IEEE 802.1X

Operating System Services and Administration Seminar

Summer Term 2008 @ HPI Potsdam
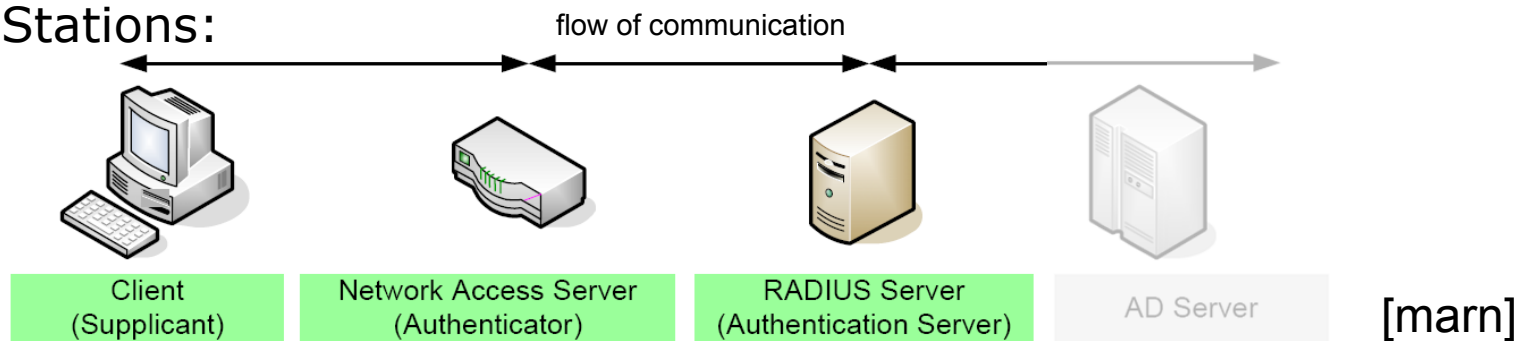
Stefan Lemme

Motivation: an Example

- Company / Institution / Organization
  - Network (LAN, WLAN)

  - WLAN used with WPA2-PSK
    - additional employee -> need PSK
    - Solution: individual authentication

  - LAN
    - physical access -> possible attack from within
    - generally authentication necessary

- developed by Microsoft, HP and 3com

- IEEE in June 2001

- most known in context with WLANs

- originally for LAN switches

- Stations:

flow of communication

| Client (Supplicant) | Network Access Server (Authenticator) | RADIUS Server (Authentication Server) | AD Server |

[marn]

- communication with client on LLC-Layer → no IP address required

- more than 40 authentication protocols possible

- most used protocol is EAP
  - □ Extensible Authentication Protocol
  - □ LEAP, EAP-FAST, EAP-MD5 (unsecure)
  - □ EAP-TLS
    - – Transport Layer Security
    - – based on certificates
  - □ PEAP
    - – Protected Extensible Authentication Protocol
    - – **PEAP-MSCHAP v2**
    - – PEAP-EAP-TLS
  - □ needs AAA server to work: e.g. RADIUS
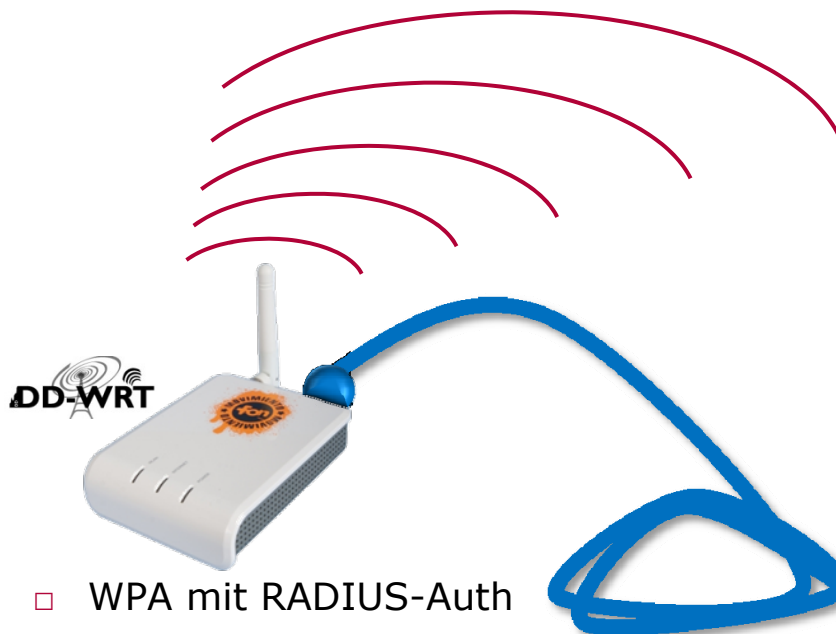
RADIUS Protocol

- **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice

- authentication, authorization and accounting (AAA server)

- 1997 published in RFC 2058 and RFC 2059

- RFC 2865, 2866, 2867, 2868, 2869

- implementations

  - Internet Authentication Service (Windows Server 2003)

  - Network Policy Server (Windows Server 2008)

  - freeRADIUS (platform independent)

  - Radiator (platform independent)

6

Windows XP SP1

Windows Server 2003 vmware

- □ Active Directory
- □ DHCP
- □ DNS
- □ CA
- □ IAS
- □ IIS

DD-WRT

- □ WPA mit RADIUS-Auth
- □ DHCP-Server

- **Windows Server 2003**
- **AD**
  - □ raise level to native
  - □ add group „WLAN-User"
  - □ add users with group membership
- **DNS**
- **DHCP**
- **CA**
  - □ install
  - □ create root certificate

- **IAS**
  - □ install
  - □ register in AD
  - □ define Friend Client
  - □ lay down Remote Access Policy

- **Fon-AP**
  - □ configure WPA with RADIUS-Auth and DHCP

Testing Environment: Basic Data

- SSID: lemmi-net
- Domain: lemmi-net
- Server: wrk-osm-dist.lemmi-net (212.176.8.1)
- Fon-AP: fonap.lemmi-net (212.176.8.2)
- Accounts:
  - Group: WLAN-User
  - user01@lemmi-net – test$01
  - user02@lemmi-net – test$02
  - user03@lemmi-net – test$03 (not a member of WLAN-User)
- http://wrk-osm-dist.lemmi-net
- mms://wrk-osm-dist.lemmi-net/myPublishingPoint

- Diameter (protocol)
  - □ successor to RADIUS

- Network Access Protection (Windows Server 2008)
  - □ authorization depending on
    - patch level
    - last virus scan

    …

References

- [marn] 802.1x Zugangskontrolle mit EAP und Radius in LAN und WLAN Umgebungen
  https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-marnau-802.1x.pdf

- IEEE 802.1X
  http://de.wikipedia.org/wiki/802.1X

- Implementieren von 802.1x Authentifizierung
  http://dnn.mssbsfaq.de/SBS2003/Server/8021xAuthentifzierung/tabid/431/language/de-DE/Default.aspx

- Network Access Protection
  http://technet.microsoft.com/de-de/network/bb545879(en-us).aspx