An Introduction to MIT Touchstone and beyond: web authentication in a federated world

IAP 2009

(recap of ITAG Luncheon Talk given in October of 2008)

Paul Hill

Information Services & Technology

Massachusetts Institute of Technology

Who?

- Bob Basch
- Vijay Konda
- Arnis Kletnieks
- Mark Silis
- Laura Watts
- Joanna Proulx
- Brian Knoll
- Paul Hill

Landscape

- People collaborate with others across traditional organizational boundaries
- Experiments may have teams that include members from dozens of organizations
- Data and other materials may be scattered across dozens of sites

What we're trying to do

- Provide a web authentication infrastructure that doesn't require everyone to have "an MIT account"
- Provide a web authentication infrastructure that doesn't require "an MIT person" to have accounts at dozens or hundreds of other sites
- Make sure the infrastructure supports "high value" transactions
- Provide "an easy way" to integrate this into your web applications

IST

Guiding principles

- Support situations where the use of X.509 certificates for user authentication are not practical
- Do not send user's password through each web server
- Provide single sign-on as much as practical
- Able to adopt new technologies
- Use technologies that are likely to be integrated into 3rd party products

Technology building blocks

- Shibboleth
  - IdP (run by IS&T, and other sites)
  - SP (your app)
  - Shib-HA (on IdP)
  - WAYF
  - SAML
  - LDAP
- Stanford WebAuth
  - Username and password
  - X.509
  - Kerberos tickets
- Collaboration Accounts
- InCommon

Collaboration Accounts

- A new accounts management system
  - "external users" by email address
- An SP
  - Self registration / self service
- An IdP and Login server
  - Email address / password
  - OpenID
  - Cross realm Kerberos

Timeline

- Pilot for MIT core community started October 11th, 2007
- Since November 2007: Stellar, Wikis.mit.edu, Jira
- Since September 18 2008: Collaboration accounts
- Open to all interested system integrators – October 2008
- Consulting services now available – October 2008
- Core MIT IdP working with InCommon – December 31st, 2008

Most Recent Applications

- devlopers.mit.edu
- Ideabank.mit.edu
- www.dreamspark.com (Students only)

Metrics by mechanism

Oct 1 to Dec 31	Total
Username / password	45222
Kerberos tickets	1025
Certificates (added 9/18)	3224
Total initial authentications	49571

Metrics by application

July 1 to Sep 30	total
Jira	1479
Wikis	1502
Stellar	62144
Teamspaces	1476
Total	66601

The total counts are not the same. The previous slide only measured initial authentications and does not take into account SSO transitions between applications. Nor session expiration.

Applications in the pipeline

- MIT Libraries
  - "Your Account" in Aleph
  - Storage Annex Document Delivery
  - Geo Web
  - Dspace
- Hermes
- Quickpages
- Thalia
- Citrix farm access
- HR applications
- scripts

Developer support now available

- Consulting services
- Staging servers for integration testing
- Installation and configuration documentation
- In process:
  - Improve the provisioning process
  - Best practices / guidelines for developers
  - Sample source code in multiple languages

Some variables available to your application: idp.mit.edu

HTTP_SHIB_AUTHENTICATION_METHOD
urn:oasis:names:tc:SAML:1.0:am:unspecified

HTTP_SHIB_EP_AFFILIATION
staff@mit.edu

HTTP_SHIB_EP_PRIMARYAFFILIATION staff

HTTP_SHIB_EP_UNSCOPEDAFFILIATION staff

HTTP_SHIB_IDENTITY_PROVIDER
https://idp.mit.edu/shibboleth

REMOTE_USER

pbh@mit.edu ***

HTTP_SHIB_EP_NICKNAME

Paul B Hill

HTTP_SHIB_INETORGPERSON_DISPLAYNAME

Paul B Hill

HTTP_SHIB_INETORGPERSON_MAIL
pbh@mit.edu

***This is a scoped attribute, not an email address.

Optional:

HTTP_SHIB_ORGPERSON_ORGUNIT
Information Services & Technology

Some variables available to your application: idp.touchstonenetwork.net

HTTP_SHIB_AUTHENTICATION_METHOD
urn:oasis:names:tc:SAML:1.0:am:password

HTTP_SHIB_IDENTITY_PROVIDER
https://idp.touchstonenetwork.net/shibboleth-idp

REMOTE_USER
john_1@touchstonenetwork.net ***

HTTP_SHIB_INETORGPERSON_DISPLAYNAME

John Doe

HTTP_SHIB_INETORGPERSON_MAIL

john@example.com

***This is a scoped attribute, not an email address.

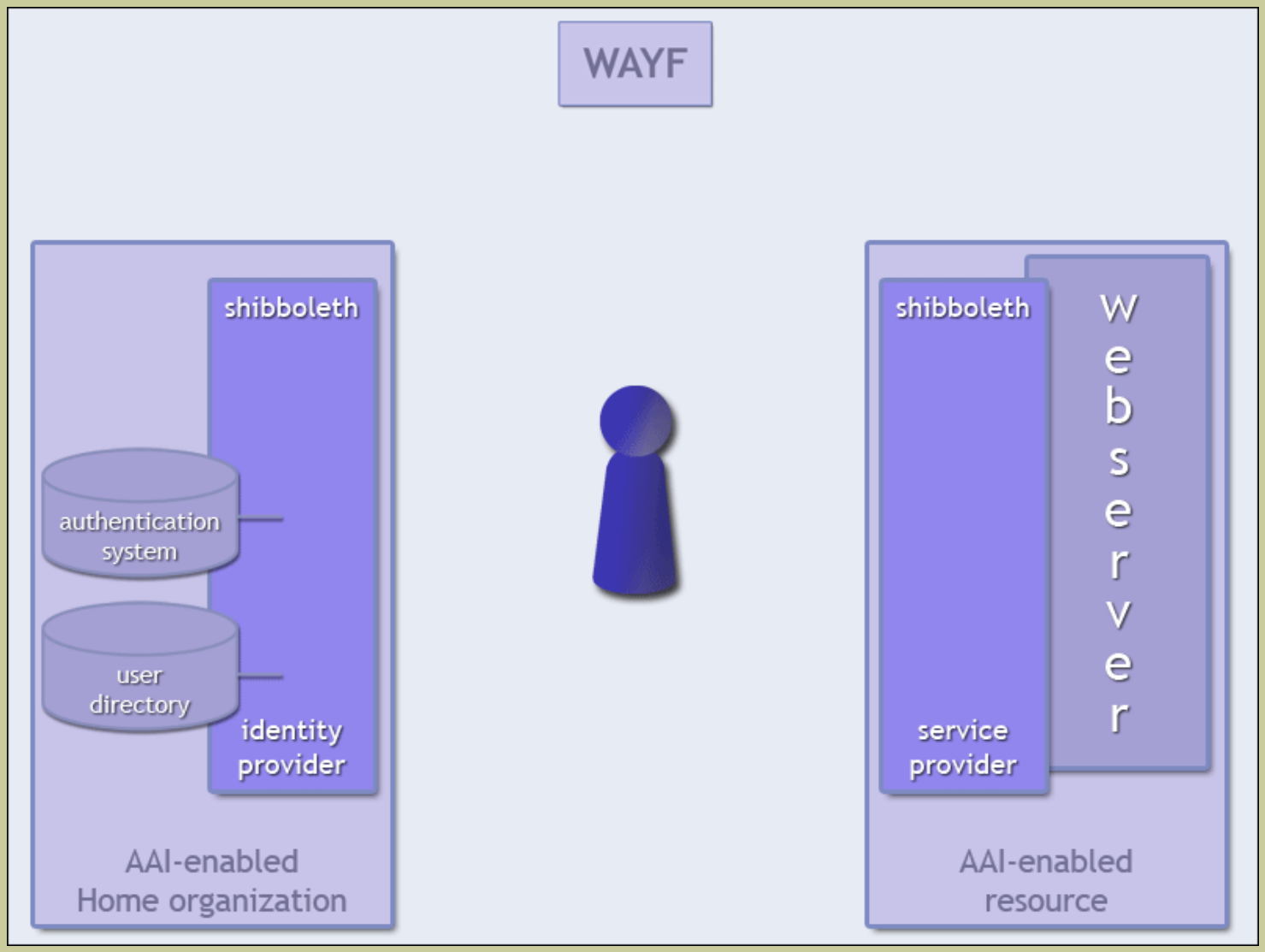
InCommon

- The mission of the InCommon Federation is to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States. - http://www.incommonfederation.org/about.cfm
- Currently has ~119 participating organizations - http://www.incommonfederation.org/participants/
- First step: add only the MIT IdP to the membership

InCommon

- Has approximately 190 IdP and SPs
  - "DreamSpark is simple, it's all about giving students Microsoft professional-level developer and design tools **at no charge"**
  - StudentsOnly is a division of StudentUniverse.com, specializing in automated student enrollment verification
  - NIH.gov federation gateway
  - http://www.info.scopus.com/archivingproject/
  - http://info.sciencedirect.com/
  - http://www.jstor.org/

Shibboleth redirects



Demo…

- Teamspaces
- Jira
- CAMS

Parting thoughts

- It’s easy
- It’s becoming mainstream
- http://mit.edu/touchstone/
- Send mail to touchstone-support