

TF-Mobility Umea, 7 jul 2008



Fondation RESTENA



RadSec – current status

Stefan Winter < [stefan.winter@restena.lu](mailto:stefan.winter@restena.lu) >

# Internet-Draft update



- Recharter is done! Radext officially takes on the work items of
  - ❑ RADIUS over TCP (STD track)
  - ❑ TLS security for RADIUS over TCP (EXP)
- RADIUS over TCP
  - ❑ Draft -00 from Alan DeKok
  - ❑ Aims for TCP/1812 as standard port
  - ❑ PDU format unchanged
- TLS security for RADIUS over TCP
  - ❑ As reported to the list



# Implementation update



- Lancom AP firmware  $\geq 7.52$ 
  - Released, working, in my AP :-)
- radsecproxy 1.1 Beta
  - Final release imminent
  - Has nice loop detection (but... see next slide)
- FreeRADIUS
  - Work started
  - TCP transport is already implemented
- **eduroam@home**
  - First non-Stefan field experiences by Vic Giralt



# Loop Detection and RadSec



## ■ RADIUS: client and server can check

- ❑ Client: if packet contains own realm, don't send
- ❑ Server: if receiving packet and would be sent back to originator, don't send

## ■ RadSec:

- ❑ <ServerRADSEC> clause doesn't offer a hint who the originating IP address that initiated request is
- ❑ (Client|Proxy)-Identifier matching won't work



# Loop Detection (2)



- Solution 1:
  - Make your clients check realms!
  - Should be the case “ever since”
- Solution 2:
  - Check IP address of connecting client and compare with server to forward to
  - A bit flaky
- Solution 3:
  - Your solution here!



# Plans

- produce a few [eduroam@home](#) APs and see how end-users like it (unchanged)
- Finish RFCs
- More dissemination work



# “Vision of the Future”



- some people are a lot more enthusiastic about RadSec than I am
- for current RADIUS “IdPs”: deploy a RadSec proxy in front of it, publish your certificate
  - proxy is lightweight
  - no critical data exposed by doing so
  - bootstrapping a roaming consortium gets easier technically:
    - user's home can be found via DNS lookup automatically
    - add the IdP's cert as “trusted” for your service
    - IdP: accept SPs cert for auth



Fondation RESTENA [www.eduroam.lu](http://www.eduroam.lu)

# Maths, RADIUS and you



- unpleasant surprise in Rome:  
very unreliable network, packet loss peaked at 20%
- International Roaming:
  - EAP over RADIUS: ~ 8 roundtrips per auth  
= 16 UDP packets per auth, end-to-end
  - 5 RADIUS (AP -> SP -> TLD -> root -> TLD -> IdP)  
= 16 \* 5 UDP packets per auth, hop-by-hop
  - assume 5 IP hops between RADIUS hops on average  
= 16 \* 5 \* 5 UDP packets, individual link  
= 400 individual packets on wire(s)



# Maths, RADIUS and you (2)



- How does reliability of individual links affect auth performance?
- Chance of success for a complete authentication session based on IP link reliab



Fondation RESTENA [www.eduroam.lu](http://www.eduroam.lu)

- 99% :  $0.99^{400}$  = 1.80%
- 99.9% :  $0.999^{400}$  = 67.02%
- 99.99% :  $0.9999^{400}$  = 96.08%  
(~ one in 25 fails!)
- 99.999% :  $0.99999^{400}$  = 99.60%  
(~ one in 250 fails!)
- 99.9999% :  $0.999999^{400}$  = 99.96%

# other news from IETF front



- phone call with three ADs: internet, security and ops area
  - EAP and payload size in RADIUS discussed, acknowledged as a problem
    - and a dim idea how to solve it
  - EAPoL and error reporting to the user discussed, acknowledged as a problem
    - suggestions to do it, but they are ugly
  - BoF: postponed, but suggestion to hold a “bar BoF”
  - SAML: met resistance by some, but based on an ancient view on SAML



# something completely different

- homogeneity of services offered
- user support
- how does the commercial world (i.e. GSM roaming) do it?
- watch the insightful picture...





Thank you!



Questions?