

TF-Mobility Marseille, 6 feb 2008



Fondation RESTENA



RadSec – current status

Stefan Winter < stefan.winter@restena.lu >

Internet-Draft update



- version -01 goes out in the coming days
- contains a section about certificate selection
- discussion with IETF Ads, dime and radiusext chairs:
request to recharter radiusext has high chances of success
- will do so in the coming days
- if successful, status would likely move to EXP



Implementation update



- Lancom AP firmware “7.40”
 - a “no frills” implementation
 - beta, works, likely in next production release (one minor condition pending: firmware size)
- radsecproxy 1.1 “alpha”
- FreeRADIUS
- rumors about Cisco ;-)

- radsecproxy and AP implementations show great promise for “eduroam@home”



eduroam deployment update



- ETLR servers both enabled
- LU as well (of course :-))
 - 1xRadiator, 1xradsecproxy 1.1-alpha (featuring: Status-Server probes with proactive failover)
 - using RadSec exclusively since several months, serving 150 int'l auth per working day
- NL: on FLRS and at least one institution
- experimental Access Points floating around
- -> RadSec is present on all hierarchy layers



Fondation RESTENA www.eduroam.lu

plans



- produce a few [eduroam@home](#) APs and see how end-users like it



- perform failover tests with 1.1-alpha (goal: finally debunk the failover “OMG-we-are-all-doomed” myth)
- take deployment experience to IETF, recharter radiusext WG, get RadSec on standards track

“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

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

- 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?