International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Integration of Eduroam Architecture in the Kerberos Protocol

Mahesh S. Tambe[1], S. K. Pathan[2]

[1] P.G. Student, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering Pune, India

[2] Assistant Professor, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering Pune, India

Abstract: ***Eduroam has become one of the important instances of network federations throughout the globe, where many of institutions permits roaming end users to operate the local network if they associated to any other eduroam member institution. In this context, this paper presents how, once the end user is validated by the network, user can operate on more federated application services (beyond the web) by means of Kerberos, without locating more cross-realm infrastructures. With the help of current eduroam architecture, this paper avoids the end user from being entirely validated by home institution again to operate the application services, which do not required to be altered. Eventually, optional advanced authentication can be implemented to give added figure services to end users. Visited institution provides these services which are very essential to define some access control contraption to access. In this paper it proposes improved authentication depends on user features that are defined in his home institution that are used to provide services to the end user who is roaming from his home institution.***

Keywords: Eduroam, Kerberos, IDP, SSO, Authorization

1. Introduction

The accumulated attributes are provided to the Policy Decision Point (PDP), which verifies the neighborhood strategies and took a decision. Then again, the eduToken is presented to be utilized for operating a crosslayer SSO technique to get resources accessible inside the federation. Eduroam operated a federated network access control concentrated around AAA architecture generated of a mechanism of RADIUS servers where the user is authenticated by technique for the EAP rule. Particularly, the most generally utilized identification framework are done by EAP strategies. From one perspective, the pseudonym utilized for operating the authorization of the user at the time of network access. Correctly, the pseudonym is utilized by the visited server for getting applicable attributes, from the Idp, so as to optain for whether the user is permitted access to the network.

In several words, the DAMe present a included cross-layer SSO solutions where end clients, fitting in with eduroam foundations, are not capable to simply to extend mechanism get to in some other foundation of the federation, additionally to get to web application management. One of these initiative is DAMe [1], made under the umbrella of the GEANT Projects [2], which similarly made eduroam. A few inventiveness in like way presents the dispersal of a verification token, which is required to be implemented for asking for access to other web application management, along these lines accomplishing a cross-layer SSO solution. Eduroam is focused around a general AAA pattern. As a triumph of eduroam various initiatives have emerged to give added services like Authentication Authorization and Accounting, a couple of activities have climbed with the measure aiming of to give combine worth security benefits over this organization.

The latest version is approachable for all important operating frameworks: Microsoft has combined it in its Windows operating framework, it is accessible for Linux under the name Heimdal, and business Unix differences and in addition Apple's OS X utilization code from the MIT used of Kerberos 5. Moreover, it is being utilized as a building piece for larger amount rule [5]. Introduced in the early 1990s [6], Kerberos 5 continues to enhance as new functionalities are added to the important rule. Kerberos [3, 4] is a successful, widely conveyed single sign-on rule that is structured to verify customers to several networked management, e.g., remote hosts or document servers.

1.1 Eduroam Infrastructure

Eduroam technology is based on 802.1X standard and a hierarchy of RADIUS proxy servers. The role of the RADIUS hierarchy is to forward the users' credentials to the users' 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 DNS domain name. Every institution (i.e. university or equivalent) that wants to participate in eduroam connects its institutional RADIUS-server to the national top-level RADIUS (NTLR) server of the country where the institution is located. The NTLR is normally operated by the National Research and Education Network (NREN) of that country. These country-level servers have a complete list of the participating eduroam institutions in that country. This is sufficient to guarantee national roaming.

For international roaming, a regional top-level RADIUS server is needed in order to roam the users request to the right country. Currently there are two main regions where eduroam is deployed: Europe and Asia-Pacific. In the case of Europe the top-level RADIUS server (ETLR) are operated by the Dutch NREN (SURFnet) and the Danish NREN (UNI-C). In the case of Asia-Pacific, the top-level RADIUS server (APTLR) is operated by the Australian NREN (AARNet) and by the University of Hong Kong.

1.2 Working of Eduroam

When a user tries to log on to the wireless network of a visited eduroam-enabled institution, the user's authentication request is sent to the user's home institution. This is done via a hierarchical system of RADIUS servers. The user's home institution verifies the user's credentials and sends to the visited institution (via the RADIUS servers) the result of such verification.

2. Literature Survey

Multiple researchers dragged towards the problem of operation like author in [9] proposed a acknowledgement for permit included access to management focused throughout the utilization of Kerberos [2] together with EAP [8]. Since Kerberos cross-domain pattern are surly not broadly conveyed in federations, the course of action provides united access to kerberized management by method for a novel Kerberos identification done before as part focused around EAP. This work presented a model where operate control to management inside an consortium is focused around Kerberos. As sort of, customers are compel to get access a ST from the went to institutions KDC to get to a particular administration. This part grants clients to confirm themselves against the went by organization's KDC by utilizing certifications that are verified by the organization's AAA server.

The expandable authentication protocol (EAP) [5] The Extensible Authentication Protocol (EAP) has been deliberate to allow diverse sorts of authentication framework through the so called EAP strategies. The EAP authenticator is generally set in the Network Access Server (NAS), the EAP server can be co-placed with the EAP authenticator. An EAP conversation comprises of a few request/response messages traded between the EAP peer and server. More absolutely, in the standalone authenticator model, the correspondence between the EAP server and standalone authenticator happens generally in the same node.

An EAP identification is needed for every management operation. A few attempt has initiating late been initiated in this course [12], in any case it is still in its starting session of definition, without giving any acceptable plan. For any condition, the plan of the ABFAB drives for federation does not provide SSO volume that permits to combine the mechanism and management access identification. In addition, ABFAB propels for consortium compel new restructure and utilization on present application administrations utilizing GSS-API to backing the EAP process. On the other hand, result does not want such changes in all, application benefits initiating now help the utilization of Kerberos. As observation, the cause behind it is that, generally, present application benefit initiating now backing GSS-API validation parts focused around the quality Kerberos rule, for instance, GSS-API Kerberos V5 [13] or Kerberos V5 SASL [14].

Once the management application gets a GSS-API token consists an EAP packet, the GSS-API can contact the disposition federation through the AAA foundation by implementing of an AAA rule. With a particular end aim to correlate the management access verification with a backend identity federation, the undertaking has outlined an modified GSS-API component that implements the EAP rule as authentication mechanism. So the management application can definitely confirm to the end client by system for EAP, which is transformed within the considered GSS-API tokens. The course of action in like manner manages end client evaluate by means of convey SAML-based attributes over the AAA system. As a subsequence of this broaden, a substitute working collecting has been restricted in the institutionalization natural item IETF (Internet Designing Task Force) with the cause for generating and institutionalizing the innovations needed for operating the character federation formed in Moonshot. This working gathering is called ABFAB (Application Bridging for United Access Beyond Web). Specifically, the working gathering is characterizing a GSS-API part for EAP [10] and a transformation for SAML-based approved data over RADIUS [11].

The measure point of this undertaking is to generate a combined access to management in point of the utilization of the GSS-API and EAP as the keystones of a non specific system for identification and privacy association foundation within the end client and the unified management. Since a few application advantages as of now backing GSS-API as the technique for identification, it is general that the backing of EAP within GSS-API could be added to them with a limited strain and complex nature. The project Moonshot [16] is a earlier build that observe the utilization of included things in applications that are not concentrated around web. Moonshot shows up under the umbrella of the TERENA EMC2 assignment force. Indeed, to amalgamate the management access identification with a backend character federation, the undertaking has structured another GSS-API system that implements the EAP rule as identification system. With the aim that the management application can validate the end client by technique for EAP, which is convey within the GSS-API tokens. Once the management application gets a GSS-API token consist an EAP packet, the GSS-API can contact the authentication federation through the AAA infrastructure by implementing an AAA rule. The solution additionally manages end client authorization [18] via handling SAML-based attributes over the AAA infrastructure. Access to the network is accepted, and how it is operated is out of the extent of this committing. Then again, the sending of the ABFAB enhancement for federation does not give SSO abilities [15] that allow to connect the network and management access identification. Actually, an EAP identification is required for each administration access. Some work has as of late been started in this direction [17], anyway it is still in its starting phases of definition, without giving any acceptable result.

3. Implementation Details

3.1 The Elements of Architecture

Most of the elements required for the proposed architecture are already present in the eduroam architecture, though some of them will include additional functionality to accomplish the objective of this proposal. In the following, an enumeration of these elements and a brief description of their functionality are presented. Figure 1 shows the elements of the architecture and the protocols that allow communication between each pair of entities.

3.1.1 End User

This entity represents an end user that first authenticates to access the network service provided by visited institution using eduroam/DAMe and, after that, desires to access services.

3.1.2 Radius Server in the home institute

This component is already present in the eduroam architecture. It communicates with the IdP.

3.1.3 Radius Server in visited institute

This component is also already present in the eduroam architecture. It communicates with the IdP. And user request is transported through this server to the respective institute.

3.1.4 IDP

This component, defined in the DAMe architecture, is responsible for providing both end user's attributes to the requesting parties and eduToken to the home RADIUS server after a successful authentication of the end user.

3.1.5 eduToken

This is a type of packet which consist of detail information about end user.

3.1.6 Access Point

This component is present on eduroam and acts as the point of attachment to the visited institution's network. It interacts with the RADIUS infrastructure to authenticate the end user and provides network connectivity after a successful authentication.

3.1.7 TGS

TGS (Ticket granting Server) is responsible for granting ticket to the end user so that the user can access different types of services in the visited institution.

3.1.8 PDP

It manages the access control policy set of the visited institution.

3.2 System Architecture

Eduroam that is education roaming is a network of network federations which is generally developed for researchers, students and staff from institutions which are part of eduroam network i.e. participating institutions. The eduroam framework supports user authentication and essential authorization systems, the DAMe (Deploying Authorization Mechanisms for federated administrations in eduroam building design) is basically used for the proposition of enhancing the federated network access situation of eduroam. Kerberos is nothing but, a protected three party protocol for authentication also key administration focused on shared secret key cryptography. Kerberos is a standard protocol which is turning into amongst the most generally deployed for authentication and key distribution in application administrations. The fundamental objective of our work is to process an authentication and authorization framework for federated administrations facilitated in the eduroam network. The basic aim of DAMe is to give progressed authorization administrations to eduroam considering not just the end user authentication process, additionally extra features like privilege, roles etc. which are assessed before giving or denying network access.

In our work, the member of institution can access the internet from any institution which is part of the eduroam by using his own credential of home institution and also able to access other services which may be provided by visited institution. Indeed it is very important to define some access control mechanism to access these services provided by visited institution. In this article this paper proposes advanced authorization based on user attributes that are defined in his home institution that are used to provide services to the end user who is roaming from his home institution. This work additionally proposes the dissemination of an authentication token, which is proposed to be utilized for access to other services, along with the cross-layer SSO (Single Sign-On). In our work, we have provide different authorities to various types of users in our system. So that priorities can be set to every user. We are focusing on attribute based authorization. So, according to parameterized access control user priority is set.

In this architecture the end user enters username & password in the browser then both the details proceeds to TGS server. The IDP block receives the user details and access the relevant data form idP. The encryption [17] process starts after accessing the data and revert back to the TGS server in encrypted form. In this operation one secrete key is generated for privacy purpose. After that the data move on to Radius server and contents referred with PDP. Now the existing data decrypted. The user provided password compared with available data content. If both the data matched then user can get access to Radius server.

Depending upon the user role in his home institute user get services. As a example for web service we have taken internet as example and for non-web service we have taken database as a service. On can take printer as a hardware as a service. Figure 1 shows the proposed system architecture.

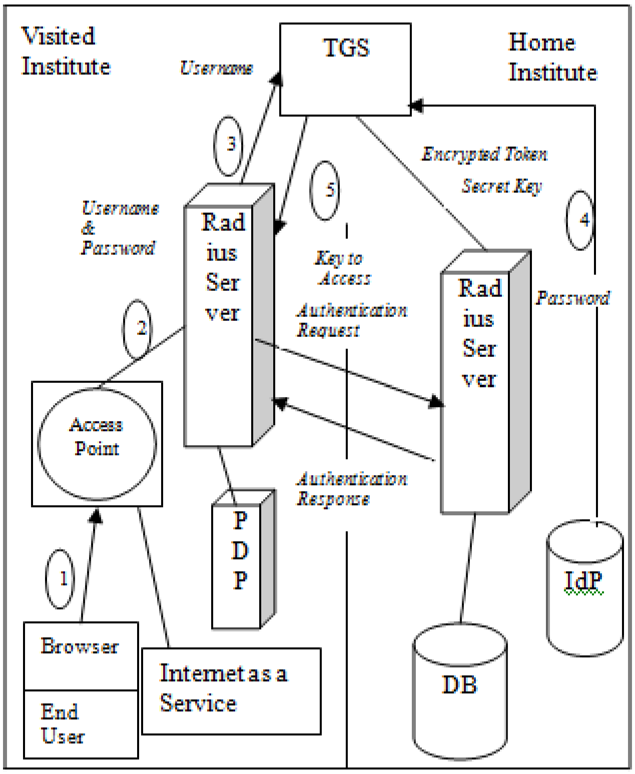

Figure 1: Proposed System Architecture

3.3 Algorithm

Following are the algorithms [7] used in our propoed system.

The following notations are used below in the algorithms.
Where,
AP- Access Point
EU- End User
IDP- Identity Provider
EAP- extensible authentication protocol
VR- Visited Institution Radius Server
HR-Home Institution Radius Server
PDP- Policy Decision Point
KDC- Key Distribution Center.
TGS – Ticket Granting Servers.

For network authentication following process is done.

1. System →: AP: Start
2. AP→EU:eap_req
3. EU→AP:eap_res
4. AP→VR:[Access-Request(anonymous@home,eap-res)]
5. VR→HR:[[Access_Request(anonymous@home,eap-res,keying material, randomizer,mac)]Mackey_vr_hr]
6. HR→VR:[Access_Challenge (anonymous@home, eap-req)]
7. VR→AP:[Access_Challenge (anonymous@home, eap-req)]
8. AP→EU: eap_req
9. Repetition of steps from 1 to 7. After several steps HR finalize the authentication.
10. VR→HR:[[Access_Request(anonymous@home,eap-res, keying material, randomizer,mac)] Mackey_vr_hr]
11. HR→IDP: {AuthnRequest(username)}HR-1} IDP
12. IDP→HR:{{SAML Response(eduToken)}IDp-1} HR
13. HR→EU:{edu token}tk
14. HR→VR:[[Access-accept(emsk_name, eap_succ,psuedonym,msk, {keying_material(dsrk)randomizer mac}mackey_vr_hr)
15. VR→AP:[Access-Accept (emsk_name, eap_succ, pseudonym, msk)]
16. AP→EU:eap_succ

Steps for Kerberos pre-authentication and TGT acquisition are as follows.

1. System →End User: Start
2. EU→KDC:AS_REQ(WELL-KNOW:ANONYMOUS, PA_PK_AS_REP (dh_eu))
3. KDC→EU:AS_REP(WELL-KNOW:ANONYMOUS, PA_PK_AS_REP(dh_kdc,{sign_data}KDC-1}
4.EU→KDC:AS_REQ(WELLKNOWN_FEDERATED,PA_FX_FAST_REQUEST({armor_TGT}key_as_tgs{enc_fast_req(PA_EDUTOKEN(eduTOKEN, emsk_name, [ts]reply_key), req_body)}armor_key))
5. KDC→VR:Access_Request(emsk_name, keying_material,randomizer,mac)]Mackey_kdc_vr]
6. VR→KDC:[[Access-Accept(emsk_name, {keying_material(dsusrk)}keymat_key_kdc_vr, randomizer, mac)]Mackey_kdc_vr]
7.KDC→EU:AS_REP(pseudonym,PA_FX_FAST_RESPONSE({enc_fast_rep}armor_key),{TGT(eduToken,session_key)}key_as_tgs, {enc-part(session-key)}reply_key)

Following are the authorization and ST acquisition steps.

1.EU→KDC:TGS_REQ(service,TGT(eduToken,session_key)}key_as_tgs,{authenticator}session_key)
2.KDC→IDP:{{AttributeQuery(pseudonym, service)}KDC-1)IDP}
3. IDP→KDC:{{SAMLResponse(attributes)}IDP-1}KDC
4. KDC→PDP: {{Authorization Decision Query(service, attributes)} KDC-1}PDP
5. PDP→ User: {User_type, authority attribute}User type – Student, Principal, Admin. Authority attribute-Modify,change, View, Read, Write, All access.
6. PDP→KDC: {{Authorization Decision Response(decision, obligation)PDP-1}KDC
7. KDC→EU: TGS_REP (pseudonym, {ST(service_session_key)}service_key,{enc-part (service_session_key)}session_key)

4. Proposed Algorithm

Following is the algorithm used in our proposed system.
1: End User → AP: Start
2: AP → EU: request for username and password
3: EU → AP: username and password
4: AP → VR :[Access-Request(TGS)]
5: VR → HR and TGS: [Access Request(username)]
6: Symmetric Key Encryption

- HR and TGS → VR:[Encryption(Key, Password)]
- TGS Encryption Process Using AES Algorithm

7: Decryption process
if(Decryption successful)
{
Authentication Successful
}
else

{
Authentication FAIL
}
8: Repetition of steps from 1 to 7. After several steps HR finalize the authentication.
9: HR → PDP: [Authorization]
9: IDP → HR: [Depending upon the privileges of End User]
10: VR → AP: [Access-Accept]
11: AP → EU: Successful

5. Mathematical Model

The system S is represented as:
S = {A, T, C, P}

a. Authentication

Consider A = {S, R}
i. client sends request to AS
Let S is a set of request sends
S = {s1,s2,s3…}
Where,
s1,s2,s3.. are the no of requests.
ii. AS respond for request to client
R = {r1,r2,r3…}
r1,r2,r3…. are the number of responds.

b. Token Generation

Let, T is a set of token generation for session
T = {t1,t2,t3,….tn}
Where, t1,t2,t3…are the number of tokens.
iii. Client request for token and token sends to client

c. Client Communication with Application Server

Let C is a set of communication happen between client and AS
C = {c1,c1,…..}
Where, c1,c2.. are the number of communication done between them.

d. Advanced Authorization

consider, P is a set for priority wise advanced authorization.
P = {p1,p2,…..}
Where, p1,p2,…are the number of priorities assigned

6. Experimental Results

In this section the results are taken by setting the eduroam architecture using two system. One system is playing as home institute role and other as visited institute role. The two systems are connected using Ethernet Lan cable. Following is the graph plotted as on x- axis we have taken different entities related to roaming end user and on y-axis time. Below graph shows details.

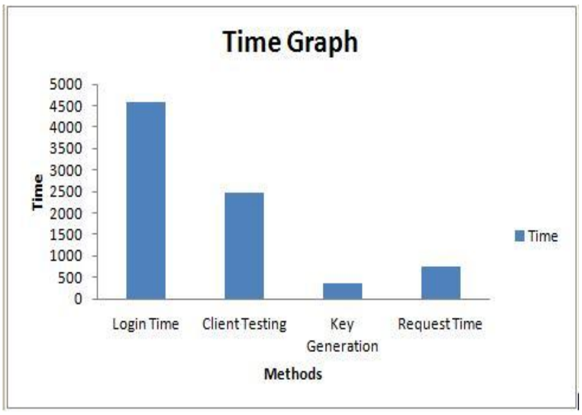

Figure 2: Resultant Graph

7. Conclusion

This paper describes how the worldwide spread eduroam system can be reached out to provide end user access to federated advantages past the web. DAMe offering gives consent what's more token circulation to establishments ready to offer added worth system access management to meandering clients. Also we describes how the roaming user attributes are used for accessing federated added value service in the visited institution and depending upon the role of user in home institution. By integrating the eduroam architecture in the Kerberos protocol. This kerberos protocol helps to achieve the eduroam properties or characteristics. As a example for web service we have taken internet as service example and for non web service we have taken database as service. As a future work one can think of integrating eduroam architecture using public key cryptography in kerberos protocol. And also more advanced authorizations can be achieved using roaming user attributes.

References

[1] Arias-Cabarcos, Patricia, Almenarez-DAMe Project. http://dame.inf.um.es.
[2] GEANT Project. http://www.geant.net/pages/home.aspx.
[3] Neuman, C., Ts'o, T.: Kerberos: An Authentication Service for Computer Networks. IEEE Communications 32 (1994) 33–38
[4] Neuman, C., Yu, T., Hartman, S., Raeburn, K.: The Kerberos Network Authentication Service (V5) (2005) http://www.ietf.org/rfc/rfc4120.
[5] Thomas, M., Vilhuber, J.: Kerberized Internet Negotiation of Keys (KINK) (2003) http://ietfreport.isoc.org/all-ids/draft-ietf-kink-kink-06.txt.
[6] Kohl, J., Neuman, C.: The Kerberos Network Authentication Service (V5) (1993) http://www.ietf.org/rfc/rfc1510.
[7] Alejandro Pérez-Méndez, Fernando Pereñíguez-García, Rafael Marín-López, Gabriel López-Millán, "A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network" International Journal of Information Security, Springer-Verlag November 2012, Volume 11, Issue 6, pp 365-388 Date: 23 Aug 2012.

[8] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP). RFC3748, June 2004.

[9] Marín-López, Rafael, Pereníguez, Fernando, López, Gabriel, Pérez-Méndez, Alejandro: Providing EAP-based Kerberos preauthentication and advanced authorization for network federations. Comput. Stand. Int. 33(5), 494–504 (2011)

[10] Hartman, S., Howlett, J.: A GSS-API Mechanism for the Extensible Authentication Protocol. IETF Internet Draft, IETF draft-ietfabfab-gss-eap-04.txt, October 2011.

[11] Howlett, J.:A RADIUS Attribute, Binding and Profiles for SAML. IETF Internet Draft, IETF draft-ietf-abfab-aaa-saml-02.txt, October 2011.

[12] Wei, Y.: Federated Cross-Layer Access. IETF Internet Draft, October 2011.

[13] Zhu, L., Jaganathan, K., Hartman, S.: The Kerberos Version 5 Generic Security Service Application Program Interface (GSSAPI) Mechanism: Version 2. IETF RFC 4121, July 2005.

[14] Melnikov, A.: The Kerberos V5 (“GSSAPI”) Simple Authentication and Security Layer (SASL) Mechanism. IETF RFC 4752, November 2006.

[15] Wen-Guey Tzeng Jianying Zhou Cheng-Kang Chu, Sherman S. M. Chow and Robert H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. Parallel and Distributed Systems, IEEE Transactions, Volume(106):468- 477, 2014.

[16] Howlett, J.: Hartman. Project Moonshot, S. (February 2010).

[17] William Stallings. Cryptography and Network Security Principles and Practice. (FifthEdition).

[18] G. Lopez, O. Canovas, A. F. Gomez-Skarmeta, and M. Sanchez, “A proposal for extending the eduroam infrastructure with authorization mechanisms,” Computer Standards Interfaces, Elsevier BV, vol. 30, pp. 418–423, 2008