Deploying web user authentication with Shibboleth

Sören Preibusch
Then said they unto him, Say now Shibboleth: and he said Shibboleth.
Agenda

1. what, why, when: Shibboleth basics
2. how: Interaction scenarios
3. who: privacy issues
4. whoops: pitfalls and hints
What is Shibboleth?

- The Shibboleth System is a standards based, open source software package for web single sign-on across or within organizational boundaries.

- It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

http://shibboleth.internet2.edu/about.html
Shibboleth in practice

- Authentication and authorisation system for Web resources

- Similar to Raven, but
  - standardised
  - globally cross-organisational
  - successor to Athens (funding stopped June 2008)
  - perceivedly slower

- cf. eduroam
authenticate people – not IP addresses

do not proliferate authentication systems
Agenda

1. what, why, when: Shibboleth basics
2. how: Interaction scenarios
3. who: privacy issues
4. whoops: pitfalls and hints
Example: Shibboleth authentication (1)
Example: Shibboleth authentication (2)

Login to Digimap Collections

Online maps and spatial data of Great Britain for UK HE and FE.

Login via UK federation [info]

To which Digimap Collections does your institution subscribe?

Having trouble logging in?

Digimap will be making use of the ‘at risk’ period between 17:30 and 20:00 hours on Tuesday 26th May. All Digimap collections will be unavailable between these times. We apologise for any inconvenience caused.

EDINA is a JISC National Data Centre based at the University of Edinburgh | Accessibility | Acknowledgements

invitation to login
Example: Shibboleth authentication (3)

https://wayf.ukfederation.org.uk/shibboleth-wayf/...
Example: Shibboleth authentication (4)

The web resource you requested requires you to identify yourself. This resource calls itself 'the Raven/Shibboleth authentication server' and is provided by the website shib.raven.cam.ac.uk. You should only proceed if you are happy to be identified to this site.

Always quit your web browser when you have finished accessing services that require authentication. Do not disclose your Raven password to anyone and only enter it on web pages with URLs that start https://raven.cam.ac.uk/. Please report attempts to obtain your password by other means.

https://raven.cam.ac.uk/auth/authenticate.html...
Example: Shibboleth authentication (5)

https://shib.raven.cam.ac.uk/arpviewer/...
Example: Shibboleth authentication (6)

https://shib.raven.cam.ac.uk/shibboleth-idp/...
Example: Shibboleth authentication (7)

http://digimap.edina.ac.uk/
Shibboleth interaction revisited: authentication

1. HTTP request
2. redirect
3. choose affiliation
4. auth
5. SAML Authentication Assertion

secured Web resource (SP)

local auth

where are you from? (WAYF)

Identity Provider (IdP)
Shibboleth interaction revisited: authorisation

1. where are you from? (WAYF)
2. secured Web resource (SP)
3. local auth
4. Identity Provider (IdP)
5. attribute request
6. attribute release
7. consent
8. redirect to orig. url
9. revert to orig. url

Jon Warbrick
Scaling up

- rôle-based authorisation (e.g. member@cam.ac.uk)
- federations for institutional trust (e.g. UK Federation)

- IdPs and SPs agree on
  - trust (authentication)
  - attribute semantics (authorisation)
Agenda

1. what, why, when: Shibboleth basics
2. how: Interaction scenarios
3. who: privacy issues
4. whoops: pitfalls and hints
Attribute release

- SPs may communicate needed attributes
- Attribute release governed by IdP
- IdP may favour some federations (e.g. Raven / Ucam Federation)
- User has take-it-or-leave-it choice

- Pseudonyms (RBAC) and identities (only one at a time)
UK federation core attributes

I agree to the following information being disclosed to 'EDINA: Digital Library Federation' and when I access this site in the future:

**eduPerson Principal Name:** sdp36@cam.ac.uk

**Anonymous identifier:** Lmj6FfXZg1TM2zeOBEURcv2rtI=@cam.ac.uk

**Status:**
- member@cam.ac.uk
- member@eresources.lib.cam.ac.uk

**Entitlement:**
- urn:mace:dir:entitlement:common-lib-terms

Buttons:
- Confirm
- Cancel

[help]
Shib-Application-ID: default
Shib-Session-ID: _c0582d05b229d54d085a14fb74ee1003
Shib-Identity-Provider: https://shib.raven.cam.ac.uk/shibboleth
affiliation: member@cam.ac.uk;member@eresources.lib.cam.ac.uk
cn: S.D. Preibusch
displayName: Sören Preibusch
entitlement: urn:mace:dir:entitlement:common-lib-terms
eppn: sdp36@cam.ac.uk
instID: CL
jdlInst: CL
mail: sdp36@cam.ac.uk
mailAlternative: Soren.Preibusch@cl.cam.ac.uk
misAffiliation: student
ou: Computer Laboratory
persistent-id: https://shib.raven.cam.ac.uk/shibboleth!https://elbe.ad.cl.cam.ac.uk/local-only!/K48zwTsLnLfwAKBerFuV597VKs=
sn: Preibusch
targeted-id: /K48zwTsLnLfwAKBerFuV597VKs=@cam.ac.uk
telephoneNumber: 63668 (Computer Laboratory office)
remote-user: sdp36@cam.ac.uk
Agenda

1. what, why, when: Shibboleth basics
2. how: Interaction scenarios
3. who: privacy issues
4. whoops: pitfalls and hints
the Cake Survey

Cake Feedback

Dear DTG member,

Please help us to improve our Monday cake supply for the upcoming term by completing the short questionnaire below.

In kind appreciation of your cooperation,
Sören & Lisen

1. I am a regular participant of the DTG Monday meeting.
   - yes
   - no
   ... and of the Monday cake session.
   - yes
   - no

2. My preferred cake variety so far has been:
   - chocolate cake
   - double-chocolate cake
   - triple-chocolate cake
   - double-chocolate gateau
   - cheese cake
   - profiterole gateau
   - lemon cake
   - lemon-cheese cake
   - blackera party cake

3. Please indicate your satisfaction with the following supermarktes and bakeries from which we have sourced in the past:
   - Aldi
   - Waitrose
   - M&S
   - Marks & Spencer
   - Tesco

We are also considering alternative suppliers:
- Aldi
- Waitrose

4. I would like to see more regional specialties.

5. I suffer from allergies and incompatibilities.

6. I have dietary requirements.

7. I am a responsible consumer.

Submit  Reset
Shibboleth installation on IIS 7

- installing Raven on IIS 7 will mess up the system
- some non-default IIS modules needed
- Shibboleth comes as binary installer, restart required
- integrates as ISAPI module
- SSL support optional
- no interference with existing auth mechanisms

⇒ roughly hassle-free
Configuring Shibboleth

- XML configuration files, pre-configured by UCS

- Server details:
  <Site id="1" name="elbe.ad.cl.cam.ac.uk"/>

- Redirects:
  <ApplicationDefaults id="default" policyId="default"
  entityId="https://elbe.ad.cl.cam.ac.uk/local-only/"
  homeURL="https://elbe.ad.cl.cam.ac.uk/local-only/"
  REMOTE_USER="eppn persistent-id targeted-id"
  signing="false" encryption="false">

- SSL:
  <Sessions handlerSSL="true">

- Miscellaneous metadata (contact information, ...)
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="elbe.ad.cl.cam.ac.uk">
      <Path name="local-only" authType="shibboleth" requireSession="true">
        <AccessControl>
          <!-- <Rule require="groupId">101065</Rule> -->
          <!-- <Rule require="instId">CL</Rule> -->
          <RuleRegex require="user">@cam.ac.uk$</RuleRegex>
        </AccessControl>
      </Path>
    </Host>
  </RequestMap>
</RequestMapper>
Expressive language for access control rules

- individual enumerable users
  `<Rule require="user">arb33@cam.ac.uk acr31@cam.ac.uk</Rule>`

- explicit rule disjunction
  `<OR> <Rule ... /> <Rule ... /> </OR>`

- regular expressions:
  `<RuleRegex require="user">@cam.ac.uk$</RuleRegex>`

- lookup.cam group membership
  `<Rule require="groupID">100852</Rule>`

- lookup.cam institution membership
  `<Rule require="instID">CS</Rule>`

- authentication only / optionally

Debugging is hard!
Joining the Ucam Federation

- Federation stores metadata about SP
- IdP displays SP-specific metadata during authentication
  - “I agree to the following information being disclosed to 'unknown Service Provider' ...”

- Advantages:
  - named SP
  - more attributes
  - hassle-free
Additional resources

- https://wiki.csx.cam.ac.uk/raven/Raven/Shibboleth
- raven-support@ucs.cam.ac.uk
- "cs-raven-discuss" mailing list
- http://shibboleth.internet2.edu
Thank you very much.

Questions and comments are welcome and highly appreciated.