Distributed Web Security for Science Gateways

Jim Basney
jbasney@illinois.edu

In collaboration with:
Rion Dooley
dooley@tacc.utexas.edu
Jeff Gaynor
gaynor@illinois.edu
Suresh Marru
smarru@indiana.edu
Marlon Pierce
marpierc@indiana.edu

This material is based upon work supported by the National Science Foundation under grant number 1127210.
Distributed Web Security for Science Gateways

- Software Development for Cyberinfrastructure grant from the NSF Office of CyberInfrastructure (www.nsf.gov/oci)
  - 3 year project: August 2011 – July 2014
- Goal: Support use of OAuth by science gateways for distributed authentication, delegation, and authorization
- Develop OAuth “profiles” for science gateway use cases
  - Getting certificates from MyProxy servers
    - Both individual and “community” credentials
  - Delegating certificates between gateway components
  - Delegated access to REST services
  - Integration with external authentication (LDAP, Kerberos, SAML, OpenID)
  - Credential refresh
  - Web Single Sign-On (OpenID Connect)

www.sciencegatewaysecurity.org
Defining Terms

- **Authentication**: *Who are you?*
  - customer #83461234987
  - name: Jim Basney
  - email: jbasney@illinois.edu

- **Authorization**: *What are you allowed to do?*
  - Access private information
  - Charge purchases to your credit card

- **Delegated Authorization**: *Authorizations you grant to others*
  - Park your car (valet key)
  - View your private photos on Flickr
  - Collaboratively edit an online Google doc

- **Credential**: *How security information is conveyed*
  - Also known as **Assertion** or **Token**
Science Gateways: Tiered Access Models

User authenticates to science gateway

Science gateway authenticates to service providers
Science Gateways: Tiered Access Models

- **Option A: Transitive Trust**
  - Bilateral agreement between science gateway & service provider
  - Bulk allocation of service to the science gateway
  - Service provider may not know who the end users are
  - Users may not know who the underlying service providers are
  - Example: XSEDE Community Account model
    - User attributes in community credential provides user info to SP

- **Option B: Delegation of Rights**
  - End user has account at underlying service provider
  - Example: Individual XSEDE account with Globus Online
  - Science Gateway explicitly acts on the user’s behalf when interacting with the underlying service providers

- Both options are useful (and can be combined)
  - Our recent work is focused on **Option B: Delegation of Rights**
Example: Using OAuth

1. Request Access to Photos

2. Authenticate & Grant Access to Photos

3. Token

4. Token

5. Token

6. Photos

www.sciencegatewaysecurity.org
Example: Science Gateway

1. Your Password
2. Your Password
3. Access

www.sciencegatewaysecurity.org
Delegated Authorization via OAuth

1. Request Access to Supercomputer

2. Authenticate & Grant Access

3. Token

4. Token

5. Token

6. Access
Delegated Authorization via OAuth

1. Request Access to iPlant Data

2. Authenticate & Grant Access

3. Token

4. Token

5. Token

6. Data

www.sciencegatewaysecurity.org
OAuth for MyProxy

- Provides an OAuth 1.0a compliant REST web interface to MyProxy for providing user certificates to science gateways
  - Eliminates the need for users to disclose their MyProxy passwords to science gateways. Instead, gateway users authenticate to their MyProxy server’s OAuth web interface to approve issuance of a certificate by MyProxy to the science gateway they are using.
- Java client & server implementations available now
  - [http://www.sciencegatewaysecurity.org/oauth-for-myproxy](http://www.sciencegatewaysecurity.org/oauth-for-myproxy)
- XSEDE MyProxy OAuth Server
  - [https://portal.xsede.org/oauth/](https://portal.xsede.org/oauth/)
  - [http://security.ncsa.illinois.edu/teragrid-oauth/](http://security.ncsa.illinois.edu/teragrid-oauth/)
    - TG11 paper: [http://dx.doi.org/10.1145/2016741.2016776](http://dx.doi.org/10.1145/2016741.2016776)
  - In use today by Globus Online
  - Supports using individual XSEDE accounts via science gateways
MyProxy Use Case

Old Approach  ➔  New Approach

1. Web Browser
   - MyProxy password
   - request certificate

2. Science Gateway
   - MyProxy password
   - OAuth token

3. MyProxy Server
   - certificate
   - OAuth token

4. Grid Service
   - access using certificate

1. Web Browser
   - MyProxy password
   - OAuth token

2. MyProxy OAuth Front-End
   - request certificate
   - OAuth token

3. MyProxy Server (unmodified)
   - certificate

4. Grid Service
   - access using certificate
Please select an endpoint above.
Activate Endpoint: xsede#forge

The administrator of this endpoint, xsede#forge, requires that you authenticate using their MyProxy OAuth server to activate the endpoint. When you click 'Continue' you will be redirected to their website.

Continue
Globus Online Example
Welcome to the XSEDE User Portal Authorization Page

Science Gateway Access
The XSEDE Science Gateway or Service below is requesting access to your XSEDE account. If you approve, please sign in with your XSEDE username and password.

Science Gateway Information
The XSEDE Science Gateway listed below is requesting access to your XSEDE account. If you approve, please sign in.

Name: Globus Online
URL: https://www.globusonline.org/

Sign In
Username: jbailey
Password: ***************

Please send any questions or comments about this site to help@xede.org
Globus Online Example

MyProxy
Credential Management Service

www.sciencegatewaysecurity.org
### Resource Selector

- **View Existing**
  - All Registered Resources
  - My Notification Settings
  - My Registered Resources

### Geospatial Extent

- **Bounding Box**
  - All Defined
  - Upper Bound
  - Lower Bound

- **Vertical Extent**
  - All Defined

- **Format**
  - DD.DDDD
  - Decimal Degrees

### Temporal Extent

- **Time Range**
  - All Defined
  - ISO Formatted Time in UTC
  - yyyy-mm-ddThhmmssZ

### Table: All Registered Resources

<table>
<thead>
<tr>
<th>Title</th>
<th>Notification Set</th>
<th>Provider</th>
<th>Type</th>
<th>Date Registered</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPOMATTOX RIVER AT MATTACA VA (0204160) - Daily Value</td>
<td>CHOPTANK RIVER NEAR CROOKSBORO MD (0410000) - Daily Value</td>
<td>USGS NWS</td>
<td>Daily Values Webservice</td>
<td>2011-8-25</td>
<td></td>
</tr>
<tr>
<td>APHRODITE RIVER AT KENT CUMBERLAND TN (0101000) - Daily Value</td>
<td>ARKANSAS RIVER AT BLOOMINGTON IL (0100000) - Daily Value</td>
<td>USGS NWS</td>
<td>Daily Values Webservice</td>
<td>2011-8-25</td>
<td></td>
</tr>
<tr>
<td>APTOS RIVER AT MONTEREY CA (0180000) - Daily Value</td>
<td>ASHLAND RIVER AT GLENDALE OR (0260000) - Daily Value</td>
<td>USGS NWS</td>
<td>Daily Values Webservice</td>
<td>2011-8-25</td>
<td></td>
</tr>
<tr>
<td>ARAKIKA RIVER AT TAKOMA PARK MD (0410000) - Daily Value</td>
<td>AIYAREI RIVER AT KUROBE CITY (0410000) - Daily Value</td>
<td>USGS NWS</td>
<td>Daily Values Webservice</td>
<td>2011-8-25</td>
<td></td>
</tr>
<tr>
<td>ARNOLDS RIVER AT TALLAHASSEE FL (0101000) - Daily Value</td>
<td>ARTHUR RIVER AT BRIDGELANDS VT (0101000) - Daily Value</td>
<td>USGS NWS</td>
<td>Daily Values Webservice</td>
<td>2011-8-25</td>
<td></td>
</tr>
</tbody>
</table>

### Other Sections

- Resource Registration Description
- Resource Registration Contact Information
- Original Source Description
- Original Source Contact Information
- Geospatial Coverage
- Temporal Coverage
- Variables
- References
OOI Example
OOI Example
You must log in to continue.

Enter your NetID: [blank]
Enter your Active Directory (AD) password: [blank]

Login

Forgot your Active Directory password?
To change or reset your Active Directory password, go to the CITES Password Manager.

More Information

Where to Get Help
Contact the CITES Help Desk at consult@illinois.edu.

What is a NetID?
Your NetID serves as your login to many University computing and networking services and also determines your University email address, which is netid@illinois.edu.
For more information, see the Your Network ID (NetID) page.

Technical Information

Service that has requested authentication:

Service Provider EntityID: https://ctilogon.illinois.edu
This login service uses the following server:
shibboleth.illinois.edu
This page's URL should start with https:// followed by the server listed above.
For most web browsers, the security padlock icon for this page should be crossed-out.
Starting the Discussion

- What are science gateways doing today for web security?
  - Using OAuth, OpenID, SAML?
  - Supporting both individual and community accounts?
  - Authenticating to REST services?
  - Sharing data across multiple gateways?

- What are current/future science gateway security needs?
  - What is your input on our project plans?
    - Getting certificates from MyProxy servers
    - Delegating certificates between gateway components
    - Delegated access to REST services
    - Integration with external authentication (LDAP, Kerberos, SAML, OpenID)
    - OAuth 2.0 update
    - Credential refresh
    - Web Single Sign-On (OpenID Connect)
  - What is your input on the XSEDE architecture?
Continuing the Discussion

- Please join our discuss@sciencegatewaysecurity.org mailing list:
  - Send email to: discuss+subscribe@sciencegatewaysecurity.org
  - Or visit:
    https://groups.google.com/a/sciencegatewaysecurity.org/group/discuss/subscribe