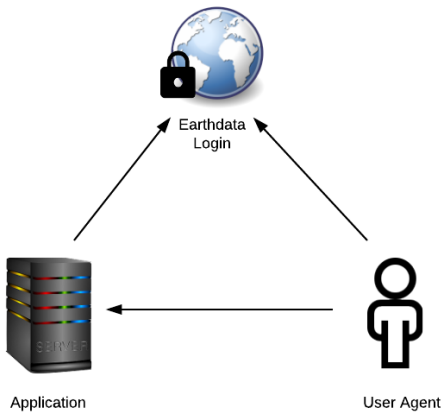
What is OAuth2?

OAuth2 is an authorization protocol that allows a user to access multiple applications using a just a single username and password. One of the major benefits of OAuth2 is that the application being accessed never get to see the user's username or password. An excellent example of this is the 'Login with Google' option you may find on many websites these days. When you use this option, the website delegates the task of identifying you to the Google OAuth2 service. Additionally, you get to decide what information about you Google can provide to the website - for example, your email address. Earthdata Login provides the same service to Earthdata applications such as Reverb, and may others located at the DAAC sites.

How Does It Work

We're going to give a simplified outline of how OAuth2 works in the context of Earthdata Login, but before we delve into the details, we need to make that sure we start off with the same terminology. In a typical scenario, there are three actors, or entities involved.



We have:

1. The **User Agent** - the tool being used by the user to access the application. This could be a web browser, an application such as Panoply, or it could even be a command line tool or script such as curl or wget.
2. The **Application** requiring user authentication. This could be a simple HTTP based data download service, a wiki, a data search tool, subsetting application, etc.
3. The OAuth2 service - in this case, **Earthdata Login**.

The process goes something like this:

Step 1

The user agent sends a request to the application for a resource - for example, a web page or file.

Step 2

The application receives the request, and decides that the user needs to be authenticated. It replies by asking the user agent to go and talk to Earthdata Login.

Step 3

The user agent sends a request to Earthdata Login.

Step 4

Earthdata Login replies by asking the user agent to provide credentials - a username and password. It may also ask you to confirm that the application be allowed to access some of your user profile information.

Step 5

The user agent send the user credentials to Earthdata Login.

Step 6

Earthdata Login verifies the credentials, and replies by telling the user agent to now go back to the application. It also provides the user agent with a special 'code' that it must present to the application.

Step 7

The user agent sends a request back to the application and presents it with the code.

Step 8

The application now talks privately to Earthdata Login, checking that the code give to it by the user agent is genuine. The two agree that it is. The application replies by sending the resource or file originally requested by the user agent.

Step 9

The user agent receives the file or resource.

You can see that your username and password is only sent to Earthdata Login, and not to the application, and Earthdata Login only accepts requests using HTTPS. This helps keep your credentials secure from prying eyes, and is one less copy of your credentials that you have to worry about being stolen.

Further Reading

For the brave: http://oauth.net/2/

For the bravest: https://tools.ietf.org/html/rfc6749