Authorization with OAuth

Rob Richards
October 22, 2009
cdatazone.org
http://xri.net/=rob.richards
Authentication

- HTTP Authentication
  - Basic
  - Digest
  - TLS/SSL
- WS-Security
- Developer Keys
- 3rd Party Authentication
  - Yahoo BBAuth
  - AOL OpenAuth
Oauth is not OpenID
Data Authorization

Enter your Yahoo details below. On the next page you will see which friends are already on Flixster and can choose to invite others.

Yahoo Email Address: Enter Your Email Address
Yahoo Password: 

Or use: Hotmail | Yahoo | Gmail | AOL

Plaxo

Find your friends on AIM

AIM Screenname: 
Password: 

Find friends in your email

Your email: email.com
Email Password: 

Find out which of your webmail contacts are already on LinkedIn.

Select your webmail service:

Username: 
Password: 
Upload Contacts
OAuth

is like a

Valet Key
OAuth

OAuth

is like a

Hotel Keycard
Guest Key: Granting Access

101 103 105 107

102 104 106 108
Guest Key: Revoking Access

[Image of hotel keycards]

101  103  105  107

102  104  106  108
Master Key Maintains Full Access
Oauth Clients

Oauth Clients

Referring to the diagram, it illustrates the process of integrating OAuth clients into a service registry. The diagram shows the flow of actions including finding, publishing, binding, and service description.

The diagram includes:
- **Service Registry**: The central part of the diagram, acting as a repository for service descriptions.
- **Service Requestor**: A component that initiates the process of finding and binding a service.
- **Service Provider**: A service that is hosted by the provider and is accessible via a web service.
- **Web Service**: The interface through which the service is accessible.

The arrows indicate the sequence of these steps:
- **Find**: The service requestor finds the service provider in the registry.
- **Publish**: The service provider publishes its service to the registry.
- **Bind**: The service requestor binds to the service provider's web service.
- **Service Description**: The service description is associated with the service provider.

The diagram is complemented by images of a smartphone and a Xbox 360, illustrating real-world applications of OAuth clients in mobile and gaming devices.

The text snippet mentions the use of OAuth clients in streaming services, highlighting their importance in modern technology integration and security.
OAuth and Netflix

developer.netflix.com
Netf lix API: User Resources

- user
  - queues (links only)
  - title_states
    - disc (feed available)
    - instant (feed available)
    - saved (feed available)
    - available (feed available)
    - saved (feed available)
    - available (feed available)
  - at_home (feed available)
    - available (feed available)
    - available (feed available)
  - rental_history (feed available)
    - shipped (feed available)
    - watched (feed available)
    - received (feed available)
  - recommendations (feed available)
    - title
    - actual (feed available)
    - predicted (feed available)
  - ratings (links only)
Netfli x Applications ... and many more

**Netflix for Nokia** by rburdick
Enables Netflix subscribers to watch movie previews, manage their Queue, search for movies, and get recommendations. Supported platform is S60 5.0. Supported devices are currently N97 and 5800 XpressMusic. ...

⭐⭐⭐⭐ Average of 17 ratings: 4.2 stars

**Netflix for Windows Mobile** by SPB
Windows Mobile now offers the first official Netflix mobile application for Windows Mobile phones for free. Netflix Mobile application makes it simple for users to search the Netflix library and add DVDs ...

⭐⭐⭐⭐ Average of 109 ratings: 3.7 stars

**Netflix in Windows Media Center** by mcc
Watch instantly, manage instant and DVD Queues, search the entire Netflix library, filter searches by titles that are available to watch instantly, and navigate it all with a remote control. Windows ...

⭐⭐⭐⭐ Average of 130 ratings: 3.5 stars

**Now Playing** by Metasyn tactic
The line at the movies starts and ends in your pocket.

With iPhone and Now Playing, you can read reviews, locate theaters and show times, even purchase tickets.
Obtaining a Consumer Key / Secret

Netflix API Application Registration

Register Your New Application

- Name of your application (you can change it later)
  
  
  Web Site
  
  Please describe what your application will do
  
  What type of application are you building?
  
    Choose one...
  
  How many people do you anticipate will use your application?
  
    Choose one...
Obtaining a Consumer Key / Secret

Netflix API Application Registration

Application Registered!

Your consumer key is:

Key: 1234567890123456789012345

Application: Rob's Test App
Key: 1234567890123456789012345
Shared Secret: 123456789012345
Status: active
Registered: 2 seconds ago

Rate Limits

<table>
<thead>
<tr>
<th>4</th>
<th>Queries per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>Queries per day</td>
</tr>
</tbody>
</table>
3-Legged OAuth
“The OAuth Dance”
Step 1: Obtaining a Request Token

http://api.netflix.com/oauth/request_token

Signed Request

Request Token & Secret
Step 1: Obtaining a Request Token

http://api.netflix.com/oauth/request_token?

oauth_callback=http%3A%2F%2Fwww.example.com%2Fcallback
&oauth_consumer_key=1234567890123456789012345
&oauth_nonce=60a3f1c4a18c2a68d8cb216f46bcebe4ad7dff32e
&oauth_signature=SB%2BjBrcHkQRgMP8XKVyps3rw6Xo%3D
&oauth_signature_method=HMAC-SHA1
&oauth_timestamp=1255631744
&oauth_version=1.0
Calculating The Signature

Calculate Base String

<HTTP method>&<canonicalized URL path>&<parameters>

GET&http%3A%2F%2Fapi.netfix.com%2Foauth
%2Frequest_token&oauth_callback%3Dhttp%253A%252F%252Fwww.example.com%252Fcallback
%26oauth_consumer_key%3D1234567890123456789012345%26oauth_nonce%3D3eb496472d2a46ceb71d65fc1b7341ae359f932c%26oauth_signature_method%3DHMAC-SHA1%26oauth_timestamp%3D1255631744%26oauth_version%3D1.0
Calculating The Signature

- Parameters are collected, sorted and concatenated into a normalized string
  - Parameters in the OAuth HTTP Authorization header excluding the realm parameter.
  - Parameters in the HTTP POST request body (with a content-type of application/x-www-form-urlencoded).
  - HTTP GET parameters added to the URLs in the query part (as defined by [RFC3986] section 3)
- The oauth_signature parameter MUST be excluded
- Parameters are sorted by name, using lexicographical byte value ordering
Calculating The Signature (Authorization Header)

GET /oauth/request_token HTTP/1.1
User-Agent: PECL::HTTP/1.6.4 (PHP/5.2.10)
Host: api.netflix.com
Accept: */*

oauth_consumer_key="1234567890123456789012345",
oauth_nonce="60a3f1c4a18c2a68d8cb216f46bceb4ad7dff32e",
oauth_signature="SB%2BJbrcHkQRgMP8XKVyps3rw6Xo%3D",
oauth_signature_method="HMAC-SHA1",
oauth_timestamp="1255631744",
oauth_version="1.0"
Calculating The Signature

Create Secret

\(<\text{consumer secret}>\&<\text{token secret}>\)

1234567890123456789012345&

Sign Base String using algorithm specified

HMAC(1234567890123456789012345&,\(<\text{Base String}>\))

Base64 encode then URL encode result:

oauth_signature=SB%2BjBrcHkQRgMP8XKVyps3rw6Xo%3D
Step 1: Obtaining a Request Token (Response)

oauth_token=bqba9rku48yacfatjxjw3fkc
&oauth_token_secret=EZ2mBk6rC2vZ
&oauth_callback_confirmed=true
&login_url=https%3A%2F%2Fapi-user.netflix.com%2Foauth%2Flogin
Step 2: User Authentication

Determined by needs of Service Provider

https://api-user.netflix.com/oauth/login?oauth_token=bqba9rku48yacfatjxjw3fkc
Step 2: User Authentication

Determined by needs of Service Provider

oauth_token=bqba9rku48yacfatjxjw3fkc&oauth_verifier=abcdefg
Step 2: User Authentication

Activate Instant Streaming

Thanks for being a member of Netflix!
At your computer, go to netflix.com/activate and enter the activation code displayed below.

Activation Code
A Matter Of Trust
Step 3: Obtaining an Access Token

http://api.netflix.com/oauth/access_token
Step 3: Obtaining an Access Token

http://api.netflix.com/oauth/access_token?
oauth_consumer_key=1234567890123456789012345
&oauth_nonce=0a5ebd08b88e3ec7d7e27c7fb8735c7aa9a7229a
&oauth_signature=FXDtkQtg6u42YYipJhBgCBvVXHI%3D
&oauth_signature_method=HMAC-SHA1
&oauth_timestamp=1255704433
&oauth_token=bqba9rku48yacfatjxjw3fkc
&oauth_verifier=abcdefg
&oauth_version=1.0
Calculating The Signature

Calculate Base String

<HTTP method>&<canonicalized URL path>&<parameters>

GET&http%3A%2F%2Fapi.netfix.com%2Foauth
   %2Faccess_token&oath_consumer_key
   %3D1234567890123456789012345%26oauth_nonce
   %3D0a5ebd08b88e3ec7d7e27c7fb8735c7aa9a7229a
   %26oauth_signature_method%3DHMAC-SHA1%26oauth_timestamp%3D1255704433%26oauth_token
   %3Dbqba9rku48yacfatjxjw3fkc%26oauth_verifer%3Dabcdefg
   %26oauth_version%3D1.0
Calculating The Signature

Create Secret

<consumer secret>&<token secret>
1234567890123456789012345&EZ2mBk6rC2vZ

Sign Base String using algorithm specified
HMAC(1234567890123456789012345&EZ2mBk6rC2vZ,<Base String>)

Base64 encode then URL encode result:
oauth_signature=eCLuRjEhSB%2BFlmlN8sqrusPd9AE%3D
Step 3: Obtaining an Access Token (Response)

oauth_token=5432109876543210987654321
&user_id=123myuserid456
&oauth_token_secret=543210987654321
Accessing Resources

http://api.netflix.com/<path to resource>
Accessing Resources

http://api.netflix.com/users/123myuserid456/queues?
oauth_consumer_key=1234567890123456789012345
&oauth_nonce=0c36fbefee5af0316687c6984a32c0184526e7b2
&oauth_signature=IXkzzAhF9hnsFLeftxEDfG0nx1s%3D
&oauth_signature_method=HMAC-SHA1
&oauth_timestamp=1255712310
&oauth_token=5432109876543210987654321
&oauth_version=1.0
&v=1.5
Calculating The Signature

Create Secret

<consumer secret>&<token secret>
1234567890123456789012345&543210987654321

Sign Base String using algorithm specified
HMAC(1234567890123456789012345&543210987654321,<Base String>)

Base64 encode then URL encode result:
oauth_signature=IXkzzAhF9hnsFleftxEdfG0nx1s%3D
<xml version="1.0" standalone="yes"?>
<resource>
  <link href="http://api.netfix.com/users/123myuserid456/queues/disc"
       rel="http://schemas.netfix.com/queues.disc" title="disc queue" />
  <link href="http://api.netfix.com/users/123myuserid456/queues/instant"
       rel="http://schemas.netfix.com/queues.instant"
       title="instant queue" />
</resource>
</xml>
Accessing Resources (Response)
Managing Access Tokens

Welcome, Robert Richards

Your Account
Manage Your Site Connections

You have authorized the following sites and applications to access Netflix on your behalf and need application or site's permission to access Netflix for you by clicking the "Remove" button next to each.

- Netflix Monitoring
- Monitor the API
- Rob's Test App
- Remove
- Xbox 360 Netflix Client
- Remove
- Mashery Test - Netflix
- Testing
- Remove
2-Legged OAuth

- No Dance Required
- Only Consumer Key and Secret required
- Application making requests on its own behalf
- Direct Access / No Delegation
- Replacement for HTTP Basic Authentication
- Sign request just as if they were requests for Request Tokens
Questions?

Authorization with OAuth

Rob Richards

http://xri.net/=rob.richards
www.cdatazone.org