Shibboleth – A Federated Authentication Approach

BRIITE
9/23/04

http://middleware.internet2.edu/shibboleth/

Sandra Senti
senti@uchicago.edu
University of Chicago

What is the problem?

- *Securing networked resources is of crucial importance*
- *High speed networks increase the need for managing and controlling access to resources*
- *Both institutions and granting agencies have a heightened focus on inter-institutional collaboration*
- *Security and identity management are critical challenges on campus today*

What is Shibboleth?

- An initiative to develop an architecture and policy framework supporting the sharing – between domains -- of secured resources and services, initially focusing on web resources

- A project delivering an open source implementation of the architecture and framework

What is Shibboleth?

A system...

…with an emphasis on privacy

- users control release of their attributes

…based on open standards (SAML) and available in open source form

…built on "federated administration"

What is Shibboleth?

- *Supports secure user access to web-based resources*
- *Enables independent organizations to federate to extend the capabilities of their existing identity-management services*
- *Supports multi-organizational federations to enable scalable use of the technology*
- *Encourages attribute-based authorization*
- *Provides controls to protect the privacy of personal information*
- *Is standards-based and open-source*
- *Is evolving to support new uses and new communities*

Shibboleth principles

- *Federated identity*
  - allows organizations using disparate authentication and authorization methods to interoperate
  - Helps users by taking advantage of their familiarity with existing sign-on systems
- *Attribute-based authorization*
  - Provides user attributes to applications during the sign-on process
  - Built-in attribute support based on eduPerson directory schema
  - Plugs into existing institutional identity management and user management systems (such as LDAP)

Shibboleth Principles

- *User privacy protection*
  - Provides mechanism for management of attribute release policies
  - Permits fine grained control of release of information based on resource provider
  - Provides methods for establishing defaults and administrator control

- *Federations must agree upon*
  - Security mechanisms used among Shib servers
  - Definition of attributes
  - How to locate the servers of other participants

How does it work?

Shibboleth has two major software components:

- Shibboleth Identity Provider (IdP)
- Shibboleth Service Provider (SP)

The players include:

- The user who wants to access a protected resource
- The resource provider web site which has installed the Shibboleth SP software
- The user's home organization which has installed the Shibboleth IdP software

What is the process?

1. *The SP software redirects the browser to a navigation page which presents the user with a list of the organizations which may access the resource.*
2. *The user navigates to the protected web resource.*
3. *The user selects the home institution and the browser is sent to home organization's web site running the IdP software. This site uses a web sign-on method chosen by the home institution.*

How does it work?

4. *The IdP software sends the browser back to the original site and includes in the message security information (assertion) that proves the user signed on. The SP software validates the assertion and then requests additional information about the user as needed.*
5. *The SP software received the user's attributes from the home organizations IdP and passes them on to the web application.*

Shib in Action

- *Student-oriented information system – Penn State and Napster Music Service*
- *Academic information provider – JSTOR (archive of scholarly journals)*
- *Outsourced employee application*
- *Extended user populations- University of Washington's Catalyst system offers educators an integrated collection of tools to make effective use of web-based instruction*

Shib in Action

- *Research collaboration*
  - Sophisticated computing resources and participants from multiple organizations
  - These virtual organizations can use Shib to control access to their web-based resources
  - University of Washington has created a research federation
  - Requirement for controlled access to non-web resources
  - Grid security researchers and Shib project members are working to integrate the two multi-institutional access infrastructures
  - Focus on Shib IdP software providing user attributes to non web-based grid applications
  - Expected completion In 2005

InCommon Federation

- *Established by Internet2*
- *Formal federation of organizations focused on creating a common framework for trust in support of research and education*
- *Includes identity providers (primarily US higher-education sites) and resource providers (partners such as commercial information and service providers as well as higher-education sites)*
- *Supports use of Shib by its participants*

Technical Components

Origin Site

- Handle Server
- Attribute Authority

Target Site

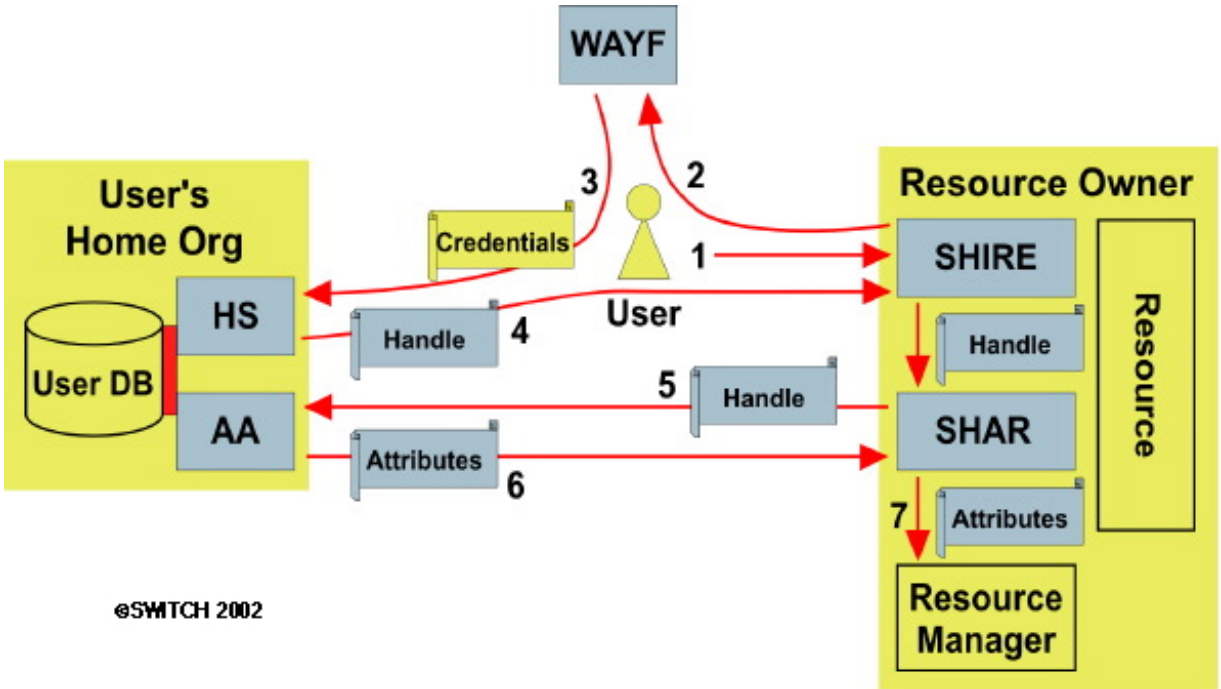
- SHIRE
- SHAR
- WAYF
- Resource Manager

Existing assumed components:

for origins - Campus directory or attribute store; Web-ISO

for targets - web servers and resource managers

High Level Architecture



Questions?