

OpenID

Muhammad Rizwan Asghar

COMPSCI 725

September 15, 2015

For template of slides,
thanks to kingsoftware.com



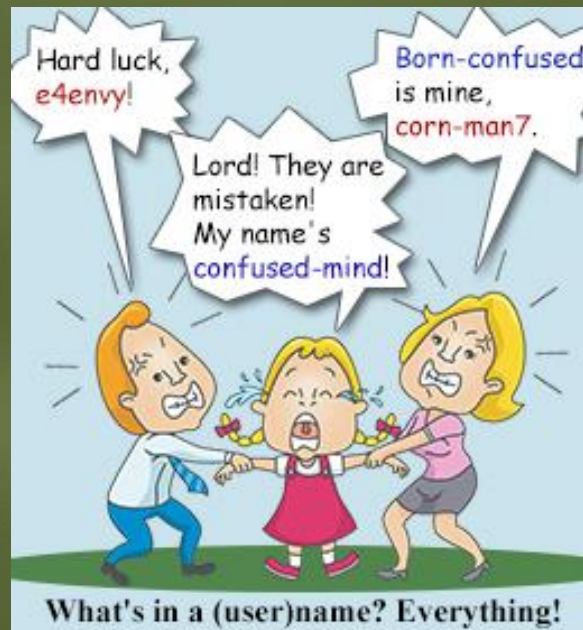
Overview of OpenID



- An open standard for authentication
- Developed by the open source community
- Created in 2005
- Decentralised, not owned by anyone
- Free

Why OpenID

- Too many user names



Source: buzzle.com

Why OpenID (2)

- Too many passwords

```
!@#$%^ !admin !ftp !manage !monitor 1 111111
123 123123 1234 12345 123456
1234567 12345678 123456789 1234567890
1234qwer 123qwe 1q2w3e 1q2w3e4r 1q2w3e4r5t
1qa2ws 1qa2ws3ed 1qaz2wsx 1qaz2wsx3edc 1qaz2wsx3edc4rfv
54321 654321 7654321 87654321 987654321 Cisco a abc
abc123 abcd1234 abcdef admin admin123 adminadmin
administrator alex alpine apache asdf1234 asdfgh asdfghijkl
backup changeme cisco cyrus default dottie ftp guest info
internet linux mail master michael mysql nagios nobody nologin
nopass nopassword oracle p@ssw0rd p@ssword passw0rd
passwd passwd123 password postgres
q1w2e3r4 q1w2e3r4t5 qazwsx qwe123 qweasdzxc qwer1234
qwerty qwerty123 qwertyuiop redhat remote root
root123 rootroot server test test123 tester testing
testuser user web webadmin webmaster zxcvbnm
```

Source: blog.iweb.com

Why OpenID (3)

- User names already taken



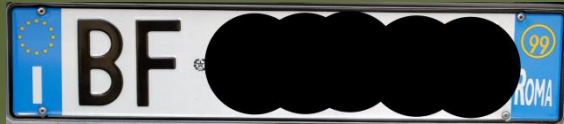
Source: <http://static.fjcdn.com/>

Basic Purpose



- Authentication
- Local credential issuers
- Using credentials for multi-purpose

How do we Identify Cars?



Car Plate Number

issued by



Authority

Identification Across Border



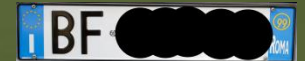
In Our Use-Case Scenario



- (Italian) Authority is an **Identity Provider**



- (Italian) Car plate is an **Identifier**

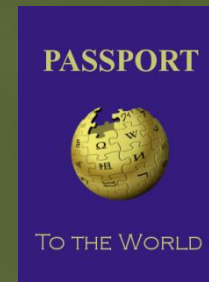


- (German) Police is a **Consumer**



Other Use-Case Scenarios

- Driving license
 - Issued by local authorities
 - Valid across provinces (even countries)
- Passport
 - Issued by a specific country
 - Valid all over the world



In OpenID



- Identity Providers issue Identifiers
- Identifiers are used for authentication for websites supporting OpenID
- Websites are Consumers

Example



- Through tripit.com, Alice would like to store and share her itinerary
- tripit.com requires Alice to register
- tripit.com also offers authentication using Google account
- Alice prefers to authenticate using her Google account

1 - Homepage of tripit.com

Firefox

TripIt - Travel Itinerary - Trip Planner

https://www.tripit.com

Search the web (Softonic)

TripIt from Concur

The All-in-One Travel Organizer

Sign up for TripIt

Email Address

Create Password

Or, sign up with...

By clicking Sign Up, you confirm that you accept the User Agreement. We don't share your email address (more info).

New York or Bust
Thu, Mar 6 - Mon, Mar 10, 2014

San Francisco to New...
Thu, Mar 6 - Fri, Mar 7, 2014

ACE Hotel Lodging
Thu, Mar 6 - Fri, Mar 7, 2014

Gramercy Tavern Res...
Fri, Mar 7 - Sat, Mar 8, 2014

The Metropolitan Mu...
Sat, Mar 8 - Sun, Mar 9, 2014

Guggenheim Museum
Sun, Mar 9 - Mon, Mar 10, 2014

American Museum of...
Mon, Mar 10 - Tue, Mar 11, 2014

Book of Mormon
Tue, Mar 11 - Wed, Mar 12, 2014

ACE Hotel Lodging
Wed, Mar 12 - Thu, Mar 13, 2014

San Francisco to Los Angeles
Mon, Mar 3 - Thu, Mar 6, 2014

SFO - LAX
United Airlines 990

10:30 Depart SFO
11:50 Arrive LAX

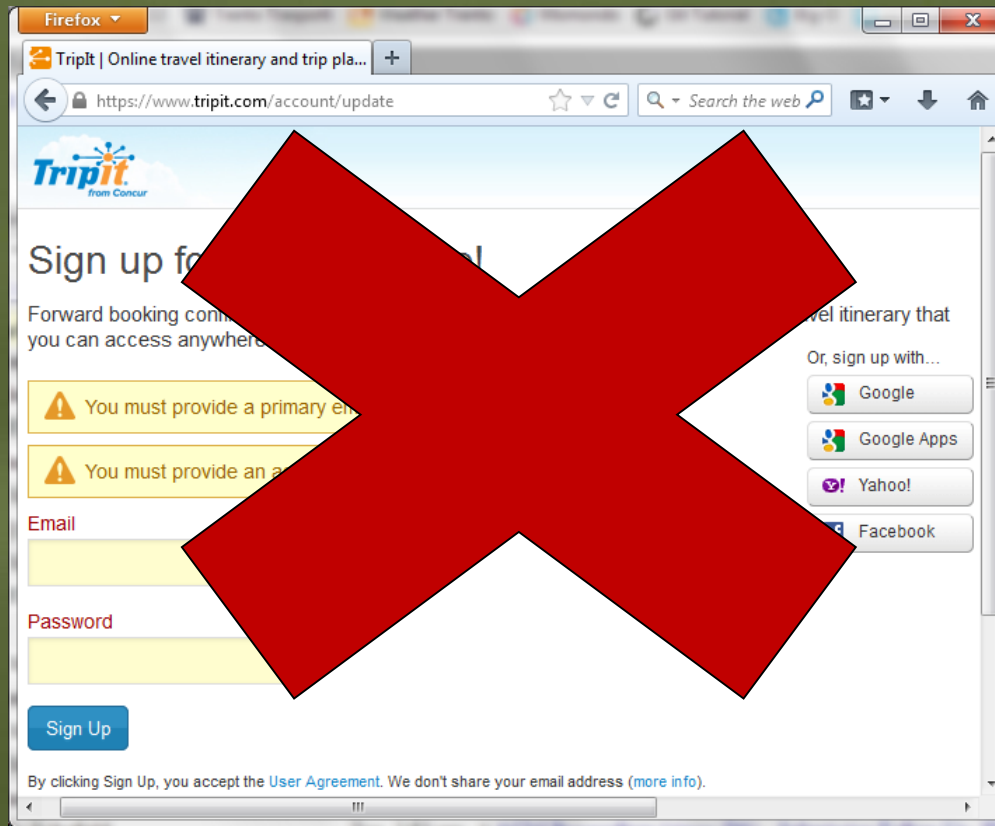
DURATION: 1H 20M

Class: HXUTBL
Cabin: 3
Seat: 86

Seat: 6A
Status: Seat Tracker

View Airline & Booking Info

Signup for tripit.com



2 - Homepage of tripit.com

Firefox

TripIt - Travel Itinerary - Trip Planner

https://www.tripit.com

Search the web (Softonic)

TripIt from Concur

The All-in-One Travel Organizer

Sign up for TripIt

Email Address

Create Password

Or, sign up with...

By clicking Sign Up, you confirm that you accept the User Agreement. We don't share your email address (more info).

New York or Bust
Thu, Mar 6 - Mon, Mar 10, 2014

San Francisco to New York
THU, MAR 6
9:20 AM Flight
6:00 AM ACE Hotel Lodging

Gramercy Tavern Res...
FRI, MAR 7
7:30 PM

The Metropolitan Mu...
SAT, MAR 8
10:00 AM

Guggenheim Museum
SAT, MAR 8
1:00 PM

American Museum of...
SAT, MAR 8
3:30 PM

Book of Mormon
SUN, MAR 9
8:00 PM

ACE Hotel Lodging
MON, MAR 10
12:00 AM

San Francisco to Los Angeles
Mon, Mar 3 - Thu, Mar 6, 2014

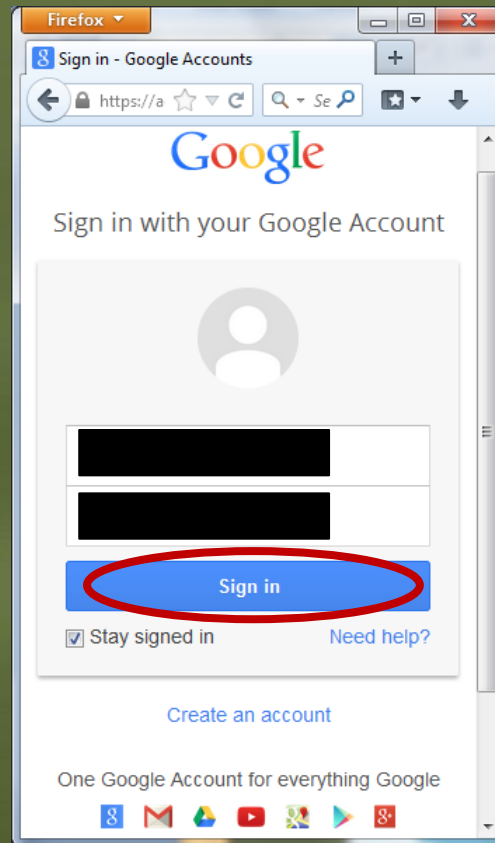
SFO - LAX
United Airlines 998

10:30 AM Depart SFO
11:50 AM Arrive LAX

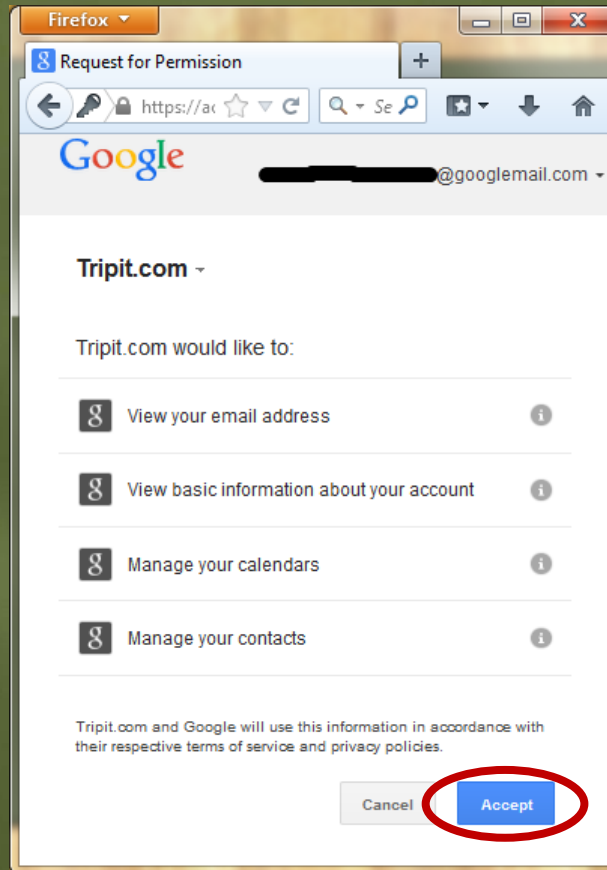
DURATION: 1H 20M
Class: HUXTBL
Cabin: 3
Seat: 86
Seat Tracker

View Airline & Booking Info

3 - Redirection to Google



4 - After Google Authentication: Accept



5 - Redirection to tripit.com

The screenshot shows the TripIt website interface. A modal window titled "WELCOME ABOARD LET'S SET UP YOUR ACCOUNT" is centered on the screen. The modal contains the following fields and options:

- First name: [Redacted]
- Last name: [Redacted]
- Password: [Redacted]
- Hometown: enter a city... [Redacted]
- Options:
 - Automatically create my itineraries (Recommended)
 - Start my free 30-day trial of TripIt Pro
 - Send me exclusive offers from TripIt's trusted partners.
- A large orange arrow pointing right with the word "NEXT" in blue text.

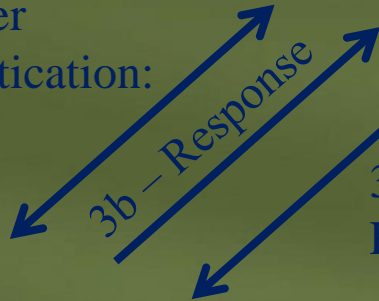
The background of the website shows a navigation menu with "Home", "Trips", "Network", "Point Tracker", "TripIt Pro", and "Teams". Below the navigation, there is a section titled "How do I create my own itinerary?" and a "Sample Itinerary" for "Apr 3 - 5, 2014 / New York, NY". The itinerary details include a flight from San Francisco to Los Angeles on 4/3/2014 via Virgin America (SFO to LAX), with a confirmation number of JH58493. The flight departs at 8:00 AM and arrives at 9:20 AM. The seat is listed as 16B. The website footer includes a status message: "Waiting for pixel.everesttech.net..."

OpenID Workflow

Google

Identity Provider

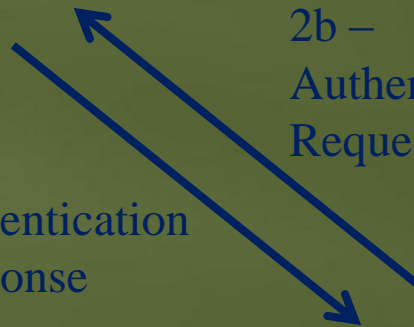
4 – After
Authentication:
Accept



3 – Sign in
Request

4b –
Authentication
Response

2b –
Authentication
Request



End User

5 – Redirection to tripit.com

2 – Choose Identity Provider

1 – Visit tripit.com



Consumer

Workflow Details



- A Consumer establishes a shared secret with Identity Provider
- Diffie-Hellman key exchange
- End User is redirected to Identity Provider for authentication
- After authentication, End User is redirected back to Consumer

Workflow Details (2)






- Shared secret is used to guard against spoofed requests
- Consumers do not see passwords
- Using **delegation**, you can use your own domain as your OpenID

Identity Providers





Google

- Google
 - GMail, Google Calendar, Google Drive, Google Picasa
- Microsoft 
- Facebook 
- Yahoo 
- AOL 

Identity Providers (2)



- myspace 
- Wordpress 
- And many more ...

Consumer: Glassdoor

The screenshot shows the Glassdoor sign-in page in a Firefox browser window. The browser's address bar displays the URL https://www.glassdoor.com/profile/login_ir. The page features a green navigation bar with links for Jobs, Companies, Salaries, Interviews, and Write a Review. Below this is a search bar with a dropdown menu set to 'Jobs' and input fields for 'Job Title, Keywords, or Company' and 'Location'. The main content area is titled 'Sign In to Glassdoor' and includes a 'Sign In with Facebook' button, which is circled in red. To the right of this button is the text '(Recommended) — Why?'. Below this is a note with a star icon: '* What you view and contribute on Glassdoor is private – it will not appear on Facebook.' The page also has an 'OR' separator, followed by input fields for 'Email' and 'Password', a 'Remember me' checkbox, and a 'Sign In' button with a 'Forgot your password?' link.

Firefox


Member Sign In | Glassdoor

https://www.glassdoor.com/profile/login_ir

Jobs Companies Salaries Interviews Write a Review

Jobs Job Title, Keywords, or Company Location

Sign In to Glassdoor

 Sign In with Facebook (Recommended) — Why?

* What you view and contribute on Glassdoor is private – it will not appear on Facebook.

OR

Email

Password

Remember me

[Forgot your password?](#)

Consumer: Expedia

Firefox

https://www.expedi.../signin?ckoflag=0&

https://www.expedia.com/user/signin?ckoflag=0&

Expedia

Sign in or select an option

Sign In with Facebook

Recommended

- We keep it private
- Share only with permission
- Quick sign in- no passwords

Or, Sign in with your email

Email Address

Password

[Forgot your password?](#)

Keep me signed in

Sign In

OpenID Identifier



- It is a personal URL
- <http://www.google.com/profiles/your.name.here>
- One can claim that one owns it
- One can prove that one owns it

Source: blog.stackoverflow.com

Is OpenID a New Concept?



- No
- Microsoft Live ID and .NET Passport
- Many single-ID solutions
- Various vendors
- No universal standard, adoption or acceptance

Replay Attack



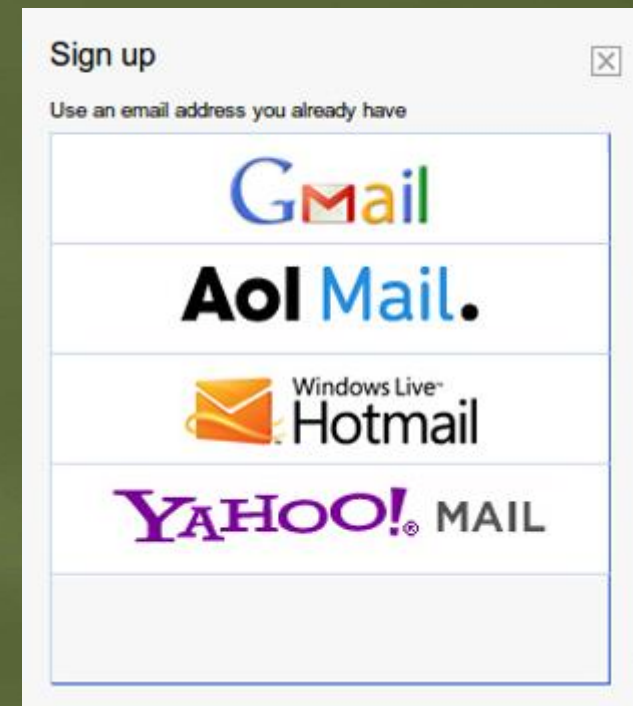
- Vulnerable to replay attack
- To withstand replay attack, OpenID suggests:
 - Self-signed nonce and
 - Timestamp

Google Identity Toolkit



- It supports multiple Identity Providers

- GMail
- AOL
- Hotmail
- Yahoo

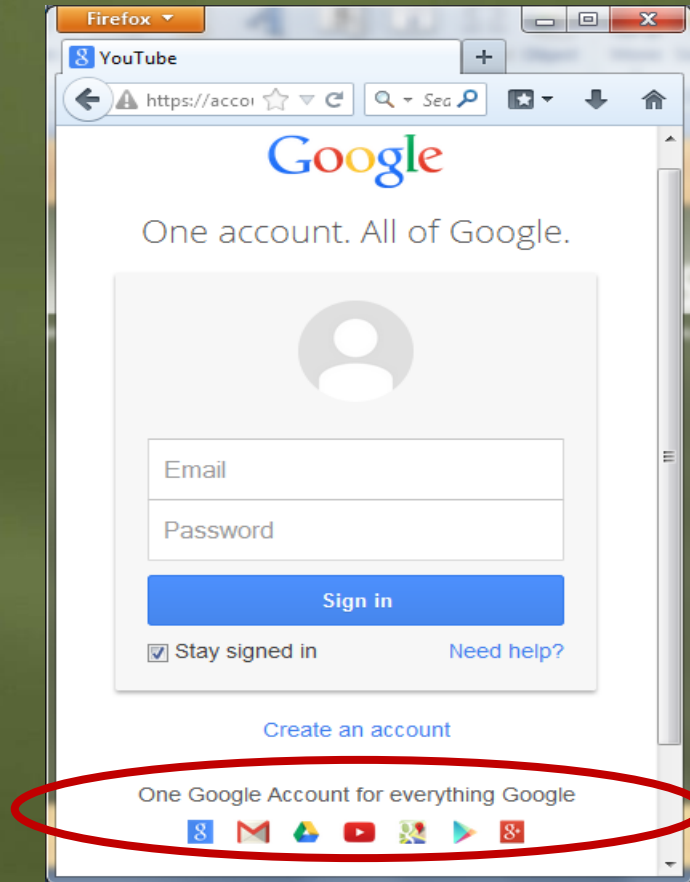


OpenID Statistics



- As of 2009
 - over 1 billion OpenID enabled accounts
 - ~9 million sites have integrated OpenID consumer support

Single Sign On (SSO)



SSO vs OpenID

- In SSO, a user logs in once for accessing multiple sites (or resources)
- SSO does not require to login again when a user switches to another site
- In OpenID, a user can use same login
- OpenID requires users to login when a user switches sites

Benefits for Users



- Provides users control
- Users decide who manages their identity online
- No registration for new accounts
- Easier
- Safer

Benefits for Developers



- Simplifies user management
- Eliminates complexities associated with securely managing passwords
- Scalable

Benefits for Business



- Attracts more users
- Less user management
- Better outcome

Limitations



- Privacy issues
 - Identity Providers will know more about End Users and Consumers
- Phishing attack
 - Attackers may get passwords of careless End Users
- Denial-of-Service (DoS) attack
 - Effect on Consumers and Identity Providers

Summary



- OpenID offers authentication using existing credentials
- It allows users to manage their own identities
- Rapid growth
- By providing its support, online businesses can attract more users



References



- OpenID, <http://openid.net/>
- OpenID Specifications, <http://openid.net/developers/specs/>
- Google Identity Toolkit: <https://developers.google.com/identity-toolkit/?csw=1>
- Implementations libraries: <http://janrain.com/openid-enabled/>