Shibboleth authentication for non-web application

ANDREA BIANCINI, INFN - Sezione Milano Bicocca
andrea.biancini@mib.infn.it
FABIO FARINA, Consortium GARR
fabio.farina@garr.it
SIMON VOCELLA, Consortium GARR
simon.vocella@garr.it

Abstract Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Categories and Subject Descriptors: C.2.2 [**Computer-Communication Networks**]: Network Protocols

General Terms: Shibboleth, PAM, JAAS

Additional Key Words and Phrases: Shibboleth, SAML, Basic authentication, PAM, JAAS, Python

ACM Reference Format:
Biancini A., Farina F., Vocella S. 2012. Shibboleth authentication for non-web application. ACM Trans. Embedd. Comput. Syst. 9, 4, Article 39 (March 2010), 3 pages.
DOI = 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

1. INTRODUCTION

User authentication and user authorization are main tasks needed to guarantee security in IT environments. One important requirement of such security solutions, is that they must be as transparent as possibile. In systems where resources sit on different systems and environments, which are a common reality for the users, a solution must be found to eliminate the need for each system to create and manage its own credential system. For such reason single sign-on (SSO, as described in [Shaer 1995]) systems have been designed and implemented to achieve such goal.

One of the most widespread SSO software package is Shibboleth [Morgan et al. 2004], which implements authentication and authorization over network resources with a federated approach. Shibboleth, designed and implemented by Internet2, provides an effective solution for secure multi-organizational access to web resources. It implements widely used federated identity standards, principally OASIS' Security Assertion Markup Language (SAML [Cantor et al. 2005]), to provide a federated single sign-on and attribute exchange framework. Shibboleth also provides extended privacy functionality allowing the browser user and their home site to control the attributes released to each application.

Using Shibboleth-enabled access simplifies management of identity and permissions for organizations supporting users and applications. Shibboleth is developed in an open and participatory environment and is freely available. For these reason it has formed the heart of many solutions for single sign-on and Authentication & Authorization Infrastructures (AAI) in real identity federations.

The architecture of Shibboleth, described in [Erdos and Cantor 2005], identifies two main components: Identity Providers (IdPs) which authenticate the users and supply user authorization attributes; the Service Providers (SPs) which consume user attributes and provide access to the secure contents.
The communication excanges between the user, the IdP and the SP are all base don SAML assertions and transit over HTTP channels. This implementation architecture permits Shibboleth to works seamlessly inside user web-browsers. However, this approach is strongly web-centric, and for this reason does not adapt well to provide SSO authentication to non web-based application.

In this article a solution is presented to permit Shibboleth authentication for non web-based application. Different implementations will be described showing how to integrate the shibboleth AAI mechanisms inside several client applications (Linux platform, Java JAAS, Python). The rest of this paper is organized as follows: the first section contains a quick overview of related works; the second section will present the architecture of the solution presented with this article; the third section will present some details about the technical implementation in the different software platform; the last section presents conclusions and future works.

2. RELATED WORKS

3. ARCHITECTURE

4. IMPLEMENTATIONS

4.1. PAM and NSS modules

4.2. JAAS module

4.3. Python

5. CONCLUSION AND FUTURE WORKS

REFERENCES

CANTOR, S., KEMP, J., PHILPOTT, R., AND MALER, E. 2005. Assertions and protocols for the OASIS security assertion markup language (SAML) v2.0. Tech. rep. 3.

ERDOS, M. AND CANTOR, S. 2005. The Shibboleth architecture. `http://shibboleth.internet2.edu/`.

MORGAN, R. L., CANTOR, S., CARMODY, S., HOEHN, W., AND KLINGENSTEIN, K. 2004. Federated security: The shibboleth approach. *EDUCAUSE Quarterly 27,* 4, 12–17.

SHAER, C. 1995. Single sign-on. *Network Security 1995,* 8, 11–15.

Received September 2012; revised September 2012; accepted September 2012