Authentication via Proxy

By: Yusuf Bhabhrawala, Project Manager, UCLA Center for Digital Humanities (CDH)

Introduction

This article describes a proposal for building a standardized authentication proxy. This proposal was written before Shibboleth 2.0 (which address many of the limitations from the previous versions). Hence the examples of CDH and Shibboleth should be taken just as that, ie. example. This type of proxy could be implemented fairly quickly by any organization and for any other authentication system as well.

Overview

The model proposed here is very widely used for providing authentication as a service. The model can be summarized using the following diagram:

1. The user login request is redirected to CDH Auth Proxy along with callback URL.
2. Since CDH Auth Proxy sits behind Shibboleth, the user is redirected to UCLA Logon page where they can authenticate themselves.
3. The UCLA Shibboleth IDP redirects the user to CDH Auth Proxy.
4. CDH Auth Proxy post's a public token to the callback URL.
5. The application uses the public token to generate a private token and requests user information from CDH Auth Proxy using it.
6. CDH Auth Proxy responds with the user information.

The above approach provides a simple authentication model that can be used to implement authentication fairly quickly, develop drag and drop authentication solutions and develop wordpress, joomla, drupal, plone etc. plugins very easily. These can then be used by UCLA Humanities division faculty, students and staff without getting into the details of shibboleth SP implementation.

Technical Details

Shared Secret

The basis of this authentication model is a secret (character string/password) shared between CDH and the application requiring authentication. This shared secret is used for generation of time stamped tokens and token validations. It also ensures that shibboleth cannot be used without some kind of prior approval or record.
Shared secret is specific to a URL. It thus ties the application with its unique shared secret ensuring that tokens are not misused across applications.

Shibboleth Data

CDH will collect and pass only the following information regarding the user:

- First Name
- Last Name
- Email ID
- UID
- Department Code

This information is already available via UCLA directory and accessible by all.

Public Token

The public token is a message digest generated using the following information:

- Email ID
- Shared Secret
- Time stamp (up to seconds)

This ensures that the token is unique to the user, to the requesting application and cannot be re-used.

Private (use once) Token

The private token ensures that the user information is securely transferred from server to server and cannot be re-used.
The private token is a message digest generated by the requesting application using the following information:

- Public Token

- Shared Secret

Each user session is maintained at CDH Auth Proxy for 30 seconds, during which it can be retrieved by the requesting application by providing the corresponding private token, which of course, is unique to the user.

CDH will respond with the user information in a JSON format as key-value pairs, one of which will always be ‘status’. Thus the status determines if the user information was successfully received.

Revision #1
Created 2010-08-27 19:52:41 UTC by Bhabhrawala, Yusuf
Updated 2010-08-27 20:05:23 UTC by Bhabhrawala, Yusuf