RESTENA

IETF 79 – radext meeting 12 nov 2010

RADIUS/TLS

Stefan Winter <stefan.winter@restena.lu>

Status of draft

- New rev -08
  - All open issues addressed (please verify!), except “Client identification”
  - One port for everything
  - Still auth server, acct server, dynauth server are separate entities

Identification and authorisation

- Client ID is difficult
  - My earlier reference to the server-id document is not adequate: document scoped exclusively towards servers
  - Different operation modes need different treatment:
    - PSK operation vs.
    - X.509 fingerprints vs.
    - X.509 proper

RADIUS/UDP

- Client ID = authorisation to exchange packets
  - IP and shared secret means that whoever connects with matching parameters is authorised
  - Which may be >1 NAS (consider NAT)
  - So, client ID != NAS ID
  - But matching Client ID = “friend”

RADIUS/TLS-PSK

- Same!
  - (TLS-Identifier analogous to IP address,
  - Shared secret analogous to TLS-PSK)
- More flexible than previous, because IP address is out, but same principles apply
  - Client ID = authorisation to send packets
  - 1 Client ID >= 1 NAS

RADIUS/TLS-X.509-FP

- Fingerprint operation similar
  - Fingerprint analogous to IP address
  - (no equivalent to shared secret)
- Again, Client ID = authorisation to send packets
- There may still be >1 NAS behind (if deploying same X.509 cert to multiple NASes, shame on you!)

RADIUS/TLS-X.509-proper

- Client identification != authorisation to send packets
- X.509 clients are uniquely identified by (Issuer, Serial Number)
- RADIUS/TLS deployments will have authorisation criteria regarding to which (identified) clients they want to talk to
  - This may be in-certificate data (policyOID)
  - Or out-certificate (query to some directory service)

Consequence for spec

- Stack needs to expose the **identification** criteria to admin:
  - Issuer, Serial Number
- And for authorisation
  - In addition to identification criteria: every property of certificate that's needed to make authorisation decision
  - That's vague...
  - For server's own purpose (logging), identification criteria suffice
    - Issuer, Serial Number

(continued)

- So, Client ID =! authorisation to send packets
- Both need to be spelt out explicitly in the draft
  - Mandate basic RFC5280 checks for every entity that tries to establish connection (notBefore, notAfter, wellformed cert)
  - Make clear that authorisation can depend on **any** property in the cert; check comes subsequent after ID check
  - Only client that succeeds in both is authorised
- Server should operate with ID checks only

(continued)

- There may still be more than one NAS behind (again, certs could have been re-used)