Bootstrapping a Global SSO from Network Access Control Mechanisms

Manuel Sánchez[1], Gabriel López[1], Óscar Cánovas[2], and Antonio F. Gómez-Skarmeta[1]

[1] Department of Information and Communications Engineering
[2] Department of Computer Engineering
University of Murcia, Spain
{msc,gabilm,skarmeta}@dif.um.es,
ocanovas@ditec.um.es

Abstract. This paper presents the details of a Single Sign On proposal which takes advantage of previously deployed authentication mechanisms. The main goal is to establish a link between authentication methods at different levels in order to provide a seamless global SSO. Specifically, the users will be authenticated once, during the network access control phase. Next, having authenticated to get on to the network using 802.1X, that authentication will automatically fetch the necessary signed tokens so that there would be no need to repeat the login at the application layer. Therefore, the application level authentication would be bootstrapped from the network access. As we will see, this involves the generation of SAML signed tokens that will be obtained by the users using a PEAP channel able to deliver the appropriate authentication credentials. Then, users will contact a federation-level validation service and there will no need to re-authenticate the user, only a query of the related user attributes will be necessary in some cases.

Keywords: SSO, authorization, SAML, federation.

1 Introduction

In the last years, we have experienced the emergence of federated approaches to resource sharing. In this approaches, trust links are established among different autonomous organizations in order to grant users in any of them access to shared resources with a single identity, stated by the organization the user belongs to. Important examples of these approaches are the establishment of academic federations worldwide, like eduroam, InCommon, HAKA or SWITCH. In those scenarios where users are moving among the different organizations pertaining to the federation, authorized users may also have additional resources at their disposal at the visited institutions.

Despite many aspects of federations have been addressed by several projects, other issues generally related with integral identity management are still open. For example, in those scenarios where authentication mechanisms have been included for network access control purposes, it would be interesting to create a seamless link between the network-layer authentication mechanism and any additional authentication step that will be needed when users try to gain access to application-level resources. This would involve the extension of the network access mechanism in order to deliver additional

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 170–180, 2007.

information (some kind of security credentials) that might be used at service-level in order to avoid further user re-authentication.

The work presented in this paper is one of the objectives defined by the DAMe project [1]. Once the eduroam infrastructure has been extended so that user mobility will be controlled by security assertions and policies expressed in standard and extensible languages, such as SAML [5] and XACML [4], the next phase is to provide a global Single Sign On (SSO) mechanism based on that extension. Eduroam constitutes an exceptional starting point in order to provide a mechanism for transmitting the user credentials that will be used by the application-level authorization systems in order to offer a full and integrated network access experience to the users. As we will see, we have defined two different steps in order to achieve the SSO. The first one is related to the delivery of a security token during the network access that will be later used to avoid unnecessary re-authentication. Then, once that token has been transmitted to the user, it will be necessary to define how an application-level service will be able to validate that information using a federation-level service. Specifically, we will follow some guidelines already stated by the technical community in order to provide global SSO.

The rest of this paper is structured as follow. Section 2 provides an overview of the DAMe project and introduces the underlying roaming infrastructure. Section 3 describes eduGAIN, an authentication and authorization infrastructure that will be used in order to provide a common validation service. Section 4 points out the set of requirements derived from a SSO scenario and section 5 describes the proposed architecture. Then, section 6 contains a survey of other proposals that informed our work. Finally, we conclude the paper with our remarks and some future directions.

2 DAMe Project: Adding Authorization to Eduroam

The eduroam network [15] is an inter-institutional roaming service based on the 802.1X architecture [8] and a hierarchical RADIUS-based infrastructure. This initiative allows users of participating institutions to access the Internet at other participants using their home institution's credentials, all this with a minimal administrative overhead. Nowadays, eduroam is a production service that is used in more than 350 institutions over 19 countries (European and Australian-Pacific) with a great success.

Figure 1 depicts the typical scenario in eduroam. It shows a user from Institution A who moves to Institution B, both pertaining to the eduroam federation. In the new institution, the user wants to get access to the wireless network. In this situation, access control is carried out following the 802.1X standard. That is, the user associates with the wireless access point (AP), which contacts its local RADIUS server in order to authenticate the user. But when this server identifies that the user belongs to a different domain, for example based on the user identifier, the authentication request is forwarded through the RADIUS hierarchy to the server located in the user's home institution. Then, the user is authenticated and the response is routed back to Institution B, where the AP enables the requested connection.

However, eduroam only takes into account the identity in order to carry out the access control process. In this way, it is not possible to offer different services or restrict the access to some resources based on the user profile, defined for example by means of