RADIUS und (W)Lan

- Überblick zu RADIUS und Geschichte
  - Was macht man damit?
  - PAP, CHAP und anderes
- EAP und (W)Lan
- EAP in RADIUS
- Und die Praxis

RADIUS Geschichte

"Remote Authentication Dial In User Service"

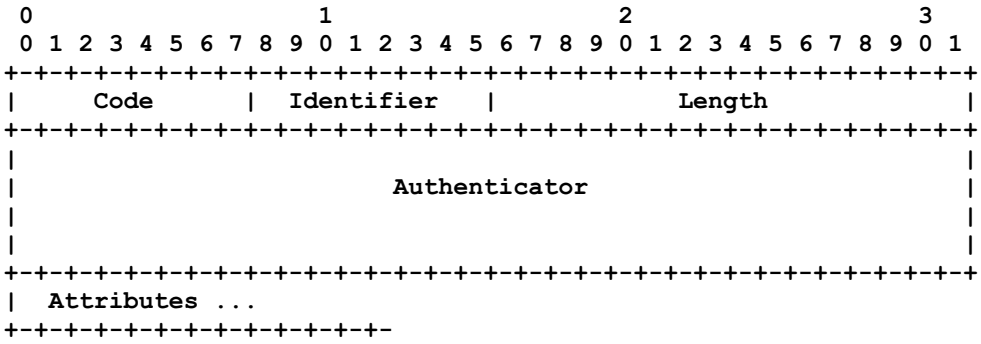
- IETF BoF: April 1995, RFC 2058: Januar 1997
- Authentisierung, Authorisierung, Accounting
- Weit verbreitet bei ISPs und Firmennetzen
- Eigentlich ein 'alter Hut' ?

Übrigens: RADIUS wurde von Livingston für die "Portmaster" entwickelt - für den ISDN- und Modemzugang in Erlangen nutzt der KNF u.a. ein solches Gerät.

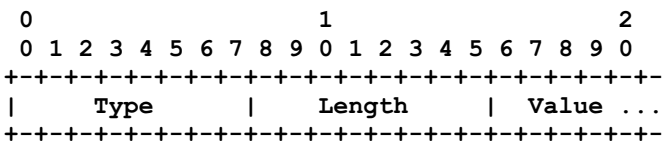
Eigenschaften von RADIUS

- Flexibel durch Type-Length-Value Tupel (TLVs)
- UDP-basiert, effizient, schnelles fail-over

Header:



Ein Attribut:



Typischer Ablauf

	Client		Server
1	Access-Request	== PAP ==>	
2		<=======	Access-Accept / Deny
3	Accounting-Request	== start ==>	
4		<=======	Accounting-Response
		... Nutzer ist aktiv ...	
5	Accounting-Request	== stop ==>	
6		<=======	Accounting-Response

Ein Nutzer im Detail

Access-Request

```
User-Password = "a.\0x19\0x8c1\0x01\0x10\0x80\0xd1wS\0xd5<Q5l"
User-Name = "052879@brt"
Acct-Session-Id = "erx fastEthernet 0/0:0005746287"
Service-Type = Framed
Framed-Protocol = PPP
Pppoe-Description = "pppoe 00:50:fc:6e:77:3a"
Calling-Station-Id = "#cyclops#E00#65535"
NAS-Port-Type = 15
NAS-Port = 65535
NAS-Port-Id = "fastEthernet 0/0"
NAS-IP-Address = 10.227.6.243
NAS-Identifier = "cyclops"
```

Access-Accept

```
Pppoe-Description = "pppoe 00:50:fc:6d:22:ee"
Filter-Id = "unlim"
Service-Type = Framed
Framed-Protocol = PPP
Framed-IP-Netmask = 255.255.255.255
Framed-Routing = None
Framed-MTU = 1500
Framed-Compression = Van-Jacobson-TCP-IP
```

Ein Nutzer im Detail

Accounting-Request

```
Acct-Status-Type = Stop
User-Name = "049757@brt"
Event-Time = "Nov 23 2003"
Acct-Delay-Time = 0
NAS-Identifier = "cyclops"
Acct-Session-Id = "erx fastEthernet 1/0:0005732470"
NAS-IP-Address = 10.227.6.243
Service-Type = Framed
Framed-Protocol = PPP
Framed-Compression = None
Pppoe-Description = "pppoe 00:50:fc:6d:22:ee"
Framed-IP-Address = 192.168.75.41
Framed-IP-Netmask = 255.255.255.255
Ingress-Policy-Name = "unlim"
Calling-Station-Id = "#cyclops#E10#65535"
Acct-Input-Gigawords = 0
Acct-Input-Octets = 6880
Acct-Output-Gigawords = 0
Acct-Output-Octets = 6458
Input-Gigapkts = 0
Acct-Input-Packets = 0
Output-Gigapkts = 0
Acct-Output-Packets = 50
NAS-Port-Type = 15
NAS-Port = 268500991
NAS-Port-Id = "fastEthernet 1/0"
Acct-Authentic = RADIUS
Acct-Session-Time = 5090
Acct-Terminate-Cause = User-Request
```

PAP & CHAP

- PAP und CHAP transportieren nur Passwörter
  - Passwort muss nicht fest sein

- Passwörter alleine reichen nicht mehr
- Andere Verfahren brauchen andere Daten
  - Public-Key, SIM-Karte

EAP

- PPP Extensible Authentication Protocol (EAP)
  RFC 2284, erschienen 1998
- EAP ist ein Transportprotokoll für eine erweiterbare Menge von Authentisierungs-"Types"
- EAP selbst verfügt über keine Sicherungs-mechanismen - die Methoden ("Types") müssen das mitbringen.
- Beispiele: MD5 (CHAP-equivalent), EAP-SIM

802.1x / EAPoL

- “EAP over LAN” ist die Basis für Authentisierung in WPA und 802.1x
- Im (W)Lan sind EAP-Pakete angreifbar, daher eine Tendenz zu ‘tunnelnden’ EAP-Typen:
  - EAP-TLS, EAP-TTLS, EAP-LEAP, EAP-PEAP

Methoden im Vergleich

LEAP - Nur Cisco (stimmt nicht mehr ganz)

EAP-TLS + Sehr sicher; schon länger verfügbar
(RFC2716, experimental)
- braucht Client Zertifikat; identity leak

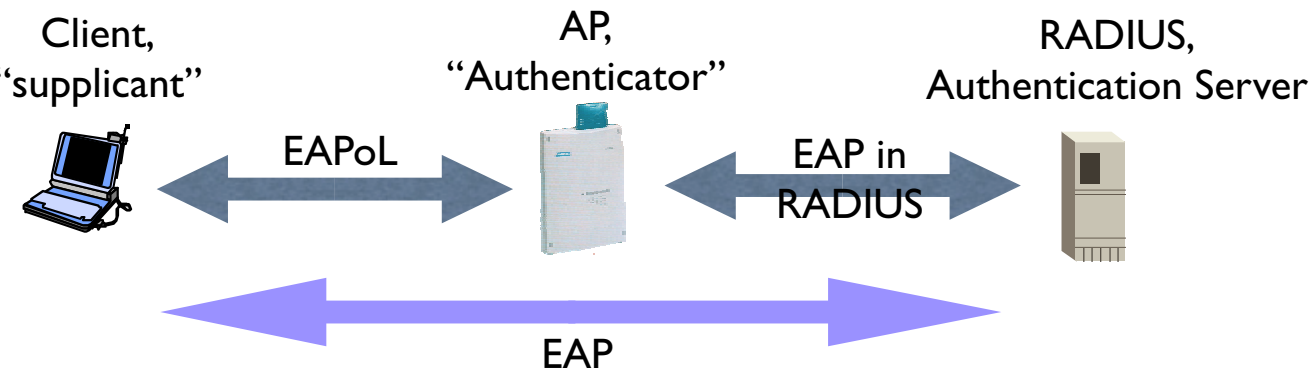
PEAP + sicher; nur Server braucht Zertifikat;
+ weit verbreitet (Microsoft, Cisco ...)
- MitM Angriff

EAP-TTLS + Ähnlich PEAP
- MitM; weniger weit verbreitet (?)

EAP in RADIUS

- September 2003:
  - RFC 3579: RADIUS Support for EAP
  - RFC 3580: IEEE 802.1x RADIUS Usage Guidelines
- EAP in Radius
  - EAP Nachrichten werden im neuen “EAP-Message” Attribut verschickt. Lange Nachrichten werde in mehrere Attribute fragmentiert.
  - Laengerer EAP-Dialog wird in Access-Request und Access-Challenge messages transportiert.

Ablauf



- Der AP kann die EAP Pakete ‘unbesehen’ durchreichen, muss nur auf EAP success/failure erkennen.
- Extra Parameter (keys) werden in RADIUS übertragen
- **Der AP braucht EAP-Methoden nicht zu verstehen!**

Beispiel: PEAP

RADIUS+EAP braucht i.A. mehr Roundtrips als PAP/CHAP

No.	Time	Source	Destination	Protocol	Info
1	0.000000	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=137)
2	0.031375	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=76)
3	0.209390	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=224)
4	0.261982	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=1476)
5	0.278185	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=150)
6	0.279207	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=1476)
7	0.287397	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=150)
8	0.288299	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=1476)
9	0.304529	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=150)
10	0.305369	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=724)
11	0.381073	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=343)
12	0.391028	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=123)
13	0.406328	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=150)
14	0.407334	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=98)
15	0.412073	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=184)
16	0.413873	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=124)
17	0.454134	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=238)
18	0.468072	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=240)
19	0.473072	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=173)
20	0.474511	RServer	WPA_AP	RADIUS	Access challenge(11) (id=1, l=108)
21	0.489438	WPA_AP	RServer	RADIUS	Access Request(1) (id=1, l=182)
22	0.492903	RServer	WPA_AP	RADIUS	Access Accept(2) (id=1, l=264)

In der Praxis - I

- Alle WPA-fähigen APs sprechen RADIUS
- Einige RADIUS server können EAP:
  - Microsoft (Server 2003), FreeRADIUS, Funk, Cisco, Interlink - nicht viel in OpenSource, es werden sicher bald noch mehr.
  - Nicht alle Server beherrschen alle EAP Typen
- Die meisten WPA clients ('supplicants') beherrschen nur wenige EAP typen.

In der Praxis - II

- WPA und RADIUS aufzusetzen ist momentan noch recht aufwendig.
- Für den Hausgebrauch reicht auch WPA mit pre-shared key.
- Diskussionen um die beste EAP Methode sind noch im Gange. PEAP scheint der Favorit, da einfacher einzusetzen und weit unterstuetzt (XP).
- Verbreitung könnte etwas dauern, da ältere WLan-Karten nicht WPA-fähig sind.

Ende

- Vielen Dank für die Aufmerksamkeit.
- Gibt es Fragen?

Martin Bokaemper
EMail: mnbokaem@pizza.franken.de

Literatur und Links:

- RADIUS, Jonathan Hassel, O'Reilly 2002
- The Alphabet Soup of EAP types
  http://www.intel.com/support/network/wireless/seceap.htm
- FreeRADIUS: http://www.freeradius.org/