Studienarbeit

Netzwerkauthentifizierung im WLAN

http://www.ibr.cs.tu-bs.de/arbeiten/schmidt/otto_eap.html

Braunschweig, 28. April 2004

Thomas Otto

Übersicht

1. Authentifizierung – Definition und Realisierung
2. Authentifizierung in IEEE 802.11
   (Open System, Shared Key)
3. Authentifizierung in IEEE 802.11 i

   IEEE 802.1x
   EAP
   Nachrichtenaustausch einer EAP Authentifizierung
   Vorstellung einiger EAP Methoden

   Trends

Fragen, Diskussion

Authentifizierung

Der Teilnehmer, ob Gerät oder Benutzer, hat einen Nachweis seiner angegebenen, behaupteten Identität zu erbringen.

In der Regel bedingt die Authentifizierung eine Authorisierung des Teilnehmers.

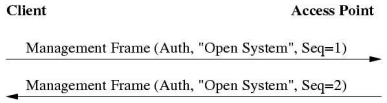
Unterscheide zwischen
- Benutzerauthentifizierung (peer authentication)
- Authentifizierung der Datenherkunft (data origin authentication).

Authentifizierung kann erfolgen durch

- Wissen (Benutzername / Passwort)
- Besitz (z.B. digitales Zertifikat, Smartcard, GSM SIM)
- Eigenschaft (biometrisches Merkmal, z.B. Fingerabdruck)

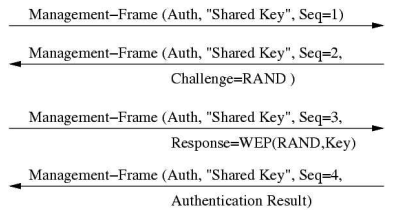
Authentifizierung in 802.11

Open System:



Ist ein Null-Algorithmus. Es findet keinerlei Überprüfung des Teilnehmers statt.

Shared Key:



Nach Aufzeichnung einer erfolgreich verlaufenen Authentifizierung kann sich ein Angreifer am System erfolgreich anmelden.

Shared Key Authentifizierung

Mit dem Challenge berechnet der Client

Challenge Response = Challenge XOR RC4 (IV, Key)

Der Schlüsselstrom ist also

RC4 (IV, Key) = Challenge Response XOR Challenge

Der 24bit Initialisierungsvektor IV wird vom **Client** gewählt.
Er wird im 802.11 Header im Klartext mitgeschickt.

Somit verwendet der Angreifer RC4 (IV, Key) einfach wieder,
kann eine korrekte Challenge Response bilden und
sich somit erfolgreich authentifizieren.

Vorher - Nachher

Prinzipielle Designfehler in IEEE 802.11:

- statisches Schlüsselmanagement, keine dynamische Schlüsselverteilung
- Verwendung von WEP optional
- ein (!) von allen Geräten geteilter Schlüssel; Verlust oder Aufdeckung führt zur Kompromittierung des gesamten WLANs
- nur Geräteauthentifizierung, keine Benutzerauthentifizierung

Verbesserungen in IEEE 802.11i:

- Verschlüsselung mit TKIP und CCMP(AES)
- Benutzerauthentifizierung mit IEEE 802.1x
- dynamische Schlüsselverteilung mit IEEE 802.1x
- Möglichkeit zur zentralen Benutzerverwaltung mit RADIUS

IEEE 802.1x

"Port-based Network Access Control"

Standard seit 2001. Ist zur Zeit noch in einer Überarbeitung, um in der gesamten IEEE 802 Architektur angewendet werden zu können.

Verwendung in Shared Media LANs muss berücksichtigt werden.

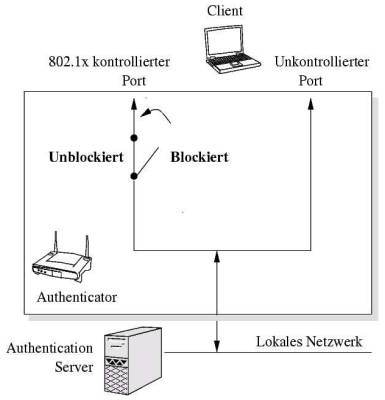
Die Spezifikation von 802.1x beschreibt

- ein Rahmenwerk für portbasierte Authentifizierung

Für den Transport von Authentifizierungsnachrichten ist EAP vorgesehen. Somit:

- EAP over LAN, Nachrichten und Paketformat

Portbasierte Zugangskontrolle



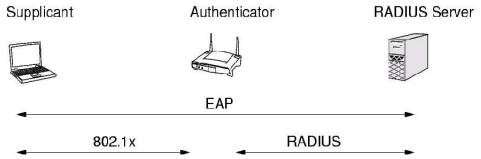
"Ports"

Zustände
- un-/ kontrolliert
- un-/ blockiert

3 Parteien

Supplicant
Authenticator
Authentication Server

802.1x, EAP und RADIUS



Die Authentifizierung findet zwischen Client und RADIUS Server statt.

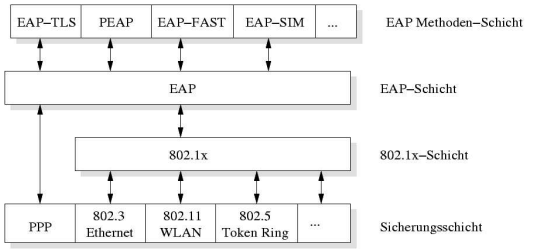
Der Access Point dient lediglich als Proxy:

Vom Client empfangene EAP Nachrichten in RADIUS bzw.
vom RADIUS Server empfangene EAP Nachrichten in 802.1x EAPOL kapseln und entsprechend weiterleiten.

Extensible Authentication Protocol (EAP)

März 1998: RFC 2284 " PPP Extensible Authentication Protocol (EAP)"

Februar 2004: Überarbeitung RFC 2284-bis09 als Proposed Standard angenommen.

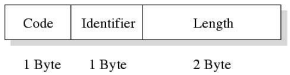


EAP Paketformat und Nachrichten

Allgemeines EAP-Paketformat

Der Typ des EAP Pakets wird durch das Code Feld angegeben:

1: EAP-Request
2: EAP-Response



3: EAP-Success
4: Failure

EAP-Request, Response: Typen

http://www.iana.org/assignments/eap-numbers

1 Identity
2 Notification
3 Legacy Nak

1-3: Spezialtypen

4 MD5-Challenge
5 One-Time Password (OTP)
6 Generic Token Card (GTC)
7 Allocated
8 Allocated

4-45: z.Zt. reservierte EAP Typen

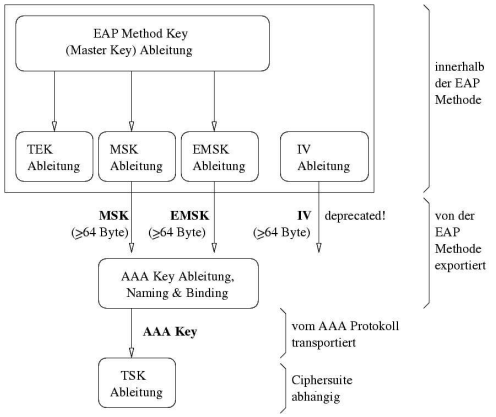
46-253, 254/x: noch verfügbar

..

13 EAP-TLS [Aboba]
17 EAP-Cisco Wireless *(aka LEAP)* [Norman]
18 Nokia IP smart card authentication (*aka EAP-SIM*) [Haverinen]

21 EAP-TTLS [Funk]
25 PEAP [Palekar]
43 EAP-FAST [Cam-Winget]

EAP – Keying framework



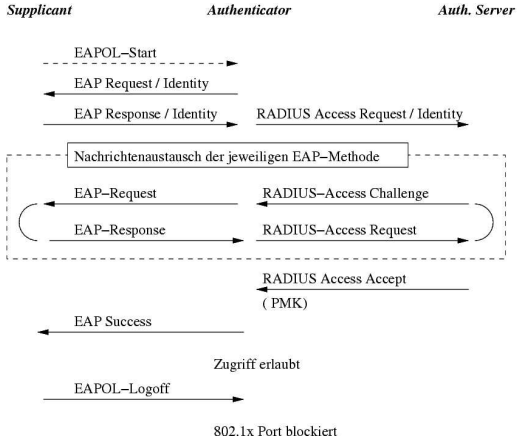
Bedingung an eine EAP Methode:

Export von 64 Byte Schlüsselmaterial, sog. **AAA Key**

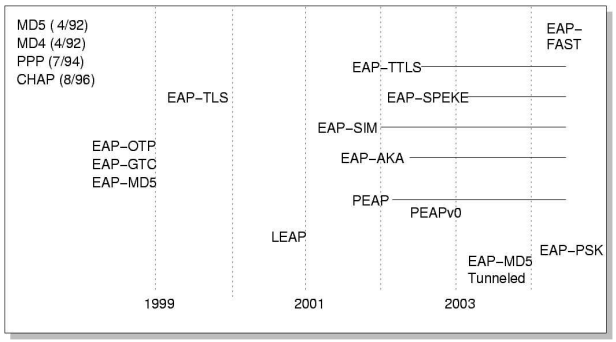
Dieser dient zur Ableitung kurzlebigen Schlüsselmaterials, z.B. des 64 Byte

Pairwise Master Key (PMK)

EAP – Nachrichtenaustausch



EAP Methoden



Anforderungen an das Design

Internet-Draft “EAP Method Requirements for Wireless LANs”, draft-walker-ieee802-req-01.txt, 31.03.04

Verpflichtende Eigenschaften:

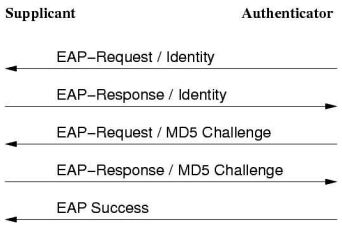
(V1) Generierung des Export-Schlüsselmaterials

(V2) Gegenseitige Authentifizierung

(V3) Schutz vor Man-in-the-Middle Angriffen

(V4) Resistenz gegen Wörterbuch Angriffe

EAP-MD5



EAP-MD5 ist in RFC 2284 (Jahr: 1998) definiert.

Ist äquivalent zu PPP-CHAP

einfaches Challenge Response Verfahren

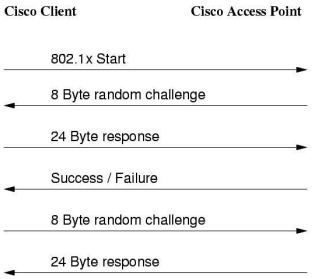
Dennoch: EAP-MD5 ist **ungeeignet** für einen Einsatz in WLAN.

Erfüllt die formalen Anforderungen nicht, z.B.
- keine Generierung des geforderten Schlüsselmaterials.
- keine gegenseitige Authentifizierung.

Client überprüft nicht die Gegenseite => “rogue” AP als MitM !

Cisco LEAP

- 2001 von Cisco Systems entwickelt
- proprietäres Protokoll, Spezifikation nicht öffentlich
- passwortbasiert (baut auf MS-CHAPv2 auf)



Vorteil zu EAP-MD5: Gegenseitige Authentifizierung.

Nachteil: Möglicher brute-force Wörterbuchangriff.

Cisco schlägt als Gegenmaßnahme die Wahl eines “starken Passworts” vor.

Weak LEAP

Beispiele für **Starke Passwörter** (Quelle: Cisco)

4yosc10cP!	for your own safety choose 10 character Password!
cnw84FriDAY	cannot wait for Friday

Beispiel für einen erfolgreichen Wörterbuchangriff

./leap-cracker <Wörterbuch>, <8 Byte Challenge>, <24 Byte Ch. Response>

```
# ./leap-cracker -f wordlist.txt \
        -t 5b79dab8bf72ed434ebca8a784466bffb28f6e94280c918d \
        -c afe811f2ae948bdb

DES1: 5b79dab8bf72ed43
DES2: 4ebca8a784466bff
DES3: b28f6e94280c918d

Matching Password = [blamo]
```

Voraussetzung: Passwort kommt im Wörterbuch *wordlist.txt* vor.

EAP-TLS

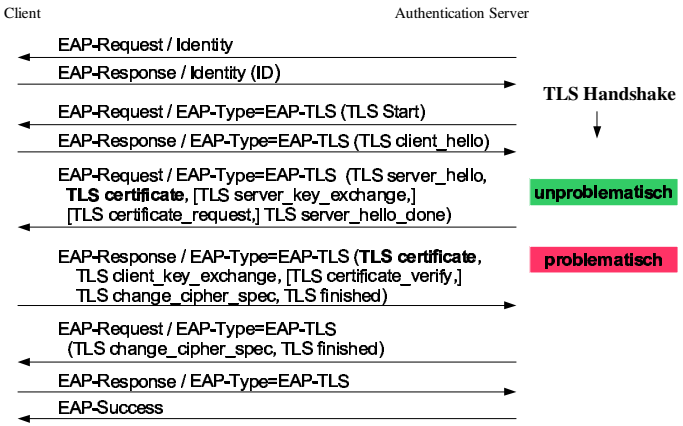
- 1999 von Microsoft entwickelt, RFC 2716
- Beschreibung, wie TLS (RFC 2246) in EAP gekapselt wird

- basiert auf client- und serverseitigen Zertifikaten
- erfüllt alle Bedingungen an eine EAP Methode im Wireless Umfeld

Nachteile:

1. Erfordert Aufbau einer Public Key Struktur (PKI), d.h. hohe Komplexität.
2. Problem der Zustellung des Credentials – vgl. Hotspot Umgebungen von WISPs.
3. Die Authentifizierungsverhandlung findet (fast) vollständig unverschlüsselt statt.

Beispiel EAP-TLS



Client Zertifikat

TLS Record Layer: Certificate

```
0000  16 03 01 07 0a 0b 00 07 06 00 07 03 00 03 97 30   ...............0
0010  82 03 93 30 82 02 fc a0 03 02 01 02 02 01 01 30   ...0...........0
0020  0d 06 09 2a 86 48 86 f7 0d 01 01 04 05 00 30 81   ...*.H........0.
0030  83 31 0b 30 09 06 03 55 04 06 13 02 44 45 31 16   .1.0...U....DE1.
0040  30 14 06 03 55 04 08 13 0d 4e 69 65 64 65 72 73   0...U....Nieders
0050  61 63 68 73 65 6e 31 15 30 13 06 03 55 04 07 13   achsen1.0...U...
0060  0c 42 72 61 75 6e 73 63 68 77 65 69 67 31 18 30   .Braunschweig1.0
0070  16 06 03 55 04 0a 13 0f 54 55 20 42 72 61 75 6e   ...U....TU Braun
0080  73 63 68 77 65 69 67 31 0b 30 09 06 03 55 04 03   schweig1.0...U..
0090  13 02 43 41 31 1e 30 1c 06 09 2a 86 48 86 f7 0d   ..CA1.0...*.H...
00a0  01 09 01 16 0f 74 2e 6f 74 74 6f 40 74 75 2d 62   .....t.otto@tu-b
00b0  73 2e 64 65 30 1e 17 0d 30 34 30 32 30 31 31 38   s.de0...04020118
00c0  35 36 35 36 5a 17 0d 30 36 31 30 32 38 31 38 35   5656Z..061028185
00d0  36 35 36 5a 30 81 87 31 0b 30 09 06 03 55 04 06   656Z0..1.0...U..
00e0  13 02 44 45 31 16 30 14 06 03 55 04 08 13 0d 4e   ..DE1.0...U....N
00f0  69 65 64 65 72 73 61 63 68 73 65 6e 31 15 30 13   iedersachsen1.0.
0100  06 03 55 04 07 13 0c 42 72 61 75 6e 73 63 68 77   ..U....Braunschw
0110  65 69 67 31 18 30 16 06 03 55 04 0a 13 0f 54 55   eig1.0...U....TU
0120  20 42 72 61 75 6e 73 63 68 77 65 69 67 31 0f 30    Braunschweig1.0
0130  0d 06 03 55 04 03 13 06 74 68 6f 6d 61 73 31 1e   ...U....thomas1.
0140  30 1c 06 09 2a 86 48 86 f7 0d 01 09 01 16 0f 74   0...*.H.......t
0150  2e 6f 74 74 6f 40 74 75 2d 62 73 2e 64 65 30 81   .otto@tu-bs.de0.
```

Ausweg: Getunnelte EAP Methoden

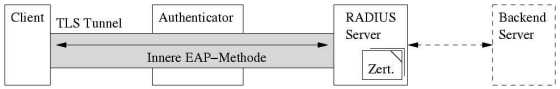
Vertreter: PEAPv2, EAP-TTLS und EAP-FAST.

Prinzip:
- Nur der Server ist mit einem Zertifikat ausgestattet.
- TLS Handshake wie bei EAP-TLS.

- Clientauthentifizierung erfolgt im TLS Tunnel.

- Das hierzu verwendete Verfahren kann in der Regel eine beliebige EAP Methode sein.

Insbesondere passwortbasierte Verfahren werden präferiert.
Grund: einfache Handhabung



Ausblick (Trends)

Als Designziele an eine EAP Methode sind anzusehen:

- Einfachheit in der Einrichtung, hohe Flexibilität und gute Skalierung

z.B. als Credential ein Hardware Token (GSM SIM, Smartcard)
=> keine Interaktion mit Benutzer nötig oder passwortbasierte Verfahren

- Einfachheit in der Anwendung für den Benutzer

- geringer Rechenbedarf (wg. beschränkten CPU und Energiereserven)

z.B. durch symmetrische kryptographische Verfahren: Benötigen gemeinsamen Schlüssel

bei größtmöglicher Sicherheit.

Sehr aussichtsreich insgesamt:
PEAPv2
EAP-FAST
EAP-PSK (als Vertreter)

An dieser Stelle soll die Präsentation
beendet und zur Diskussion übergegangen
werden.

Ich danke für das Interesse und
die Aufmerksamkeit.

Fragen?