

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-ICS, Greece*

ISC '11 – October 28, 2011

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

Sign In

Email

Password

 [Forgot?](#)

Sign In Keep me signed in

Don't have an account? [Create One.](#)

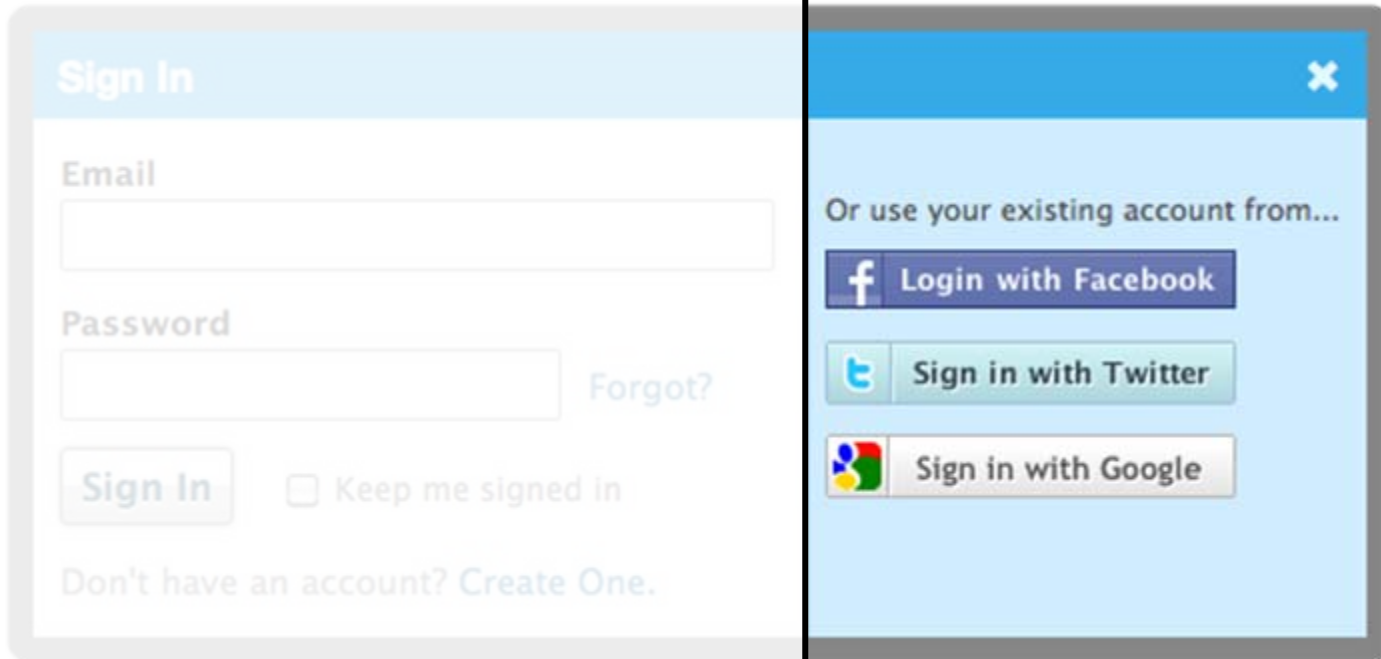
Or use your existing account from...

Login with Facebook

Sign in with Twitter

Sign in with Google

Create yet another account...



**Sign in with a
single click...**

Social Login

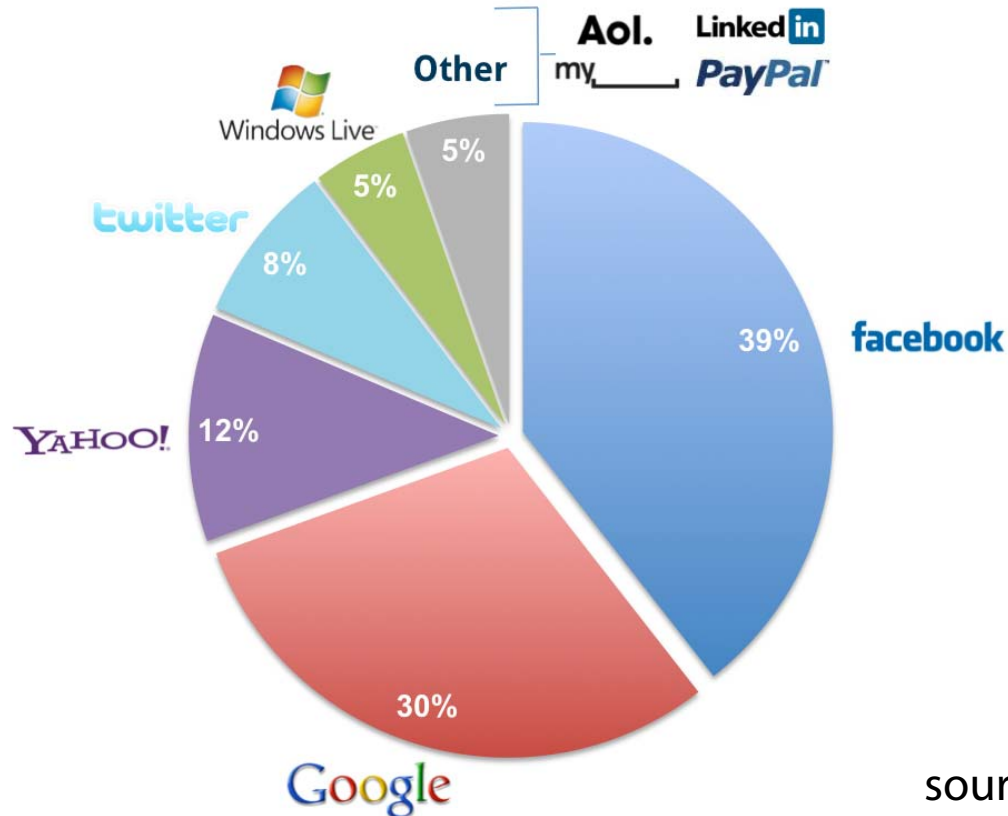
- ✓ Convenience – fewer passwords to remember
- ✓ Rich experience through social features
- ✓ Outsource user registration and management
- ✗ Same credentials for multiple sites
- ✗ User tracking
- ✗ Access to user's profile

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









Request for Permission - Google Chrome

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

f Request for Permission

surfingneighbors.com is requesting permission to do the following:

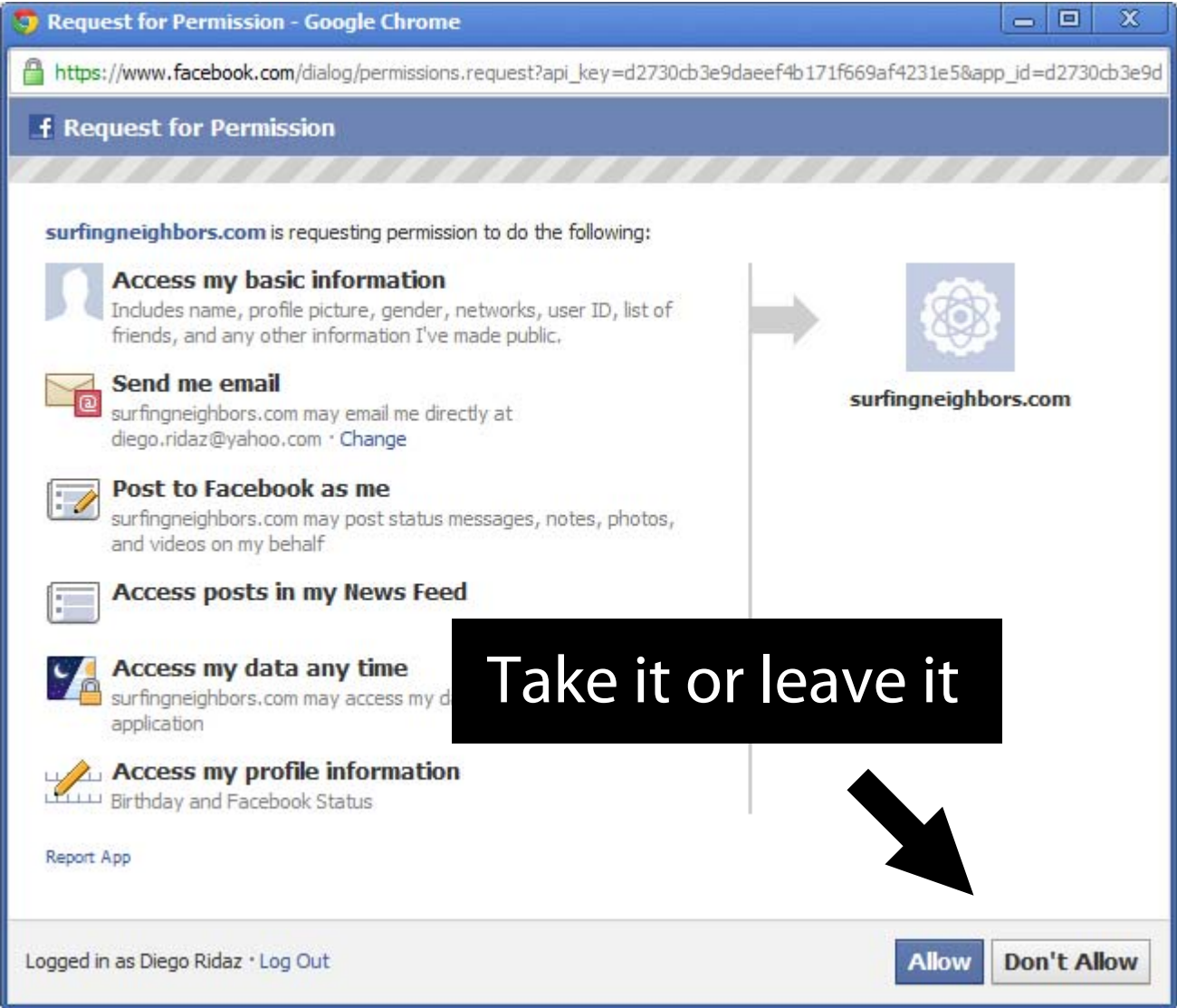
-  **Access my basic information**
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.
-  **Send me email**
surfingneighbors.com may email me directly at diego.ridaz@yahoo.com · [Change](#)
-  **Post to Facebook as me**
surfingneighbors.com 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 data at any time while the application is installed on your device.
-  **Access my profile information**
Birthday and Facebook Status

[Report App](#)

Logged in as Diego Ridaz · [Log Out](#)

Take it or leave it

[Allow](#) [Don't Allow](#)



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 others' 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 place of the user



Post to Facebook as me

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

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

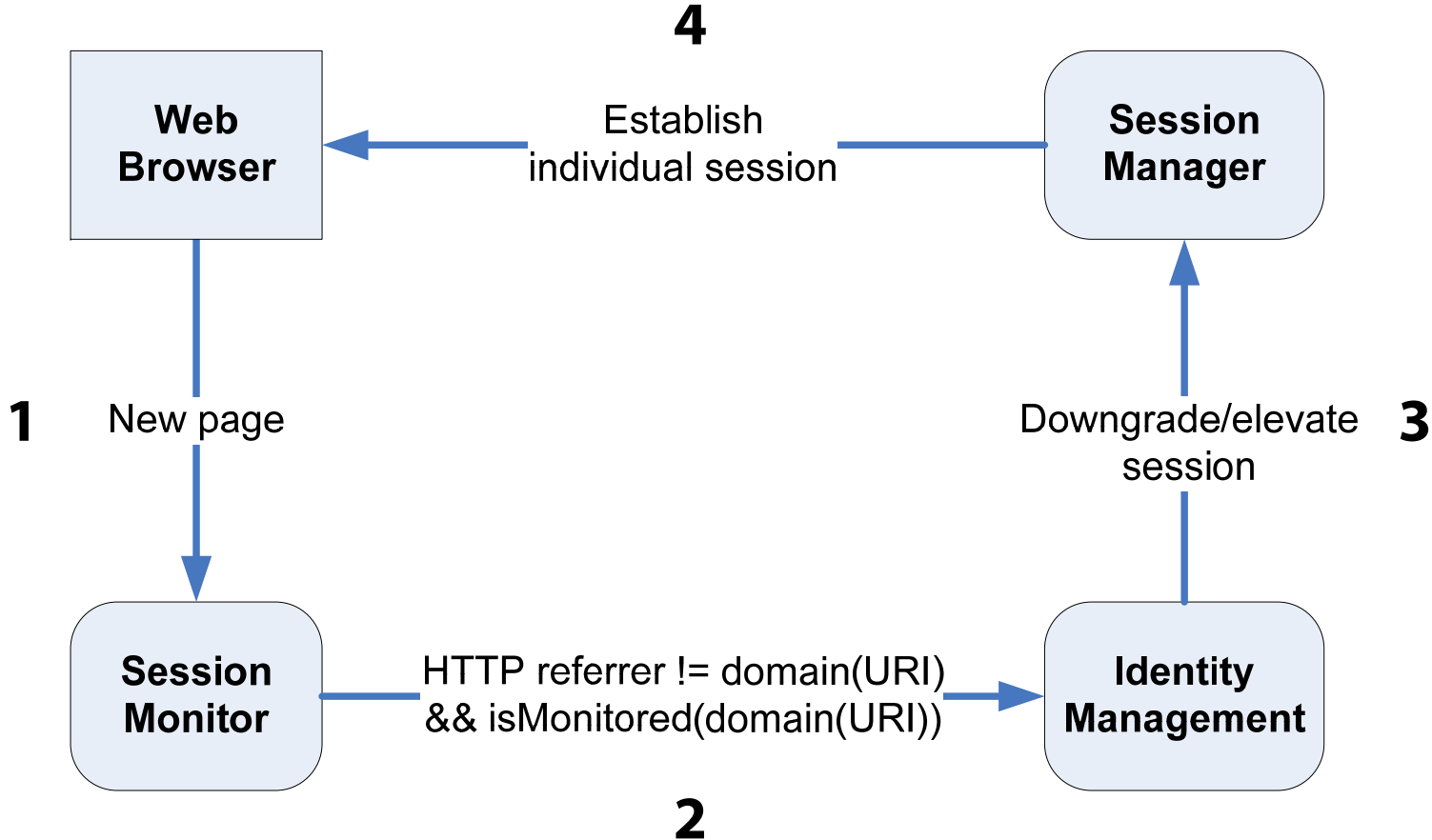
Transparent operation

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



The image shows the Chrome browser's 'Extensions' settings page. The address bar displays 'chrome://settings/extensionSettings'. On the left, a sidebar titled 'Options' contains a search box and a list of categories: 'Basics', 'Personal Stuff', 'Under the Hood', and 'Extensions' (which is selected). The main content area is titled 'Extensions' and includes a 'Developer mode' checkbox (checked). Below this are three buttons: 'Load unpacked extension...', 'Pack extension...', and 'Update extensions now'. A list of installed extensions is shown, with the first one being 'SudoWeb 0.5 (Unpacked)'. It is marked as 'Enabled' and has a 'Remove' button. The description for SudoWeb reads: 'Use a secondary, disposable Facebook account to sing in on third-party sites [Options](#)'. A black arrow points from a black box with the text 'Initial configuration' to the 'Options' link in the extension's description. Below the extension list is a 'Get more extensions' link with a colorful icon.

Initial
configuration

Extensions x chrome-extension://objmbdckk x +

← → ↻ 🔍 ☆ ⚙

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



Extensions x chrome-extension://objmbdck x f Welcome to Facebook - Log In x +

← → ↻ 🔍 ☆ ⚙

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: [masked] Log In

Keep me logged in Forgot your password?

Heading out? Stay connected
Visit facebook.com on your mobile phone.

Sign Up
It's free and always will be.

Get Facebook Mobile

Log in using secondary account

I am: Select Sex: [dropdown]
Birthday: Month: [dropdown] Day: [dropdown] Year: [dropdown]
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

Extensions x chrome-extension://objmbdck x f Welcome to Facebook - Log In x +

← → ↻ 🔍 ☆ ⚙

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

Configure secondary identity



Extensions x chrome-extension://objmbdck x Facebook x +

← → ↻ 🔍 ☆ ⚙

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!

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

Diego Ridaz

Docstoc – Documents, Templa

www.docstoc.com

login Sign In Register

Home Upload

Million Professional Documents All Documents Search

Document Categories

- DocStore
- Legal
- Business
- Personal Finance
- Technology
- Education
- Jobs & Careers
- Tax
- Real Estate
- Current Events

Show more categories

Start Using Docstoc

Login with Facebook

We Make Every

Small Business and Professional Life

DOCUMENTS PACKAGES RESOURCES

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.

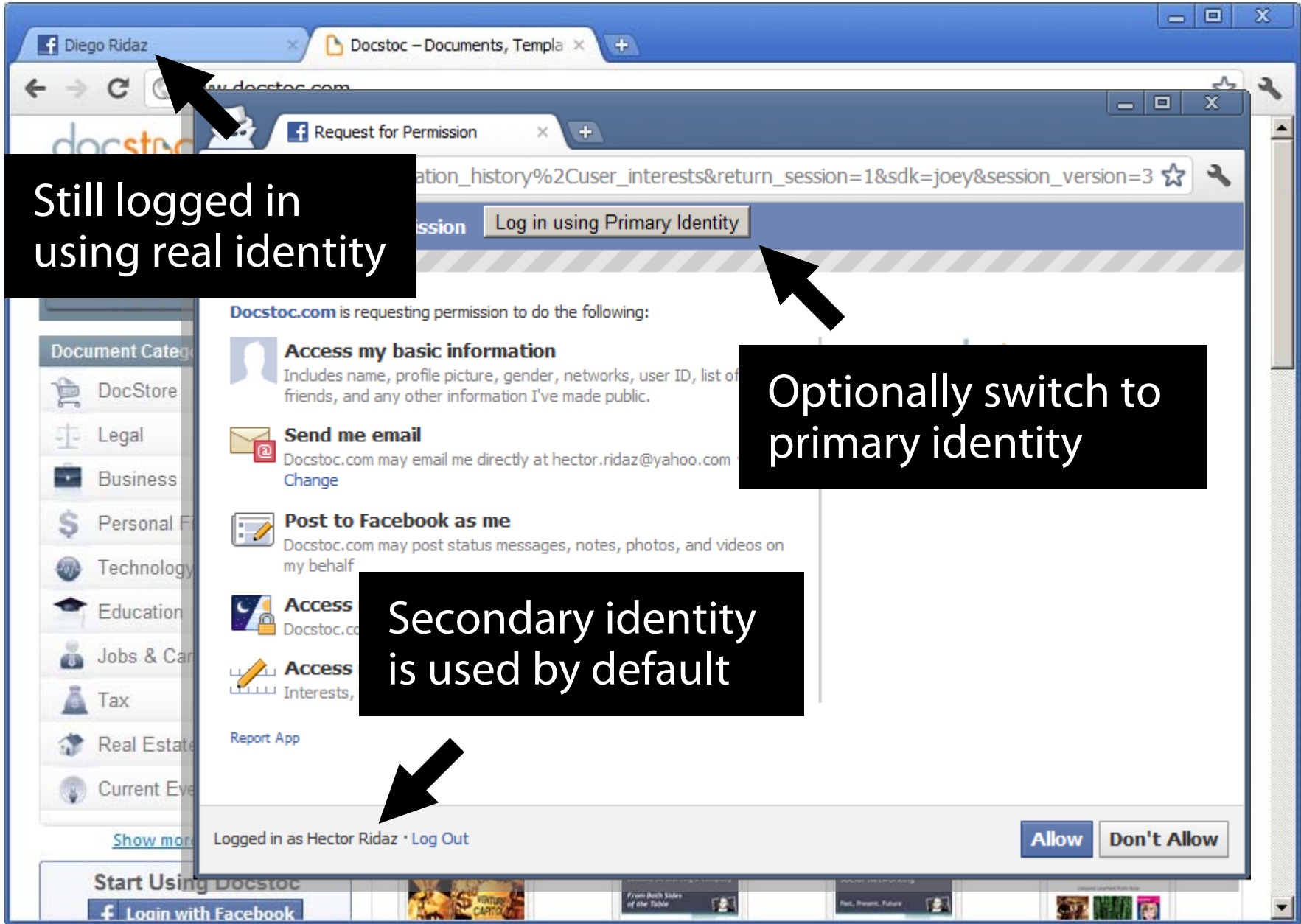
Top Presentations by Mark Suster of BothSidesofTheTable.com

Lessons on Starting a Company From Both Sides of the Table

Social Networking Past, Present, Future

Already logged in using real identity

login Sign In



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*

ISC '11 – October 28, 2011