Advisory: Filtering of Invalid Realms in Auth Requests sent to the NRPS

May 2014 - 15/05/2014

This advisory is relevant to ALL Visited (SP) service organisations participating in eduroam in the UK. It describes the recommendation, which will be included in the next revision of the Technical Specification, to filter out bad and doomed authentication requests containing malformed or 'homeless' usernames in order to reduce unnecessary loading of the national proxy servers.

In order to help maximise the efficiency of the National RADIUS Proxy Servers (NRPSs) all organisations providing Visited services should filter malformed outgoing RADIUS authentication requests on their border Organisation RADIUS Proxy Servers (ORPSs) and not pass bad requests to the NRPSs. This minimises the unsuccessful authentication attempts (ones which will never succeed) and means that genuine authentication requests are dealt with as quickly as possible. To this end section 4.2.1 of the eduroam Technical Specification (version 1.3) states:

- Visited organisations MUST forward RADIUS requests originating from eduroam Network Access Servers (NASs) which contain user names with non-local realms to a NRPS via an ORPS.

and

- Visited organisations MUST NOT forward requests containing user names which do not include a realm nor any which are non-NAI compliant.

The first part of that statement is simple, user names MUST contain an "@" symbol (e.g. username@camford.ac.uk [1]) and so bare usernames (e.g. "username" in this case) are NOT allowed. The second part is a little more complicated however. The definition of "NAI compliant" for the realm part is quite complex but basically it boils down meaning that it must be syntactically valid, i.e. the realm part of the user name must meet all of the following requirements:

- MUST contain at least one dot ("."), e.g. "camford.ac.uk" is OK,
- MUST NOT start or end with a dot, e.g. ".camford.ac.uk" or "camford.ac.uk." are both invalid,
- MUST NOT have two or more sequential dots, e.g. "camford.ac..uk" is invalid,
- MUST consist only of alphanumeric, hyphen and dot characters, so that's a-z, 0-9, "-" and ".", spaces are explicitly not permitted, e.g. "camford.ac uk" is invalid,
- following on from the previous point the realm MUST NOT start or end with a space, e.g. "camford.ac.uk " is invalid,

We also request that sites do NOT forward requests with user names matching any of the following,

- ends with ax.uk
- ends with ax.edu
- ends with @ac.uk
- ends with sc.uk
- ends with ac.edu
- ends with ac.u
- ends with .local
- ends with the organisation's own realm without the .ac.uk (e.g. ends in camford rather than camford.ac.uk. Nb. this applies only to organisations providing both Home and Visited services)
- contains common typo errors in the organisation's realm name (e.g. canford.ac.uk - check your NRPS error log for hints!)

There is also a list of common realms which we ask Visited organisations to reject locally rather than forward as, whilst they are syntactically valid, they are not eduroam members at this time and are not expected to be in the future. This list currently comprises:

- myabc.com
- 3gppnetwork.org (plus all subrealms thereof)
- 3gppnetworks.org (plus all subrealms thereof)
- gmail.com
- googlemail.com
- hotmail.com
- hotmail.co.uk
- live.com
- outlook.com
- yahoo.com
- yahoo.cn
- unimail.com

A description of how to implement the above recommendations is beyond the scope of this document since there are various different RADIUS servers deployed by members and each platform requires difference configuration methods.

Links

[1] mailto:username@camford.ac.uk