InCommon eduroam IdP Testing Solution

Date: 9-March-2022 Version: 0.1

1. Executive Summary

This paper proposes a solution to the InCommon eduroam subscribers' requirements for Identity Provider (IdP) testing. We propose to add functionality to the Federation Manager that allows an eduroam administrator to enter user credentials which will be used to issue an eduroam authentication request to (one of) the administrator's IDP realm(s).

2. Problem statement

Eduroam enables roaming users associated with a subscribing IdP organisation to connect to a Wi-Fi network operated by a subscribing Service Provider (SP) organization.

An IdP that joins eduroam must deploy and configure a RADIUS server and a user management system to allow the IdP's end users to access eduroam locally and when roaming to remote locations. Testing that the IdP works from remote locations can be challenging, especially for IdPs that are not located in close proximity to other Service Providers (SPs).

3. Requirements

There are several requirements that must be met by an IdP Testing solution:

ID	Name	Description
1	End-to-end authentication	The solution must facilitate an end-to-end authentication identical to the standard eduroam connection workflow.
2	Easy to use	The solution must be usable by a typical wireless network administrator. It should not require any specialist knowledge of eduroam or its technologies. It should not have any unusual dependencies or requirements.
3	Integration with Federation Manager	The IdP testing mechanism must be accessible from the Federation Manager.
4	Self-service	The solution must be fully self-service. It should not require cooperation from other eduroam IdPs or SPs. The entire mechanism must be usable from an eduroam administrator's web browser.
5	Support for PEAP and EAP-TLS credentials	The solution must support the use of either PEAP (userid/password) or EAP-TLS (certificate-based) authentication methods [PEAP, EAP-TLS], including entry of both types of credentials into the Federation Manager.
6	No persistent storage of user credentials	The credentials provided to the Federation Manager must not be stored in a database or other long-term storage – they will be used for a single authentication and discarded.
7	No leaking of user credentials	User credentials will be encrypted (or passed via an encrypted channel) whenever they are passed over a network or messaging system that might expose them to view by third parties.

8	Ability to support IdPs with multiple realms	If an IdP has multiple realms configured, it must be possible for the IdP to choose which realm will be used for authentication.
9	Authentication restricted to the administrator's realms	Authentication should only be performed against realms that are administrated by the administrator performing the test. This will prevent the possibility of FM being used as a means to attack other realms.
8	Integration with eduroam logging	The eduroam logging system must expose logs of test authentications. This will make it easier for IdP administrators and InCommon to troubleshoot problems.

4. Proposed Solution

Our proposed solution is the add fields to the IdP section of the Federation Manager to perform IdP Testing, as follows:

- The ability to choose from among the realms associated with this IdP.
- The ability to choose the authentication type, PEAP, EAP-TTLS, or EAP-TLS.
- The ability to supply a credential for the specified authentication type
    - Username and password for PEAP or EAP-TTLS, or
    - Certificate upload for EAP-TLS.

Users will enter their credentials into the Federation Manager, click on a button labelled "Test Authentication", and receive the results of their authentication (Pass or Fail for each of TLRS1 and TLRS2). In the event of failure, a reason string may be provided to help with further debugging.

Internally, the FM "Test Authentication" button will make an API call to a module that will call the "eapol_test" [EAPOL] tool with the realm and credentials provided. Results will be returned to FM in the form of a numeric result code and, in some cases, a user-readable response string. This exchange will be conducted over HTTP TLS or an encrypted message queue, ensuring that the contents of the exchange are protected from external view. The connection between FM and the eapol_test module should be authenticated, so that the eapol_test module cannot be misused by attackers.

The response in FM will consist of a clear pass/fail indication for the authentication, and display of a user-readable message, if provided.

In the event of an authentication failure, the IdP administrator can debug the issue using the user-readable response string, the eduroam top-level proxy logs available through FM, or local logs from the IdP RADIUS server.

5. References

[EAP-TLS] RFC 5216: "The EAP-TLS Authentication Protocol", D. Simon, et. al., March 2008. https://datatracker.ietf.org/doc/html/rfc5216

[PEAP] "Protected EAP (PEAP)", D. Simon, et. al., March 2003. https://datatracker.ietf.org/doc/html/draft-josefsson-pppext-eap-tls-eap-06.txt

[EAPOL] https://wiki.freeradius.org/guide/eduroam#tooling_eapol_test