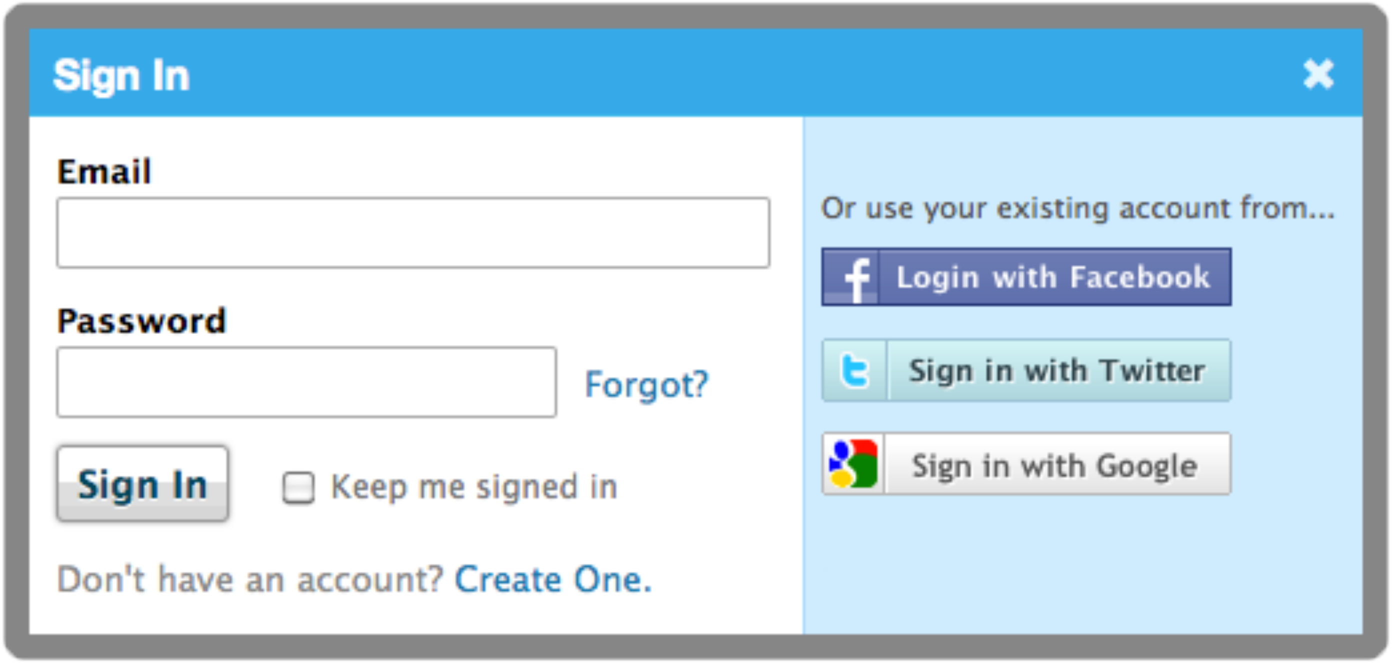
SudoWeb: Minimizing Information Disclosure to Third Parties in Single Sign-On Platforms

Georgios Kontaxis, *Columbia University, USA*
Michalis Polychronakis, *Columbia University, USA*

Evangelos P. Markatos,
FORTH and University of Crete
Greece

The Problem

- Single-sign on approaches in
  - Third-party web sites



Sign In

Email

Password

Forgot?

Sign In

□ Keep me signed in

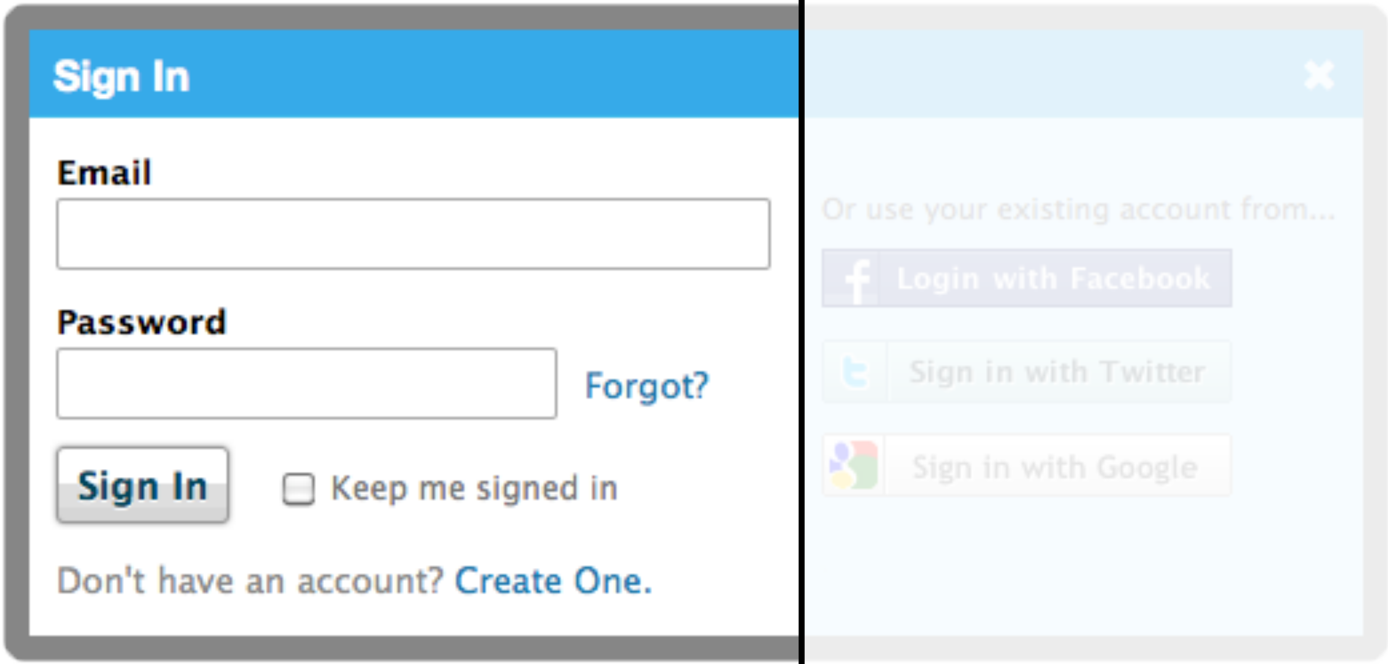
Don't have an account? Create One.

Or use your existing account from...

Login with Facebook

Sign in with Twitter

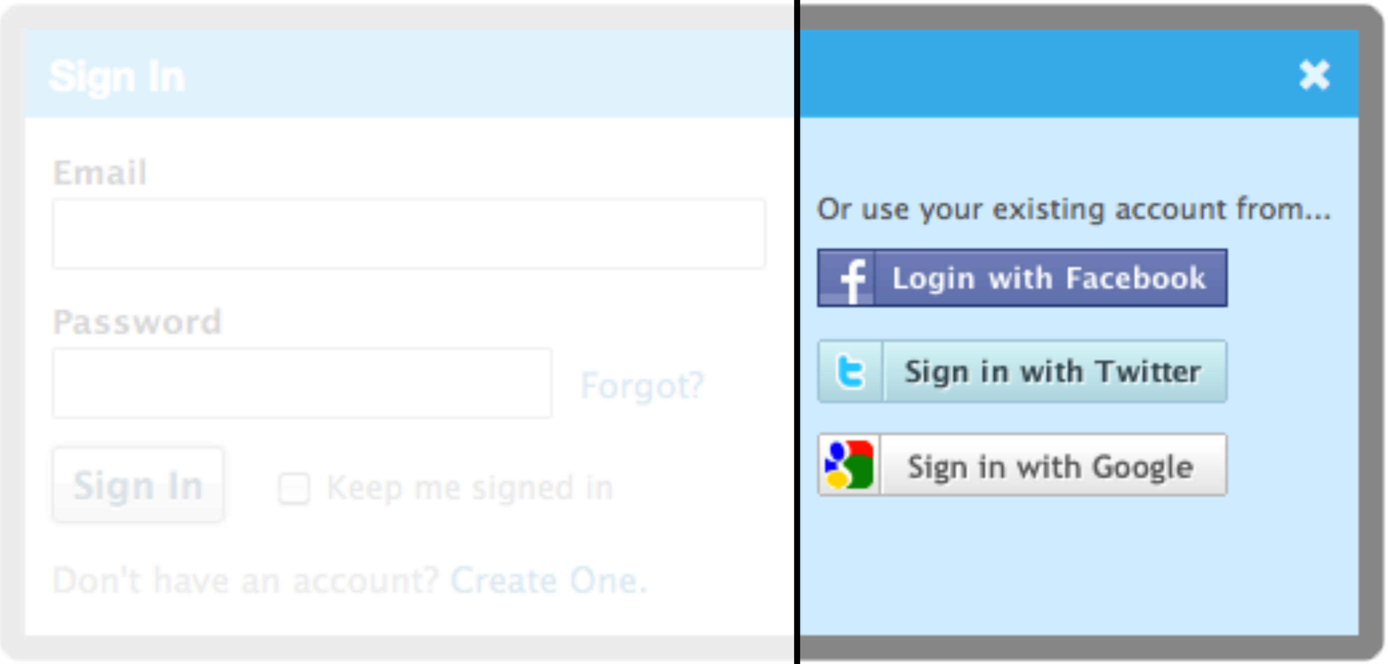
Sign in with Google



Don't have an account? Create One.

Or use your existing account from...

Create yet another account…



Sign In

Email

Password

Forgot?

Sign In

□ Keep me signed in

Don't have an account? Create One.

Or use your existing account from...

Sign in with a single click…

Social Login

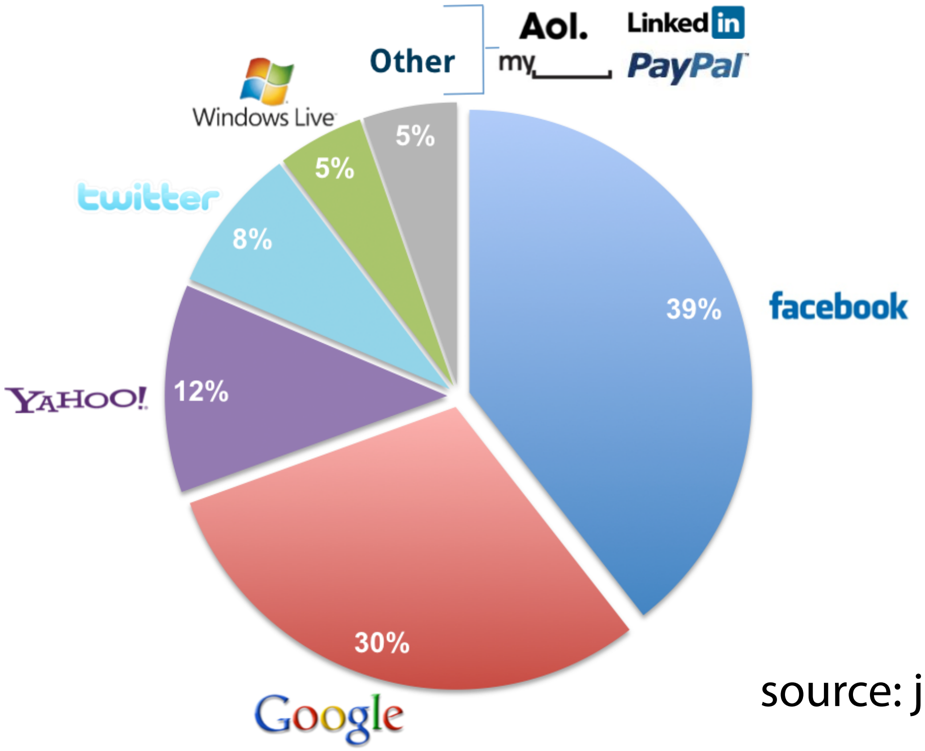
- ✓ Convenience – fewer passwords to remember
- ✓ Rich experience through social features
- ✓ Outsource user registration and management
- ✘ Same credentials for multiple sites
- ✘ User tracking (future work)
- ✘ Access to user’s profile (this work)

Users Like Social Login

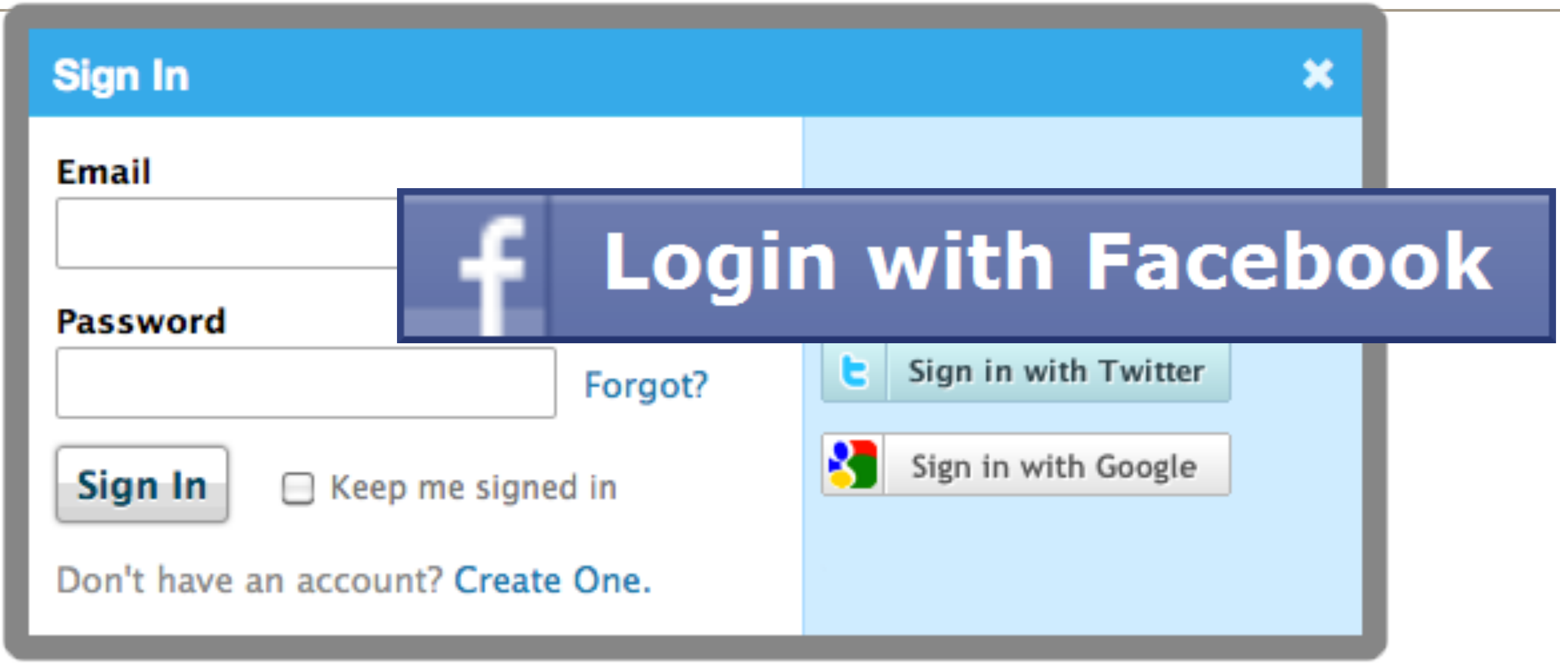
66% prefer it vs. 34% traditional login

- 76% admit to having given incorrect registration info

Social login preferences Q2, 2011



source: janrain.com



Sign In ✖

Email

Password

Forgot?

Sign In

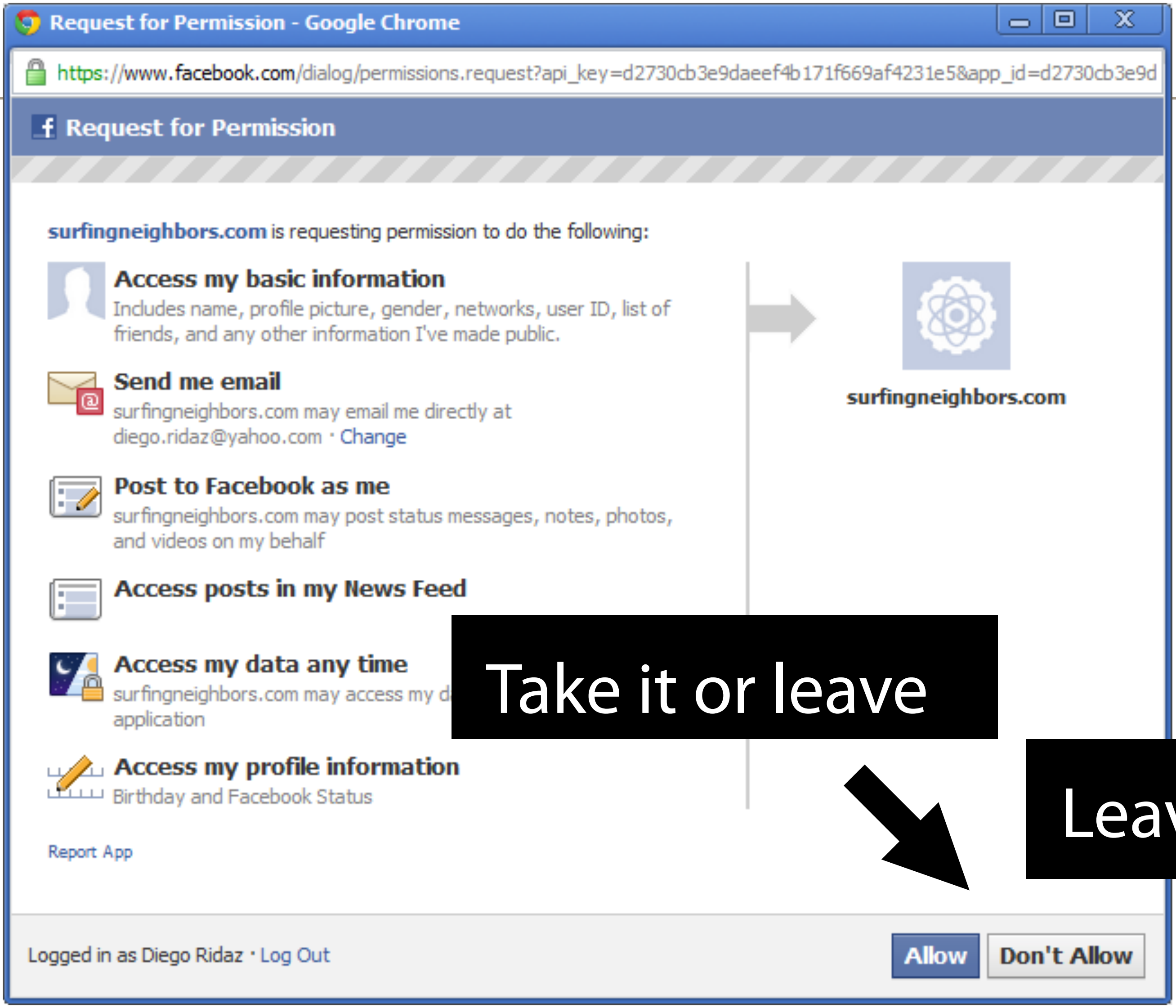
□ Keep me signed in

Don't have an account? Create One.

Login with Facebook

Sign in with Twitter

Sign in with Google



https://www.facebook.com/dialog/permissions.request?api_key=d2730cb3e9daeef4b171f669af4231e5&app_id=d2730cb3e9d

Request for Permission

surfingneighbors.com is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.

Send me email
surfingneighbors.com may email me directly at diego.ridaz@yahoo.com · Change

Post to Facebook as me
surfingneighbors.com may post status messages, notes, photos, and videos on my behalf

Access posts in my News Feed

Access my data any time
surfingneighbors.com may access my d
application

Access my profile information
Birthday and Facebook Status

surfingneighbors.com

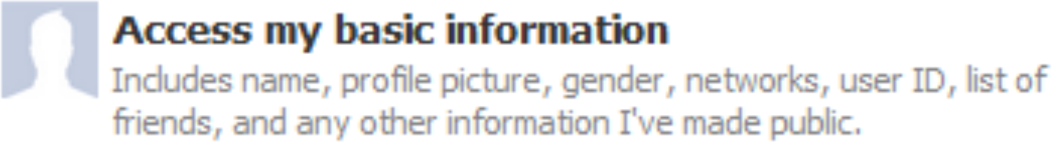
Report App

Logged in as Diego Ridaz · Log Out

Take it or leave

Leave

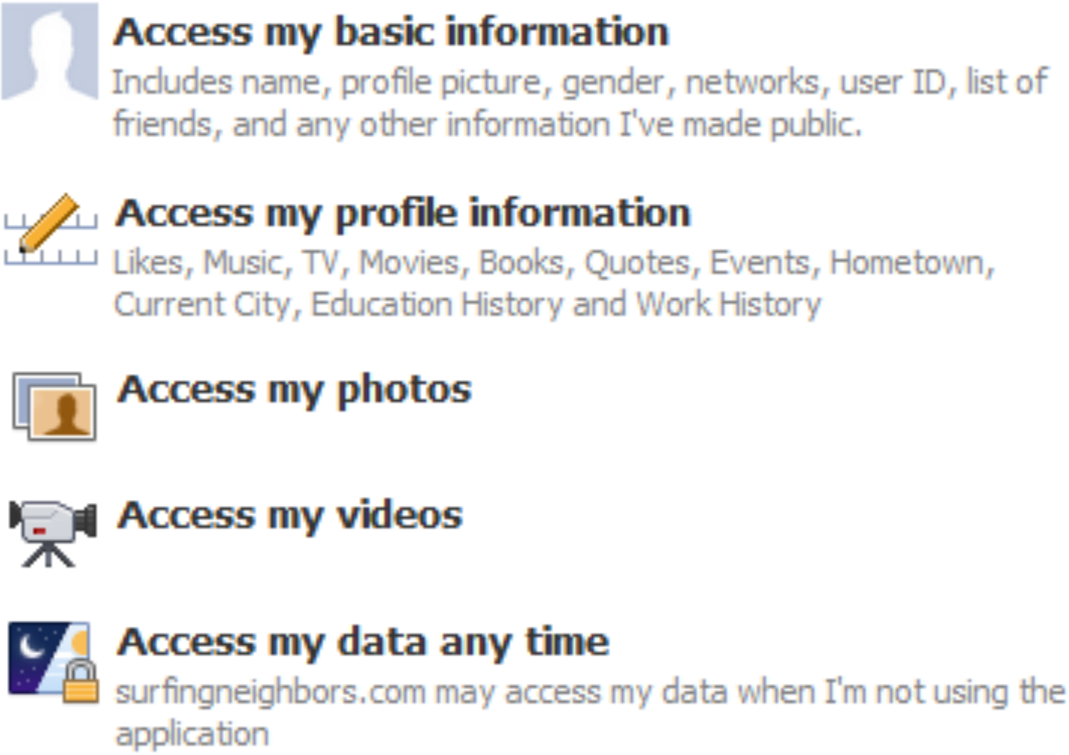
Loss of anonymity



Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.

Access to private data



Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.

Access my profile information

Likes, Music, TV, Movies, Books, Quotes, Events, Hometown, Current City, Education History and Work History

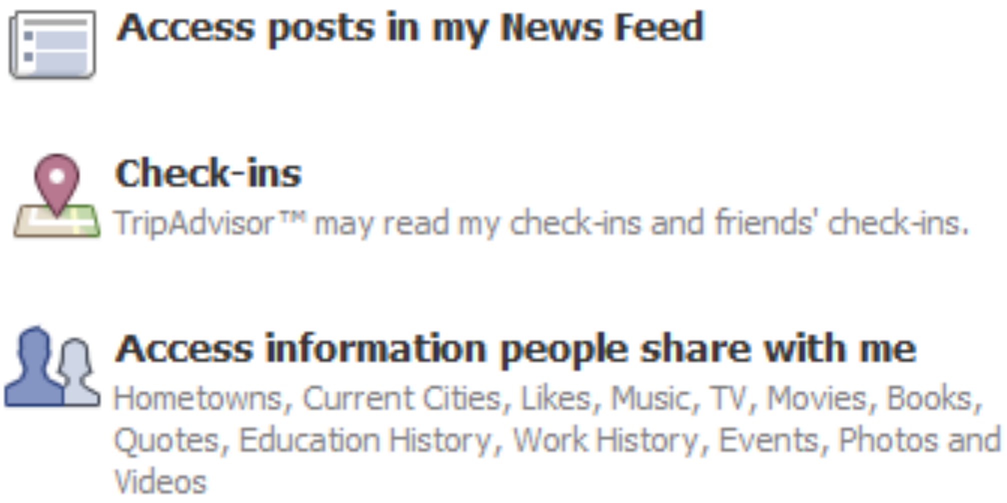
Access my photos

Access my videos

Access my data any time

surfingneighbors.com may access my data when I'm not using the application

Access to other’s private data



Access posts in my News Feed

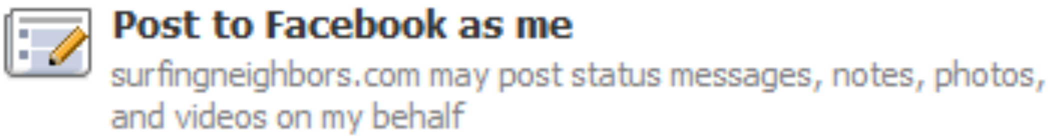
Check-ins

TripAdvisor™ may read my check-ins and friends' check-ins.

Access information people share with me

Hometowns, Current Cities, Likes, Music, TV, Movies, Books, Quotes, Education History, Work History, Events, Photos and Videos

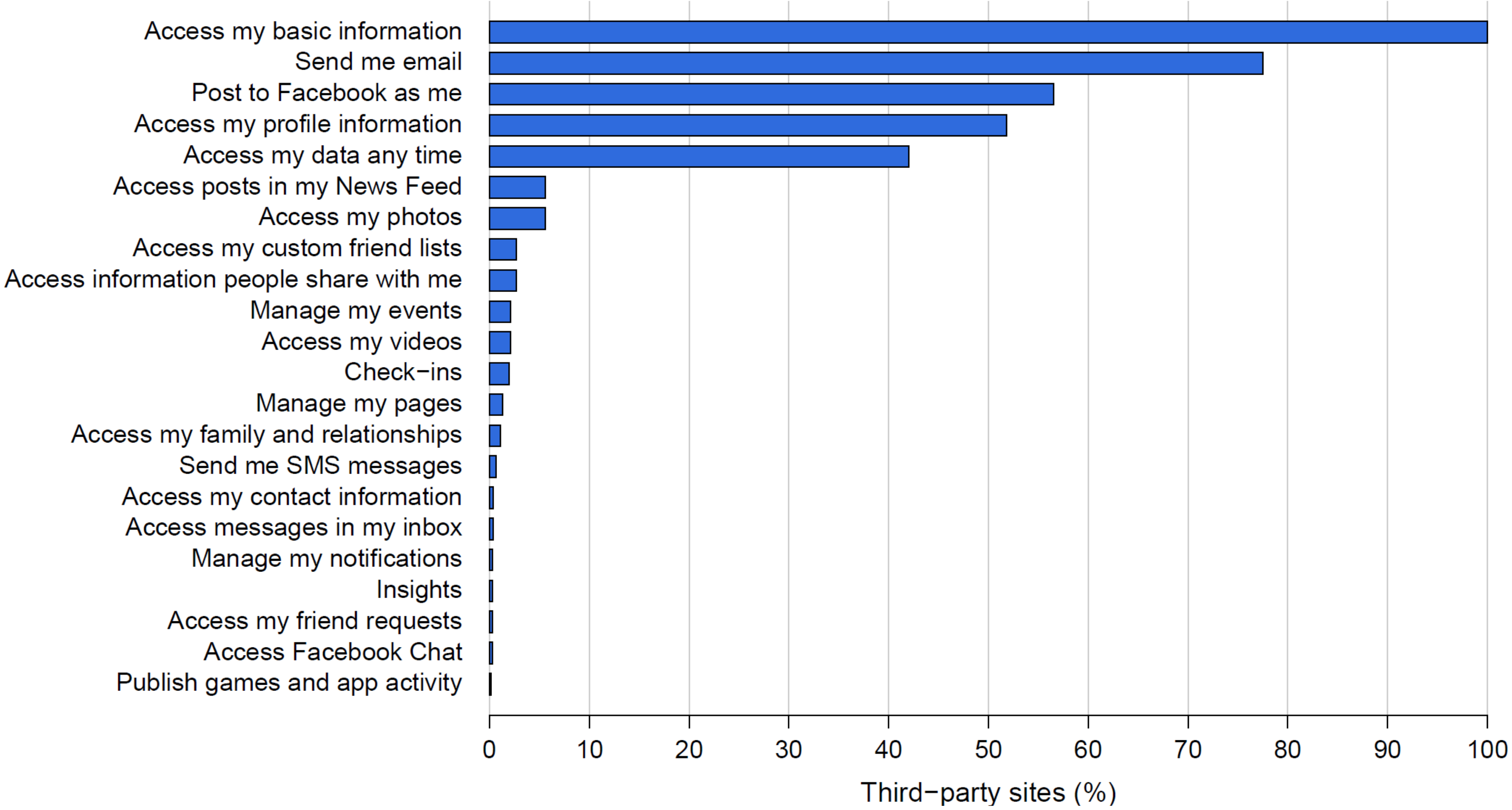
Act in the place of user



Post to Facebook as me

surfingneighbors.com may post status messages, notes, photos, and videos on my behalf

Distribution of Requested Permissions



Random sample of 755 websites that have incorporated Facebook's social login platform

Threats

An untrustworthy (or compromised) site can…

- Sell private data to third parties
- Post spam messages
- Build behavioral profiles
- Provide accidental access to third parties [Symantec '11]
- …

Sites usually ask for much more permissions than what actually needed… [Felt '08]

- And have perpetual access to personal data, including those added in the *future*

Like running a webserver as root…

```
SU(1)                   User Commands                   SU(1)

NAME
       su - change user ID or become superuser

SYNOPSIS
       su [options] [username]

DESCRIPTION
       The su command is used to become another user during a
       login session. Invoked without a username, su defaults
       to becoming the superuser. The optional argument - may
       be used to provide an environment similar to what the
       user would expect had the user logged in directly.
```

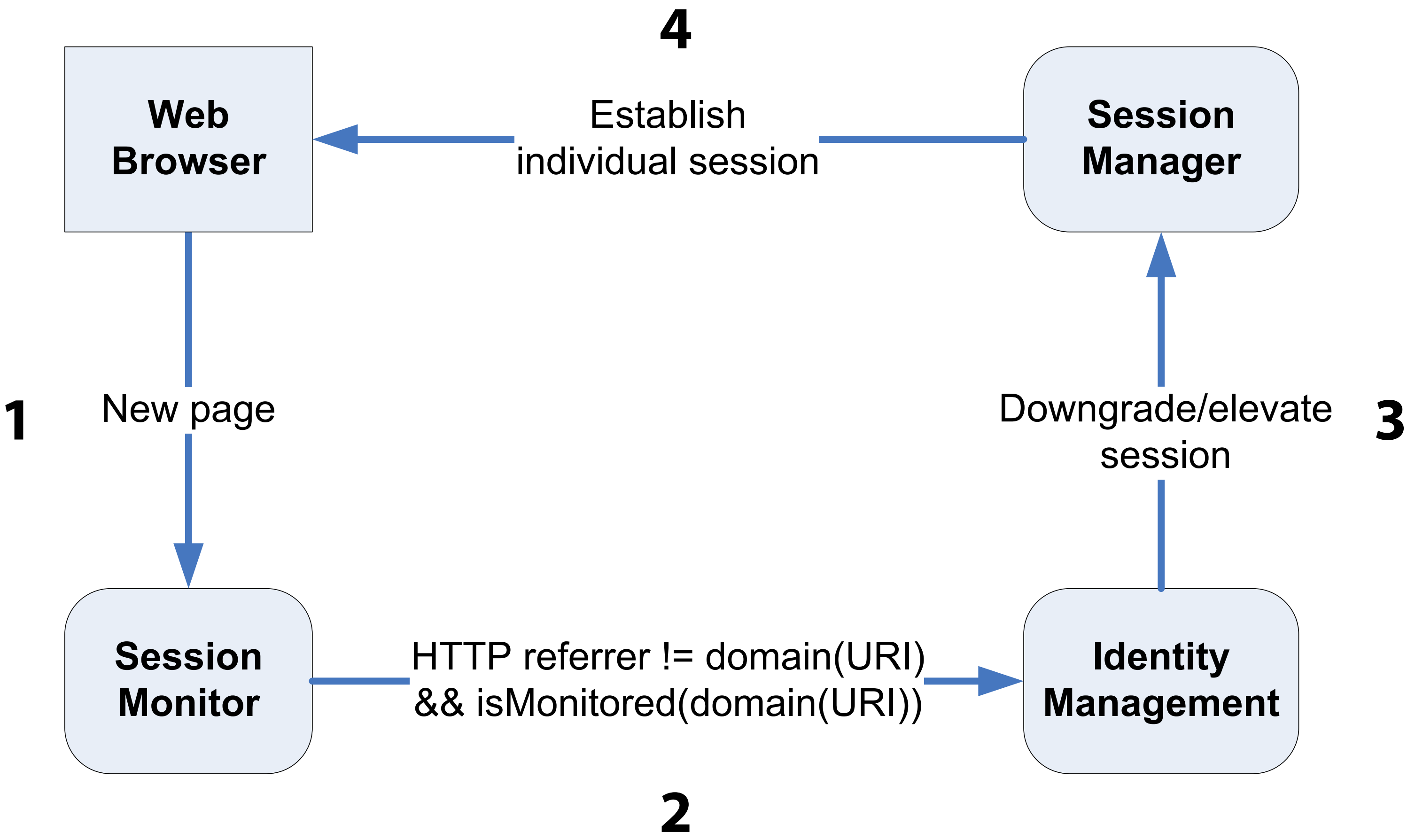
SudoWeb

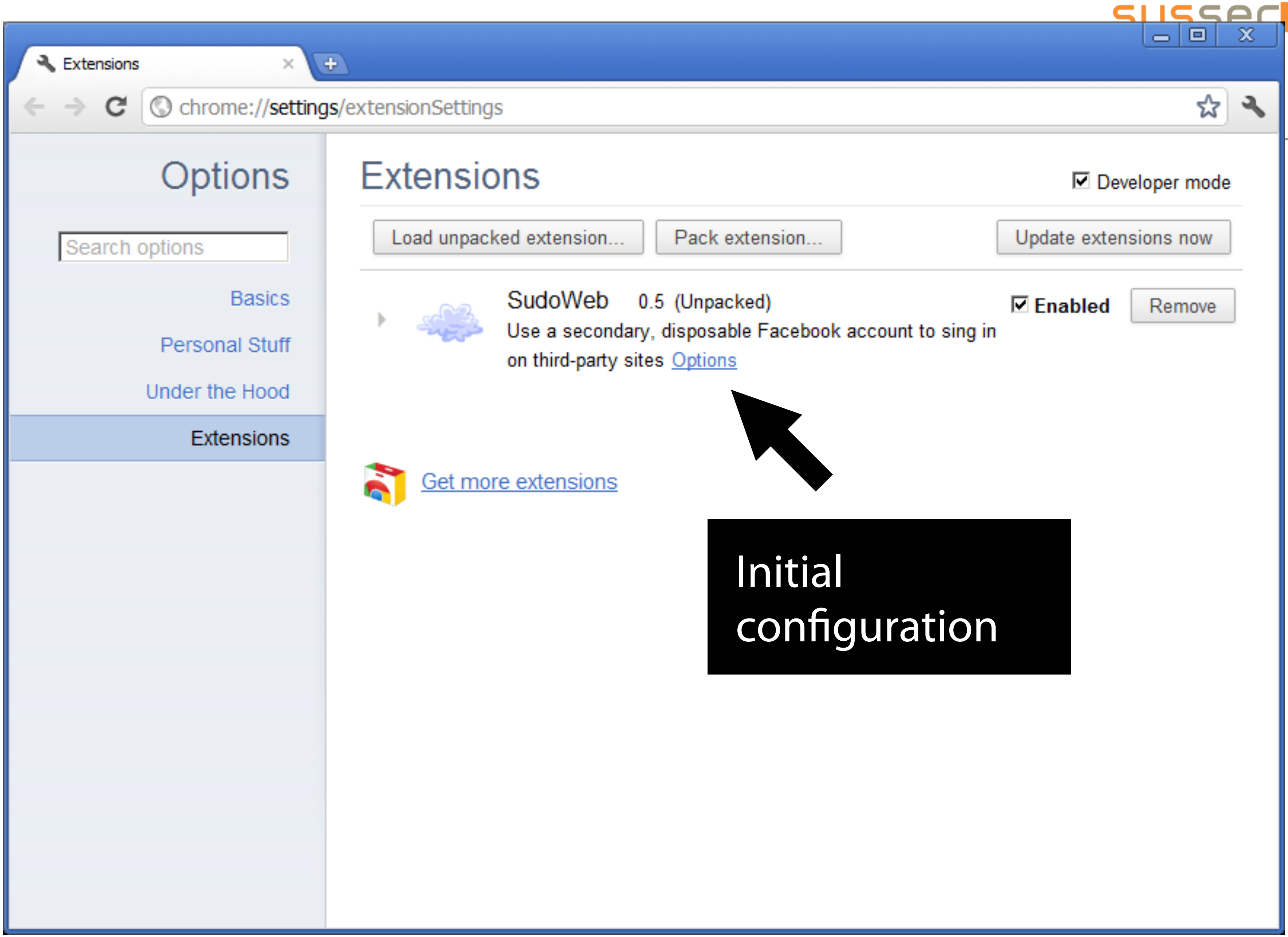
- Bring the least privilege paradigm in social login platforms
- Root account vs. normal user account analogy
- Primary profile == root account
  - Use carefully! Contains sensitive private information!
  - Should never be used as a default account
- Secondary profile == normal user account
  - Does not contain any sensitive information – *disposable*
  - Should be used by default

Design and Implementation

- Maintain multiple concurrent sessions
  - Use primary account for direct interaction with the social network
  - Automatically switch to the secondary account for all interactions with third-party sites
  - *Transparent operation*
- Implemented as an extension for Chrome
  - Current prototype supports Facebook
  - Takes advantage of Chrome's "incognito" mode for maintaining concurrent sessions with different sets of credentials

Workflow


4
Web Browser
Establish individual session
Session Manager
1
New page
Downgrade/elevate session
3
Session Monitor
HTTP referrer != domain(URI) && isMonitored(domain(URI))
Identity Management
2



Extensions

chrome://settings/extensionSettings

Options

Search options

Basics

Personal Stuff

Under the Hood

Extensions

Extensions

☑ Developer mode

Load unpacked extension... | Pack extension... | Update extensions now

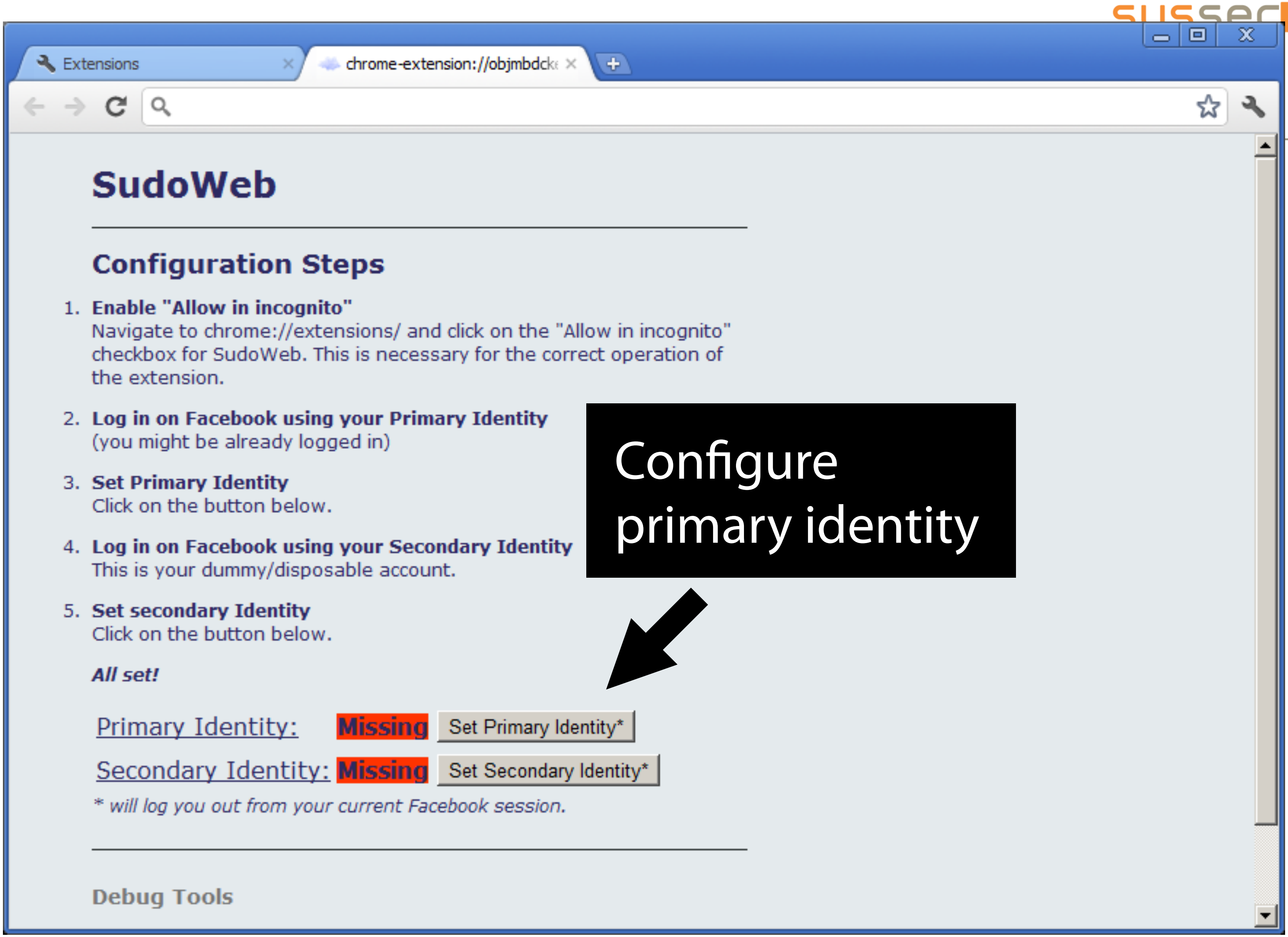
SudoWeb 0.5 (Unpacked)

Use a secondary, disposable Facebook account to sing in on third-party sites Options

☑ Enabled | Remove

Get more extensions

Initial configuration



SudoWeb

Configuration Steps

1. **Enable "Allow in incognito"**
   Navigate to chrome://extensions/ and click on the "Allow in incognito" checkbox for SudoWeb. This is necessary for the correct operation of the extension.
2. **Log in on Facebook using your Primary Identity**
   (you might be already logged in)
3. **Set Primary Identity**
   Click on the button below.
4. **Log in on Facebook using your Secondary Identity**
   This is your dummy/disposable account.
5. **Set secondary Identity**
   Click on the button below.

All set!

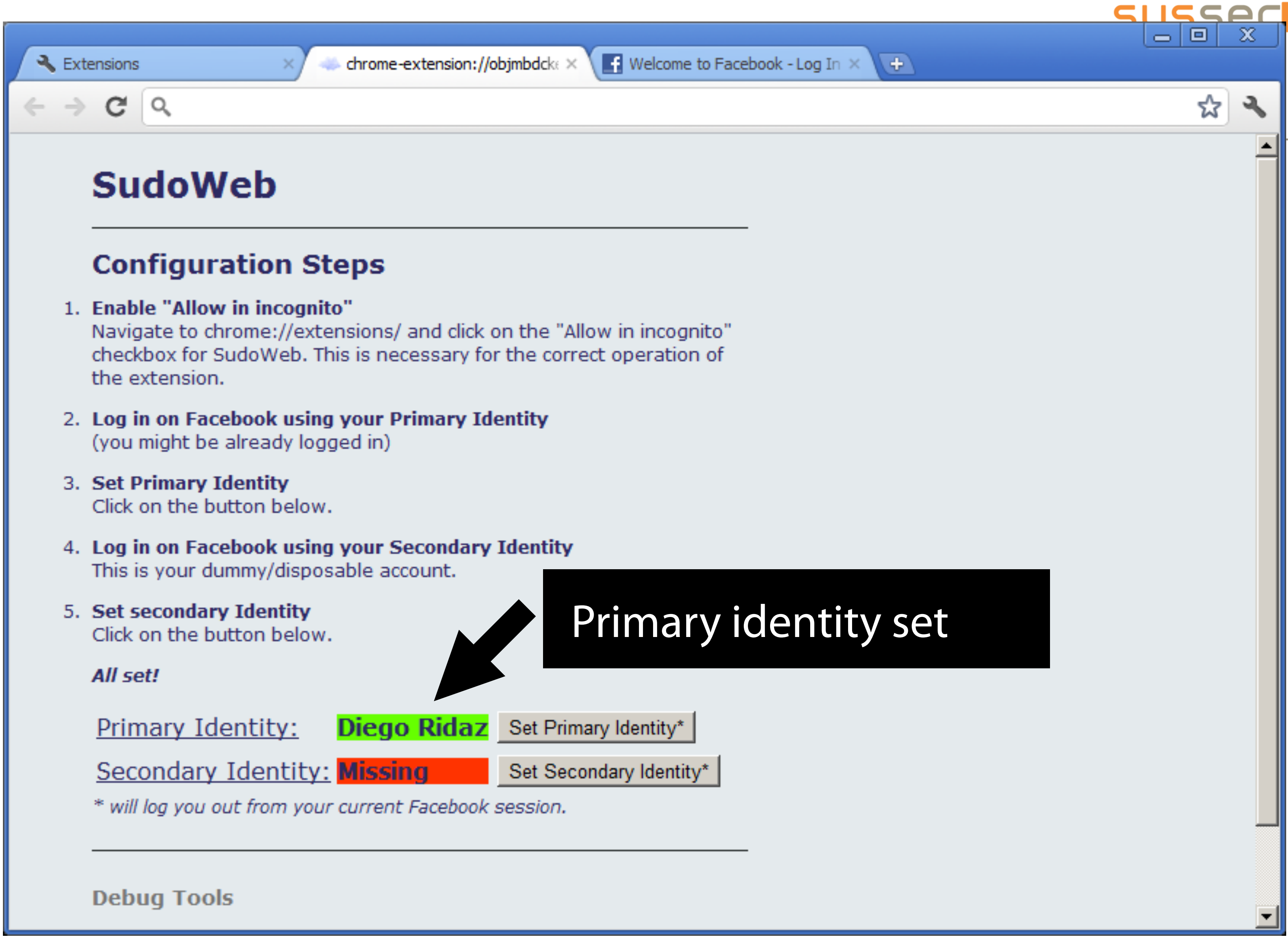
Primary Identity: Missing

Secondary Identity: Missing

** will log you out from your current Facebook session.*

Debug Tools

Configure primary identity



SudoWeb

Configuration Steps

1. **Enable "Allow in incognito"**
   Navigate to chrome://extensions/ and click on the "Allow in incognito" checkbox for SudoWeb. This is necessary for the correct operation of the extension.
2. **Log in on Facebook using your Primary Identity**
   (you might be already logged in)
3. **Set Primary Identity**
   Click on the button below.
4. **Log in on Facebook using your Secondary Identity**
   This is your dummy/disposable account.
5. **Set secondary Identity**
   Click on the button below.

All set!

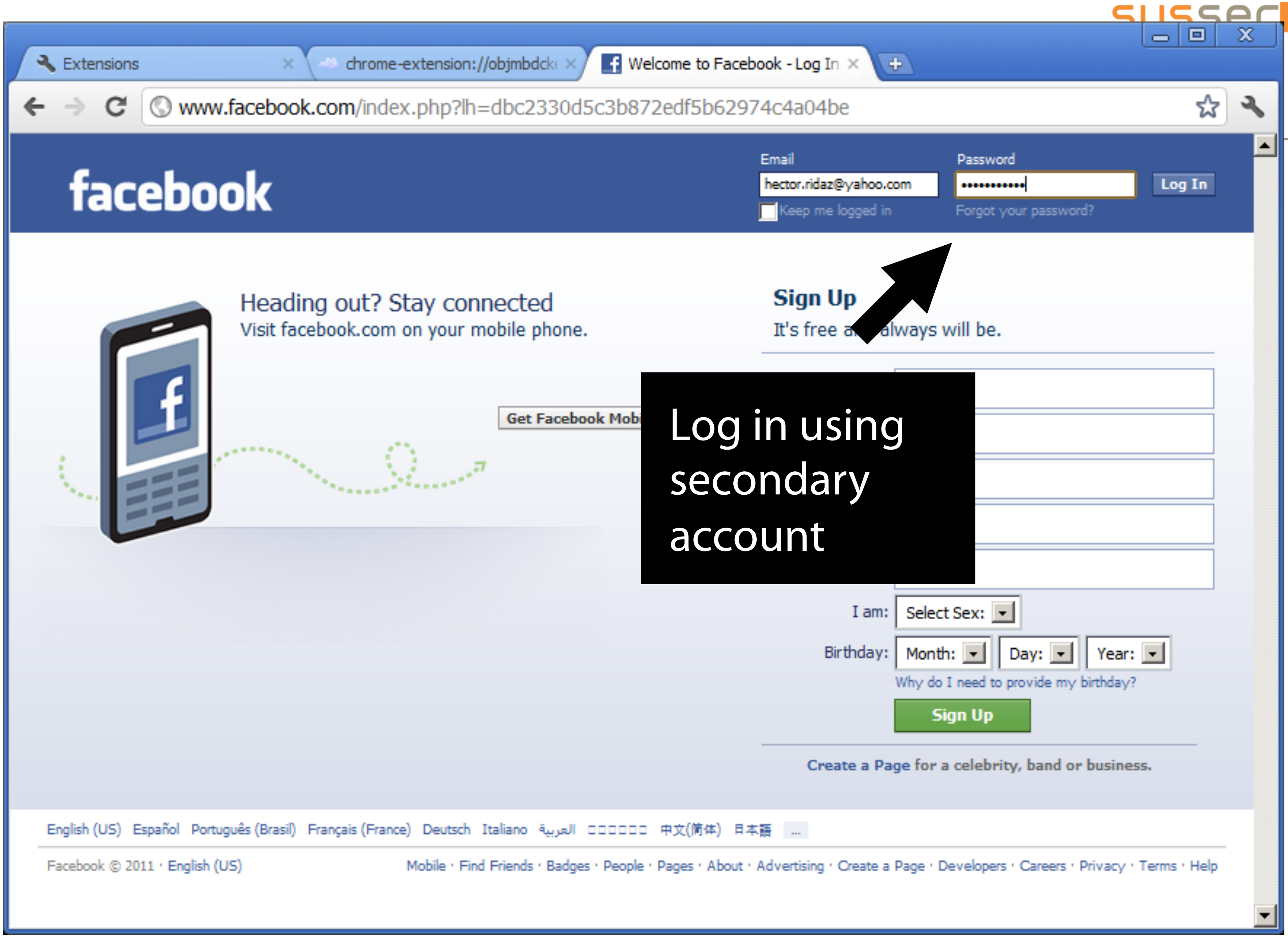
Primary Identity: Diego Ridaz

Secondary Identity: Missing

** will log you out from your current Facebook session.*

Debug Tools

Primary identity set



Extensions

chrome-extension://objmbdck

Welcome to Facebook - Log In

www.facebook.com/index.php?lh=dbc2330d5c3b872edf5b62974c4a04be

facebook

Email: hector.ridaz@yahoo.com

Password: ••••••••••••

Log In

□ Keep me logged in

Forgot your password?

Heading out? Stay connected

Visit facebook.com on your mobile phone.

Get Facebook Mobi

Sign Up

It's free a always will be.

I am: Select Sex:

Birthday: Month: Day: Year:

Why do I need to provide my birthday?

Sign Up

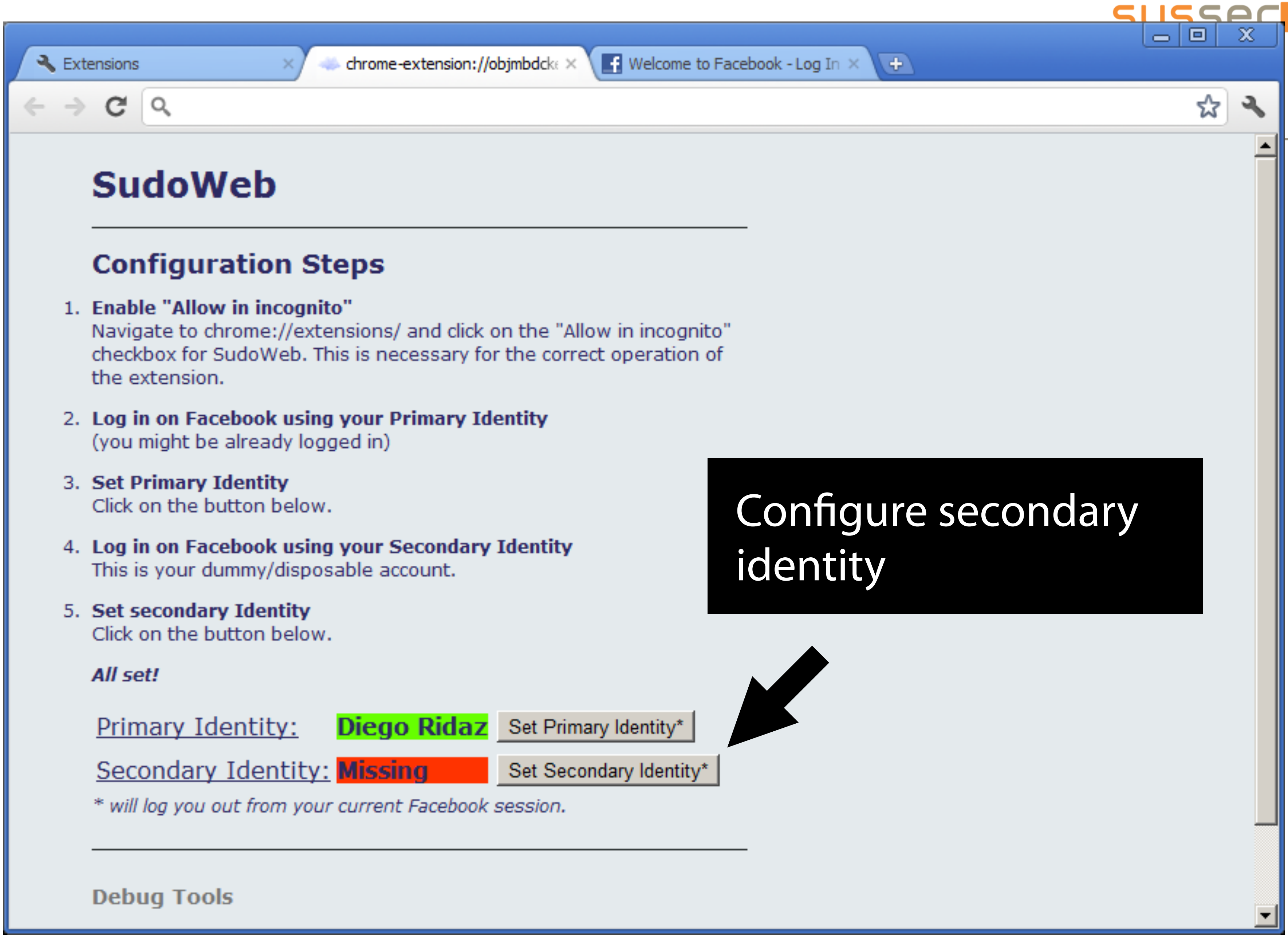
Create a Page for a celebrity, band or business.

English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية □□□□□□ 中文(简体) 日本語 ...

Facebook © 2011 · English (US)

Mobile · Find Friends · Badges · People · Pages · About · Advertising · Create a Page · Developers · Careers · Privacy · Terms · Help

Log in using secondary account



SudoWeb

Configuration Steps

1. **Enable "Allow in incognito"**
   Navigate to chrome://extensions/ and click on the "Allow in incognito" checkbox for SudoWeb. This is necessary for the correct operation of the extension.
2. **Log in on Facebook using your Primary Identity**
   (you might be already logged in)
3. **Set Primary Identity**
   Click on the button below.
4. **Log in on Facebook using your Secondary Identity**
   This is your dummy/disposable account.
5. **Set secondary Identity**
   Click on the button below.

All set!

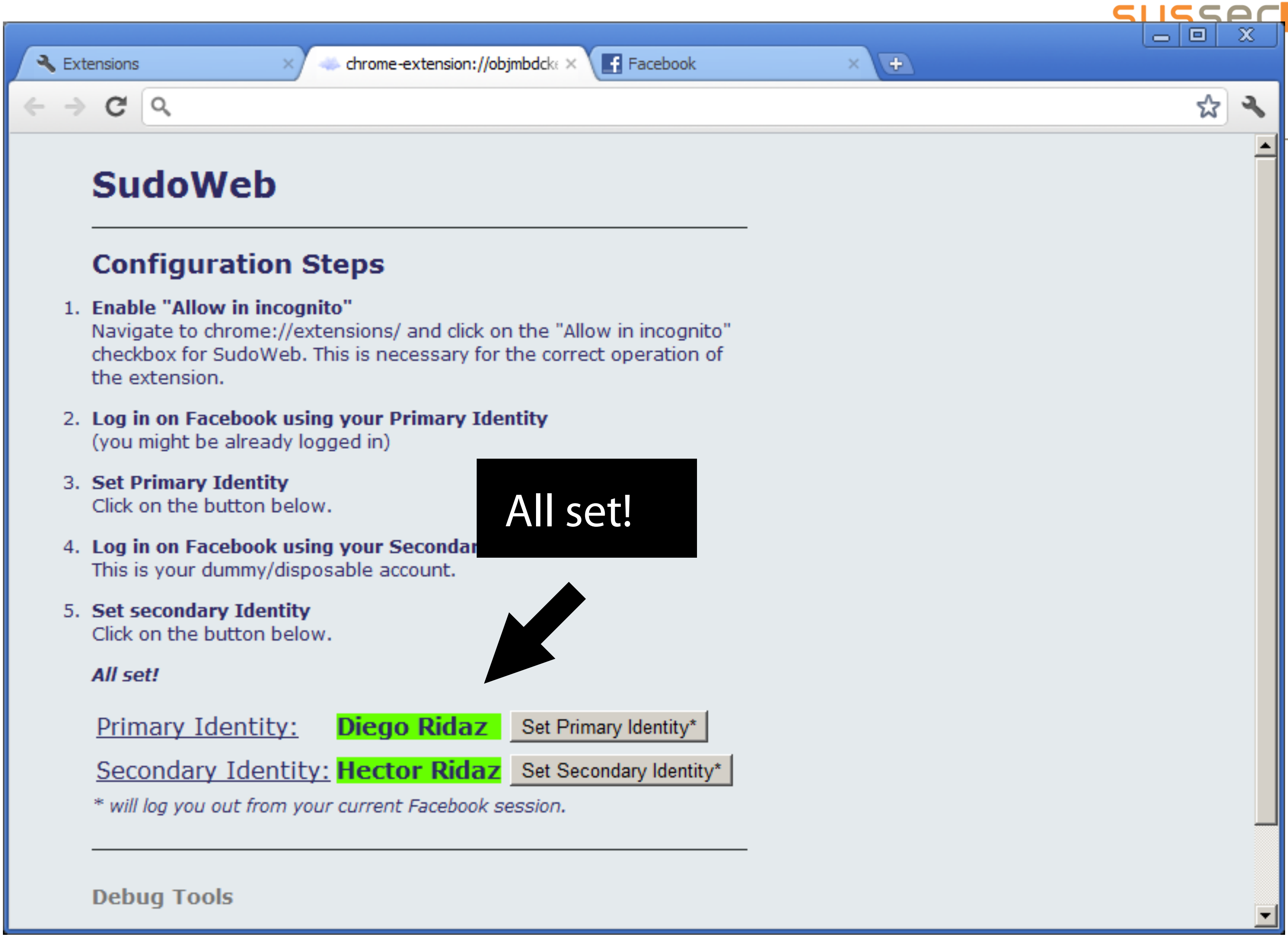
Primary Identity: Diego Ridaz [Set Primary Identity*]

Secondary Identity: Missing [Set Secondary Identity*]

** will log you out from your current Facebook session.*

Debug Tools

Configure secondary identity



SudoWeb

Configuration Steps

1. **Enable "Allow in incognito"**
   Navigate to chrome://extensions/ and click on the "Allow in incognito" checkbox for SudoWeb. This is necessary for the correct operation of the extension.
2. **Log in on Facebook using your Primary Identity**
   (you might be already logged in)
3. **Set Primary Identity**
   Click on the button below.
4. **Log in on Facebook using your Secondar**
   This is your dummy/disposable account.
5. **Set secondary Identity**
   Click on the button below.

All set!

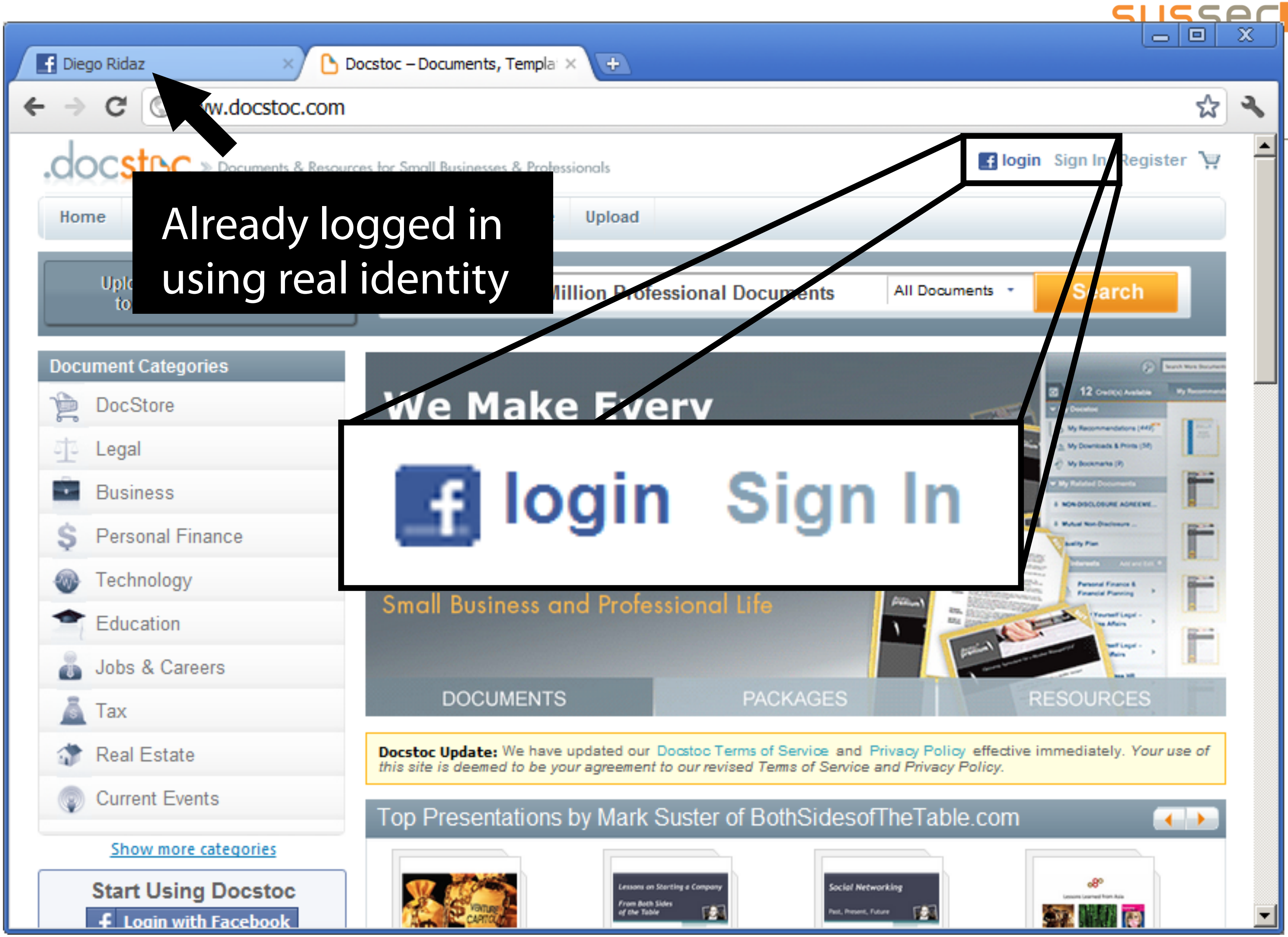
Primary Identity: **Diego Ridaz** Set Primary Identity*

Secondary Identity: **Hector Ridaz** Set Secondary Identity*

** will log you out from your current Facebook session.*

Debug Tools

All set!

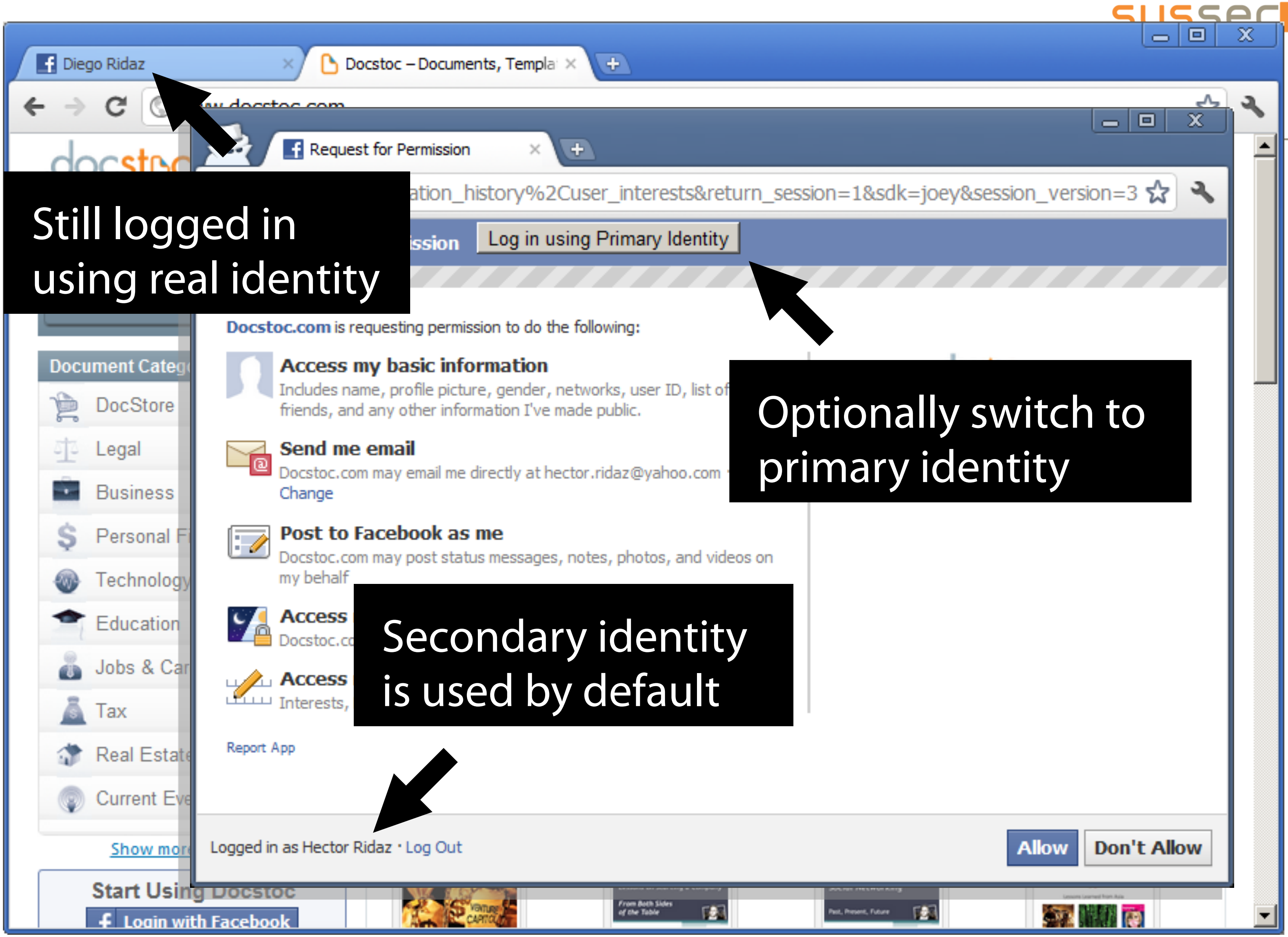


Already logged in using real identity

login Sign In

Docstoc Update: We have updated our Docstoc Terms of Service and Privacy Policy effective immediately. *Your use of this site is deemed to be your agreement to our revised Terms of Service and Privacy Policy.*

Top Presentations by Mark Suster of BothSidesofTheTable.com



Docstoc.com is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.

Send me email
Docstoc.com may email me directly at hector.ridaz@yahoo.com
Change

Post to Facebook as me
Docstoc.com may post status messages, notes, photos, and videos on my behalf

Access
Docstoc.c

Access
Interests,

Logged in as Hector Ridaz · Log Out

Still logged in using real identity

Optionally switch to primary identity

Secondary identity is used by default

Summary

Social login platforms pose threats to user privacy

SudoWeb: don’t surf as root!

https://code.google.com/p/sudoweb/

https://code.google.com/p/sudoweb/

thank you!

Georgios Kontaxis, *kontaxis@cs.columbia.edu*
Michalis Polychronakis, *mikepo@cs.columbia.edu*
Evangelos P. Markatos, *markatos@ics.forth.gr*