Mathematical Problems of Computer Science 52, 61--65, 2019.

UDC 004

Identity Infrastructure Boost Concept for eduroam Service

Arthur S. Petrosyan, Gurgen S. Petrosyan, Robert N. Tadevosyan and Kevork Kh. Arsalanian

Institute for Informatics and Automation Problems of NASRA
e-mail: arthur@sci.am, gurgen@sci.am, robert@sci.am, kevork.arsalanian@sci.am

Abstract

This paper presents the concept of authenticating eduroam users via their organization's IMAP server. The concept described is based on the fact that most organizations, even lacking their 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 within a particular organization can be used as an identity source for eduroam authentication. The paper describes the components required to implement the concept, as well as some expected limitations for this solution. The concept is planned to be implemented in ASNET-AM network in order to stimulate more rapid use of eduroam service in Armenia.

Keywords: eduroam, WiFi, Wireless, Authentication, Authorization, Identity, IMAP, PAM

1. Introduction

eduroam (education roaming) [1] is a secure, global wireless network roaming access service developed for the international research and education community. It allows users (researchers, teachers, students, staff) from different institutions to securely gain WiFi Internet access, while being within the 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.

eduroam is based on the IEEE 802.1X standard technology and a hierarchy of authorizing 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. So,

each institution participating in eduroam has its Institutional RADIUS server (IRS) connected to the federation level RADIUS server (FLRS) of the country where the institution is located.

The FLRS 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. In case of Armenia, ASNET-AM is the Armenian NREN acting as a National Roaming Operator (NRO).

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

Instead of using the simple "one-password-for-all" principle to provide WiFi Internet access, eduroam service instead requires connecting users to provide their personal credentials (username/password) from home institution in order to gain WiFi access. For territories, where Research and Education organizations would like to participate in eduroam, but lack their own personnel identity database or have it for internal purpose use only, it might take long time to launch eduroam. For such cases we propose to use organization's corporate email service, since it generally means they would have working IMAP server for their organization domain name. Thus, 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.

Institutions that would like their staff members or students to use their institution's email username/password as an identity source for eduroam authentication, should install and configure their IRS in a specific way. First 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 (Fig. 1.).

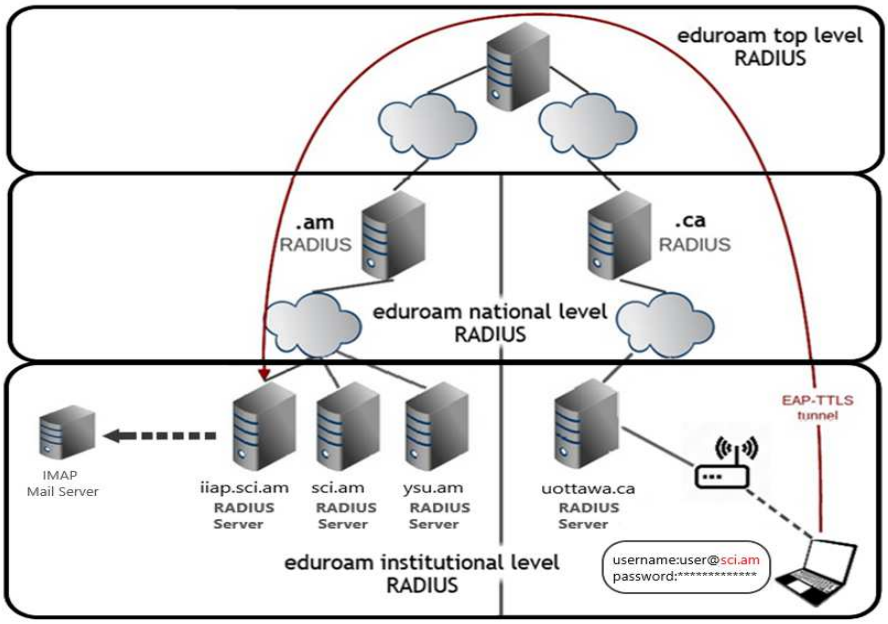

Fig.1.

Current version of FreeRADIUS [3] does not include authentication against 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 provide dynamic authentication support for applications and services in a Linux. 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.

Another approach is described in [6] and is based on several Python 3 modules (imaplib,sys,ssl). It requires creating an external IMAP connector - an application or script that can be invoked by the FreeRADIUS server process on demand for verifying the user name and password pairs against external IMAP server. The connector gets the user name/password and returns back an exit status value (return value) on completion. If that value is zero, the FreeRADIUS sever process considers the user credentials verified.

Both solutions support secure IMAP connection method – IMAPS, which is mostly used nowadays. But there are some limitations for the use of the concept described above.

3. Limitations

Since FreeRADIUS has no access to a cleartext password when authenticating via the methods mentioned above, only PAP can be used as an inner (phase two) authentication method. This typically means clients (WiFi devices) need to be configured to use TTLS/PAP. TTLS was not originally supported out-the-box by Windows operating systems, but Windows 10 now includes a TTLS supplicant. Other modern operating systems now support TTLS too.

Another limitation is scalability. IMAP servers are slow authenticators, compared to those based on LDAP or Active Directory. So setting up an IMAP connection is rather slow (about 2 seconds) and more resource intensive than other authentication methods. This means that the IMAP approach likely does not scale too much. Of course PAM solution can provide some caching of credentials, which may improve this.

4. Advantages

The concept described in this paper has several advantages. First advantage is that in case of authenticating eduroam users via their organization's IMAP server, users will likely refrain from sharing their credentials with anyone, since it would potentially give others access to their mailbox too. Another advantage of this concept is that it allows to easily manage eduroam access simultaneously with mailbox access. So, if the user leaves organization and his/her mailbox is being disabled or removed, then that user automatically is being restricted from using eduroam too.

5. Conclusion

This solution may be interesting for cases, where organization decides to restrict access to the authentication database or does not yet have such a database at all. It enables to launch the eduroam service by authenticating the users of the RADIUS server against publicly available service like IMAP, and the existing email username/password within a particular organization's domain name can be used as an identity source for eduroam authentication.

References

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

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

[3] [Online]. Available: https://freeradius.org/

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

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

[6] [Online]. Available: https://vessokolev.blogspot.com/2018/09/imap-connector-for-freeradius-to.html

Submitted 02.09.2019, accepted 28.11.2019.

eduroam ծառայության ենթակառուցվածքների զարգացումը խթանող գաղափար

Արթուր Ս. Պետրոսյան, Գուրգեն Ս. Պետրոսյան, Ռոբերտ Ն. Թադևոսյան և Գէորգ Խ. Արսալանյան

ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտ
e-mail: arthur@sci.am, gurgen@sci.am, robert@sci.am, kevork.arsalanian@sci.am

Ամփոփում

Հոդվածում նկարագրված է eduroam ենթակառուցվածքի զարգացումը խթանող գաղափար, որը իրականացվելու է ASNET-AM ցանցում՝ Հայաստանում eduroam ծառայության առավել արագ օգտագործմանը նպաստելու համար: Նկարագրված գաղափարը հիմնված է այն փաստի վրա, որ որոշ կազմակերպություններ չունեն անձնակազմի ինքնության տվյալների բազա, սակայն ունեն էլ. փոստի ծառայություն և այդպիսով ունեն IMAP սերվեր իրենց կազմակերպության դոմենային տիրույթի անվանման համար: Այսպիսով, որոշակի կազմակերպության ներսում առկա էլ.

փոստի անունը/գաղտնաբառը կարող է օգտագործվել որպես eduroam ծառայության վավերացման ինքնության աղբյուր: Հոդվածը նկարագրում է գաղափարի իրականացման համար անհրաժեշտ բաղադրիչները, ինչպես նաև՝ առաջարկվող լուծման որոշ սահմանափակումներ:

Բանալի բառեր՝ eduroam, WiFi, անլար, նույնականացում, թույլտվություն, ինքնություն, IMAP, PAM

Концепция ускоренного развития идентификационной инфраструктуры для сервиса eduroam

Артур С. Петросян, Гурген С. Петросян, Роберт Н. Тадевосян и Кеворк Х. Арсаланян

Институт проблем информатики и автоматизации НАН РА
e-mail: arthur@sci.am, gurgen@sci.am, robert@sci.am, kevork.arsalanian@sci.am

Аннотация

В статье представлена концепция ускоренного внедрения инфраструктуры eduroam в организациях. Описанная концепция основана на том факте, что даже если организации не имеют собственной базы данных идентификации персонала, они имеют по крайней мере службу электронной почты и, таким образом, имеют рабочий сервер IMAP для доменного имени своей организации. Таким образом, существующее имя пользователя/пароль электронной почты в конкретной организации может использоваться как источник идентификации для аутентификации eduroam. В статье описываются компоненты, необходимые для реализации концепции, а также некоторые ожидаемые ограничения и преимущества описанного решения. Концепцию планируется реализовать в сети ASNET-AM, для стимуляции ускоренного расширения использования услуги eduroam в Армении.

Ключевые слова: eduroam, WiFi, беспроводная связь, аутентификация, авторизация, идентификация, IMAP, PAM