Deploying eduroam

Deyan Stoykov, BREN
E-infrastructure Autumn Workshops
8 September, 2014
Introduction to eduroam

- eduroam is a secure international roaming service for members of the European eduroam Confederation (*eduroam Service Definition, July 2012*)
- provides consistent and secure wireless access across research and education institutions
- based on a hierarchy of RADIUS servers
- username is in user@realm format
eduroam infrastructure elements

- European Top-level RADIUS servers (ETLRS)
  - operated by the eduroam Operations Team (OT)
  - located in Denmark and Netherlands
  - hub for the European Confederation
  - provide inter-federation roaming
- Federation-level RADIUS servers (FLRS)
  - operated by the National Roaming Operators (NROs)
  - provide intra-federation roaming
  - in case of inter-federation roaming, forward the request to an ETLR
Service providers (SPs)
- provide network access to local or visiting users
- receive RADIUS requests from NAS devices (wireless APs, switches)
- forward the request to user’s IdP
- grant or reject access

Identity providers (IdPs)
- responsible for authenticating the users in a specific domain (realm)
- receive RADIUS access request from SPs
- consult a user database
- grant or reject access

Access points / switches

Supplicants
eduroam infrastructure – static routing

- IdP Federation RADIUS server
- IdP RADIUS server
- User database
- SP Federation RADIUS server
- SP RADIUS server
- AP
- Client

Confederation RADIUS server
eduroam infrastructure – dynamic routing

- Confederation RADIUS server
  - IdP Federation RADIUS server
  - IdP RADIUS server
  - User database
- SP Federation RADIUS server
  - SP RADIUS server
  - AP
  - Client
eduroam infrastructure – dynamic routing
RADIUS
- provides AAA (authentication, authorization and accounting)
  - *accounting is generally not used in eduroam*
- relies on shared secrets for mutual authentication
- gradually superseded by RADSEC (RADIUS over TCP/TLS)

802.1x

EAP
- EAP-TLS (authentication with TLS certificate)
- PEAP (EAP-MSCHAPv2)
- EAP-TTLS (PAP, CHAP, MS-CHAP)
- Outer and inner tunnel
  - *Allows usage of anonymous identity*
    - *Outer tunnel: anonymous@realm*
    - *Inner tunnel: username@realm*
RADIUS server software

- FreeRADIUS
  - open source license
  - most popular RADIUS server
  - version 3 includes RADSEC support and other improvements
- Radiator
  - commercial license
  - targeting telco and other high-end market segments
- Radsecproxy
  - open source license
  - only supports proxying, not usable for an IdP
- Microsoft IAS/NPS
NRO requirements/recommendations

- Sign the eduroam policy
- Maintain a web-site at www.eduroam.[cc]
- Provide user support form
- Allow requests from the eduroam monitoring service
- Configure logging with F-Ticks
- Maintain the eduroam database
- Keep logs for at least 6 month
eduroam database

- Aggregated automatically from predefined locations
  - www.eduroam.[cc]/general/realm.xml
  - www.eduroam.[cc]/general/institution.xml

- institution.xml is populated in a federation-specific method, usually manually

- Used for contact data and coverage map
F-ticks

- Collects statistics for roaming authentication requests within the confederation to a central location
- FreeRADIUS configuration

```plaintext
linelog f_ticks {
    filename = syslog
    format = ""
    reference = "f_ticks.%{reply:Packet-Type}:-format"
    f_ticks {
        Access-Accept = "F-TICKS/eduroam/1.0#REALM=%{Realm}#VIS_COUNTRY=BG#CSI=%{Calling-Station-Id}#RESULT=OK#"
        Access-Reject = "F-TICKS/eduroam/1.0#REALM=%{Realm}#VIS_COUNTRY=BG#CSI=%{Calling-Station-Id}#RESULT=FAIL#"
    }
}

- rsyslog configuration

msg, contains, "F-TICKS" @1.2.3.4
Choosing EAP method

- PEAP (EAP-MSCHAPv2)
- EAP-TTLS (PAP, CHAP, MS-CHAP)

Authentication backend support

- **PEAP**: plaintext password or NT hash available
- **TTLS**: any (with PAP)

OS support

- **PEAP**: Windows Vista/7/8, iOS, Android
- **TTLS**: Windows 8, iOS, Android
Setting up an IdP

- Generate EAP certificates
  - Current recommendation is to set up a private CA specifically for eduroam
  - Use a long enough validity period (20 years?)
  - Commercial CA doesn’t provide additional security for EAP
Setting up an IdP

- Provide assistance to users
  - eduroam CAT
    - [http://cat.eduroam.org](http://cat.eduroam.org)
  - web-site with instructions
  - Promo materials at [www.eduroam.org](http://www.eduroam.org)
Setting up an IdP

- Enabling dynamic discovery
  - DNS records for dynamic discovery

```
example.com.     43200 IN NAPTR  00 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.example.com.

_radsec._tcp.example.com. 43200 IN SRV 10 0 2083 radius.example.com.
_radsec._tcp.example.com. 43200 IN SRV 5 0 2083 radius.example.com.
```

- Additionally, a PKI layer will verify the realm/domain is owned by a research/education institution.
- Currently in pilot state in 10 NRENs
Setting up a SP

- Wireless equipment choice and setup
- Controller-based or standalone APs
  - Controller-based solutions provide centralized management and other benefits such as better roaming experience
  - Standalone APs require smaller initial investment
- Client isolation
- General wireless networking best practices (coverage, channel selection, etc.)
- Extra SSID for initial setup (eduroam-help)
Setting up a SP

- Dynamic VLAN assignment

```c
# VLAN for staff
if ( Realm == "uni-ruse.bg" ) {
    update reply {
        Tunnel-type := VLAN
        Tunnel-Medium-Type := 802
        Tunnel-Private-Group-ID := 29
    }
}

# VLAN for students
if ( Realm == "stud.uni-ruse.bg" ) {
    update reply {
        Tunnel-type := VLAN
        Tunnel-Medium-Type := 802
        Tunnel-Private-Group-ID := 31
    }
}
```
Setting up a SP

- Establish and publish policy
- Keep authentication logs for at least 6 months
- Set the Operator-Name attribute

```ruby
authorize {
  update request {
    Operator-Name := "yourdomain.tld"
  }
}
```

- What NOT to do:
  - don’t use web logins
  - not recommended to do port restrictions
    - *port 25 can still be blocked (465 and 587 are on the minimum list)*
  - not recommended to use transparent proxies or force users to configure their systems to use a proxy
  - not recommended to use NAT
Further references

- http://www.eduroam.org/
- http://monitor.eduroam.org/
- https://wiki.terena.org/display/H2eduroam
Questions?
Thank you!