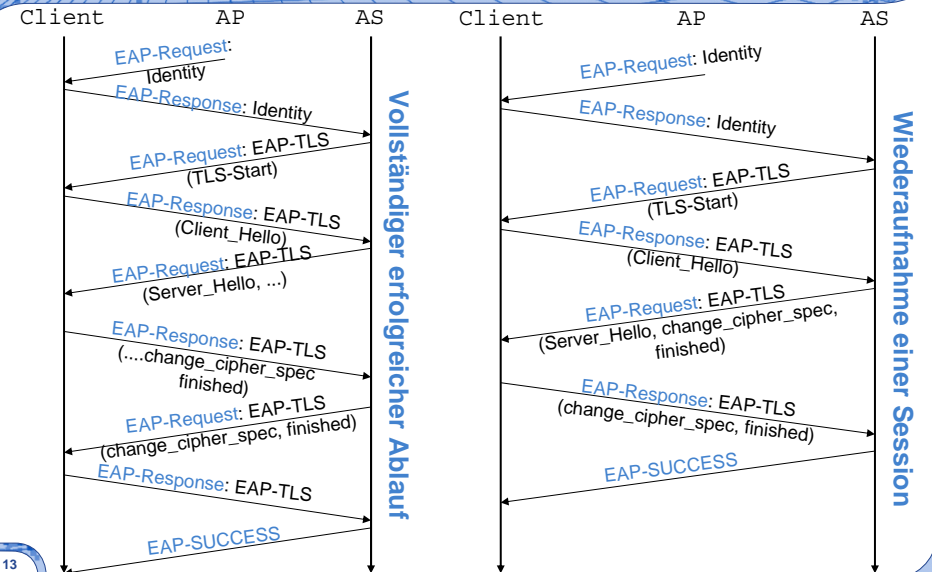
EAP-TLS

- Authentifizierung *beider* Kommunikationspartner
- Aushandlung einer Cipher-Suite
- Vorteile
 - Nutzung eines bewährten und geprüften Protokolls
 - Wiederaufnahme einer Session möglich
- Nachteile
 - Fragmentierung notwendig, falls TLS-Records zu lang
 - Authentifizierung des Clients über Zertifikate
 - Identitäten werden unverschlüsselt übertragen
 - Validierung des Serverzertifikates u.U. nicht möglich



12

•EAP-TLS ist in RFC2716 definiert



13

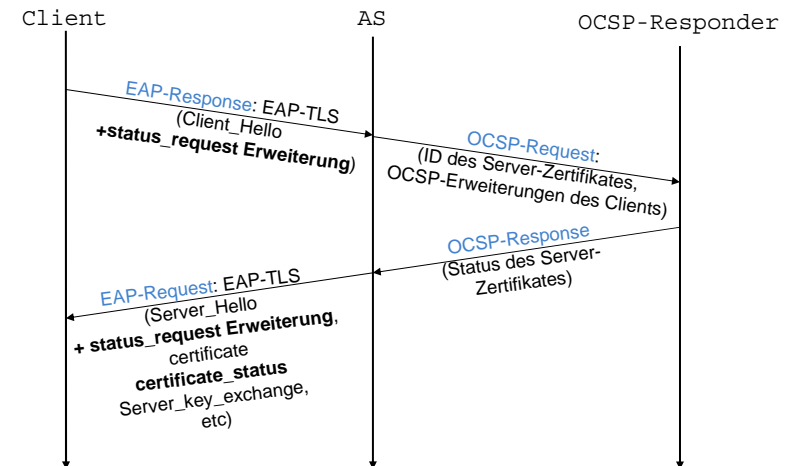
Problem: Clients im Fall von 802.1x haben keine IP-Konnektivität
 → Statusüberprüfung für Serverzertifikate nicht möglich

Transport Layer Security Extensions

- Client kann vom Server OCSP-Bestätigung verlangen
- Client sendet erweitertes Client_Hello mit Erweiterung status_request mit akzeptablen OCSP-Respondern
- Wenn Server Erweiterung unterstützt
 - Weiterleitung der OCSP-Anfrage an OCSP-Responder mit vom Client mitgeschickten OCSP-Erweiterungen (z.B. Nonce)
 - Antworten mit Server_Hello-Nachricht mit Erweiterung status_request als Indikation dafür, dass Erweiterung bekannt
 - Senden der Antwort des OCSP-Responders (Certificate_Status)

14

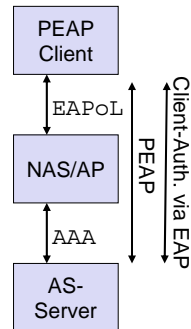
- OCSP: Online Certification Status Protocol. Siehe auch Kapitel PKI.
- Transport Layer Security (TLS) Extensions [RFC 4366]



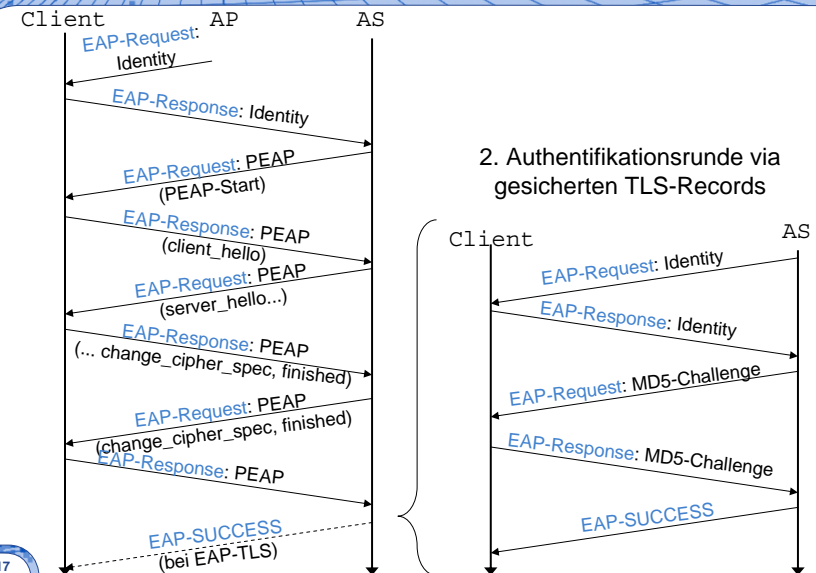
15

Protected EAP (PEAP)

- adressiert Probleme von EAP-TLS
- besteht aus 2 Phasen
 - Phase 1: Aufbau TLS-Verbindung (Client anonym)
 - Phase 2: geschützte Authentifizierung mit EAP
- Wiederaufnahme von Session ohne Phase 2
- Nachteile von PEAP
 - keine Aushandlung von Parametern für Sicherungsschicht
 - Client kann u.U. Server-Zertifikat nicht validieren
 - Umkopieren von AS Daten von EAP nach AAA bei Roaming



16



17

- Protected EAP (PEAP [draft-josefsson-pppext-eap-tls-eap-10.txt / abgelaufen])

Adressierte EAP-TLS-Probleme:

Authentifikation von Clients über Zertifikate nicht immer sinnvoll/möglich
Identitäten werden nicht geschützt

Besteht aus 2 Phasen

wie EAP-TLS, Authentifikation des Clients allerdings optional
zweite Authentifikationsrunde mit „normalem EAP“ über sicheren Kanal

Bei Wiederaufnahme einer Session entfällt Phase 2

Bei gescheiterter Phase 2 muss die TLS-Session gelöscht werden, damit keine Wiederaufnahme möglich ist

Interessante Nutzung:

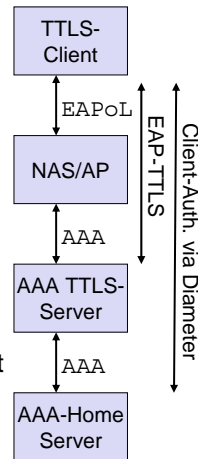
Client-Rechner authentifiziert sich über Zertifikat in Phase 1 (Rechner Authentifizierung)

Nutzer authentifiziert sich in Phase 2 (Nutzer Authentifizierung)

Kontrollfrage: In welchen Anwendungsfällen würde man das nutzen?

EAP Tunneled TLS Authentication Protocol

- 2 Phasen, gleiche Motivation wie PEAP, aber weitergehend
- in Phase 2 auch nicht-EAP-Mechanismen von PPP (z.B. CHAP)
- Unterschiede zu PEAP
 - Authentifizierung des Clients syntaktisch in Form von Diameter-PDUs
 - ▶ somit einfaches Weiterleiten der Authentifikationsdaten bei Roaming (kein Umsetzen von EAP nach Diameter)
 - Aushandlung von Algorithmen zur Sicherungsschicht zwischen Client und AP/NAS
 - Erzeugung und Verteilung von Schlüsselmateriale zur Sicherung des Link-Layers zwischen Client und NAS/AP



- EAP Tunneled TLS Authentication Protocol (EAP-TTLS [draft-funk-eap-ttls-v1-05.txt])

Ebenfalls 2 Phasen

Ablauf wie EAP-TLS, Authentifikation des Clients allerdings optional
Nutzung der über TLS ausgehandelten Algorithmen und Schlüsseln zum Schutz einer zweiten Authentifizierungsrunde, in der der Client authentifiziert wird der Verteilung weiterer Daten, z.B. von Schlüsselmateriale für Schicht 2

LEAP

- Cisco Light EAP
- unsicher
 - Passwörter nur mittels MS-CHAP geschützt
 - schwache Passwörter können gefunden werden (<http://asleap.sourceforge.net>)

EAP-FAST

- Nachfolger von LEAP: soll einfach wie LEAP und sicher wie PEAP sein
- basiert auf 2-Phasen-Ansatz
 - zuerst sicheren Tunnel aufbauen
 - dann MS-CHAP oder ähnliches für Passwortüberprüfung

EAP-SIM

- EAP mit GSM-Authentifizierung (SIM-Karte)

EAP-AKA

- EAP mit UMTS-Authentifizierung

EAP-IKEv2

- EAP mit IKEv2-Authentifizierung (Password, Preshared Key, Zertifikate, ...)

- EAP-FAST, RFC4851
- EAP-SIM, RFC4186
- EAP-AKA, RFC4187
- EAP-IKEv2, RFC5106

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



1. Motivation
2. Der Weg ins Internet
3. Überblick

4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung



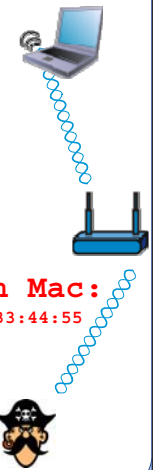
Protected Management Frames

IEEE 802.11w Protected Management Frames

MAC:
00:11:22:33:44:55

- Problem
 - Bisher nur Rahmen mit Nutzdaten geschützt
 - Management-Rahmen ungeschützt
 - Angriffe
 - DoS-Angriffe gegen Clients
 - ▶ z.B. Deauthentication-Flooding
 - neu aufkommende Funktionalität transportiert sensitive Daten in Management Frames
 - ▶ Fast Handoff, Radio Ressource Management, Wireless Network Management, ...
- Schutz von Management Frames notwendig

Deauth Mac:
00:11:22:33:44:55



21

Netzicherheit – Architekturen und Protokolle

Infrastruktursicherheit

Institut für Telematik www.tm.kit.edu
Karlsruher Institut für Technologie (KIT)



• Mit einer gefälschten Deauthentication-Nachricht kann ein Angreifer ein Opfer vom AP abmelden. Macht er dies mehrfach in sehr kurzen Abständen, ist keine (stabile) Kommunikation für das Opfer mehr möglich. Man spricht vom Deauthentication-Flooding. Man bemerke, dass die Anmeldung (Authentication) aufwändiger als die gefälschte Abmeldung (Deauthentication). Diese Angriffe sind auch bei WPA und WPA2/802.11i möglich.

• Deauthentication-Flooding ist nur ein Beispiel für Angriff mit Hilfe gefälschter Management-Nachrichten.

- 802.11w fügt wichtigen Management-Rahmen einen Message Integrity Code (MIC) hinzu
 - Disassociation, Deauthentication, Action
 - Schutz vor Fälschung
- für **Unicast** Management-Rahmen wird das bisherige AES-CCMP-Verfahren genutzt
 - paarweise Schlüssel sind notwendig
 - TKIP wird nicht unterstützt
- **Multicast/Broadcast** Management-Rahmen werden wie mit AES-128-CMAC geschützt
 - AES-128-CMAC authentifiziert Daten mit Hilfe der AES-CBC Verschlüsselungsfunktion
 - Gruppenschlüssel

22

• Für den Schutz des unicast Management-Rahmen kann das bisher eingesetzte AES-CCMP (WPA2) eingesetzt werden, da eine Schlüsselhierarchie und somit paarweise Schlüssel ausgehandelt werden. Da gilt nicht für WEP-40, WEP-104 und TKIP, da diese im Gegensatz zu AES-CCMP auf gemeinsame Geheimnisse aufsetzen.

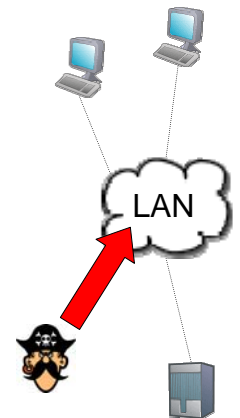
• Der Schutz von broadcast/multicast Management-Rahmen kann nicht mit Hilfe paarweise Schlüssel erfolgen, da sonst fast alle Empfänger die Authentizität der Rahmen nicht prüfen können. Hierfür musste ein neues Verfahren entwickelt werden. In IEEE 802.11w D4.0 wird AES-128-CMAC [vgl. RFC 4493] hierfür vorgeschlagen. AES-CMAC basiert auf AES-MAC, vermeidet allerdings die Schwächen vom AES-MAC für Nachrichten mit beliebiger Länge, ähnlich wie AES-XCBC.

• Siehe auch

• Morris Dworkin: „NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication“

• http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

- **Angriffe auf drahtgebundene Netze** noch möglich (z.B. Ethernet)
- 802.1X löst nicht alle Probleme
- man hätte gerne noch
 - Geheimhaltung
 - Authentizität
 - Schutz vor Wiederholungsangriffen
 - Schutz vor DoS-Angriffen
- und volle Ethernet-Geschwindigkeit (z.B. 10 Gbit/s) soll erhalten werden



23

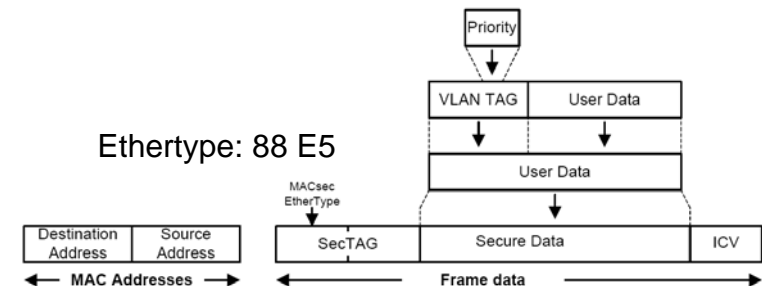
- IEEE 802.1AE-2006 spezifiziert MACsec
- MACsec bietet (laut Standard)
 - Datenintegrität (Schutz gegen Veränderung)
 - Datenauthentifizierung (Herkunftsschutz)
 - Geheimhaltung (durch Verschlüsselung)
 - Wiederholungsschutz
 - Verzögerungsschutz
- Und damit
 - Schutz gegen Denial-of-Service
 - Aber **keine** Nicht-Abstreitbarkeit
 - Und **kein** Schutz gegen Verkehrsanalyse

24

•IEEE 802.1AE-2006: „IEEE Standard for Local and Metropolitan Area Networks-Media Access Control (MAC) Security“, http://ieeexplore.ieee.org/xpls/abs_all.jsp?tp=&isnumber=35305&arnumber=1678345&punumber=11085

•Soll nicht für IEEE 802.11 verwendet werden, ersetzt also nicht 802.11i!

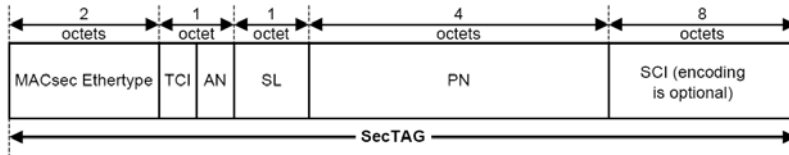
- MACsec wird mittels verändertem MAC-Rahmen implementiert
 - Vergleichbar mit VLAN-Tags



25

•IEEE 802.1AE-2006: „IEEE Standard for Local and Metropolitan Area Networks-Media Access Control (MAC) Security“, http://ieeexplore.ieee.org/xpls/abs_all.jsp?tp=&isnumber=35305&arnumber=1678345&punumber=11085

•Soll nicht für IEEE 802.11 verwendet werden, ersetzt also nicht 802.11i!



- **TAG Control Info (TCI)**
 - Version, Optionen, ...
- **Association Number (AN) [2 Bits]**
 - 4 verschiedene „SAs“ pro Security Channel
 - erlaubt einfaches Rekeying
 - Rahmen müssen nicht in Reihenfolge sein (beim Umschalten)
- **Short Length (SL)**
- **Packet Number (PN)**
- **Optional Secure Channel Identifier**
 - hiermit kann Multicast implementiert werden

26

- **Galois/Counter Mode (GCM) für AES 128**
 - Vergleichbar mit CCM-Operationsmodus
- **Aber was ist mit Broadcast/Multicast?**
 - Mit SCI-Feld realisierbar
 - Ethernet aber zumeist Punkt-zu-Punkt
- **Schlüsselaustausch?**
 - IEEE 802.1af (Erweiterung zu IEEE 802.1X)

27

Bücher

Security in Wireless LANs and MANs, Hardjono und Dondeti, 2005

→ sehr gutes Buch, 802.1X, Radius, PAP, CHAP, EAP-TLS, PEAP, EAP-TTLS, EAP-SIM, EAP-AKA, WEP, 802.11i

Real 802.11 Security, Edney und Arbaugh, 2004

→ sehr ausführliches Buch über 802.11i

802.11 Security, Potter und Fleck, 2002

→ kurzes gutes Buch, leider veraltet

Sichere Netzwerkkommunikation, Bless et al, 2005

→ kurz und prägnant dargestellt

Weitere Literatur

[Wha01]: S. Whalen, *An Introduction to ARP Spoofing*, 2001

<http://www.node99.org/projects/arpspoof/arpspoof.pdf>

J. Romkey; *A nonstandard for transmission of IP Datagrams over serial lines: SLIP*; RFC 1055; 1988

W. Simpson; *The Point-to-Point Protocol (PPP)*; RFC 1661; 1994

D. Rand; *The PPP Compression Protocol (CCP)*; RFC 1962; 1996

G. Meyer; *The PPP Encryption Protocol (ECP)*; RFC 1968; 1996

W. Simpson; *PPP Vendor Extensions*; RFC 2153; 1997

G. Zorn, S. Cobb; *Microsoft PPP CHAP Extension*; RFC 2433; 1998

L. Mamakos et al; *A Method for Transmitting PPP Over Ethernet (PPPoE)*; RFC 2516; 1999

B. Aboba, D. Simon; *PPP EAP TLS Authentication Protocol*; RFC 2716; 1999

G. Zorn; *Microsoft PPP CHAP Extension, Version 2*; RFC 2759; 2000

B. Aboba et al; *Extensible Authentication Protocol (EAP)*; RFC 3748; 2004

S. Blake/Wilson et al; *Transport Layer Security (TLS) Extensions*; RFC 4366; 2006

IEEE Standard: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; 802.11-1999; 1999

IEEE Standard: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Amendment 6: Medium Access Control (MAC) Security Enhancements*; 802.11i-2004; 2004

IEEE Standard: *Port-Based Network Access Control*; 802.1X-2004 (Revision to 802.1X-2001); 2004