OAuth

Authorization Made Simple….Sort of

Overview

- A brief history of OAuth

- Why does it exist?

  - Authorization versus Authentication

- How Does it Work?

- Major Versions

  - Revision A

 - Signatures versus SSL

A Brief History

- Nov. 2006: Blaine Cooke, Chris Messina, and David Recordon meet with other OpenID users to discuss existing solutions

  - A new authorization standard was needed

- April 2007: The OpenAuth Google group is born

  - Later changed to Oauth to prevent conflict with AOL's OpenAuth protocol

- July 2007: The group goes public

- December 2007: The 1.0 spec is finalized

- June 2009 – Revision A is released (following a security advisory release in April)

Why does it Exist

- No more username and password sharing

- Separate authentication from authorization

- Standardization of authorization solutions

  - Flikr Auth

  - Google AuthSub

  - Yahoo! BBAuth

Didn't OpenID Do This?

- Common question on Stack Overflow and similar sites
- Answer: Partially
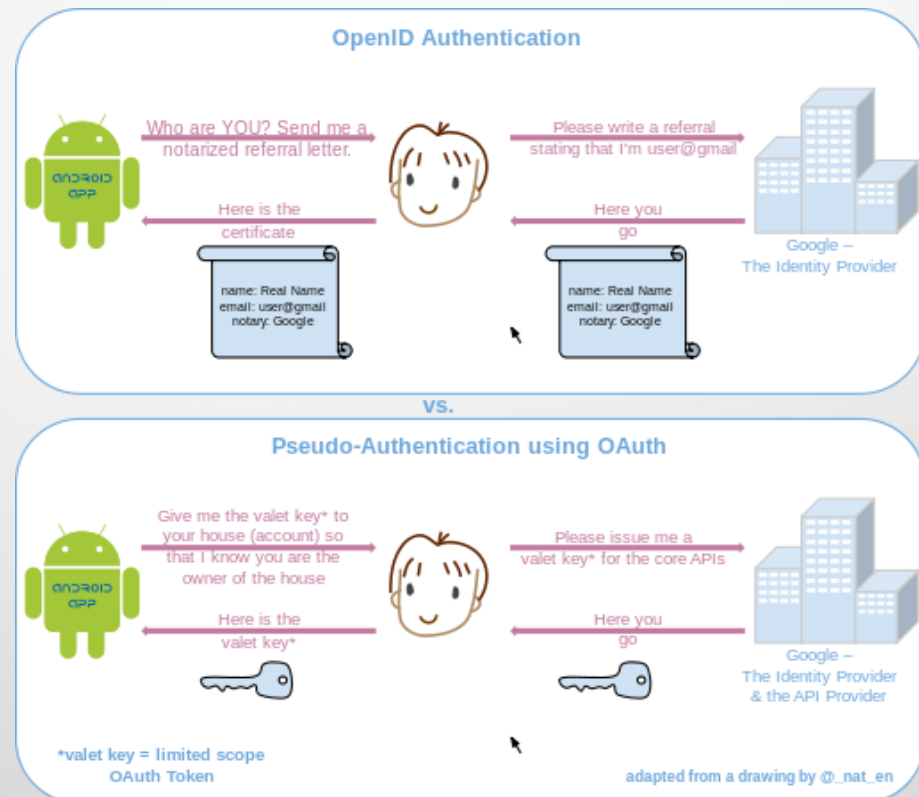
*Imaged borrowed from wikipedia

Authorization v. Authentication

- Authentication
  - Who is this person?
  - Verification of user credentials
  - Association of credentials with user data
- Authorization
  - What can the person with these credentials do?
- By providing my password, exchange is able to verify I am [tstokes](#).
- By using the user information associated with [tstokes](#), it is able to authorize me to view my mailbox, but not someone else's.

How Does it Work?
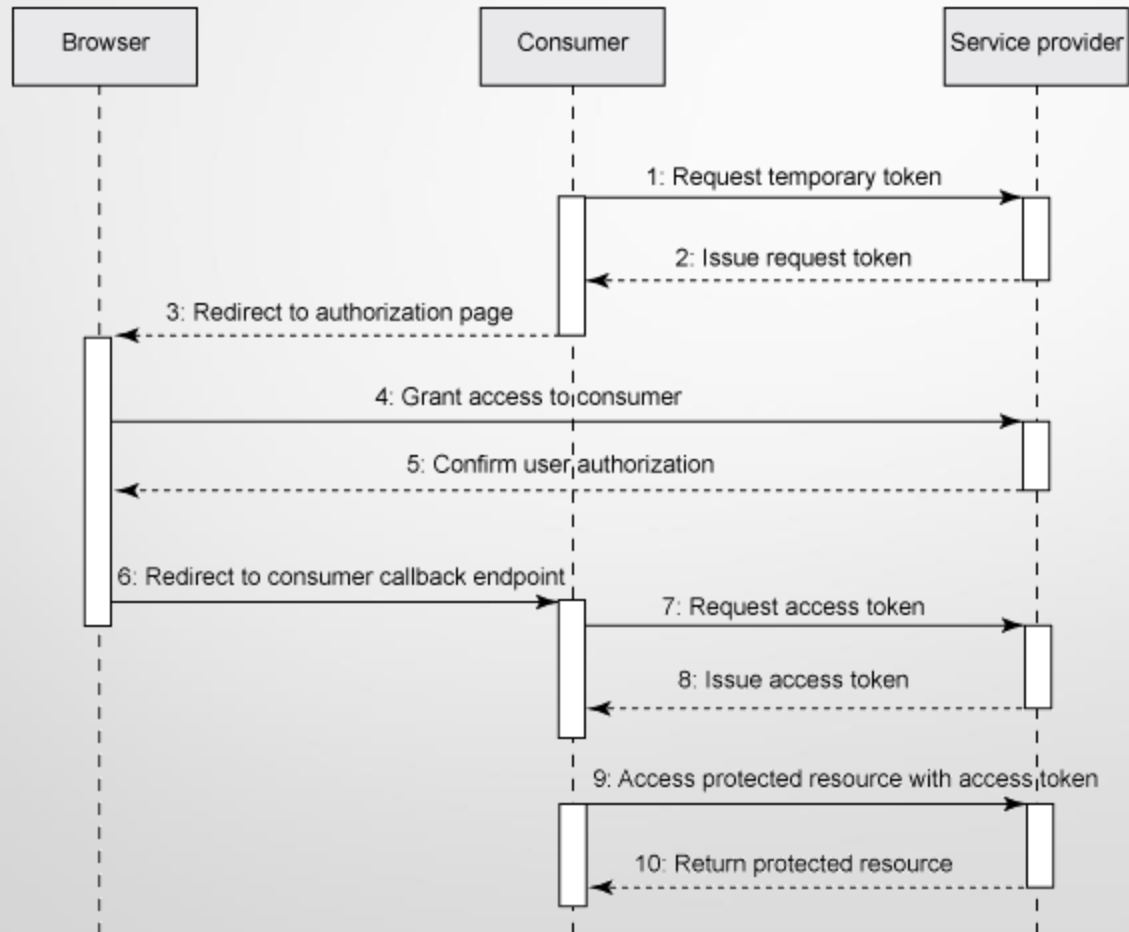
Request Security

- Signatures – OAuth 1.0
  - OAuth allows dynamic determination of algorithm
- Nonce
  - Unique request identifier
- Timestamp
  - Allows expiration and re-use of Nonce values

References

- Eric Hammer-Lahav
  - http://hueniverse.com/oauth/guide/history/
  - Primary reference for history of Oauth
- Wikipedia: OpenID vs. Oauth Psuedo-Authentication Graphic
  - http://en.wikipedia.org/wiki/File:OpenIDvs.Pseudo-AuthenticationusingOAuth.svg
- OAuth Community Site
  - http://oauth.net/
- IBM – Three Legged OAuth
  - http://www.ibm.com/developerworks/web/library/wa-oauthsupport/ThreeLeggedOAuthDance.gif