AmberProposal

Amber

Abstract

The following proposal is about Apache Amber, a Java development framework mainly aimed to build OAuth-aware applications. After a brief explanation of the OAuth protocol, the following proposal describes how Apache Amber solves issues related to the implementation of applications that adhere to such specification.

Proposal

Amber will have no or negligible dependencies and will provide both an API specification for, and an unconditionally compliant implementation of, the OAuth v1.0, v1.0a and v2.0 specifications. The API specification will be provided as a separate JAR file allowing re-use by other developers and permits configuration:

- by XML
- by the Java JAR Services "ServiceLoader" mechanism
- programmatically

The API component specifies that an implementation must provide default classes for Provider, Consumer and Token objects making Amber easy to integrate with existing infrastructure and OAuth client interactions possible with virtually no additional configuration. The API is flexible enough to allow programmatic customisation or replacement of much of the implementation, including the default HTTP transport.

Amber will provide both client and server functionality, enabling developers to deploy robust OAuth services with minimal effort.

Background

Roughly, OAuth is a mechanism that allows users to share their private resources, like photo, videos or contacts, stored on a site with another site avoiding giving their username and password credentials. Hence, from the user point-of-view, OAuth could be the way to improve their experience across different applications with an enhanced privacy and security control in a simple and standard method from desktop and web applications. The protocol was initially developed by the oauth.net community and now is under IETF standardization process.

The main idea behind OAuth is represented by the token concept. Each token grants access to a site, for a specific resource (or a group of resources), and for a precise time-interval. The user is only required to authenticate with the Provider of their original account, after which that entity provides a re-usable to token to the Consumer who can use it to access resources at the Provider, on the users behalf.

Moreover, the total transparency to the user, that is completely unaware of using the protocol, represents one of the main valuable characteristics of the specification.

Apache Amber community aims not just to create a simple low-level library, but rather to provide a complete OAuth framework easy to use with Java code, on top of which users can build new-generation killer applications.

There are currently three implementation efforts going on in ASF for OAuth v1. A stable implementation of OAuth v1 is present in Apache Shindig, but it is not actively developed and not shared with other projects. A Lab having Simone Tripodi as its PI is working on an implementation for an OAuth library that could be used by other products. Zhihong Zhang wrote an OAuth plugin for JMeter.

At the same time, on the IETF OAuth v2 mailing list, other people expressed interest for a Java API and implementation, among them two Apache committers and one active contributor.

Outside the ASF there are three known Java OAuth 1.0/1.0a libraries

- The oauth.net reference implementation by John Kristian, Praveen Alavilli and Dirk Balfanz.
- OAuth SignPost - a simple OAuth message signing client for Java and Apache HttpComponents by Matthias Kaeppler.
- OAuth Scribe - a simple OAuth client by Pablo Fernandez.
- asmx-oauth (on google code) - a complete open source OAuth 1.0 Consumer and Service Provider implementation provided by Asemantics Srl (Simone Tripodi was involved).

Rationale

The key role played by the OAuth specification, within the overall Open Stack technologies, jointly with its high degree of adoption and maturity, strongly suggest having an Apache leaded incubator for suitable reference implementation. Furthermore, the OAuth specification is currently gaining value due to its involvement in a standardization process within the IETF, as the actual internet draft. Having the Apache Amber as an Apache Incubator could be an opportunity to enforce the actual Apache projects that already reference other IETF specifications.

Moreover, other Apache Projects, such as Abdera, Shindig and Wink, are currently supporting the OAuth protocol, so having the OAuth Apache reference implementation should benefit not only the project and the related commmunity itself, but also existing and active Apache projects. Combining efforts from existing Apache projects is a logical step.

Providing an Apache licensed library will make it easier for other Apache projects to integrate OAuth, like, for example:

- It could be the foundation framework for Consumer developers;

- It could be the foundation Framework for Service Provider developers;
- It could be integrated into Apache Shindig;
- It could be integrated into Apache Abdera;
- It could be integrated into Apache Wink;
- It could be integrated into Spring Security;
- It could be integrated with JAAS (and be deployed in Tomcat-based Servlet Containers);
- It could be integrated into Jakarta JMeter;
- Apache Wookie (incubating) expressed interest in an OAuth implementation;
- Most importantly, it could be a backend for dozens of useful new innovative projects that no-one has envisioned yet.

Current Status

Code in the Amber Lab and in Apache Shindig is already licensed to the ASF. More contributions of code and ideas are expected from initial committers, so an implementation of OAuth v1 should be reached quickly, and act as a base for an OAuth v2 API and implementation.

Meritocracy

As a majority of the initial project members are existing ASF committers, we recognize the desirability of running the project as a meritocracy. We are eager to engage other members of the community and operate to the standard of meritocracy that Apache emphasizes; we believe this is the most effective method of growing our community and enabling widespread adoption.

Community

The amount of interest in the OAuth protocol from enterprises, social networks and individual developers suggests a strong community will develop once the framework to support one is laid.

Core Developers

- Simone Gianni <simoneg at apache dot org> (Semeru)
- Simone Tripodi <simonetripodi at apache dot org> (Sourcesense)
- Stuart "Pid" Williams <pid at pidster dot com> (Clubtickets.com)
- David Recordon <recordond at apache dot org> (Facebook)
- Tommaso Teofili <tommaso at apache dot org> (Sourcesense)

Alignment

The purpose of the project is to develop an implementation of OAuth v1 and OAuth v2 that can be used by other Apache projects.

Known Risks

Orphaned Products

Being OAuth a standard receiving a lot of interest, and being v2 an ongoing work in IETF, we believe there is minimal risks of this work becoming non-strategic and the contributors are confident that a larger community will form within the project in a relatively short space of time.

Inexperience with Open Source

All of the committers have experience working in one or more open source projects inside and outside ASF.

Homogeneous Developers

The list of initial committers are geographically distributed across the U.S. and Europe with no one company being associated with a majority of the developers. Many of these initial developers are experienced Apache committers already and all are experienced with working in distributed development communities.

Reliance on Salaried Developers

To the best of our knowledge, none of the initial committers are being paid to develop code for this project.

Relationships with Other Apache Products

A number of existing ASF projects could benefit from an OAuth implementation, including Apache Shindig, Apache Abdera, Apache Wink, Jmeter which are already using partial and non standardized OAuth implementations. Basically any other server-side framework or application could benefit by using Amber. It is hoped that members of those projects will be interested in contributing to and adopting this implementation.

A Excessive Fascination with the Apache Brand

Amber fits naturally in the ASF because :

- It is an implementation of an open standard
- It is a server component on which many other projects can depend on

Documentation

[1] More information about OAuth can be found here:
http://www.oauth.net/

[2] The IETF discussion about the emerging OAuth v2.0 specification is occuring on this mailing list
oauth@ietf.org

Initial Source

The intial source comprises code developed inside Apache Labs, other Apache projects and contributed under the CLA.

Source and Intellectual Property Submission Plan

Source code will be moved from SVN space of Apache Labs, Apache Shindig and other appropriately licensed sources inside the SVN space of the podling.

External Dependencies

None known

Cryptography

The project will use cryptographic utilities available as standard in Java 6.

Required Resources

- Mailing lists
  - amber-private (with moderated subscriptions)
  - amber-dev
  - amber-user
  - amber-commits
- Subversion directory
  - https://svn.apache.org/repos/asf/incubator/amber
- Website
  - Confluence (AMBER)
- Issue Tracking
  - JIRA (AMBER)

Initial Committers

Names of initial committers with affiliation and current ASF status:

- Simone Gianni <simoneg at apache dot org> (Semeru)
- Simone Tripodi <simonetripodi at apache dot org> (Sourcesense)
- Stuart "Pid" Williams <pid at pidster dot com> (Clubtickets.com) (CLA filed)
- David Recordon <recordond at apache dot org> (Facebook)
- Tommaso Teofili <tommaso at apache dot org> (Sourcesense)
- Paul Lindner <lindner at inuus dot com> (LinkedIn)
- Pablo Fernandez <fernandezpablo85 at gmail dot com> (LinkedIn)
- Praveen Neppalli Naga <praveen.neppalli at gmail dot com> (LinkedIn)

Sponsors

Champion

- Brian McCallister <brianm at apache dot org>

Nominated Mentors

- Henning Schmiedehausen <henning at apache dot org>
- Jean-Frederic Clere <jfclere at gmail dot com>
- Gianugo Rabellino <gianugo at apache dot org>
- David Jencks <djencks at apache dot org> (Waiting on IPMC)

Sponsoring Entity

- Shindig PMC - Confirmed Apr 29, 2010

Other interested people

- Saleem Shafi <mshafi at paypal dot com>
- Chirag Shah (Apache Shindig Committer)
- Greg Brail <gbrail at sonoasystems dot com>
- Tim Howe <vsync at qt dot quadium dot net>
- Murali VP <muralive at gmail dot com>