

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



1. Motivation
2. Der Weg ins Internet
3. Überblick
4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung



Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



1. Motivation
2. Der Weg ins Internet
3. Überblick
4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung

nächste VL



- Welche **Zugangsmöglichkeiten** zum Internet?
 - DSL, Modem, ISDN, DUKATH, Ethernet, Satellit,



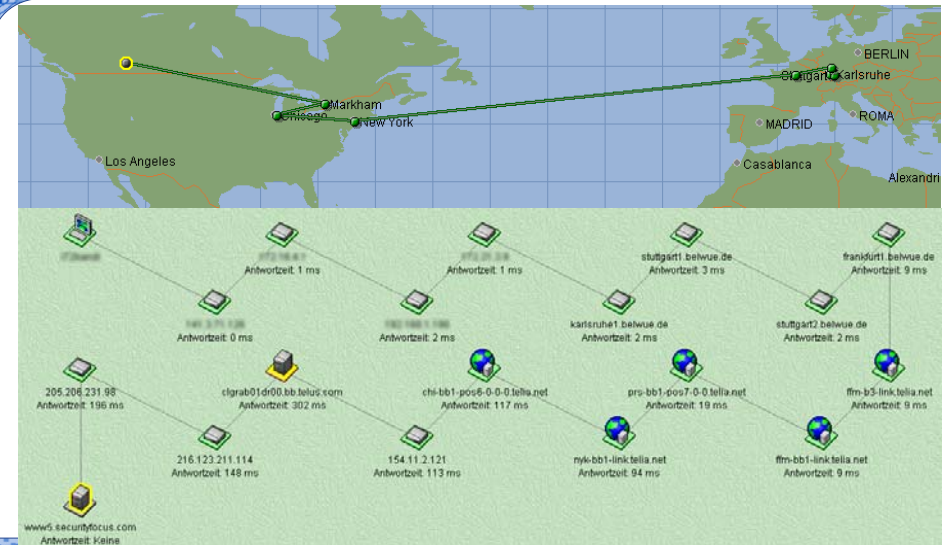
- Wie geht es *im Netz* weiter?

- **> traceroute www.securityfocus.com**
 - ▶ Daten laufen über mehrere Netzwerke (17 Hops)
 - ▶ BelWue (4 Hops), Telia (5 Hops), Telus, ...
 - ▶ 3 Hops ohne DNS Eintrag



- Schutzbedarf

- wie kann der **Zugang zum Internet** geschützt werden?
- ... und im Netz **Schutz der Infrastruktur**!?



- Beispiel **Netzinfrastruktur: Router**
 - Autorisierung über Passwort im Klartext (z.B. Telnet oder Weboberfläche über HTTP)
 - was kann ein Angreifer tun?
 - ▶ Passwort mitschneiden und sich selbst anmelden
- Beispiel **Netzzugang: WLAN**
 - ungesicherter WLAN-Zugang noch weit verbreitet
 - ▶ wir sicher ist denn ein LAN-Zugang?
 - was kann ein Angreifer tun?
 - ▶ über ARP-Spoofing allen Verkehr mitschneiden und Passwörter mitlesen
 - wie kann man sich schützen?
 - ▶ Mechanismen zur Verschlüsselung (WEP,WPA)
 - ▶ bis zu welchem Punkt schützen diese?

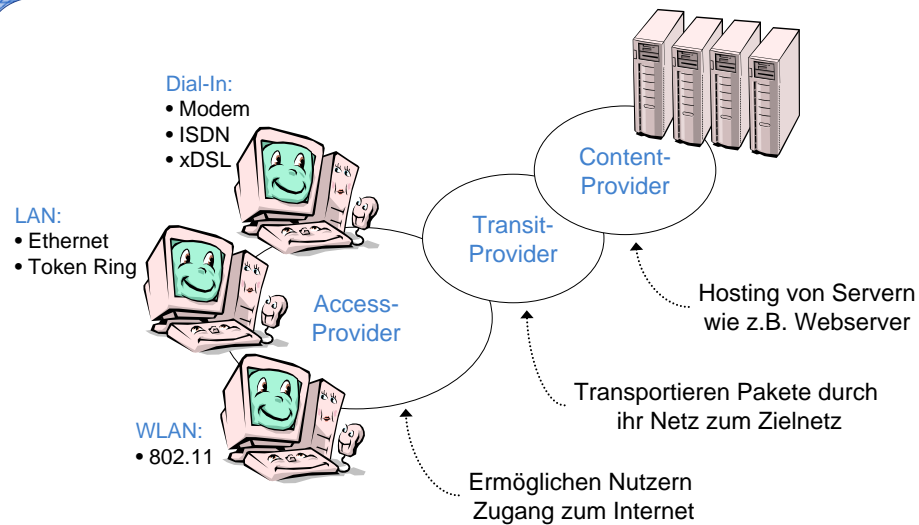
Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



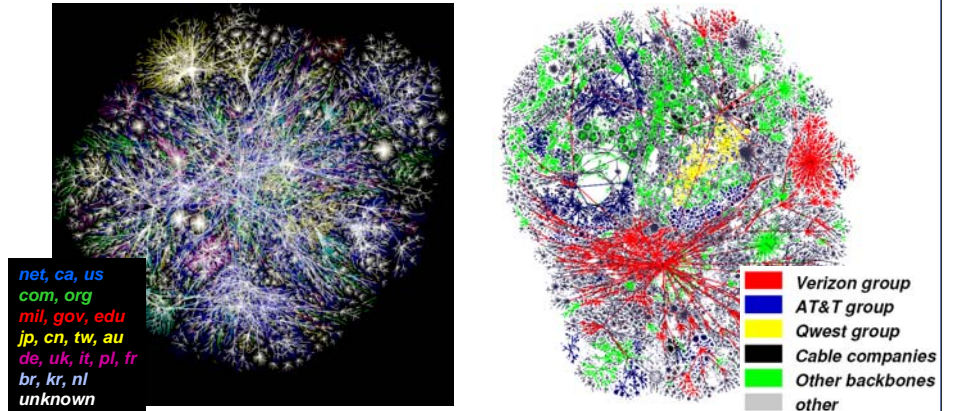
1. Motivation
2. Der Weg ins Internet
3. Überblick

4. Netzzugang
5. Drahtloser Netzzugang
6. Aktuelle Entwicklung





- Viele Zugänge, viele Provider, viele Netze, ...
→ überall **Sicherheitsmechanismen** notwendig



<http://www.opte.org/maps>

http://advice.cio.com/themes/CIO.com/cache/Internet_map_labels_0.pdf

•Linkes Bild

- zeigt die Struktur des Internet

- Farben entsprechen Domainendungen: blau (net, ca, us), grün (com, org), rot (mil, gov, edu), gelb (jp, cn, tw, au) (siehe <http://www.opte.org/maps/>)

•Das rechte Bild zeigt die Struktur mit zugehörigem Provider

- Jeder Farbe stellt dabei einen anderen Provider dar

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit

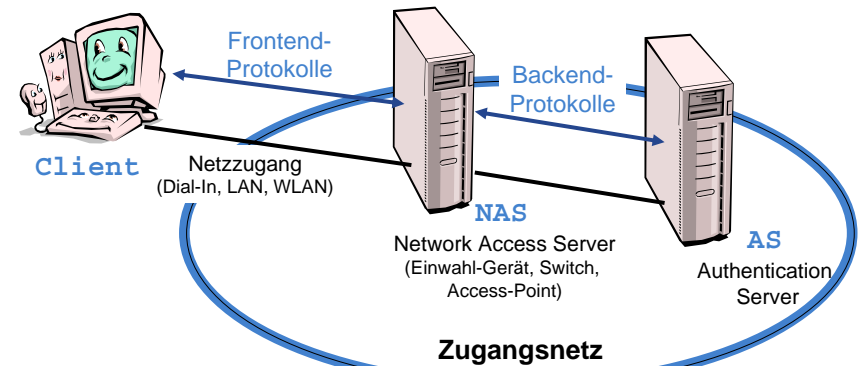


- | | |
|-------------------------|--------------------------|
| 1. Motivation | 4. Netzzugang |
| 2. Der Weg ins Internet | 5. Drahtloser Netzzugang |
| 3. Überblick | 6. Aktuelle Entwicklung |



Überblick

- Protokolle zur **Zugangskontrolle**
 - **Frontend-Protokolle**: zwischen **Client** und **NAS**
 - **Backend-Protokolle**: zwischen **NAS** und **AS**



- Der NAS kann z.B. ein Switch sein, dann wird über die Ports des Switches die Zugangskontrolle realisiert, da Ports gesperrt und freigeschalten werden können
- Zu Beginn soll der Client nur mit dem AS sprechen können und nicht mit dem lokalen Netz, welches am NAS hängt. Dies wird techn. realisiert, da Ports an einem Switch zwei logische Ausgänge haben. Standardmäßig ist dann nur der Port zum AS freigeschaltet und der Port zum lokalen Netz gesperrt
- Es wird von einer Punkt-zu-Punkt Verbindung zwischen Client und NAS ausgegangen.
- Nach erfolgreicher Authentifizierung wird der Port zum lokalen Netz freigeschaltet. Der AS kann jedoch den Client jederzeit erneut um Authentifizierung fragen, falls diese schiefgeht, wird der Port zum lokalen Netz wieder gesperrt. Der Port wird auch immer dann automatisch deaktiviert, wenn das Kabel gezogen wurde. Somit kann ein Angreifer nicht einen bereits freigeschalteten Port verwenden

- **Frontend-Protokolle:** *Kommunikation zwischen Endbenutzer und Netzwerkzugangsserver*
 - für Punkt-zu-Punkt Verbindungen: SLIP, PPP
 - für LAN: PPPoE, EAPoL (802.1x)
 - für WLAN: WEP (802.11), EAPoL (802.1x), WPA/WPA2 (802.11i)
- **Backend-Protokolle:** *Kommunikation zwischen Netzwerkzugangsserver und Authentifikationsserver*
 - auch AAA-Protokolle genannt (Authentifikation, Autorisierung, Accounting)
 - RADIUS
 - TACACS+
 - Diameter (Nachfolger von RADIUS)

Netzicherheit – Architekturen und Protokolle Infrastruktursicherheit



- | | |
|-------------------------|--------------------------|
| 1. Motivation | 4. Netzzugang |
| 2. Der Weg ins Internet | 5. Drahtloser Netzzugang |
| 3. Überblick | 6. Aktuelle Entwicklung |



- **RADIUS**

- Zugriffsschutz für Netzwerkressourcen
- Authentication, Authorization, Accounting (AAA)

- **PPP**

- Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
- **PAP, CHAP**: Einfache Authentifizierung
- **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung

- **PPPoE**

- Ethernet Verbindungen über xDSL

- **802.1x**

- Port-basierte Authentifizierung von Endgeräten

Backend

Frontend

12

- **RADIUS**

- Zugriffsschutz für Netzwerkressourcen
- Authentication, Authorization, Accounting (AAA)

- **PPP**

- Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
- **PAP, CHAP**: Einfache Authentifizierung
- **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung

- **PPPoE**

- Ethernet Verbindungen über xDSL

- **802.1x**

- Port-basierte Authentifizierung von Endgeräten

13

- Früher: Speicherung von Authentifikationsdaten auf **NAS**
 - Replizierung bei mehreren NAS Zugangspunkten
 - **Sicherheit der Authentifikationsdaten**
- Heute: Auslagerung auf **AS**
 - Protokoll zur Kommunikation zwischen NAS und AS notwendig

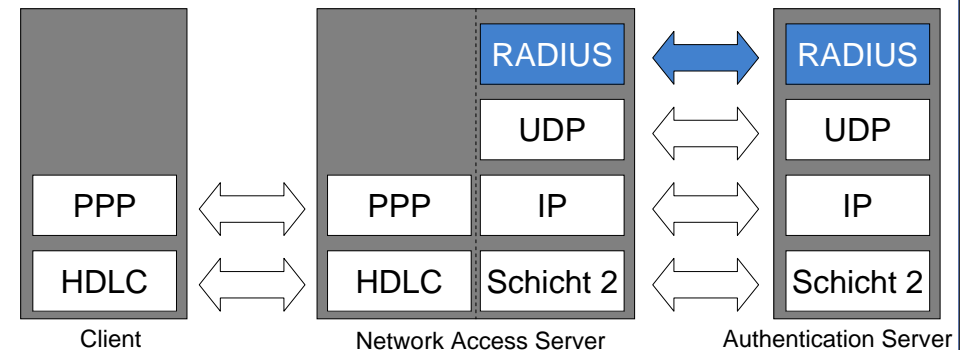
RADIUS: *Remote Authentication Dial In User Service*

- **Backend-Protokoll** zum Transport von Daten zur
 - Authentifikation, Autorisation, Konfiguration des Einwahlbenutzers zwischen **NAS** und **AS**
- Einsatz bei
 - Modem-/ISDN-Einwahlserver, DSL-Zugangsserver
 - anderen Servern wie z.B. Netzwerkinfrastruktur
 - *Uni Karlsruhe DUKATH: RADIUS + IPSec*

14

•RFC 2865 und 2866

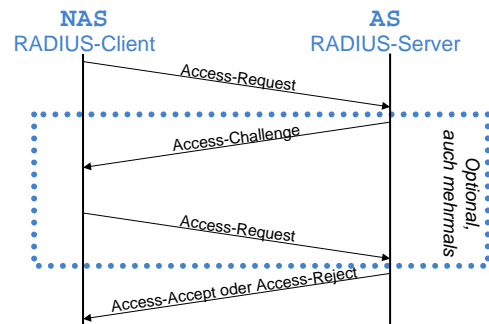
- Radius
 - arbeitet auf Anwendungsschicht über UDP
 - nur zwischen NAS und AS, Client nicht beteiligt



15

Rollen bei RADIUS

- **NAS** ist Client
 - transportiert Authentifikationsdaten aus Frontend-Protokoll zwischen Einwahlbenutzer und **AS**
- **AS** ist Server
 - authentifiziert Benutzer direkt oder
 - leitet Daten als Proxy zu einem anderen **AS** weiter (→ *Roaming*)



16

Protokollablauf:

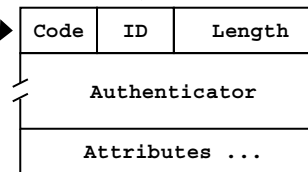
- Client sendet Authentifikationsanfrage
- Server sendet optional eine Challenge
- Client leitet Challenge an Benutzer weiter,
antwortet mit Antwort des Benutzers
- Evtl. weitere Challenges
- Server akzeptiert Anfrage (und sendet evtl.
Konfigurationsdaten für Benutzer oder NAS
mit) oder lehnt ab

Art des RADIUS
Pakets

Identifikator zum Matching
von Reply auf Request

Länge des Paktes
incl. Attributen

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 11 Access-Challenge
- ...



Authentifizierung
von Paketen

Beliebige Anzahl an
Attributen der Form:

- 1 User-Name
- 2 User-Passwort
- 3 CHAP-Passwort
- ...

Type	Length	Value
------	--------	-------

17

Schutz der Integrität von Nachrichten

• Request-Authenticator

- Pakete mit Code **Access-Request**
- Client wählt 16 Byte lange Zufallszahl

• Response-Authenticator

- Pakete mit Code **Access-Challenge**, **Access-Accept** und **Access-Reject**
- Anwendung von **MD5 auf Paket und Schlüssel**

```
MD5 (  Code +  ID +  Length      +
      RequestAuthenticator      +
      Attribute + Schlüssel      )
```

18

• Geschützte Übertragung von Attributen

→ z.B. **Benutzerpasswort** (Typ 2 **User-Password**)

• Verschlüsselung von Attributen

- Partitionierung d. Attributs in 16-Byte-Blöcke p_1, \dots, p_n
- 16 Byte langer Schlüssel S
- Berechnung: **Stromchiffre mit MD5 als PRF**

$$\begin{aligned}
 c_1 &= p_1 \text{ xor MD5}(S + \text{RequestAuth}) \\
 c_2 &= p_2 \text{ xor MD5}(S + c_1) \\
 &\dots \\
 c_i &= p_i \text{ xor MD5}(S + c_{i-1})
 \end{aligned}$$

• Übertragung von c_1, \dots, c_i an Stelle von p_1, \dots, p_i

19

Zusammenfassung RADIUS

Angriffspunkte? Was muss geschützt werden? Wie wurde dies realisiert?

- **Authentizität** des Kommunikationspartners
 - Preshared Keys und MD5
 - **Authenticator**-Feld im RADIUS-Paket
- **Vertraulichkeit** der Authentifikationsdaten
 - Verschlüsselung sensibler Daten
 - *hidden attributes* mit Hilfe des Preshared Keys und MD5
- Schutz vor **Wiederholungsangriffen**
 - Verwendung von Zufallszahlen
 - **ID**-Feld im RADIUS-Paket

20

- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication, Authorization, Accounting (AAA)
- **PPP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
 - **PAP, CHAP**: Einfache Authentifizierung
 - **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

Backend

Frontend

21

- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication, Authorization, Accounting (AAA)
- **PPP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
 - **PAP, CHAP**: Einfache Authentifizierung
 - **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

- Punkt-zu-Punkt-Verbindungen (**Point-to-Point**, PtP)
 - **Frontend-Protokolle** zum Verbinden von zwei Geräten
 - Übertragen Daten meist seriell
 - Übertragungsrichtungen parallel nutzbar (full duplex)
- Zwei typische Anwendungsszenarien
 - Dynamisch: **Einwahl** (z.B. ISDN, DSL)
 - Statisch: **WAN-Verbindungen** zwischen Routern (z.B. PDH/SDH)

- WAN-Verbindungen sind meist permanent und statisch (z.B. bei SDH/PDH), so dass wenig Bedarf an Zugangskontrollmechanismen besteht.
- Anders jedoch Einwahl-Verbindungen über das Telefonnetz, die temporär sind und wechselnde Endpunkte auf Client-Seite haben; hier haben sich die meisten Zugangskontrollmechanismen entwickelt.

Point-to-Point Protokoll (PPP) – Protokoll für PtP-Verbindungen

Erweiterungen

- Compression Control Protocol (CCP)
- Encryption Control Protocol (ECP)

Schicht 3-Konfiguration

- Initialisierung und Konfiguration von Schicht-3-Protokollen
- Network Configuration Protocol (**NCP**)

Schicht 2-Konfiguration

- Aufbau u. Test von Schicht-2-Verbindungen
- Link Configuration Protocol (**LCP**)

Protokollmultiplexing

- Multiplexing von Schicht-3-Protokollen

Optionsaushandlung: Kern von PPP

- Erweiterbarer Mechanismus zur Aushandlung von Optionen
- Aushandlung in beide Richtungen individuell

Compression Control Protocol (CCP), RFC1962

Encryption Control Protocol (ECP), RFC1968

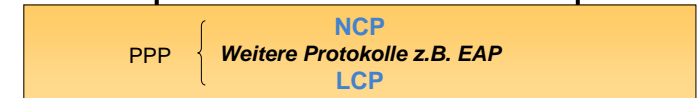
Schicht 3 Netzwerkschicht

Schicht-3-Instanz 1
z.B. IP

...

Schicht-3-Instanz n
z.B. IPX

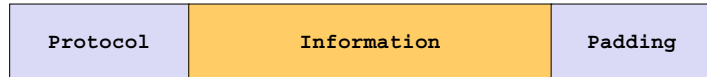
NCPs: Initialisierung und Konfiguration



LCP: Verbindungsaufbau,
Test und Überwachung

Schicht 2 Sicherheitsschicht

Schicht-2-Instanz
z.B. HDLC, Ethernet, AAL5



- **Protocol:**
 - 8 oder 16 Bit: Mechanismus für erweiterbare Adressfelder
 - **Identifiziert den Inhalt des Rahmens**, ermöglicht somit (De)-Multiplexing
- **Information:**
 - **Enthält Daten** des durch Protocol identifizierten Protokolls
 - Maximum Receive Unit (MRU): maximale Länge inkl. Padding (Default 1500 Bytes, andere Längen verhandelbar)
- **Padding:**
 - Optional beliebige Anzahl von Padding-Bytes (bis zur MRU)

26

- **Transport von PPP über Link-Layer-Protokolle**
 - HDLC (z.B. ISDN, SDH/SONET)
 - Ethernet
 - Frame-Relay
 - ATM-Adaption-Layer (AAL2, AAL5)

PPP in HDLC, z.B. PPP over SDH/SONET

Flag	Address	Protocol	PPP-Rahmen	FCS	Flag
01111110	11111111	00000011		16/32 Bits	01111110

PPP over Ethernet (PPPoE)

Destination	Source	EtherType	PPP-Rahmen	FCS
		=0x8864		

AAL5, z.B. LLC encapsulated PPP

LLC-Header	NLPID	PPP-Rahmen	Padding	CPCS-PDU
	=0xCF			Trailer

27

Link Configuration Protocol (LCP)

- Auf- und Abbau von Schicht-2-Verbindungen
 - Aushandlung von Optionen (Rahmenformat, max. Paketgröße)
 - Erkennung von Fehlern
 - ▶ z.B. Loop-back: gesendete Pakete werden wieder empfangen
- LCP verhandelt optional
 - Protokoll für Authentifikation des Kommunikationspartners
 - ▶ *Password Authentication Protocol* (PAP)
 - ▶ *Challenge Handshake Authentication Protocol* (CHAP)
 - ▶ *Extensible Authentication Protocol* (EAP)
 - Protokoll für Test und Überwachung der Qualität der Verbindung
 - ▶ *PPP Link Quality Monitoring*
 - Kompression

28

Behandelte Authentifikationsprotokolle für PPP

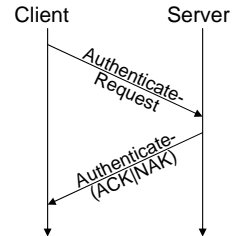
- Grundmechanismen (*diese VL*)
 - PAP: *Password Authentication Protocol*
 - CHAP: *Challenge Handshake Authentication Protocol*
 - EAP: *Extensible Authentication Protocol*
- für WLAN: EAP-Erweiterungen auf TLS (*nächste VL*)
 - EAP-TLS: *EAP Transport Layer Security*
 - PEAP: *Protected EAP*
 - EAP-TTLS: *EAP Tunneled TLS*

29

- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication, Authorization, Accounting (AAA)
- **PPP, LCP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
- **PAP, CHAP: Einfache Authentifizierung**
- **EAP, EAP-OTP: Generisches Protokoll zur Authentifizierung**
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

Password Authentication Protocol (PAP)

- **Ablauf**
 - Client schickt ID/Passwort-Paar
 - Server bestätigt oder beendet Verbindung
- **Schwächen**
 - **Übertragung des Passwort im Klartext**
 - ▶ Replay-Angriffe möglich
 - Client ist Initiator
 - ▶ kann Anfrage-Frequenz bestimmen
 - ▶ dadurch DoS-Angriffe möglich
 - beide Teilnehmer müssen das Passwort in Klartext kennen
- PAP nur **Notlösung**, wenn kein anderes Protokoll verhandelt werden konnte



•PAP [RFC 1334]

Challenge Handshake Authentication Protocol (CHAP)

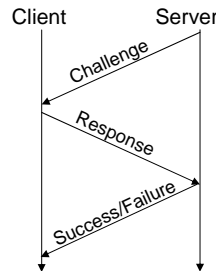
3-way Handshake

- Server schickt Challenge (Zufallszahl)
- Client sendet errechnete Response
 - ▶ z.B. MD5 (Challenge, Passwort)
- Server prüft Ergebnis, antwortet entsprechend

Vorteile von CHAP gegenüber PAP

- Passwort nicht im Klartext
- Replay-Angriff nicht möglich (bei guter Challenge)
- Server ist Initiator
 - ▶ kann Zeitpunkt und Frequenz der Anfragen bestimmen
 - ▶ legt bei Misserfolg Wiederholung fest
- Algorithmen wählbar: MD5, SHA-1, MS-CHAP

- **Nachteil:** auch hier muss **Passwort auf dem Server in Klartext** gespeichert werden



32

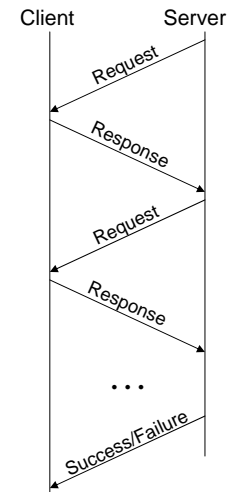
Extensible Authentication Protocol (EAP)

Generisches Protokoll zur Authentifizierung

- von LCP wie PAP/CHAP ausgehandelt
- tatsächlich verwendeter Mechanismus erst während der EAP-Protokoll-Phase ermittelt
- ermöglicht Einholen von weiteren Daten vor der Entscheidung für Mechanismus

Ablauf

- Server (eine oder mehrere) Anfragen an Client
 - ▶ z.B. Frage nach ID, Senden einer Challenge
- Client sendet angeforderte Daten zurück oder lehnt Anfrage ab (mit Gegenvorschlag)
- Server antwortet mit Erfolg/Misserfolg, wenn keine weiteren Fragen anstehen bzw. wenn Ergebnis der Authentifikation feststeht



33

EAP standardisierte Request/Response-Typen

- **Identity**
 - Ermittlung der ID des zu authentifizierenden Clients
 - meist erster Protokoll-Austausch
- **Notification**
 - Übertragung einer Nachricht an den Client, die bestätigt werden muss
 - z.B. Warnungen, dass Passwort bald erneuert werden muss
- **NAK** (nur als Antwort verwendbar)
 - Ablehnung einer Anfrage
- **MD5-Challenge** (wie CHAP aber mit folgenden Unterschieden)
 - enthält Gegenvorschlag
 - Client kann Mechanismus ablehnen (NAK), Gegenvorschlag machen
- **Generic Token Card**
 - wie CHAP, nur Hardware-basiert
- **One-Time Password** (OTP)
 - siehe nächste Folien

34

Code	ID	Length	Typ	Data
------	----	--------	-----	------

- **Code: Typ des Pakets**
 - 1 Request
 - 2 Response
 - 3 Success
 - 4 Failure
- **ID: ermöglicht Zuordnung von Antworten auf Anfragen**
- **Typ: Request/Response-Typ an**
 - z.B. 1=Identity

35

- One-Time Password (OTP)

- Verhindern von Replay-Angriffen durch Einmal-Passwörter
- Mechanismus erstmals von Leslie Lamport veröffentlicht (1981)
- Implementierung S/KEY diente als Grundlage für OTP

- Initialisierung

- Client vereinbart mit Server Passphrase, Seed, Hash-Algorithmus
- Client berechnet Einmal-Passwörter
 - $S_0 = \text{hash}(\text{Passphrase} + \text{Seed})$
 - $S_1 = \text{hash}(S_0)$
 - ...
 - $S_{n-1} = \text{hash}(S_{n-2})$
- Server berechnet S_n , speichert Paar $\{n, S_n\}$ und vergisst dann die Passphrase (!)

36

- OTP ist in RFC 2289 standardisiert

- S/KEY ist in RFC 1760 standardisiert

- Bei der Berechnung der Einmal-Passwörter wird der Hash auf 64 Bit abgeschnitten

Ablauf der Authentifikation

- Server schickt Client Challenge
 - $\{\text{Seed}, \text{Hash-Funktion}, n-1\}$
- Client sendet S_{n-1} zurück
- Server
 - Verifiziert $\text{hash}(S_{n-1}) \stackrel{?}{=} S_n$
 - Speichert Paar $\{n-1, S_{n-1}\}$ für nächste Authentifikation
 - wenn letztes Passwort S_0 benutzt wurde, neue Initialisierung

Darstellung des Einmal-Passworts

- Hexadezimal-kodiert (schwer zu merken)
- Six-Word-Format
 - 64 Bit durch Prüfbits auf 66 Bit erweitert und in 6x11 Bit unterteilt
 - 11 Bit dienen als Schlüssel in Wörterbuch mit 2048 Einträgen
 - Ergebnis-Beispiel: OUST COAT FOAL MUG BEAK TOTE

37

0 RESERVED	25 PEAP
1 Identity	26 MS-EAP-Authentication]
2 Notification	27 Mutual Authentication w/Key Exchange (MAKE)
3 Legacy Nak	28 CRYPTOCARD
4 MD5-Challenge	29 EAP-MSCHAP-V2
5 One-Time Password (OTP)	30 DynamID
6 Generic Token Card (GTC)	31 Rob EAP]
7 Allocated	32 Protected One-Time Password
8 Allocated	33 MS-Authentication-TLV
9 RSA Public Key Authentication	34 SentiNET
10 DSS Unilateral	35 EAP-Actiontec Wireless
11 KEA	36 Cogent Systems Biometrics Authentication EAP
12 KEA-VALIDATE	37 AirFortress EAP
13 EAP-TLS	38 EAP-HTTP Digest
14 Defender Token (AXENT)	39 SecureSuite EAP
15 RSA Security SecurID EAP	40 DeviceConnect EAP
16 Arcot Systems EAP	41 EAP-SPEKE
17 EAP-Cisco Wireless	42 EAP-MOBAC
18 GSM Subscriber Identity Modules (EAP-SIM)	43 EAP-FAST
19 SRP-SHA1	44 ZoneLabs EAP (ZLXEEP)
20 AVAILABLE	45 EAP-Link
21 EAP-TTLS	46 EAP-PAX
22 Remote Access Service	47 EAP-PSK
23 EAP-AKA Authentication	
24 EAP-3Com Wireless	

- Problem bei **RADIUS mit EAP**
 - **NAS** authentifiziert Client meist über PPP/EAP oder 802.1x/EAPoL
 - muss Daten zwischen EAP-Paketen und Radius-Attributen kopieren
- **RADIUS-Erweiterung**
 - neues RADIUS-Attribut
 - ▶ **EAP-Message**: Transport von EAP-Paketen zwischen Client und Server
 - EAP-Pakete können direkt zwischen PPP und RADIUS kopiert werden

- Erweiterung von RADIUS in RFC 2869 definiert

- RADIUS

- Zugriffsschutz für Netzwerkressourcen
- Authentication, Authorization, Accounting (AAA)

- PPP, LCP

- Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
- PAP, CHAP: Einfache Authentifizierung
- EAP, EAP-OTP: Generisches Protokoll zur Authentifizierung

- PPPoE

- Ethernet Verbindungen über xDSL

- 802.1x

- Port-basierte Authentifizierung von Endgeräten

40

Problem

- Ethernet als Anschlusstechnologie für Kundengeräte (*Customer Premises Equipment*) attraktiv
- aber: fehlende Funktionalität in Ethernet
 - ▶ Authentifikation, Aushandlung von Optionen, Accounting

Lösung: PPP over Ethernet (PPPoE)

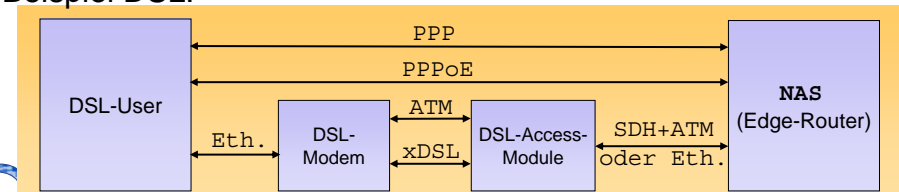
- Discovery Stage

- ▶ Client lokalisiert NAS und handelt mit NAS Session aus
- ▶ Client oder Server können jeder Zeit Session terminieren

- PPP Session Stage

- ▶ PPP-Rahmen werden in Ethernet-Rahmen übertragen

Beispiel DSL:

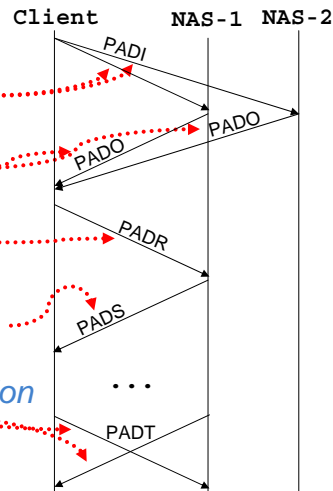


41

•PPPoE ist in RFC 2516 definiert

• Sitzungsaushandlung

- *PPPoE Active Discovery Initiation* (PADI)
- *PPPoE Active Discovery Offer* (PADO)
- *PPPoE Active Discovery Request* (PADR)
- *PPPoE Active Discovery Session-Confirmation* (PADS)
- *PPPoE Active Discovery Termination* (PADT)



42

- **PPPoE Active Discovery Initiation (PADI)**
 - Client broadcastet die Anfrage nach NASen
 - Rahmen mit EtherType 0x8863 = Discovery Stage
 - Rahmen enthält Spezifikation der Service-Anfrage (ISP-Name, CoS/QoS-Dienst)
- **PPPoE Active Discovery Offer (PADO)**
 - NASe antworten via Unicast an Client-MAC-Adresse, wenn sie den Dienst anbieten können
 - NAS kann als Vorbeugung gegen DoS-Angriffe den Zustand via Cookie mitschicken
 - Client lernt hierbei die MAC-Adresse der NASe
- **PPPoE Active Discovery Request (PADR)**
 - Client wählt einen NAS aus und fragt Session an
- **PPPoE Active Discovery Session-Confirmation (PADS)**
 - Server antwortet mit Session-ID
- **PPPoE Active Discovery Termination (PADT)**
 - Beendigung der Verbindung durch Client oder NAS

Ethernet-Rahmen
(Client-Server)

Destination	Source	EtherType	Payload	FCS
-------------	--------	-----------	---------	-----

wobei EtherType=0x8864

PPPoE-Rahmen

Version	Code	Session ID	PPP-Rahmen
---------	------	------------	------------

• Fazit

- Nutzung von PPP Mechanismen wie Authentifikation und Accounting
- einheitlicher Mechanismus beim Access-Provider für Einwahl und erleichtertes Management

• Aber:

- nicht sinnvoll im großen Stil
 - ▶ z.B. jeder Rechner in LAN-Segment baut PPPoE-Verbindung zu Gateway auf
- Portbasierte Authentifizierung: 802.1x

43

- **RADIUS**
 - Zugriffsschutz für Netzwerkressourcen
 - Authentication, Authorization, Accounting (AAA)
- **PPP, LCP**
 - Punkt-zu-Punkt Verbindungen (z.B. zur Einwahl)
 - **PAP, CHAP**: Einfache Authentifizierung
 - **EAP, EAP-OTP**: Generisches Protokoll zur Authentifizierung
- **PPPoE**
 - Ethernet Verbindungen über xDSL
- **802.1x**
 - Port-basierte Authentifizierung von Endgeräten

- Probleme
 - unautorisierte Nutzung ungenutzter Switch-Ports
 - Missbrauch schon genutzter Ports
- **802.1x: IEEE Standard for Local and metropolitan area networks – Port based Access Control**
 - Authentifizierung von Geräten, die über PtP-Verbindung angeschlossen werden (z.B. an dedizierten Switch-Port)
 - Freischaltung des Ports nach erfolgreicher Authentifikation
 - ▶ vorher nur Authentifikationsverkehr zugelassen
 - Reauthentifizierung
 - ▶ nach definierter Zeitspanne
 - ▶ wenn Port inaktiv wurde (z.B. durch Abziehen des Kabels)
- 802.1x verwendet EAP-Mechanismen von PPP
 - EAP direkt in Ethernet-Rahmen eingebettet
 - **EAP over LANs** (EAPoL)

- **Port Access Entities** (PAE, Teilnehmer des PtP-Links) nehmen folgende Rollen an
 - Client, als **Supplicant** bezeichnet, authentifiziert sich
 - NAS, als **Authenticator** bezeichnet, schaltet Port nach erfolgreicher Authentifikation frei
 - Beide Teilnehmer können bei Bedarf beide Rollen annehmen (z.B. Verbindung zwischen zwei Switches)
 - Prüfung der Authentifizierungsdaten durch NAS oder durch AS (z.B. via RADIUS)
- **Authentifizierung durch EAP-Protokoll**
 - Zwischen Client und NAS via Ethernet-Rahmen
 - Zwischen NAS und AS via Backend-Protokoll (z.B. RADIUS mit EAP-Erweiterung)

