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.
National Center for Supercomputing Applications (NCSA)

- Located at University of Illinois at Urbana-Champaign
- Established in 1986 by NSF Supercomputer Centers Program

www.ncsa.illinois.edu
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
• Co-PIs: Marlon Pierce (IU), Rion Dooley (TACC)

• *What is cyberinfrastructure?*
  • Supercomputers, mass-storage systems, data repositories, networks, software and more
  • Supporting science and engineering research and education
Motivating Example: Photo Printing

1. Your flickr Password
2. Your flickr Password
3. Photos

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 photos on Flickr
  - Collaboratively edit an online Google doc

- **Credential**: How security information is conveyed
  - Also known as **Assertion** or **Token**
Delegated Authorization

1. Request Access to Photos
2. Authenticate & Grant Access to Photos
3. Token
4. Token
5. Token
6. Photos
OAuth

• An open protocol for delegated authorization (oauth.net)

• Development
  • OAuth 1.0 released (October 2007)
  • OpenID+OAuth hybrid developed (2009)
  • OAuth 1.0a revision (June 2009)
    • RFC 5849 (Informational), April 2010
  • OAuth WRAP (2009-2010)
    • Basis for OAuth 2.0
  • OAuth 2.0 Standards Track RFC coming soon
  • OpenID Connect based on OAuth 2.0

• Used by Flickr, Twitter, Facebook, Google, Netflix, …
FeedFlikks wants to access your Netflix Account.

To confirm, please login to Netflix:

Login: ********
Password: ********

Yes, Link This Account

You should not authorize FeedFlikks unless you trust them with access to your account. By confirming, you allow FeedFlikks to access, share and update your Netflix data, including your queue, rental history, and ratings.

This page is provided by Netflix to authorize third-party applications, but has not been configured to send requests securely. If you grant access but you did not initiate this request at FeedFlikks, it may be possible for other users of FeedFlikks to access your data. We recommend you deny access unless you are certain that you initiated this request directly within FeedFlikks.

Your password will always remain private, but FeedFlikks will have ongoing access to your account. You can remove access at any time in Your Account. Your usage of any third party application that interacts with Netflix is governed by the Netflix Terms of Use.
OAuth 1.0 Model

1. Request Access

2. Authenticate & Grant Access

3. Token

4. Token

5. Token

6. Resource

Client

Server

Resource Owner
OAuth 2.0 Model

1. Request Access

2. Authenticate & Grant Access

3. Token

4. Token

5. Token

6. Validate Token

7. Resource

8. Token Refresh

Resource Owner

Authorization Server

Client

Resource Server
Google accounts

You are signing in to Sourceforge.net with your Google Account jbasney@sciencegatewaysecurity.org

Sign in  Cancel

Remember me

You can always change your Google Account approval settings. Sourceforge.net is not owned, operated, or controlled by Google or its owners. Learn more
Find, Create, and Publish Open Source software for free

Search from thousands of software titles

Jim Basney
Authentication Model

Examples: OpenID, SAML
Authentication Via Delegation

1. **Who are you?**
2. **Authenticate & Grant Access to My Info**
3. **Token**
4. **Token**
5. **Token**
6. **User Information**

**Example: OpenID Connect**

- **Resource Owner**
- **Identity/Resource Provider**
- **App**
Authentication Via Delegation

- **Bad Idea**
  - App: Who are you?
  - User: Here’s full access to my Twitter account.

- **Better Idea**
  - App: Who are you?
  - User: Here’s read access to my Twitter account profile.

- **Delegated access to user’s profile information**

- **Example:** **OpenID Connect** built on OAuth
OAuth 1.0 Model (Again)
**External Authentication**

Examples: LDAP, RADIUS, PAM, Kerberos
Token-based Authentication

Examples: OpenID, SAML, Kerberos
Science Gateways
Computational Chemistry Grid:
Production Cyberinfrastructure for Computational Chemistry

For more information, please visit www.gridchem.org or contact help@gridchem.org.

How CCG Works

Middleware Server
- authentication
- data management
- resource specification
- routes jobs
- provides client with job status information
- provides access to job data for analysis
- input, output, job details stored in mass storage archive
- resource discovery
- accounting management
- system and job monitoring

Grid Services
Leveraging NMI Software

CCG Resources
3,525,000 CPU hours available annually

JAVA WEB START
Client Application runs on Local Machine

BUILD MOLECULE

DOWNLOAD RESULTS

BUILD INPUT FILE

SUBMIT

POST PROCESS REVIEW
Science Gateways: Accessing Resources

user accesses science gateway

science gateway uses external resources (supercomputers, compute clusters, data stores)
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

• Option B: Delegation of Rights
  • End user has account at underlying service provider
    • Goal: Use underlying services via science gateway interfaces
  • Science Gateway explicitly acts on the user’s behalf when interacting with the underlying service providers

• Both options are useful
  • Today let’s focus on Option B: Delegation of Rights
Motivating 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

AuthToken & Delegation via OAuth

www.sciencegatewaysecurity.org
Challenge: Multi-Tier Science Gateways

- Web Browser
- Gadget Container
- Gadget Backing Service
- Service Factory
- Service Factory
- Data Store
- Info Service
- Compute Cluster
- External Services
Long-Running Science Gateway Workflows

• Common Science Gateway Use Case:
  • Scientist launches workflow (computational simulation, data analysis, data movement/replication, visualization)
  • Workflow runs for hours/days/weeks
  • Scientist monitors workflow / receives notifications of completion

• Challenge: Duration of Delegation
  • “How long can the science gateway act on my behalf?”
    • Ideally: only as needed for the workflow to complete
    • Limit duration of delegation to minimize window of exposure
    • Difficult / inconvenient to predict workflow duration
    • Approaches: refresh / renewal / revocation

• OAuth 2.0 refresh is needed!
Globus Online Example

Kerberos Authentication Server
Back-end Authentication (Again)

- Resource Owner
- Client
- Server
- AuthN Service

1. Resource Owner sends Password to Server.
2. Server verifies Password.
3. Server returns credentials to Client.
Globus Online Example
Globus Online Example

Kerberos Authentication Server

www.sciencegatewaysecurity.org
Token-based Authentication (Again)

- Resource Owner
- Server
- IdP
- Client

- 2a: Who are you?
- 2b: Password
- 2c: Assertion
- 2d: Assertion

User Attributes
Select an identity provider:

- University of Alabama at Birmingham
- University of California-San Diego
- University of Chicago
- University of Delaware
- University of Illinois at Chicago
- University of Illinois at Urbana-Champaign
- University of Iowa
- University of Maryland Baltimore County
- University of Michigan
- University of Missouri System

Search: [ ]
Remember this selection: [ ]

By selecting "Continue", you agree toCiLogon's privacy policy.

CONTINUE
CANCEL

For questions about this site, please see the FAQ or send email to help@ciLogon.org.
Know your responsibilities for using the CiLogon Service.
This material is based upon work supported by the National Science Foundation under grant number 0943633.
Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
OOI Example
Wrap Up

• More info
  • www.sciencegatewaysecurity.org
  • jbasney@illinois.edu

• References

www.sciencegatewaysecurity.org

Thanks for your interest!