Shibboleth: Molecules, Music, and Middleware

(Pictures omitted for copyright compliance)
Caveats/Assumptions

• Assumption
  – familiarity with Internet2/NMI-EDIT acronyms, vocabulary, terminology
  – If we don't spell something out, call us out immediately – please don't wait

• Caveats
  – "I'm with stupid"-Renee
  – "I'm with sleep deprived -> " -Kevin
Outline

- Problem statement
- Solution space – Shibboleth and Federations
- Description of Shibboleth
  - 3 example of Shib uses at Penn State
- Description of Federations
  - A look at InCommon
- What's it take to do all of this?
What's the problem?

- We're serving lots of people (120,000)
- Those people want access to web-based information resources
- Rising legal, ethical, and economic development concerns about legal consumption and distribution of digital information
- Continued concerns about privacy, growing concerns about privacy
What's a solution?

- Shibboleth
  - Let's use our existing infrastructures, processes, identities
  - Preserves anonymity, provides tools for managing privacy
  - We can provide pathways for appropriate/legal consumption and distribution of digital materials
What's a solution?

• Federations
  - Provides an infrastructure of trust ("trust fabric")
  - Associations of enterprises come together to exchange information about their users and resources in order to enable collaborations and transactions
  - Built on the premise of "Enroll, authenticate and attribute locally...Act federally."
  - Two well known federations in higher education in the U.S. are InQueue and InCommon
Shibboleth – What is it?

- An Internet2 middleware initiative designed to provide federated access management between Web-based resources
- Allows you to authenticate locally and access Web resources from other institutions or sites
- Can be used to make complex, directory-based authorization decisions
- Preserves privacy of individual from remote site
Shibboleth
High Level Architecture

- Service Provider site (SP) and (Identity Provider) IdP site collaborate to provide a privacy-preserving “context” for Shibboleth users

- IdP authenticates user, asserts Attributes

- Destination site (SP) requests attributes about user directly from IdP site

- Destination site makes an Access Control Decision

- Users (and IdP organizations) can control what attributes are released

- Federations provide common Policy and Trust (more later)
Architecture (continued)

Identity Provider

Service Provider Web Site

1. User DB
2. ACS
3. Handle
4. WAYF
5. HS
6. Handle
7. Credentials
8. AR
9. Handle
10. Attributes

© SWITCH
Shibboleth at Penn State

- **Example 1 - WebAssign**
  - Access to course materials at another university
  - NC State, WebAssign, Penn State Dept. of Physics

- **Example 2 - Napster Experiment**
  - Access to digital repositories

- **Example 3 - LionShare**
  - Authenticated peer-to-peer file sharing
Example 1 - WebAssign

- **Summer 2002**
  - ~20 students, 2 weeks, 1 course
- **Fall 2002**
  - ~200 students
  - 3 courses
- **Spring 2003**
  - ~1800 students
  - Successful login: 63,026
  - All physics courses at UP location can use Shibboleth
- **Fall 2003 - Production!**
Example 1 - WebAssign

• Before Shib:
  - 1st 2 weeks, 30 questions/day
  - Most questions about login

• After Shib
  - Down to 1-2 questions/day
  - Non Shib sections still at 15 questions/day
Example 2 - Napster Experiment

- Technical challenge
  - Enable residence hall students access to web based music resource in less than 40 days
  - Initial community size ~18,000
  - 24 campus locations throughout PA
  - Roll-out to all of Penn State following semester
    - Community size ~100,000
Example 2 - Napster Experiment

• Using Shibboleth allowed/allows us to:
  • authenticate locally to the near universally-adopted Penn State Access Account
  • query attributes of individual and determine eligibility
  • present Napster with a role and unique identifier, without exposing the identity of the individual
  • hand–off transaction to Napster where individual sets up Napster account
  • execute the terms and conditions of the contract AND preserve the individual's ability to maintain the Napster relationship after eligibility changes
Example 3 - LionShare

- A federated peer-to-peer file search application
- Users can identify each other and restrict sharing
- Leverages Internet2's InCommon federation and Shibboleth middleware for trust
- Authorization is attribute-based:
  - Ex: “Share syllabus.pdf with any student at Penn State in English 202A section 15.”
Back to Federations......
Why Federations?

- Institutional users acquiring content from popular providers (Napster, etc.) and academic providers (Elsevier, JSTOR, EBSCO, Pro-Quest, etc.)
- Institutions working with outsourced service providers, e.g. grading services, scheduling systems
- Inter-institutional collaborations, including shared courses and students, research computing sharing, etc.
- Shared network security monitoring, interactions between students and federal applications, peering with international activities, etc.
Examples of Federations

- InQueue
- InCommon
- SWITCH
- ws-*
- Liberty Alliance
- Others are being developed
Deeper look at InCommon

- A federation to support the R&E community in inter-institutional collaborations
- InCommon operates at a high level of security and trustworthiness
- InCommon requires its participants to post their relevant operational procedures on identity management, privacy, etc
- InCommon will be constructive and help its participants move to higher levels of assurance as applications warrant
- InCommon will work closely with other national and international federations
How'd you do that?
“If you want to make an apple pie from scratch, you must first create the universe.”

-Carl Sagan
Baking Shibboleth/Federations

- Processes, procedures and policies for distributing and managing digital identities
  - Signature Stations, AD-20, enforcement tools, etc. -> identity management
- An eduPerson compliant enterprise directory
- Authentication method(s)
- Acceptance of the identifier
- Strategies for protecting the identifier
- Put in the oven....
Shibboleth speeds/feeds at PSU

- 7 Shibboleth servers
  - 2 for WebAssign
  - 5 for Napster
- Load balance using SLB
- Software
  - Shibboleth 1.1
- Hardware
  - IBM Blade HS20 proc 2.4GHz mem 2.5GB
Useful URLs/pointers

- http://shibboleth.internet2.edu
- Subscribe to shib mailing lists
- http://www.incommonfederation.org/
- http://lionshare.its.psu.edu
- Emerging issues/technologies/recipes
  - http://middleware.internet2.edu/signet/
  - SAML 2.0: http://www.oasis-open.org/
Contact Information

• Kevin Morooney
  – kxm @ psu.edu

• Renee Shuey
  – Rshuey @ psu.edu

• This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/2.0/ or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.