eduroam

RADIUS background and practical session

exercise: build an eduroam IdP

- Using FreeRADIUS + OpenLDAP
- Largely following GÉANT's documentation:
  - https://wiki.geant.org/display/H2eduroam/freeradius-sp
  - https://wiki.geant.org/display/H2eduroam/freeradius-idp

- But first we need to fill in some gaps

F/Ticks

- Simple statistical logging format:

```
F-TICKS/eduroam/1.0#REALM=wf.uct.ac.za#VISCOUNTRY=ZA#
VISINST=1uwc.ac.za#CSI=4c-fb-45-de-ad-f1#RESULT=OK#
```

- This shows a visitor from the University of Cape Town (REALM=wf.uct.ac.za) visiting the University of the Western Cape (VISINST=1uwc.ac.za) in South Africa (VISCOUNTRY=ZA)

- CSI = Calling-Station-ID = MAC address [privacy]

Operator-Name

- Provides a way to identify the [remote] service provider
- There are a number of different formats, identified by the first character
  - eduroam uses the REALM type, identified by “1”
  - The REALM type uses a DNS-based scope

- 1renu.ac.ug
- 1out.ac.tz
- 1ku.ac.ke

Chargeable-User-Identity

- A pseudo-anonymous, opaque, persistent, targeted, privacy-preserving identifier
- Chargeable-User-Identity := 2a8cd315aec15e3bc3f5a3820f4466a7c4653bb8
- SHA1 hash of a secret salt, User-Name, and Operator-Name
  - (see policy.d/cui line 72)

FreeRADIUS & virtual servers

- FreeRADIUS supports virtual hosts/servers, in much the same way as Apache does
- Selected based on client, port, or explicitly in config
- This can be used to simplify the processing of outer and inner identifiers

Federation-level RADIUS servers

For South Africa

- IPs:
  - flr-cpt.eduroam.ac.za (155.232.195.20)
  - flr-jnb.eduroam.ac.za (155.232.195.21)
- Shared secret:
  - Supplied by NRO (TENET)
- Realm:
  - your DNS domain

For this exercise

- IPs:
  - 137.63.190.37
  -
- Shared secret:
  - 9999
- Realm:
  - *yourname*.local

EAP Types

EAP type

- PEAP
- TTLS
- GTC

- TLS
- MD5
- SIM

Phase 2

- MSCHAPv2
- PAP

LDAP Modules

- FreeRADIUS supports LDAP, but you need to enable the module by symlinking mods-available/ldap -> mods-enabled/ldap
- For the exercise, you need to configure it to talk to our test OpenLDAP directory
- In a real situation, could be your Active Directory, eDirectory, etc

- NB! What LDAP backend you use affects what EAP types you can use!

Exercise details

FLR Server

- IP:
  - 137.63.190.37
- Shared secret:
  - 9999
- Realm:
  - *yourname*.local

LDAP Server

- IP:
  - 137.63.190.38
- Bind DN:
  - cn=admin,dc=ws,dc=ubuntunet, dc=net
- Bind password:
  - uaroot
- Base DN:
  - ou=people,dc=ws,dc=ubuntunet, dc=net