eduroam in a nutshell (BEGINNER)

eduroam in a nutshell

General overview

eduroam stands for **edu**cation **roam**ing. It offers users from participating academic institutions secure Internet access at any other eduroam participating location. The eduroam architecture that makes this possible is based on a number of technologies and agreements, which together provide the eduroam user experience: "open your laptop and be online".

The crucial agreement underpinning the foundation of eduroam involves the mechanism by which authentication and authorisation works:

- The authentication of a user is carried out at their Identity Provider (IdP), using their specific authentication method.
- The authorisation decision allowing access to the network resources upon proper authentication is done by the Service Provider (SP), typically a WiFi hotspot (University campus, etc.).

In order to transport the authentication request of a user from the Service Provider to his Identity Provider and the authentication response back, a world-wide system of RADIUS servers is created. Typically every Identity Provider deploys a RADIUS server, which is connected to a local user database. This RADIUS server is connected to a federation level RADIUS server, which is either in turn connected to the upstream RADIUS server infrastructure or can connect to other RADIUS servers dynamically (using the protocol RADIUS/TLS). Because users are using usernames of the format "user@realm", where realm is the IdP's DNS domain name often of the form institution.tld (tld=top-level domain; both country-code TLDs and generic TLDs are supported), the RADIUS servers can use this information to route the request to the appropriate next RADIUS server until the IdP is reached. An example of the RADIUS hierarchy is shown in Figure 2.1.

To transfer the user's authentication information securely across the RADIUS-infrastructure to their IdP, and to prevent other users from hijacking the connection after successful authentication, the access points or switches deployed by the SP use the IEEE 802.1X standard that encompasses the use of the Extensible Authentication Protocol (EAP). EAP is a container that carries the actual authentication data inside, the so-called EAP methods. There are many EAP methods an IdP can choose from.

eduroam requires that the chosen EAP method must allow

- mutual authentication (i.e. the user can verify that he is connected to "his" IdP whereever the user is
- encryption of the credentials used (i.e. only the user and his IdP will see the actual credential exchange; it will be invisible to the Service Provider and all intermediate proxies)

Some popular EAP methods in use in eduroam are

- PEAP ("Protected EAP") - a Microsoft protocol that establishes a TLS tunnel, and sends usernames and passwords in MS-CHAPv2 hashes inside)
- TTLS ("Tunneled TLS") - an IETF protocol that establishes a TLS tunnel, and sends usernames and passwords in multiple configurable formats inside)
- TLS ("Transport Layer Security") - an IETF protocol that authenticates users and the IdP with two X.509 certificates
- FAST ("Flexible Authentication via Secure Tunneling") - a Cisco protocol that establishes a TLS tunnel, and sends usernames and passwords in a custom way inside)

RADIUS transports the user's name in an attribute User-Name, which is visible in cleartext to all intermediate hosts on the way. Some EAP methods allow to put a different User-Name into the RADIUS packet than in the EAP payload. In that case, the following terms are used:

- outer identity: this is the User-Name in the RADIUS packet and visible to all intermediate parties
- inner identity: this is the actual user identification. It is only visible to the user himself and the Identity Provider

When using such EAP methods, and activating this option, the real username is not visible in RADIUS (it will only see the outer identity). Doing so will enhance the user's privacy, and is encouraged. Outer identities should be in the format "@realm" (nothing left of the @ sign, but the realm is the same as with the actual username). The realm part still must be the correct one as it is used to route the request to the respective Identity Provider. Once the IdP server decrypts the TLS tunnel in the EAP payload, it gets the inner identity and can authenticate the user.

After successful authentication by the Identity Provider and authorisation by the Service Provider, this SP grants network access to the user, possibly by placing the user in a specific VLAN intended for guests.

In the next chapter the various elements of this architecture and their functions is described.

Note: On responsibility for actions of the user: Directive 2001/31/EC article 12 defines the liability of a service provider:

- Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
  (a) does not initiate the transmission;
  (b) does not select the receiver of the transmission; and
  (c) does not select or modify the information contained in the transmission.

- The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

- This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

The complete Directive can be found at EUR-Lex1.

Please refer to deliverable DJ5.1.4 "Inter-NREN Roaming Architecture: Description and Development Items" for an in-depth description of eduroam and the underlying architecture.

Elements of the eduroam infrastructure

Confederation top-level RADIUS Server (TLR)

The confederation top-level RADIUS Servers, at the time of writing, are located in the Netherlands and Denmark for the European confederation, and Australia and Hong Kong for the Asian and Pacific region. Each have a list of connected country domains (.nl, .dk, .au, .cn etc.) serving the appropriate National Roaming Operators (NROs). They accept requests for federation domains for which they are authoritative, and subsequently forward them to the associated RADIUS server for that federation (and transport the result of the authentication request back). Requests for federation domains they are not responsible for are forwarded to the proper confederation TLR.

Federation-Level RADIUS servers (FLRs)

A federation RADIUS server has a list of connected IdP and SP servers and the associated realms.Typically, a FLR is authoritative for all RADIUS realms ending in its own top-level domain (e.g. a FLR for Antarctica would be authoritative for *.aq); it may also serve a number of domains in other top-level domains (e.g. .com, .net, .org, ...) but it is not authoritative for those entire top-level domains.

The FLR receives requests from the confederation servers and IdP/SP it is connected to and forwards them to the proper server. For its authoritative top-level domain, it rejects requests for non-existent realms inside the top-level domain.

IdP and SP RADIUS infrastructure

eduroam IdPs operate a RADIUS server which is responsible for authenticating its own users, by checking the credentials against a local identity management system.

eduroam SPs operate RADIUS capable equipment like Access Points or switches (see below). Large SPs typically also deploy an own RADIUS server, which is then responsible for forwarding requests from visiting users to the respective federation RADIUS server. Upon proper authentication of a user the SP RADIUS server may assign a VLAN to the user. Small SPs which do not require VLAN assignments can connect their RADIUS equipment directly to their FLR server, if the FLR permits that mode of operation.

Institutions which opt to be eduroam IdP and eduroam SP at the same time can have one RADIUS server that fulfills both roles simultaneously. This is the most popular deployment model in eduroam.

Note that the IdP RADIUS server is the most complex of all. Whereas the other RADIUS servers merely proxy requests, the IdP server also needs to handle the requests, and therefore needs to be able to terminate EAP requests and perform identity management system lookups.

Identity Management System

The Identity Management System of eduroam IdPs contains the information of the end users; for instance usernames and passwords. They must be kept up-to-date by the responsible IdP. An IdP RADIUS server will query the Identity management system to parform the actual authentication for a user as he tries to log in.

Supplicants

A supplicant is a piece of software (often built into the Operating System but also available as a separate program) that uses the 802.1X protocol to send authentication request information using EAP. Supplicants are installed and operate on end-user computing devices (e.g. notebooks, PDAs, WiFi-enabled cell phones, and so on).

Access Points

Access Points are Wireless LAN access devices conformant to IEEE 802.11 and need to be IEEE 802.1X capable. They must be able to forward access requests coming from a supplicant to the SP RADIUS server, to give network access upon proper authentication, and to possibly assign users to specific VLANs based on information received from the RADIUS server. Furthermore Access Points exchange keying material (initialisation vectors, public and session keys, etc.) with client systems to prevent session hijacking.

Switches

Switches need to be able to forward access requests coming from a supplicant to the SP RADIUS server, to grant network access upon proper authentication and to possibly assign users to specific VLANs based on information received from the RADIUS server.