Shibboleth at CISTI
Introducing, prototyping and extending

Glen Newton, David Dearman, Carolyn Brown
Canada Institute for Scientific and Technical Information (CISTI)
The National Research Council
Ottawa, ON
Outline

- Intro to Shibboleth
Outline

- Intro to Shibboleth

- Shibboleth @ CISTI
Outline

- Intro to Shibboleth
  - What is Shibboleth?
  - What problem(s) does Shibboleth solve?
  - Shibboleth architecture
  - How does it work?
- Shibboleth @ CISTI
Outline

- Intro to Shibboleth
  - What is Shibboleth?
  - What problem(s) does Shibboleth solve?
  - Shibboleth architecture
  - How does it work?
- Shibboleth @ CISTI
  - Why?
  - Prototyping
  - Extensions
What is Shibboleth?

“Inter-realm Attribute-based authorization for Web Services”

National Research Council
What is Shibboleth?

“Inter-realm Attribute-based authorization for Web Services”

- Architecture and technology to support inter-institutional sharing of resources
- Based on a federated administration trust framework
- Controlled dissemination of attribute information, based on administration defaults and user preferences

National Research Council
What is Shibboleth? (cont.)

Founding Assumptions:
What is Shibboleth? (cont.)

Founding Assumptions:

- Federated administration
- Lightweight mechanisms: disturb as little of existing infrastructure as possible
- Leverage vendor and standards activity wherever possible
What problem(s) does Shibboleth address/solve?
What problem(s) does Shibboleth address/solve?

- Resource consumer
- Resource producer
What is Shibboleth (cont.)

What problem(s) does Shibboleth address/solve?

- Resource consumer
  - Access from on-campus

- Resource producer
What is Shibboleth (cont.)

What problem(s) does Shibboleth address/solve?

- Resource consumer
  - Access from on-campus
  - Access from off-campus

- Resource producer
What problem(s) does Shibboleth address/solve?

- Resource consumer
  - Access from on-campus
  - Access from off-campus
  - User account proliferation
- Resource producer
What problem(s) does Shibboleth address/solve?

- Resource consumer
  - Access from on-campus
  - Access from off-campus
  - User account proliferation
- Resource producer
  - IP management
What is Shibboleth (cont.)

What problem(s) does Shibboleth address/solve?

- Resource consumer
  - Access from on-campus
  - Access from off-campus
  - User account proliferation
- Resource producer
  - IP management
  - IP spoofing
What problem(s) does Shibboleth address/solve?

- Resource consumer
  - Access from on-campus
  - Access from off-campus
  - User account proliferation
- Resource producer
  - IP management
  - IP spoofing
  - User account management

National Research Council
Shibboleth Architecture

Players:

- Browser user: resource consumer
Shibboleth Architecture

Players:
- Browser user: resource consumer
- Origin Site: resource consumer’s organization
Shibboleth Architecture

Players:

- Browser user: resource consumer
- Origin Site: resource consumer’s organization
- Target Site: resource producer
Shibboleth Architecture (cont.)

Components:

- Origin Site
  - Handle Server
  - Attribute Authority
- Target Site:
  - SHIRE
  - SHAR
  - WAYF
  - Resource manager
How does it work?

1. User requests resource from publisher's website (Target)
2. User is asked to self-identify her organization (Origin)
3. User is redirected to Origin & authenticates
4. User attributes are transferred to Target
5. Target compares attributes against Policy associated with requested resource
6. User gets resource
How does it work?

1. User requests resource from publisher’s web site (Target)
How does it work?

1. User requests resource from publisher’s website (Target)
2. User is asked to self-identify her organization (Origin)
How does it work?

1. User requests resource from publisher’s website (Target)
2. User is asked to self-identify her organization (Origin)
3. User is re-directed to Origin & authenticates
How does it work?

1. User requests resource from publisher’s web site (Target)
2. User is asked to self-identify her organization (Origin)
3. User is re-directed to Origin & authenticates
4. User attributes are transferred to Target
How does it work?

1. User requests resource from publisher’s website (Target)
2. User is asked to self-identify her organization (Origin)
3. User is re-directed to Origin & authenticates
4. User attributes are transferred to Target
5. Target compares attributes against Policy associated with requested resource
How does it work?

1. User requests resource from publisher’s website (Target)

2. User is asked to self-identify her organization (Origin)

3. User is re-directed to Origin & authenticates

4. User attributes are transferred to Target

5. Target compares attributes against Policy associated with requested resource

6. User gets resource
How does it work? (cont.)
Shibboleth @ CISTI: Why?
Shibboleth @ CISTI: Why?

What is CISTI?
Shibboleth @ CISTI: Why?

What is CISTI?

- Virtual library for 3000+ NRC researchers
What is CISTI?

- Virtual library for 3000+ NRC researchers
- Scientific publisher: NRC Research Press: 15 scholarly journals (Canadian Journal Botany, etc)
Shibboleth @ CISTI: Why?

What is CISTI?

- Virtual library for 3000+ NRC researchers
- Scientific publisher: NRC Research Press: 15 scholarly journals (Canadian Journal Botany, etc)
- National and International DocDel hub (4000+ documents per day)
Shibboleth @ CISTI: Why?

What is CISTI?

- Virtual library for 3000+ NRC researchers
- Scientific publisher: NRC Research Press: 15 scholarly journals (Canadian Journal Botany, etc)
- National and International DocDel hub (4000+ documents per day)
- Canadian National Science and Technology Library
Shibboleth @ CISTI: Why? (cont.)

Why CISTI?

- a resource consumer (NRC Virtual Library)
- a resource producer (NRC Research Press)
Prototyping

- Implemented prototype for 3 NRC Research Press journals
- Authentication from LDAP and MySQL
- Tested for problems: none
- Did not test for many multiple users, etc.
Shibboleth @ CISTI (cont.)

Extensions

- Wanted attributes from MySQL database (historical problems with LDAP)
- Implemented, tested and donated code to Shibboleth
Shibboleth @ CISTI (cont.)

The NRC Virtual Library

- Interested in Shibboleth & evaluating impact on work-flow
- Initially concerned with user account / resource matching overhead
- Also looking in to possible impact on licensing
The Future

- Possible Shibboleth implementation for NRC Research Press
- Possible implementation of Shibboleth for the NRC Virtual Library
- Adoption by resource producers / resource consumers
- Designing way of doing E-Commerce (Pay-per-view) using Shibboleth