



Hannes Tschofenig, Blaine Cook

# The Problem

## Build your network (Why?)



### Find contacts who are already on LinkedIn



#### Web email contacts

Check your address book to find contacts who are on LinkedIn.



Windows Live Hotmail



Gmail



Other



YAHOO!



AOL

Username:

@gmail.com

Password:

Upload Contacts



#### Address book contacts

Outlook, Apple Mail, etc.

Find

# The OAuth Approach

## Build your network (Why?)



### Find contacts who are already on LinkedIn



#### Web email contacts

Check your address book to find contacts who are on LinkedIn.



Windows Live Hotmail



Gmail



Other



YAHOO!



AOL

Login to Yahoo!

You will be taken to Yahoo! to enter your username and password.



#### Address book contacts

Outlook, Apple Mail, etc.

Find



# User Authorizes Consumer to access Service

Yahoo! - Terms - Microsoft Internet Explorer provided by NOKIA

File Edit View Favorites Tools Help

Address [https://api.login.yahoo.com/WsLogin/v1/wslogin?appid=cVa\\_PAF1kY2kYgtd2KZejiTUNp8FLBx4KmA&ts=1215323357&sig=a1401bd223c0127d681911983863a6338&scrumb=hmM0aryi.3I](https://api.login.yahoo.com/WsLogin/v1/wslogin?appid=cVa_PAF1kY2kYgtd2KZejiTUNp8FLBx4KmA&ts=1215323357&sig=a1401bd223c0127d681911983863a6338&scrumb=hmM0aryi.3I) Go Links SnagIt

Yahoo! - Help

## Now we need your permission to grant access to your Yahoo! account

<http://www.linkedin.com> is asking you and Yahoo! for the ability to automatically log you into your Yahoo! account through a service or application that is provided by <http://www.linkedin.com>, and to:

- read your data in **Yahoo! Address Book**
- read and write to your data in **Yahoo! Address Book**

By clicking "I Agree" below, you give Yahoo! permission to enable <http://www.linkedin.com> to access your Yahoo! account for this purpose, and further agree to the Automatic Login Terms of Service below.

Keep in mind:

- <http://www.linkedin.com> will not be able to access any data you keep on Yahoo! other than the data identified above.
- The permission will expire in 2 weeks.
- You can change this permission by visiting the [My Account](#) page and selecting the **Partner Accounts** link. Note that revoking permission may take up to 24 hours.
- If you change your password, you may be required to give permission again.
- The Yahoo! privacy policy does not apply to <http://www.linkedin.com>; please read their privacy policy to learn more about how they treat your personal information.
- Yahoo! has no affiliation with <http://www.linkedin.com> and cannot guarantee the security of any user data that you permit <http://www.linkedin.com> to access.

**Sign-in Permissions**

Please review the following terms and indicate your agreement below. [View all and print](#)

Automatic Login Terms of Service - Please read carefully

Your use of automatic login with third party sites is at your sole risk. While Yahoo! takes measures to protect the privacy and

By clicking "I agree", you agree that you have read and understand these terms.

# Consumer calls the Service Provider API

The screenshot shows a Microsoft Internet Explorer browser window displaying the LinkedIn 'Imported Contacts' page. The browser's address bar shows the URL: `http://www.linkedin.com/uploadContacts?checkUpload=&handle=%2Fp%2F2%2F000%2F00c%2F1ba%2F2f4701f%2Etxt&taskType=importContacts&refreshCount=1&context=5&sortAction=lastnam`. The LinkedIn page header includes the logo, navigation tabs (People, Jobs, Answers, Companies), and a search bar. A green notification banner at the top states 'We added 20 contact(s)'. The main content area is titled 'Contacts' and features tabs for 'Connections', 'Imported Contacts', and 'Network Statistics'. A message reads: 'These are your newly added contacts that are not yet connected to you on LinkedIn. Invite them to connect!'. Below this, a list of 20 contacts is shown, with the first few visible: A. Razool, Babu, Sudheer, C. P. Mahir, C. Hari, goel, amit, and K. Ranjith. A green arrow points from the 'Imported Contacts' tab to a selection box on the right containing the names of the selected contacts: Razool, A; Sudheer, Babu; Mahir, C P; Hari, C; amit, goel; Ranjith, K; Sajil, Koroth; Amitava, Kundu; Rghunathan, Navaneethan; and Ram, P N. A checkbox for 'Add a personal note to your invitation' is present, and a blue button labeled 'Invite selected contacts' is at the bottom of the selection box.



# History

# History

- November 2006: Blaine Cook was looking into the possibility of using OpenID to accomplish the functionality for delegated authentication. He got in touch with some other folks that had a similar need.
- December 2006: Blaine wrote a "reference implementation" for Twitter based on all the existing OAuth-patterned APIs, which Blaine and Kellan Elliott-McCrea turned into a rough functional draft
- April 2007: [Google group](#) was created with a small group of implementers to write a proposal for an open protocol.
- July 2007: OAuth 1.0 (with code for major programming languages)
- September 2007: Re-write of specification to focus on a single flow (instead of "web", "mobile", and "desktop" flows)
- Deployment of OAuth well on it's way:  
<http://wiki.oauth.net/ServiceProviders>

# History, cont.

- 1<sup>st</sup> OAuth BOF (Minneapolis, November 2008, IETF#73)
  - BOF Chairs: Sam Hartman, Mark Nottingham
  - BOF went OK but a couple of charter questions couldn't be resolved.
- 2<sup>nd</sup> OAuth BOF (San Francisco, March 2009, IETF#74)
  - BOF Chairs: Hannes Tschofenig, Blaine Cook
  - Charter discussed on the mailing list and also during the meeting. Finalized shortly after the meeting
- IETF wide review of the OAuth charter text (28<sup>th</sup> April 2009)
  - Announcement:  
<http://www.ietf.org/mail-archive/web/ietf-announce/current/msg06009.html>
- OAuth working group was created (May 2009)
  - Chairs: Blaine Cook, Peter Saint Andre
- Feb 2010: 'The OAuth 1.0 Protocol ' approved as Informational RFC:
  - <http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07047.html>

# The Protocol

- \* requesting a token
- \* **presenting the token**

# Presenting a Token

- A → B: HTTP || Token [|| {Header, ..., timestamp}<sub>key</sub>]
- A ← B: HTTP (200 OK)
- Questions:
  - What is signed and how?
  - Where does the *token* come from?
  - Where does the *key* come from?

# Signatures

- Used to show ownership of token.
- 'The OAuth 1.0 Protocol'
  - <http://www.ietf.org/internet-drafts/draft-hammer-oauth-10.txt>
- Signatures based on symmetric & asymmetric key supported:
  - HMAC-SHA1
  - RSA-SHA1
- No signature = “bearer token”/ PLAINTEXT
- Extensions exist that sign other parts of the message:
  - OAuth Request Body Hash:
    - <http://tools.ietf.org/html/draft-eaton-oauth-bodyhash-00>
    - [http://oauth.googlecode.com/svn/spec/ext/body\\_hash/1.0/drafts/1/spec.html](http://oauth.googlecode.com/svn/spec/ext/body_hash/1.0/drafts/1/spec.html)
  - Going beyond HTTP → OAuth over XMPP
    - <http://xmpp.org/extensions/xep-0235.html>

# The Protocol

- \* requesting a token
- \* presenting the token

# Requesting a Token

- Different ways to get a token exist.
- Example: WRAP
  - A → KDC: HTTP (get request access token) || credentials
  - A ← KDC: Access Token [, Expires in](also offers the approach of using a refresh token exchange)
- Example: OAuth 1.0
  - A → B: HTTP (get request token) || credentials
  - A ← B: request token
  - <<A gets resource owner to tell B to authorize request token>>
  - A → B: HTTP (get access token) || request token
  - A ← B: access token
- Other “flows” have been specified in WRAP
- Various authentication mechanisms specified.



# Token

# Token

- The token format is not standardized.
- Out-of-scope: \*which\* permissions were granted, and \*how\* those permissions are enforced
- Token may be created with constraints, for example regarding lifetime
  - OAuth 1.0 does not specify anything with this regard
  - WRAP <http://tools.ietf.org/id/draft-hardt-oauth-01.txt> provides a expires\_in parameter.

# Summary

- Work on delegated authentication in the APPs area in the OAuth group.
- OAuth 1.0: Community version published
- OAuth 2.0: Fusing WRAP, initial OAuth 2.0
- OAuth WG met Monday afternoon. Interim meeting will be scheduled.
- Participation and early feedback desired, especially from security community