RADIUS/TLS and Dynamic Discovery Status

Stefan Winter, RESTENA

TF-Mobility, Internetland, 30 june 2011

Certificates

- EduPKI CA running and waiting for your requests.
- You need to be authenticated to the Ras (Stefan, Milan, Miro) – currently, TCS signatures or verified GPG keys are supported

- We are currently looking into assuring your company is what you say it is
  - O= attribute in certificates needs special care
  - “Legal name” of organisation has to go in there
  - We'll stick our heads together with eduPKI to find a reasonably simple, yet assertive way of checking the O= attribute

- Please excuse if this leads to a delay in processing

RADIUS/TLS: static

- ETLRs have been re-configured towards eduPKI CA root
- As soon as you have your certificate, you can use it send Access-Requests upstream (AuthBy RadSEC).
  - We'd still appreciate to let OT know in advance, so they can verify everything is in working order
- If you want traffic to your federation to come in via RADIUS/TLS, enable receiving in your configuration (ServerRADSEC), and tell OT to re-configure their routing to you
- This is proven technology; no experimentation or heart attacks involved

RADIUS/TLS: dynamic

- There are discoverable realms
  - guest.showcase.surfnet.nl would be reached in Phase-2-dynamic, if you enabled AuthBy DNSRoam
  - At LU TLD servers, tld1.eduroam.lu does it, monitored by Nagios
- Implementations
  - Radiator needed several recent fixes to really work the way we like it to
    - *Particularly: If multiple realms resolve to the same RADIUS/TLS host, re-use the existing session!*
    - *Use most recent patchset and be happy :-)*
  - radsecproxy: hunting a bug where enabling dynamic discovery "sometimes" crashes radsecproxy
    - *We are thinking of doing dynamic discovery in a better way for the next release*

RADIUS/TLS: Implementations (2)

FreeRADIUS

- finally has (static) TLS support in the 3.0 branch
- is being tested by eduroam participants, mainly JANET(UK)
- usable, but not production ready

- hold your breath for FreeRADIUS 3.0 :-)

Using DNS

Institutions:

Need to deploy NAPTR which points towards an SRV

(for phase 1, that's all; for phase 2, they would need an SRV which points to their own RADIUS/TLS server)

Federation:

Have an SRV which points to your RADIUS/TLS servers

(notably: the “fallback” of using an SRV directly if no NAPTR exists, is currently not well enough supported)

Realm check tool

European participants have requested an online test tool to verify the DNS configuration.

Here is a first iteration:

http://ticker.eduroam.lu/cat/check-dynamic.php?realm=yourrealm

- Goes through NAPTR → SRV → hostname → A/AAAA records
- will complain on any inconcistencies

Missing features:
- make an actual TLS connection, check if certs from all CAs are accepted
- make RADIUS request (for e.g. checking Operator-Name weirdnesses)

Screenshot: realm OK

Checking realm guest.showcase.surfnet.nl

This realm has 1 NAPTR records.

This realm has 1 eduroam NAPTR records.

Checking NAPTR format compliance: flag = S and regex = (empty) ...

Trying to resolve the SRVs into host names ...

1 host names discovered.

1 IP addresses discovered.

Realm is **DYNAMIC** with no errors encountered. Everything is alright!

Screenshot: realm with errors

Checking realm test-naptr-broken-target.dummy.restena.lu

This realm has 1 NAPTR records.

This realm has 1 eduroam NAPTR records.

Checking NAPTR format compliance: flag = S and regex = (empty) ...

Trying to resolve the SRVs into host names ...

Error: SRV entry _xyznonexist._broken.dummy.restena.lu could not be resolved!

0 host names discovered.

0 IP addresses discovered.

Realm is **DYNAMIC** but there were errors! Check them!