Update on RadSec

Stefan Winter <stefan.winter@restena.lu>

(presented by Stig Venaas <stig.venaas@uninett.no>
Outline

- implementation updates
  - FreeRADIUS
  - LANCOM Access Points
- I-D updates
Implementation updates

- **FreeRADIUS**
  - Alan DeKok seriously considering implementation
  - either TCP+TLS in server OR only TCP in server, TLS with stunnel (triggered by FR)
  - TCP-only opens way for more transports (SSH tunneling...)

- **Access Points**
  - LANCOM Systems (based in Germany) has alpha release of LCOS with RadSec support
  - own implementation, targeted release LCOS 7.40 (their next feature release)
Interoperability tests

- radsecproxy ↔ Radiator (already last IETF)
- LCOS → Radiator
- LCOS → radsecproxy

- radsecproxy|Radiator → LCOS: TBD
  (LCOS currently has RadSec client, server part is in the works)

- I.e. three independent implementations in the wild
I-D updates

-01 in the works

rework TLS text to reflect that non X.509 uses are possible (i.e. shared key)

eliminate appendix eduroam (not relevant)

suggest use of CA DistinguishedNames in TLS CertificateRequest (RFC4346 7.4.4)

- may enable easier cert selection in federated roaming (-> next slide)
- based on input from LANCOM implementation
CA DNs

- applies to TLS operation not only in RadSec but also Diameter
- consider node with roaming agreements to two roaming consortia A and B
- is in possession of two client certs fitting to A and B respectively
- uses dynamic lookup with SRVs (no info which CA is in use by resulting server...)
- gets server cert, server requests client cert
- which one to use? if server sends acceptable CA DNs, selection is easier [though still not necessarily unique!]