2023-07 Advisory: Addressing the Issue of Leakage of Harmful RADIUS Attributes

Date: 4/08/2023

This advisory is relevant to all eduroam(UK) service organisations. It describes the background to and rationale for the implementation of filtering of all but essential attributes at the NRPS. The necessary changes to the eduroam(UK) Technical Specification to support this will be implemented in version 1.5 [1], due to come into effect in Q4 2023.

Please review the proposed new version of the specification and send any comments to us before 20th August. In addition to the planned introduction of filtering of spurious attributes at the NRPS, a further measure that could be introduced is the active insertion of certain attributes that some organisations have included in their configurations for roaming users. Whilst it is not intended to implement this as part of this Advisory, your feedback and comments are warmly invited.

Overview

We are taking the opportunity presented by the update of the forthcoming Technical Specification (to version 1.5 [1]) to address one of the problems that has long beset roaming user authentication. Your consideration of and feedback on this is proposal invited.

During roaming user authentication and connection of user devices to eduroam guest networks, the inclusion/'leakage' of harmful attributes within Access-Accept requests sent from Visited sites can in some circumstances cause difficulties. Since such attributes normally play no part in supporting authentication of roaming users and since configuration of RADIUS systems to prevent/neutralise these is sometimes complicated or not possible, we are proposing to filter out all but essential attributes at the National RADIUS Proxy servers. The result will be that Home sites will receive Access-Accepts without spurious/harmful attributes.

Background and rationale

Connection failures due to attribute leakage: During the process of authentication of roaming users, due to deficiencies in the design of some RADIUS platforms or poor configuration of the RADIUS server, it is possible for unnecessary RADIUS attributes to be

exchanged between visited and home sites. Some attributes are merely spurious, but some can be harmful. Attributes that, on campus, are highly beneficial - for instance those utilised for dynamic assignment of VLANs based on the group that the user belongs to - can be harmful when returned to a remote site that a user is visiting. For example, if an Access-Accept reaches the AP at the Visited site and the designated VLAN identifier value is not be defined, user device connection may fail.

Attributes associated with network segregation: The implementation of dynamic VLAN assignment and resulting segregation of user devices on the home campus is, we would argue, an essential element of network security. The separation of own students, own staff, eduroam visitors and non-eduroam visitors should be the minimum level of segregation. The particular attributes necessary to achieve this depend on the vendor of the WLAN equipment, but the following are in common use:

- Tunnel-Type (attribute 64) ?
- Tunnel-Private-Group-ID (attribute 81)?
- Tunnel-Medium-Type (attribute 65)
- Aruba-User-Vlan
- Trapeze-VLAN-Name

Essential attributes/spurious attributes: The eduroam Technical Specification to date has stated what attributes MUST be forwarded unaltered (ref. Requirement 14) – these are the attributes that are essential for roaming user authentication. There are however a number of other attributes that, whilst useful on campus, play no part in the decision making applying to the authentication of roaming users. Such attributes are in the context of the authentication of roaming users, spurious and may be harmful.

Configuration issues with some RADIUS services rules/conditions: In addition to the forwarding of spurious VLAN assignment attributes from Home sites, it has been noticed that some Visited organisations are forwarding NAS-Port-Type and/or Service-Type attributes in the Access-Requests from users roaming to their Visited site venues. NAS-Port-Type values include ‘Wireless-IEEE-802-11’ and ‘Ethernet’. Service-Type attribute values are more varied and include ‘Framed-User’, ’Login-User’, ’Authenticate-Only’, ‘Call-Check’ and ‘Authorize-Only’. These attributes may have some valid purpose in the on-campus context (and some vendor how-to documentation includes these in the conditions to be met for authentication) but these should form no part in the decision by the Home site with regard to the authentication of users roaming to other eduroam venues.

However, it has been noticed that in some of our members’ RADIUS configurations, the service rule for authentication requests received from the NRPS (i.e. for supporting their roaming users), contains conditions based on some of those attributes, specifically NAS-Port-Type and Service-Type. This misconfiguration has resulted in variable roaming user authentication failures depending on the particular site the user has roamed to.

Increasing volume of spurious/harmful attributes: With the continuing increase in the size of the eduroam community and its increasing diversity, the range and mix of RADIUS software type has skewed towards more problematic platforms such as Microsoft NPS. This has led to an ever increasing volume of spurious attributes being sent and in many cases consequent prevention of successful connection of authenticated user devices to eduroam network services. Incomplete authentication and connection in turn leads to tying up RADIUS

resources and retries from client devices. It is believed that the exchange of ‘harmful’ attributes is a now major factor in current widespread performance issues.

Avoiding inclusion of/dependency on harmful/spurious attributes: Documentation on the Community eduroam website has attempted to describe how the inclusion of potentially harmful attributes can be avoided and in some cases to be overwritten with non-harmful ones for the local network (1). Documentation on the Community web site has also been updated to guide Home organisations to configure their systems to not be dependent on attributes that are applicable only to the Home campus.

Nevertheless, for many system administrators who are increasingly under time constraints, the configuration of RADIUS systems to achieve robust deployments is a continuing challenge and this has informed our proposal to implement attribute filtering at the NPRS as described below.

It should be noted that once attribute filtering at the NRPS has been implemented, it will be essential that Home service configurations comply with best practice guidance as per eduroam(UK) published documentation.

(1) https://community.jisc.ac.uk/library/janet-services-documentation/radius... [2]

eduroam Technical Specification: to date the Technical Specification has stated what attributes MUST be forwarded unaltered (ref. Requirement 14), i.e. the ones that are essential for roaming user authentication; it has only made the recommendation that the unnecessary/harmful ‘spurious’ attributes should be filtered out (ref. section 2.4.3 Discussion). It is of course better that the RADIUS configuration is such that these attributes are not sent at all rather than be filtered out.

Filtering all but essential attributes at the NRPS: one solution to eliminating the exchange of spurious/harmful attributes and one that lifts the burden from the system admin of doing this, where the RADIUS platform is difficult or impossible to configure, is for this work to be done by the NRPS. The NRPS already check for and add Operator-Name where this has no be included by the Visited organisation.

Proposed Implementation of Filtering at the NRPS

Context: For many years, the approach of eduroam(UK) has been to minimise the scope of intervention of the NRPSs on the exchange of RADIUS packets. The NRPS generate Access-Rejects to clear backlogs of stacked up authentication requests for an individual organisation when no working host conditions arise (when ORPSs are non-responsive) and they also inject Operator-Name attribute when the attribute has not been included by a Visited organisation (based on the value of the ‘Identifier’ parameter in Organisation settings on Support server). Now, however, due to the current scale and diversity of the eduroam ORPS population and the consequent increasing volume of spurious attributes being exchanged, it is considered expedient and reasonable to configure the NRPS to actively filter attributes to improve the robustness of the service as a whole. It is worth noting that attribute filtering has been implemented by a number of our European NRO counterparts.

NRPS behaviour: for every participating organisation, unless a specific participating organisation requests otherwise, the NRPSs will by default strip from RADIUS packets any attribute that is not listed in the Technical Specification section 2.4.1 Requirement 14.

Support server interface: an organisation wishing to be excluded from the NRPS filtering out of non-listed attributes may notify eduroam(UK) of this – likely to be by way of a tick box in the RADIUS settings box reached from the RADIUS servers panel on the organisation's Configure page on Support server portal.

Tech Spec 1.5 [1] **changes:** Section 2.4.2, replacement Recommendation 3 For all RADIUS hosts, attributes relevant only to the Home campus, including VLAN VSAs and NAS-Port-Type and Service-Type, SHOULD NOT be forwarded to the NRPS.

Section 3.6.2, Recommendation 9 For Home service provider organisations the new version of the Tech Spec will state that unnecessary/harmful 'spurious' attributes SHOULD if possible be filtered out. Since some platforms only support the overwriting of attribute values rather than complete removal, this requirement will not be enforced as a MUST.

For Visited organisations the new version of the Tech Spec states that organisations SHOULD NOT include unnecessary attributes in visitor authentication requests forwarded to the NRPS.

To improve the robustness of the service as a whole, the eduroam(UK) NRPSs will by default strip from RADIUS packets any attribute that is not listed in section 2.4.1 requirement 14, unless the participating organisation requests eduroam(UK) to allow all attributes.

The proposal to allow each member organisation to opt out of the default stripping from packets of non-specified attributes, will accommodate any organisations that have formed an agreement with others for the common usage of attributes.

Timeframe: attribute filtering at the NRPS will be implemented shortly after the Tech Spec v.1.5 becomes current.

Further possible measure for consideration – active insertion of NAS-Port and Service-Type attributes

As noted in the above section 'Configuration issues with some RADIUS services rules/conditions' misconfiguration of some RADIUS servers has resulted in a dependency on NAS-Port and Service-Type attributes – which, since they are relevant in the Home campus context only, should not form part in the decision by the Home site with regard to the authentication of users roaming to other eduroam venues. The eduroam(UK) recommendation is that organisations should check their RADIUS configurations to ensure that their configuration for roaming users does not include such dependencies and to correct any misconfigurations if discovered.

Nevertheless, it would be feasible to implement proactive insertion of the two attributes NAS-IP-Address and NAS-Port-Type (and populate these with some nominal value) where these are not present in the Access-Requests from Visited organisations. This would allow misconfigured Home services to operate without the need for configuration changes - at the expense of unwarranted inclusion of those attributes and support of not best practice

configurations. Implementation of this measure is not currently planned. But we wish to seek the views of the community and your comments/recommendations are welcomed.

Comments/Feedback/Objections

Any objections from the community to the implementation of attribute filtering at the NRPS with the option to an opt out will be taken into consideration and may influence the final draft of the new Tech Spec. Comments/recommendations are warmly welcomed - please send any feedback before 20th August.

We would also like to cordially request comments/feedback/recommendations regarding the possibility of implementing NAS-Port and Service-Type attribute injection by the NRPS to solve certain RADIUS misconfiguration issues.

Links
[1] https://community.jisc.ac.uk/library/network-and-technology-service-docs/eduroamuk-technical-specification-15-draft
[2] https://community.jisc.ac.uk/library/janet-services-documentation/radius-attribute-filtering-microsoft-ias-and-nps