CSIT Conference 2019, Yerevan, Armenia, September 23-27

User Blacklisting Solution for IMAP Eduroam Authentication

Arthur Petrosyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: arthur@sci.am

Gurgen Petrosyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: gurgen@sci.am

Robert Tadevosyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: robert@sci.am

ABSTRACT

This paper presents the concept of blacklisting the eduroam users, that are being authenticated on eduroam via their organization's IMAP server. The concept described is based on the fact, that most organizations, even lacking for the own personnel identity database, have at least an email service in place and, thus, have a working IMAP server for their organization domain name. Thus, the existing email username/password in a particular organization can be used as an identity source for eduroam authentication. Paper describes the possibility to blacklist some users in case it will be necessary, so that not all owners of email account, could automatically use eduroam service.

Keywords

eduroam, IMAP, PAM, Wi-Fi, Wireless, Authentication, Blacklist

1. INTRODUCTION

eduroam (education roaming) [1] is the worldwide wireless network access service, that allows users (researchers, teachers, students, staff) from different institutions to securely gain WiFi Internet access while, being within WiFi coverage area of any eduroam-enabled institution around the globe. The eduroam principle is based on the fact that the user’s authentication is done by the user’s home institution, whereas the authorization decision allowing access to the network resources is done by the visited network.

The technology behind eduroam is based on the IEEE 802.1X standard and a hierarchy of RADIUS servers [2]. The role of the RADIUS hierarchy is to forward user credentials to the user’s home institution, where they can be verified and validated. When a user requests authentication, the user’s realm determines where the request is routed to. The realm is the suffix of the user-name, delimited with ‘@’, and is derived from the organization’s domain name. Every institution that wants to participate in eduroam should have its institutional RADIUS server (IRS) connected to the federation level RADIUS server (FLRS) of the country where the institution is located.

The FLR is normally operated by the National Research and Education Network (NREN) of that territory. These federation-level servers have a complete list of the participating eduroam institutions in that country. This is sufficient to guarantee roaming operations. ASNET-AM, being the Armenian NREN, acts as the National Roaming Operator (NRO) on behalf of Armenia.

International roaming in eduroam is operated by means of two top-level RADIUS servers deployed in Europe, which forward the users request to the right territory.

2. CONCEPT ARCHITECTURE

The principle of getting Wi-Fi Internet access in eduroam is not like “one-password-for-all”, but instead requires connecting users to provide their personal credentials (username/password) from a home institution in order to gain Internet access.

Currently, there are a number of Research and Education organizations in Armenia, that would like to praticipate in eduroam, but don’t have their own personnel identity database or have it for internal purpose use only. If such organization has a corporate email service in place and, thus, has working IMAP server for its organization domain name, then one possible way of quickly starting to use the eduroam service with minimal administrative overhead is to use the existing email username/password within a particular organization as an identity source for eduroam authentication.

For each institution, that would like its staff members or students to use their institution’s email username/password as an identity source for eduroam authentication, specific IRS should be installed and configured. IRS should be properly registered at FLRS within the NRO. Specific configuration should include the RADIUS server module to do the authentication via IMAP server. Current version of FreeRADIUS [3] is not authenticated on IMAP servers. But there are several solutions that can be used to overcome that limitation.

One of them is described in [4] and requires pam-imap pluggable authentication module to be used. In this case, FreeRADIUS authentication will go through Linux Pluggable Authentication Modules (PAM) [5] solution to reach the IMAP server. PAM provides dynamic authentication support for applications and services in a Linux. The pam-imap module should be configured to connect to a particular remote IMAP server for authentication. In this concept, FreeRADIUS server, using pam-imap module will treat the remote users as local to the Linux system running the RADIUS server. The above solution supports the secure IMAP connection method – IMAPS, which is mostly used nowadays.

3. BLACKLISTING SOLUTION

The possibility to blacklist some users if necessary, so that not all owners of email account, could automatically use eduroam service, can be simply implemented in FreeRADIUS configuration. The way we propose to do it is having that particular user, who is to be blacklisted, be listed in the FreeRADIUS text file configuration, where the authentication is configured, before the pam-imap module usage description.

4. CONCLUSION

Thus, by indicating that particular user before pam-imap configuration and providing a wrong password for him, we can prevent that user from being authenticated. Users selected in this way can be easily blacklisted, and not all owners of email accounts at those organizations domain name, could automatically use eduroam service.

REFERENCES

[1] https://www.eduroam.org/

[2] IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines

[3] https://freeradius.org/

[4] https://github.com/asnet-am/eduroam-imap-playbook

[5] http://www.linux-pam.org/