Single Sign-On for the Internet: A Security Story

eugene@tsyrklevich.name
vlad902@gmail.com

BlackHat USA, Las Vegas 2007

How do you manage your 169 Web 2.0 accounts today?

Spongecell
Hula
kiko
Trumba
eskobo
mayomi
Pageflakes
vimeo
skobee
shadows
grouvee
YouTube
Zimbra
LookSmart FURL
smugmug
newsgator
Blogniscient
TinFinger
shutterfly
PodDater
Feedster
favoor
Planzo.com
ZAZZLE
Tailrank
TagWorld
nuvvo
dogear
yakalike
grouper
ODDPOST
QOOP
iNods
Lulu
BA
blish
flagr
FireAnt
simplyhired
Veoh
theadcloud
rbloc.com
pixagogo
gather
Agatra
browsr
oyogi
cafepress
Renkoo
YEDDA
standpoint
meebo
EXTRA TASTY!
last.fm
Jotspot
Frappr!
jeteye
dabble db
Writeboard
SHOUTWIRE
iKarma
Kanoodle
AirSet
tech.memeorandum
CalendarHub
Suprglu
pando
zigtag
Findory
backfence
clipmarks
wayfaring
gOFFICE
AllPeers
orb
Rallypoint
Zoozio
blogbeat
Ziggs
zooto
vSocial
Boltfolio
wink
riya
Wordcast
Opinity
reddit
measure map
gumshoo
bluepulse
BETA
STREAMLOAD
Ta-da Lists
FeedSky
jellyBarn.INC
nativetext
CONGOO
PODZINGER
RSS MAD
FeedTier
phanfare
WIKIPEDIA
Fruitcast
PubSub
dPolls
flickr
Ning
Ookles
Strongspace
zoominfo
CASTPOST
yubnub
AC
Bloop
ProjectSpaces
FeedBurner
Bloglines
purevolume.com
FOTOLOG
ourmedia
Yub.com
Spot Runner
myspace
NewsAlloy
Allmydata.com
gabbr.com
Gcast
blinkx
openomy
riffs
ajchat
jambo
ROLLYO
ClipShack
chatsum
PANDORA
looklater
PROTOPAGE
squish
WebJay
PLAZES
Noodly
30 BETA
wondir
diigo
box
Jots
Xdrive
vizu
digg
del.icio.us
omni drive
AlmondRocks
Tagyu
30 GIGS
writely
Simpy
Gtalkr
TRUVEO
egoSurf
mozy
Quimble
pegasus
remember the milk
SQUIDOO
picturecloud
newsvine
Clipfire
Basecamp
Netvibes
goowy
My Video karaoke
Lexxe alpha
SOOKSTER
PXN8
measure map
facebook
43 Things
Technorati
Platial
Backpack
GMail
yelp
Smarkets
inform
filangy
magnolia
ShoZu
wrickr.com
feedmarker
mercora MusicSearch
SU
Meet With Approval.com
HomePortals
Spin spy

Does your “SSO” consist of

A login

(e.g. johndoe)

+

2 passwords

(one insecure for web 2.0 sites and one secure for banking sites)

?

Attack #1

a. Fail a user’s login

b. Observe the user try every single combination of their username and password, including the secure password..

Oliver Colin · London · 2003 ©

Lesson #1

Complexity
breeds
insecurity

One login to rule them all…

…a story about reducing complexity

OpenID

Proves that a user owns a URL

You get to choose who manages your identity

e.g. http://john.doe.name/ or http://jonny.myopenid.com/

OpenID

Answers the who? question (authentication)

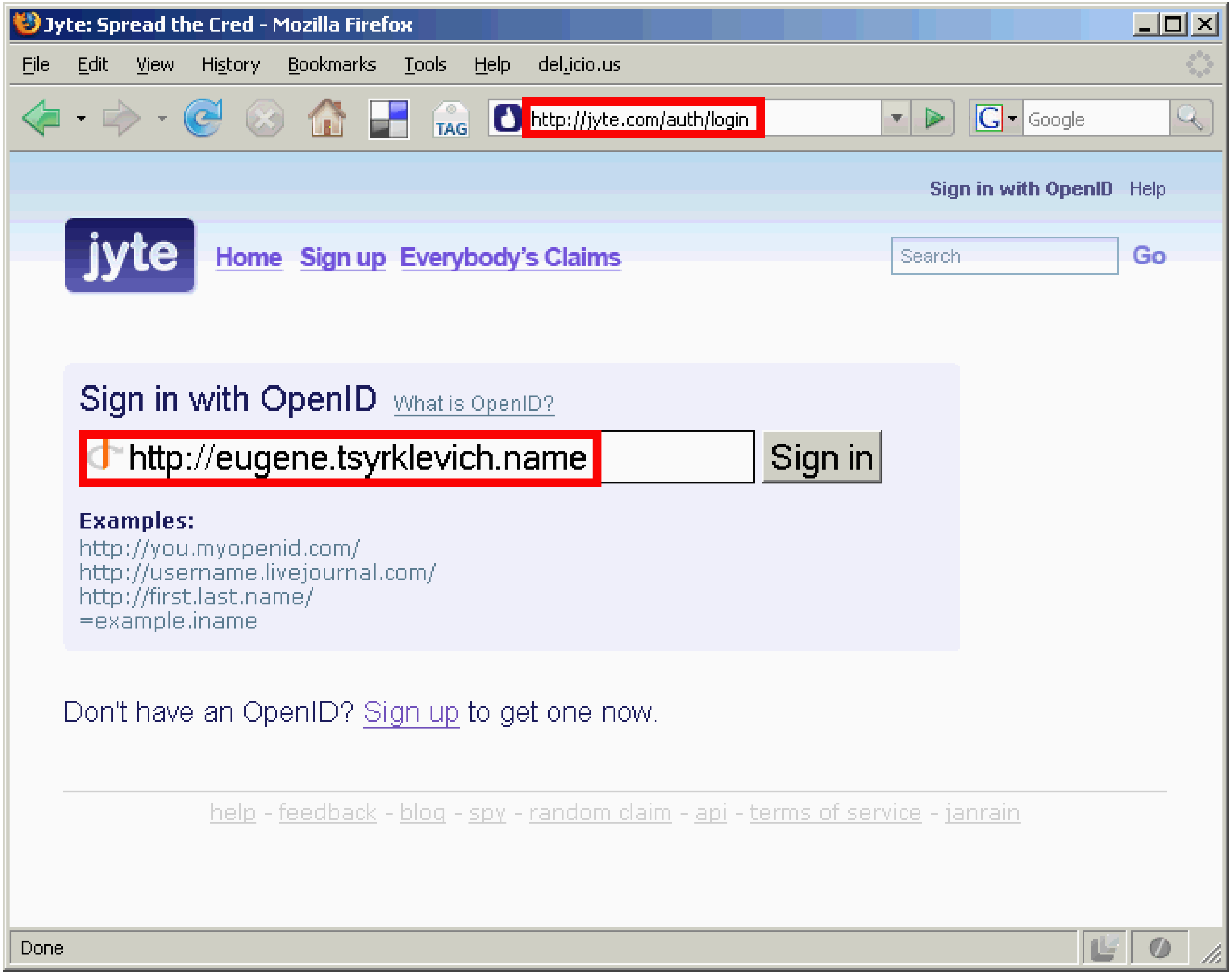
are you john.doe.name?

Does NOT answer the what? (authorization)

is john.doe.name allowed to access this page?

How?

(demo)



http://jyte.com/auth/login

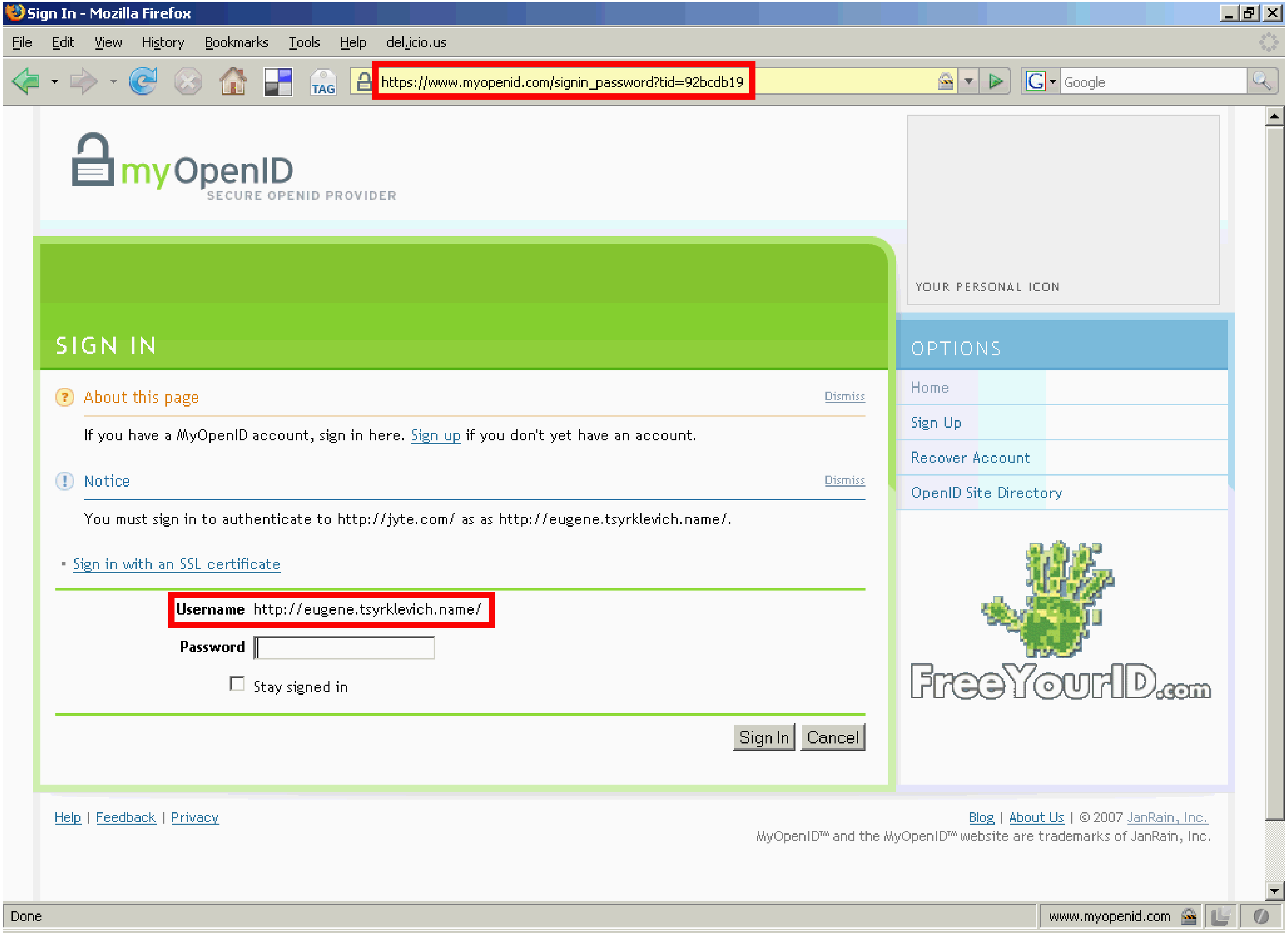
Sign in with OpenID What is OpenID?

http://eugene.tsyrklevich.name

Examples:
http://you.myopenid.com/
http://username.livejournal.com/
http://first.last.name/
=example.iname

Don't have an OpenID? Sign up to get one now.

help - feedback - blog - spy - random claim - api - terms of service - janrain
Done



Sign In - Mozilla Firefox
File Edit View History Bookmarks Tools Help del.icio.us
TAG
https://www.myopenid.com/signin_password?tid=92bcdb19
Google

myOpenID
SECURE OPENID PROVIDER

YOUR PERSONAL ICON

SIGN IN

About this page — Dismiss

If you have a MyOpenID account, sign in here. Sign up if you don't yet have an account.

Notice — Dismiss

You must sign in to authenticate to http://jyte.com/ as as http://eugene.tsyrklevich.name/.

- Sign in with an SSL certificate

Username http://eugene.tsyrklevich.name/

Password

□ Stay signed in

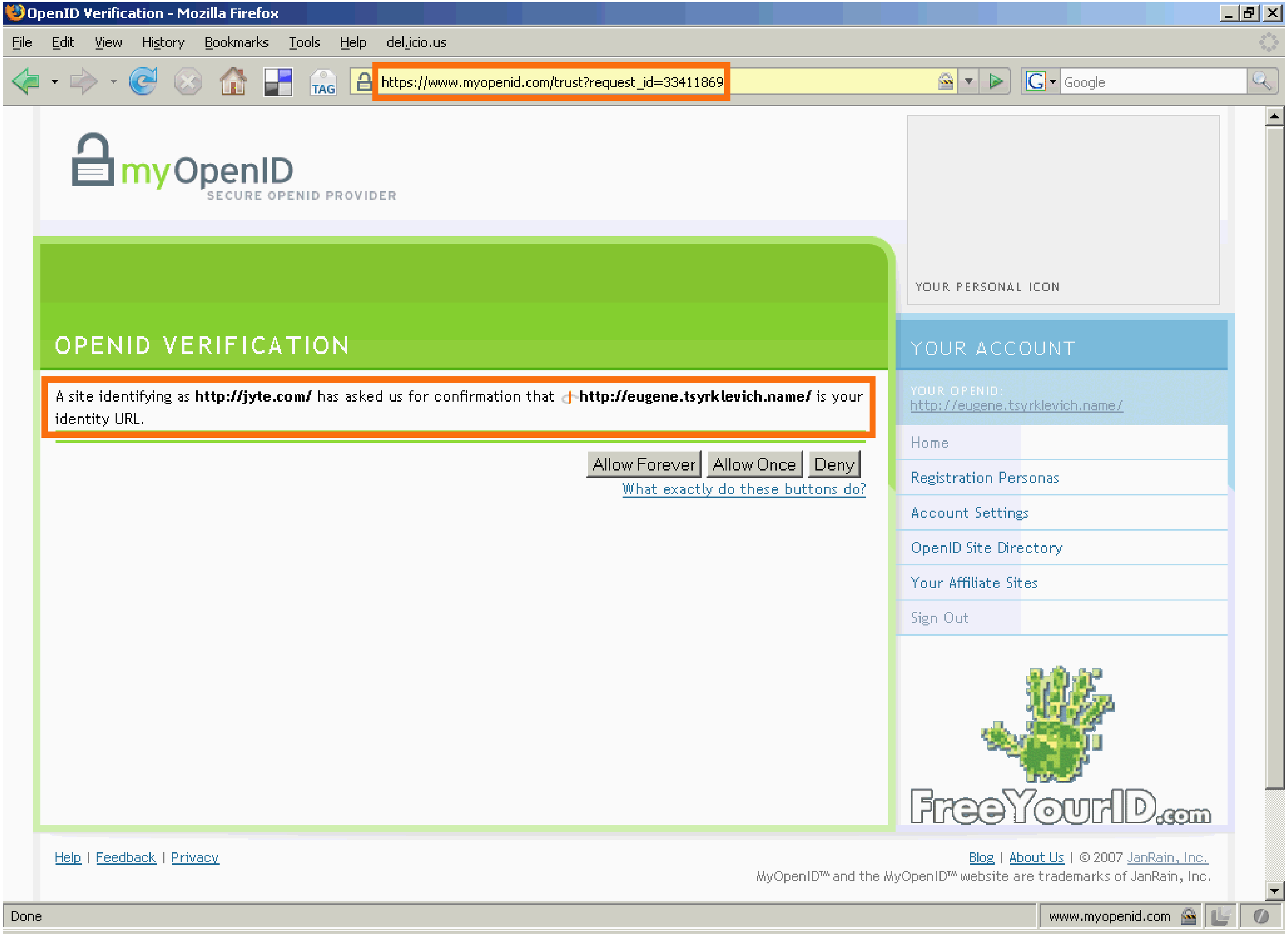
Sign In Cancel

OPTIONS

- Home
- Sign Up
- Recover Account
- OpenID Site Directory

Help | Feedback | Privacy

Blog | About Us | © 2007 JanRain, Inc.
MyOpenID™ and the MyOpenID™ website are trademarks of JanRain, Inc.


OpenID Verification - Mozilla Firefox
File Edit View History Bookmarks Tools Help del.icio.us
TAG
Google

https://www.myopenid.com/trust?request_id=33411869

myOpenID
SECURE OPENID PROVIDER

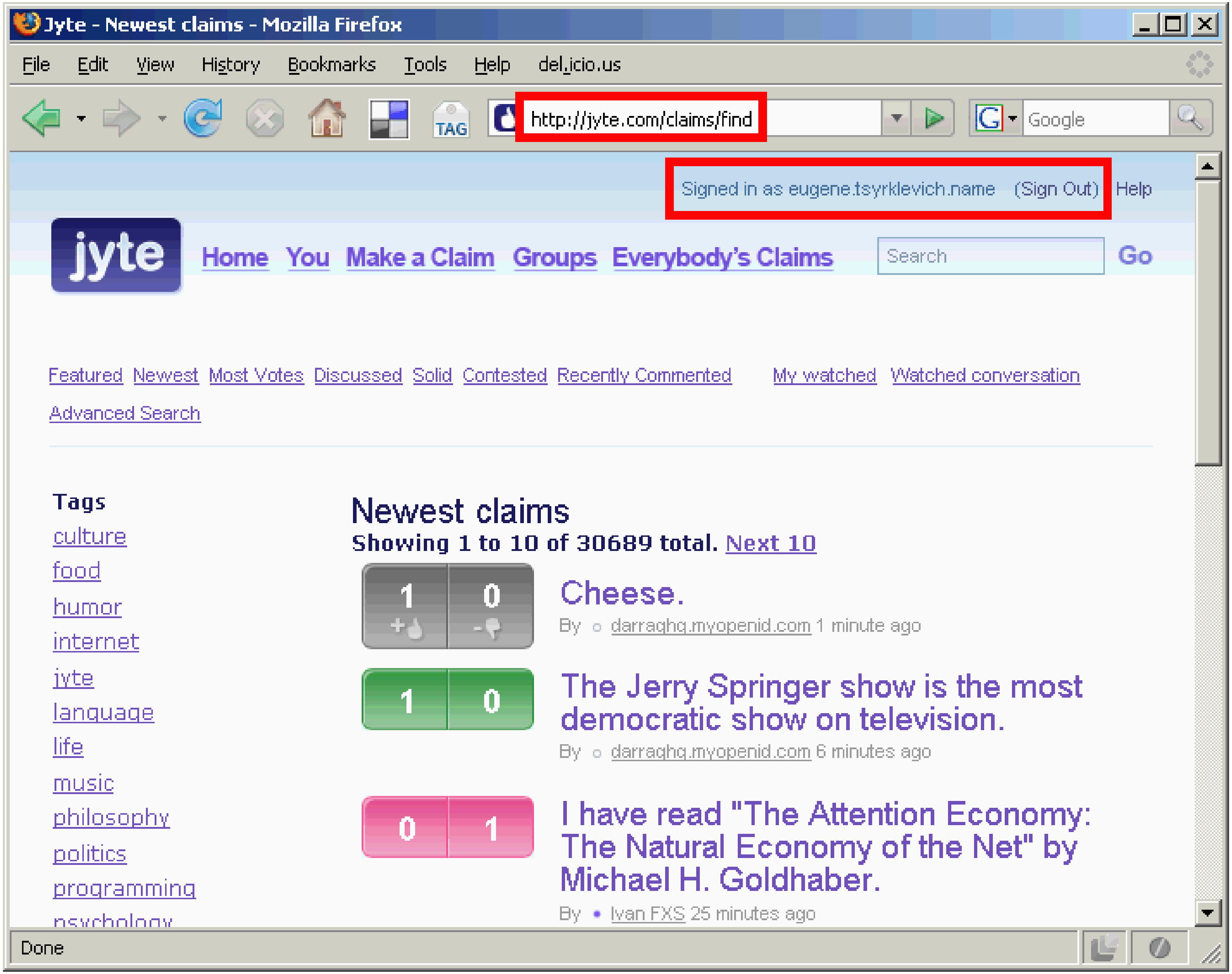
OPENID VERIFICATION

A site identifying as **http://jyte.com/** has asked us for confirmation that **http://eugene.tsyrklevich.name/** is your identity URL.

Allow Forever
Allow Once
Deny
What exactly do these buttons do?
YOUR PERSONAL ICON
YOUR ACCOUNT

YOUR OPENID:
http://eugene.tsyrklevich.name/

Home
Registration Personas
Account Settings
OpenID Site Directory
Your Affiliate Sites
Sign Out
FreeYourID.com
Help | Feedback | Privacy
Blog | About Us | © 2007 JanRain, Inc.
MyOpenID™ and the MyOpenID™ website are trademarks of JanRain, Inc.
Done
www.myopenid.com


Jyte - Newest claims - Mozilla Firefox
File Edit View History Bookmarks Tools Help del.icio.us
TAG
http://jyte.com/claims/find
Google
Signed in as eugene.tsyrklevich.name (Sign Out)
Help
jyte
Home
You
Make a Claim
Groups
Everybody's Claims
Search
Go
Featured Newest Most Votes Discussed Solid Contested Recently Commented My watched Watched conversation
Advanced Search
Done

Tags

culture
food
humor
internet
jyte
language
life
music
philosophy
politics
programming
psychology

Newest claims

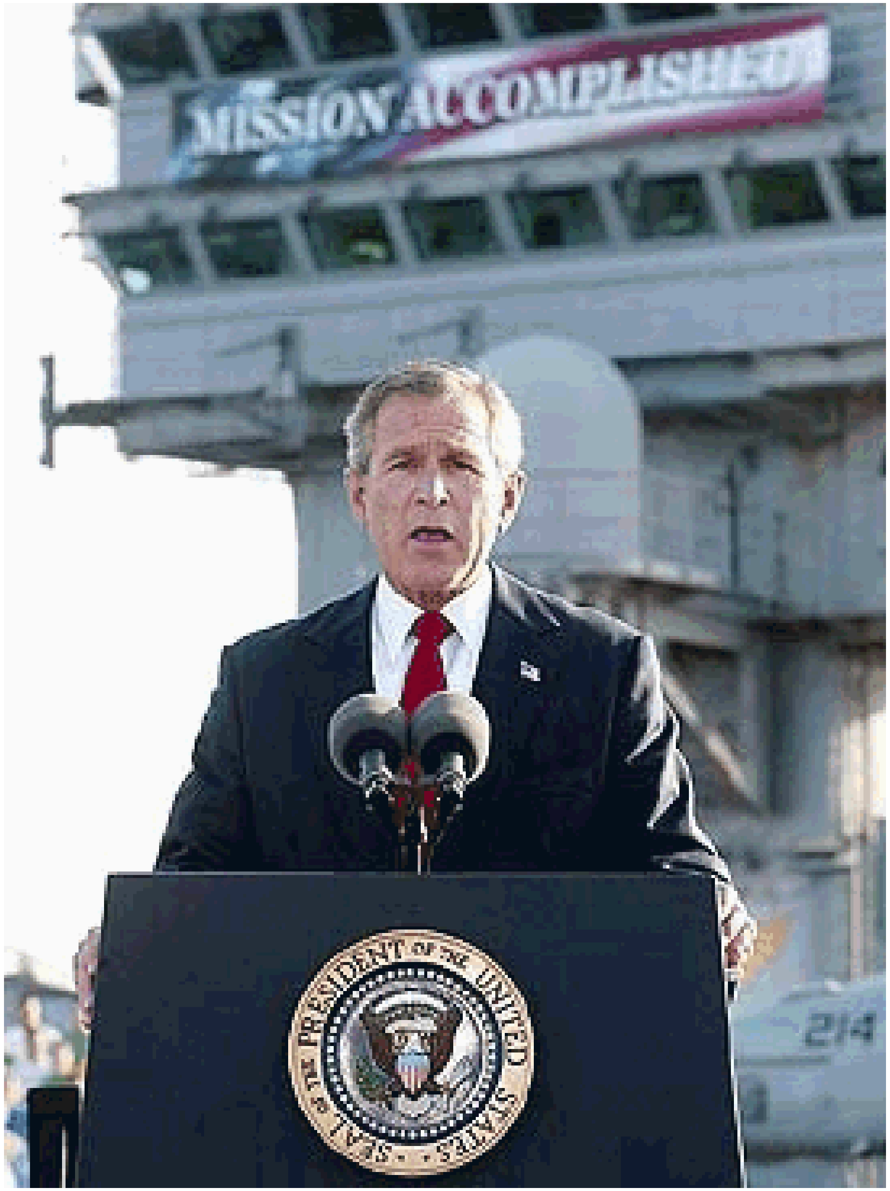
Showing 1 to 10 of 30689 total. Next 10

1 0 Cheese.
By darraghq.myopenid.com 1 minute ago

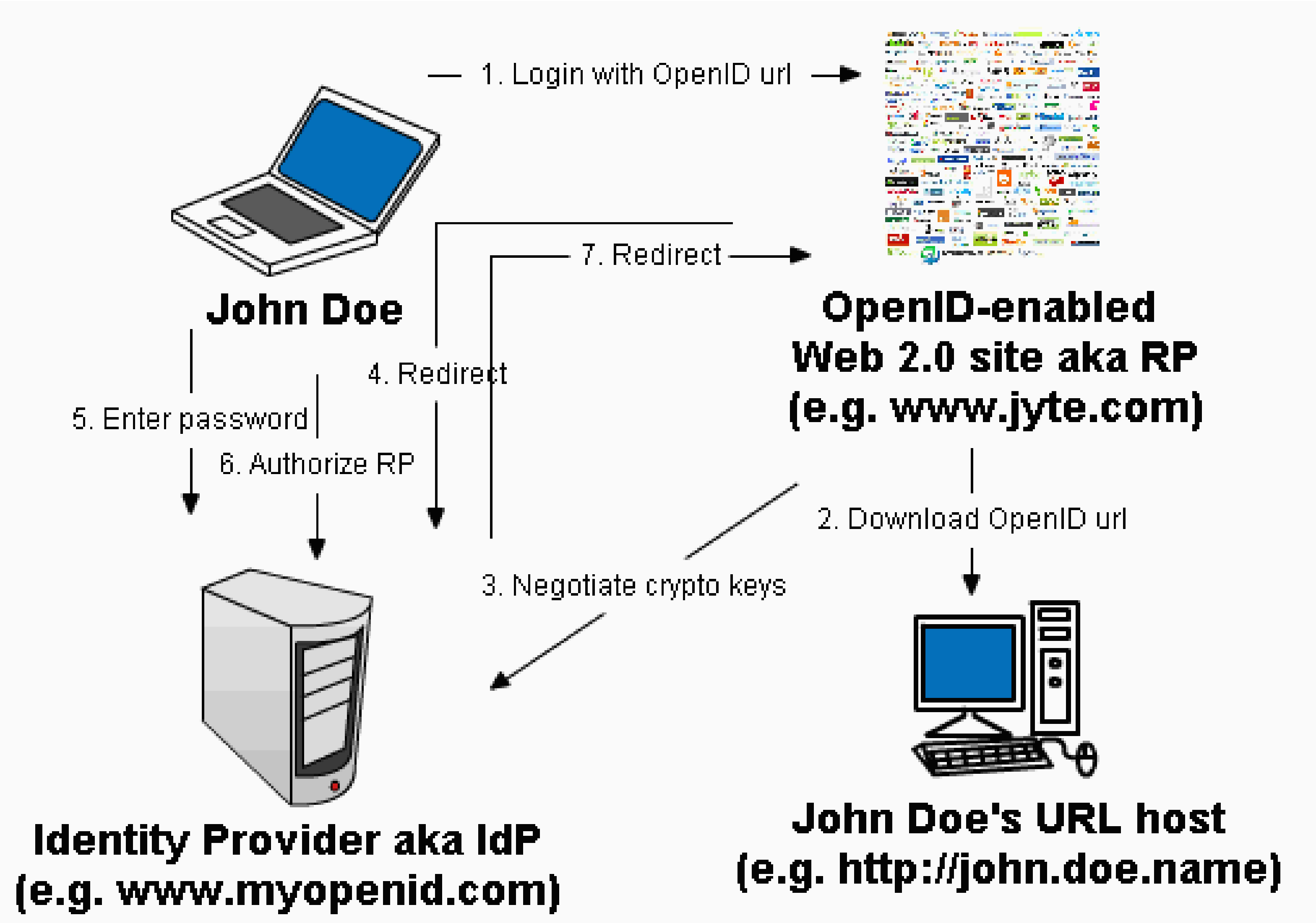
1 0 The Jerry Springer show is the most democratic show on television.
By darraghq.myopenid.com 6 minutes ago

0 1 I have read "The Attention Economy: The Natural Economy of the Net" by Michael H. Goldhaber.
By Ivan FXS 25 minutes ago

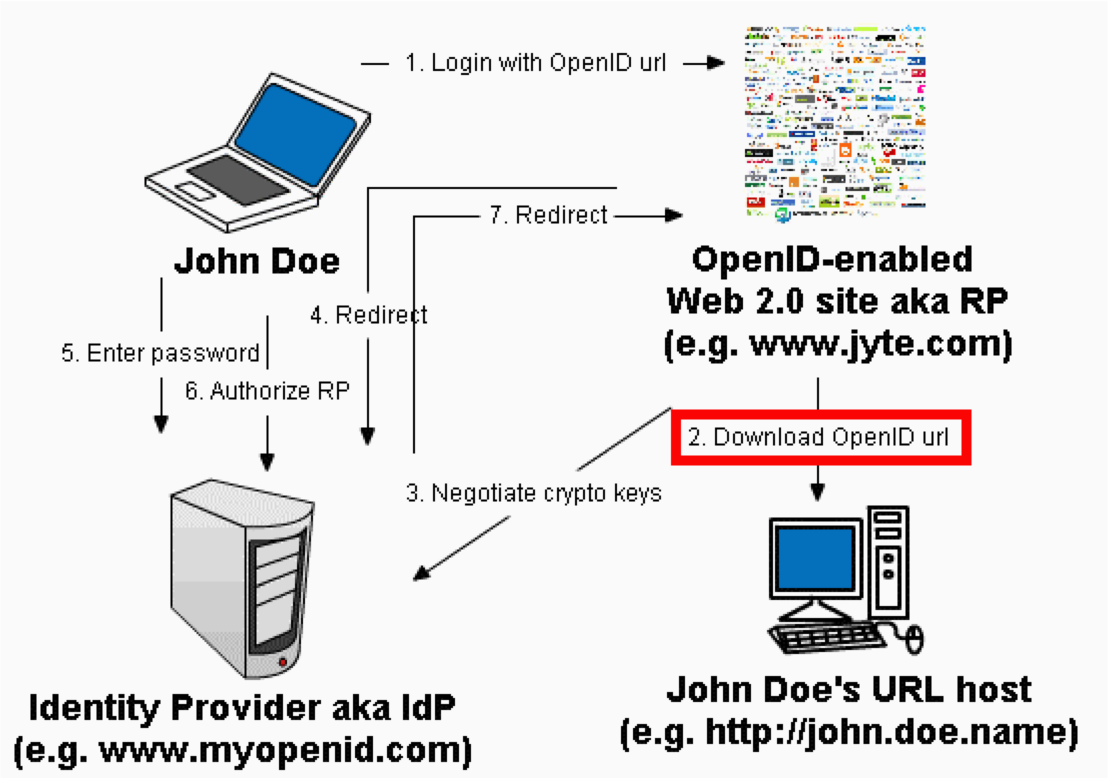
That was easy!



Oh. Never mind.



Let’s start at the beginning



Attack #2 – Which one are you?

http://nsa.gov:1/, http://nsa.gov:2/, ...

https://192.168.1.15/internal/auth?ip=1.1.1.1

http://localhost:8080/

http://www.youtube.com/largemovie.flv

http://www.tarpit.com/cgi-bin/hang.pl

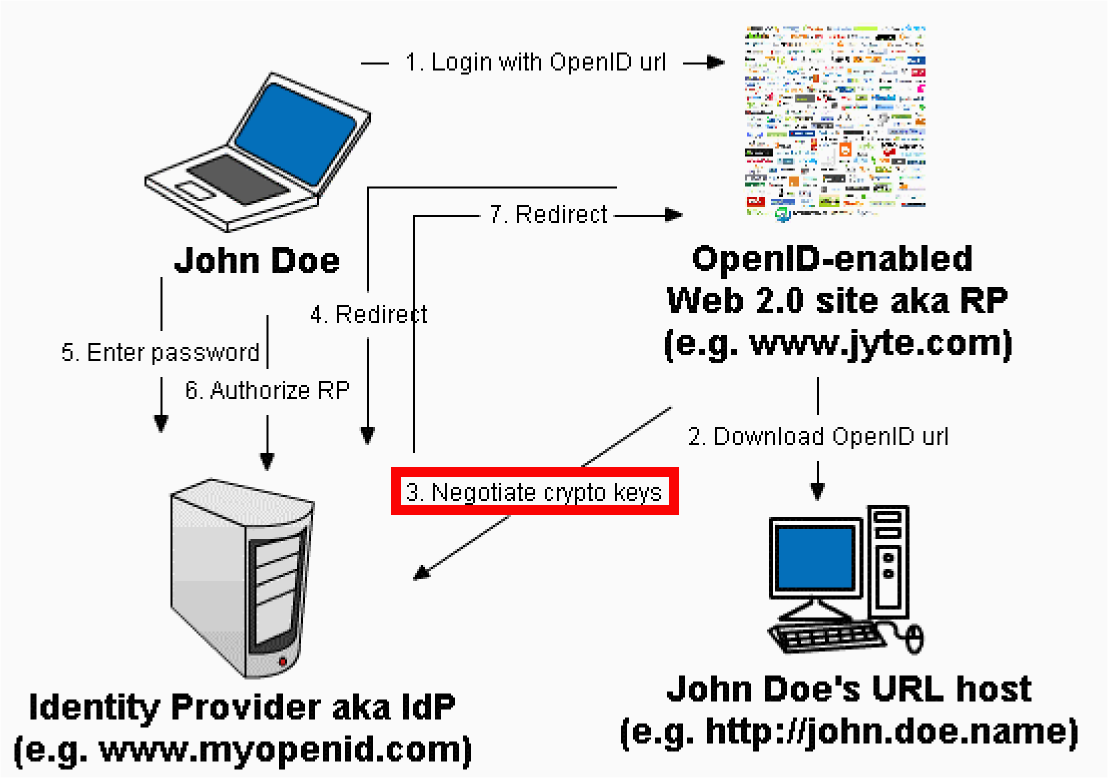
file:///dev/null

Lesson #2

Flexibility and security do not get along

(or, why it's important to be less flexible and more paranoid)

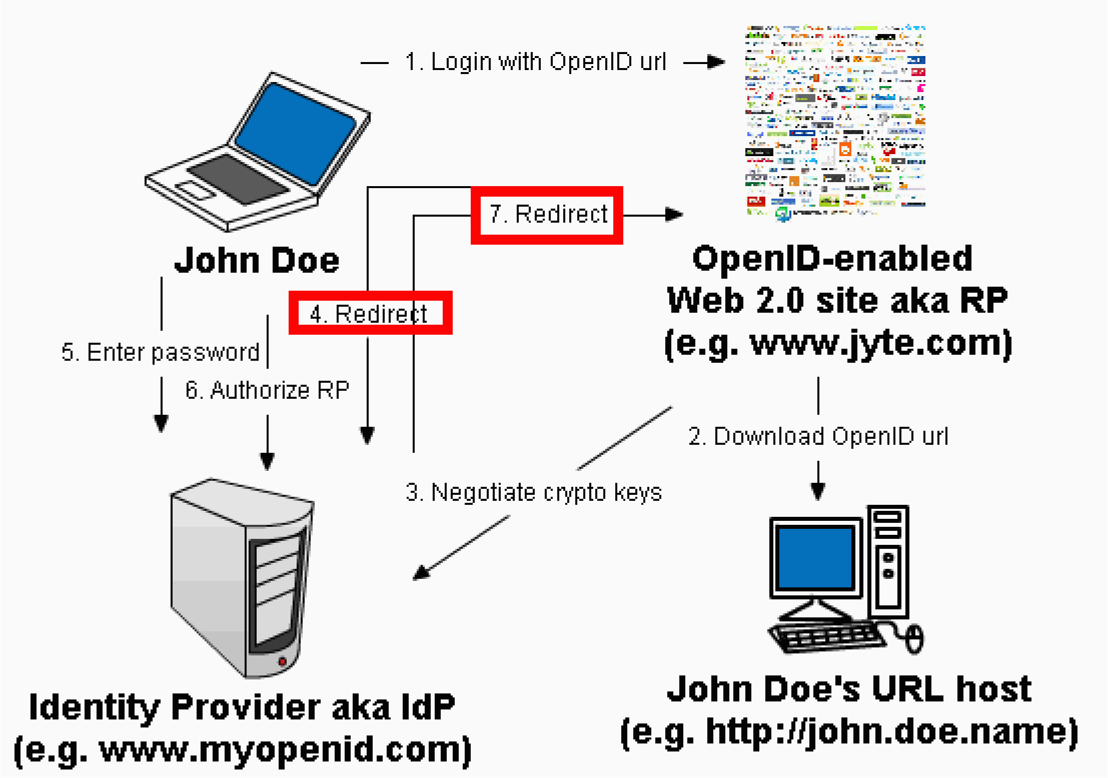
Everybody loves crypto



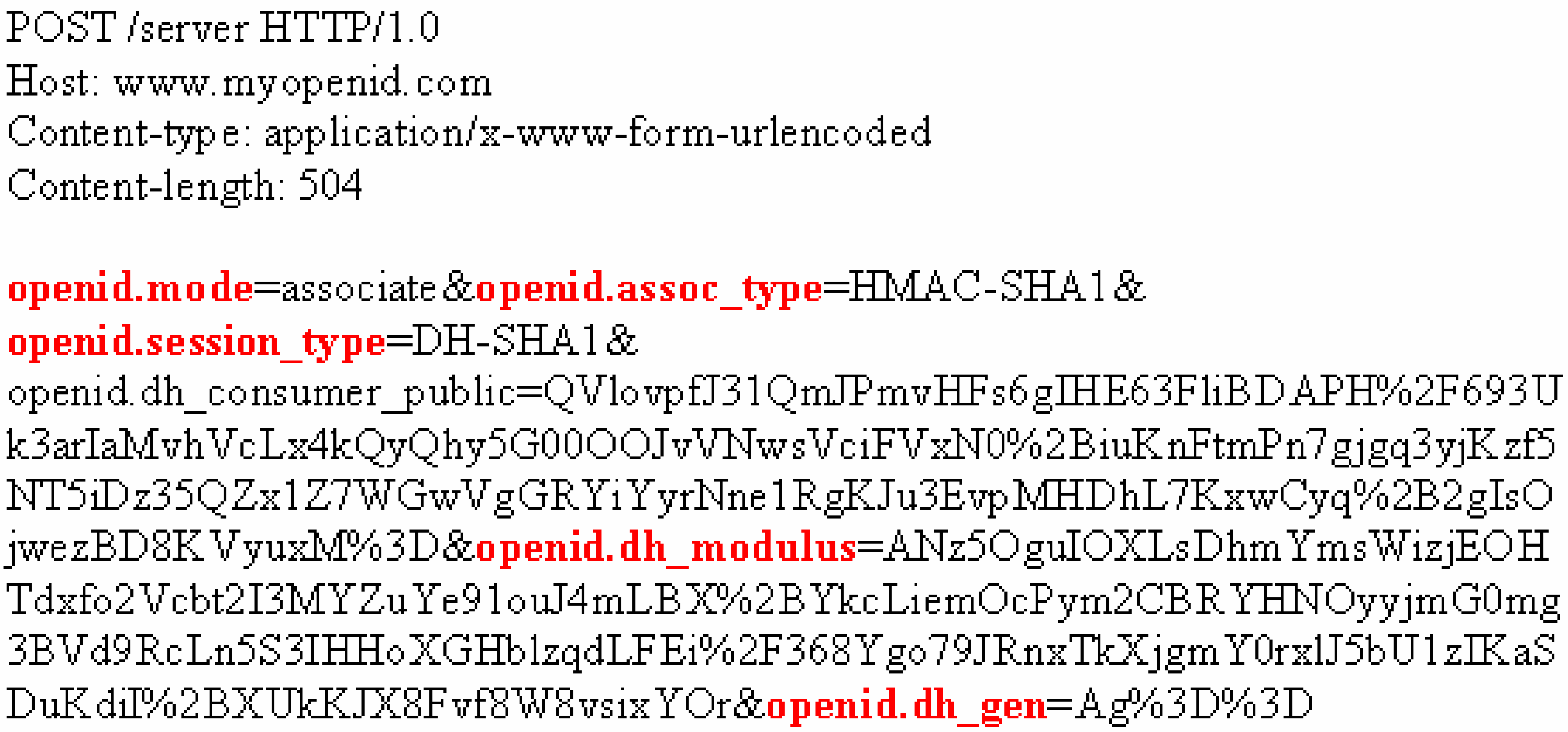
“associate mode”

Why is crypto required?

to protect request & response URLs



Shared symmetric key is generated using Diffie-Hellman



```
POST /server HTTP/1.0
Host: www.myopenid.com
Content-type: application/x-www-form-urlencoded
Content-length: 504

openid.mode=associate&openid.assoc_type=HMAC-SHA1&
openid.session_type=DH-SHA1&
openid.dh_consumer_public=QVlovpfJ31QmJPmvHFs6gIHE63FliBDAPH%2F693U
k3arIaMvhVcLx4kQyQhy5G00OOJvVNwsVciFVxN0%2BiuKnFtmPn7gjgq3yjKzf5
NT5iDz35QZx1Z7WGwVgGRYiYyrNne1RgKJu3EvpMHDhL7KxwCyq%2B2gIsO
jwezBD8KVyuxM%3D&openid.dh_modulus=ANz5OguIOXLsDhmYmsWizjEOH
Tdxfo2Vcbt2I3MYZuYe91ouJ4mLBX%2BYkcLiemOcPym2CBRYHNOyyjmG0mg
3BVd9RcLn5S3IHHoXGHblzqdLFEi%2F368Ygo79JRnxTkXjgmY0rxlJ5bU1zIKaS
DuKdiI%2BXUkKJX8Fvf8W8vsixYOr&openid.dh_gen=Ag%3D%3D
```

Attack #3 - Diffie-Hellman is vulnerable to man-in-the-middle attacks!

The spec suggests running DH over https to improve protocol security

So what’s the point of using DH in the first place?

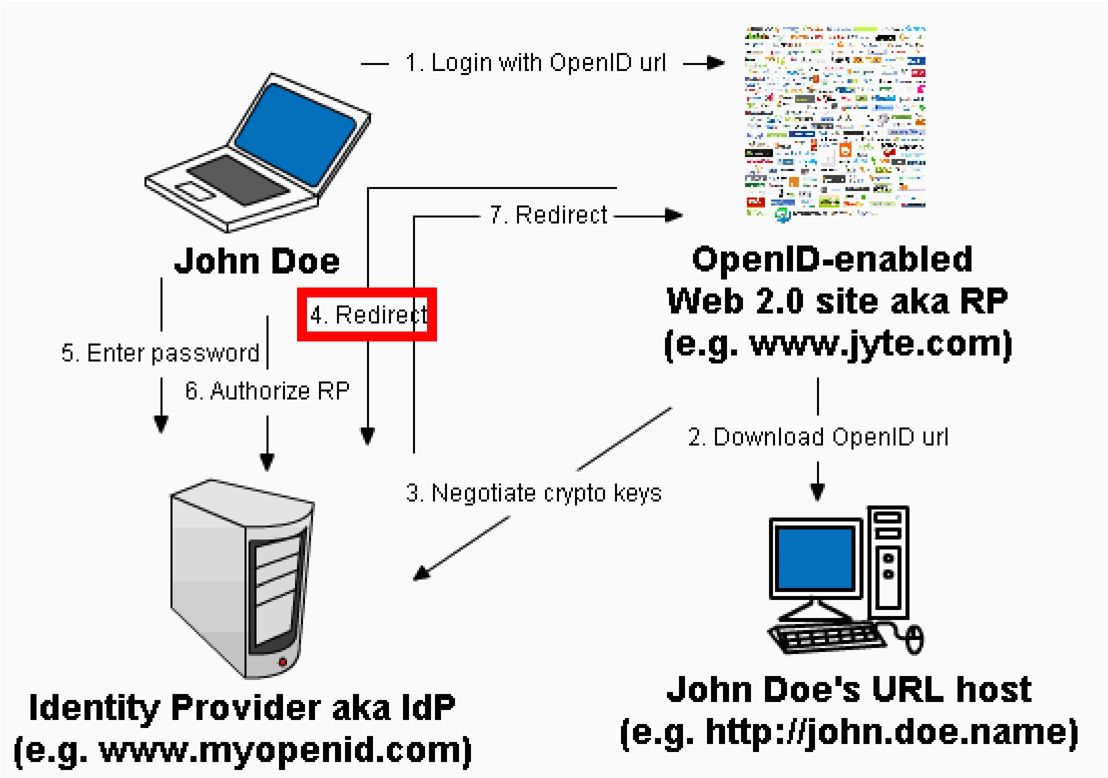
Lesson #3

Home brewed crypto is a no no

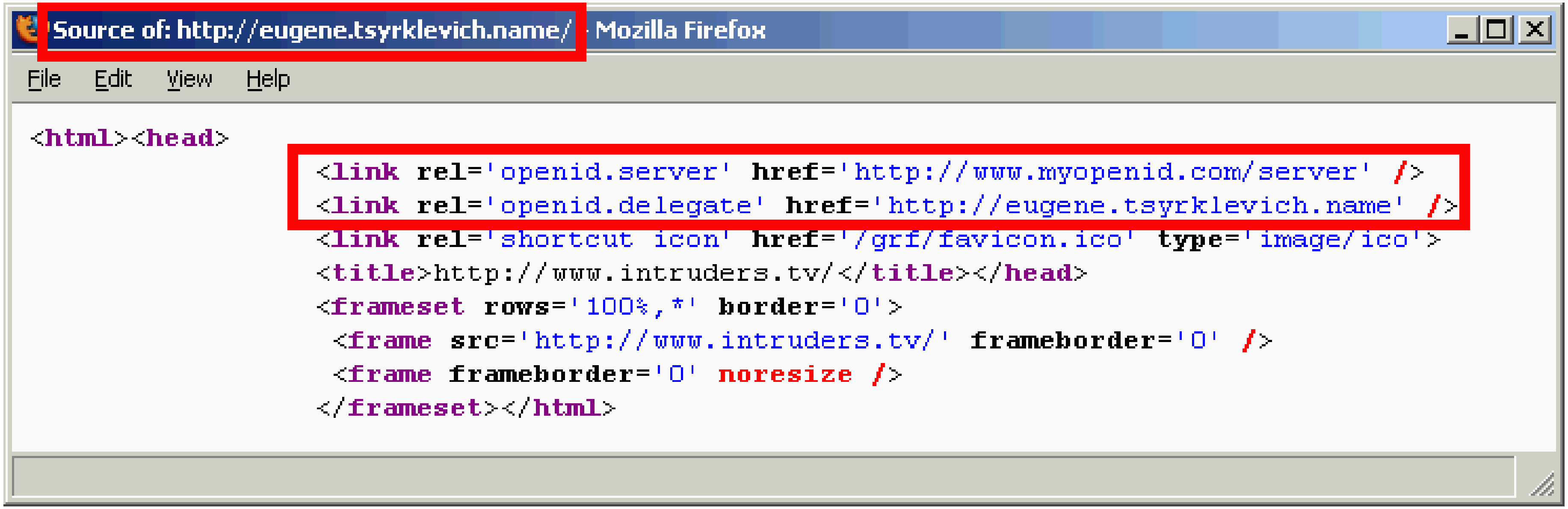
(or, why you should stick to https)

"Never, ever, think outside the box."

Where are you going?



This way! No, that way!

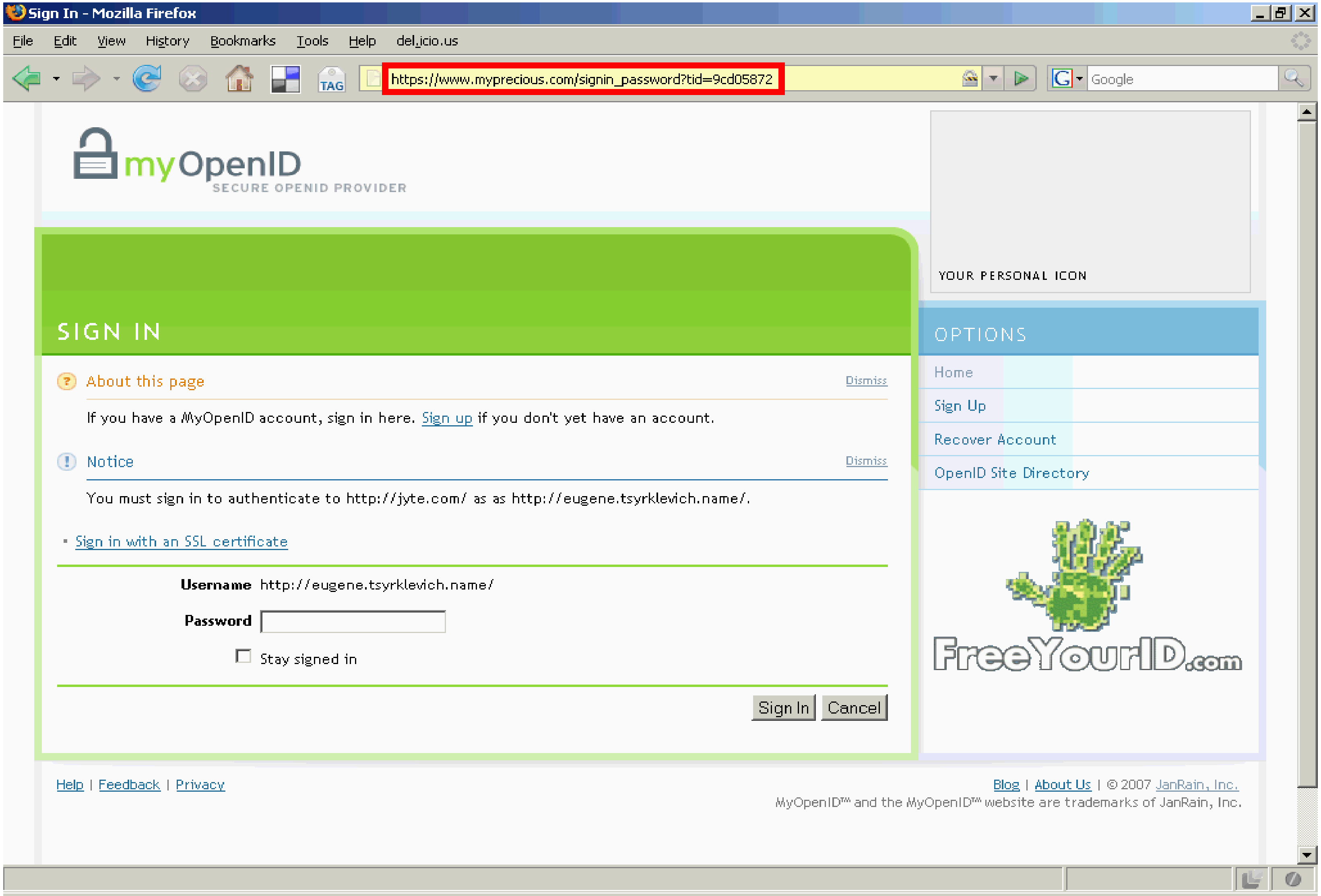


Source of: http://eugene.tsyrklevich.name/ - Mozilla Firefox
File
Edit
View
Help

```
<html><head>
                 <link rel='openid.server' href='http://www.myopenid.com/server' />
                 <link rel='openid.delegate' href='http://eugene.tsyrklevich.name' />
                 <link rel='shortcut icon' href='/grf/favicon.ico' type='image/ico'>
                 <title>http://www.intruders.tv/</title></head>
                 <frameset rows='100%,*' border='0'>
                  <frame src='http://www.intruders.tv/' frameborder='0' />
                  <frame frameborder='0' noresize />
                 </frameset></html>
```

Location: http://www.myopenid.com/server?
openid.assoc_handle=%7BHMAC-SHA1%7D%7B4..&
openid.identity=http%3A%2F%2Fjohn.doe.name%2F&
openid.mode=checkid_setup&
openid.return_to=http%3A%2F%2www.somesite.com%2F&
openid.trust_root=http%3A%2F%2www.somesite.com%2F

Attack #4a
Phishing with malicious RPs



Sign In - Mozilla Firefox
File Edit View History Bookmarks Tools Help del.icio.us
TAG
Google
myOpenID
SECURE OPENID PROVIDER
YOUR PERSONAL ICON
FreeYourID.com

https://www.myprecious.com/signin_password?tid=9cd05872

SIGN IN

About this page — Dismiss

If you have a MyOpenID account, sign in here. Sign up if you don't yet have an account.

Notice — Dismiss

You must sign in to authenticate to http://jyte.com/ as as http://eugene.tsyrklevich.name/.

- Sign in with an SSL certificate

Username http://eugene.tsyrklevich.name/

Password

□ Stay signed in

Sign In | Cancel

OPTIONS

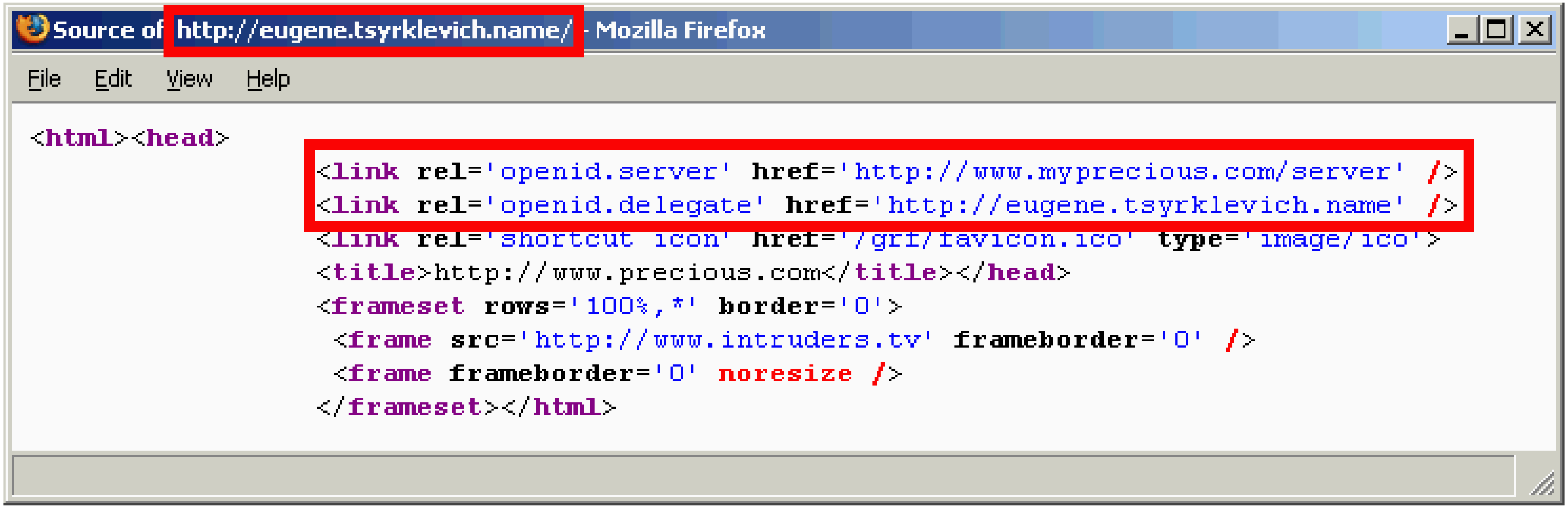
- Home
- Sign Up
- Recover Account
- OpenID Site Directory

Help | Feedback | Privacy

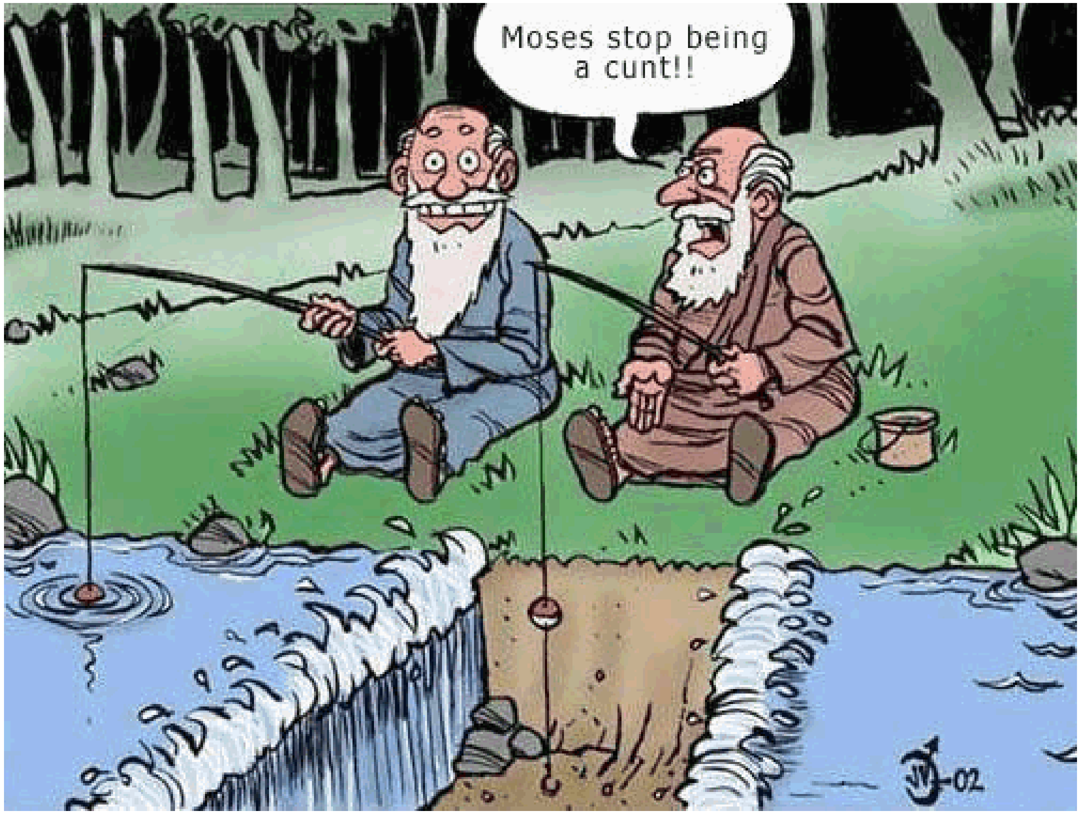
Blog | About Us | © 2007 JanRain, Inc.

MyOpenID™ and the MyOpenID™ website are trademarks of JanRain, Inc.

Attack #4b
Phishing with malicious URL hosts



```
<html><head>
                  <link rel='openid.server' href='http://www.myprecious.com/server' />
                  <link rel='openid.delegate' href='http://eugene.tsyrklevich.name' />
                  <link rel='shortcut icon' href='/grf/favicon.ico' type='image/ico'>
                  <title>http://www.precious.com</title></head>
                  <frameset rows='100%,*' border='0'>
                   <frame src='http://www.intruders.tv' frameborder='0' />
                   <frame frameborder='0' noresize />
                  </frameset></html>
```

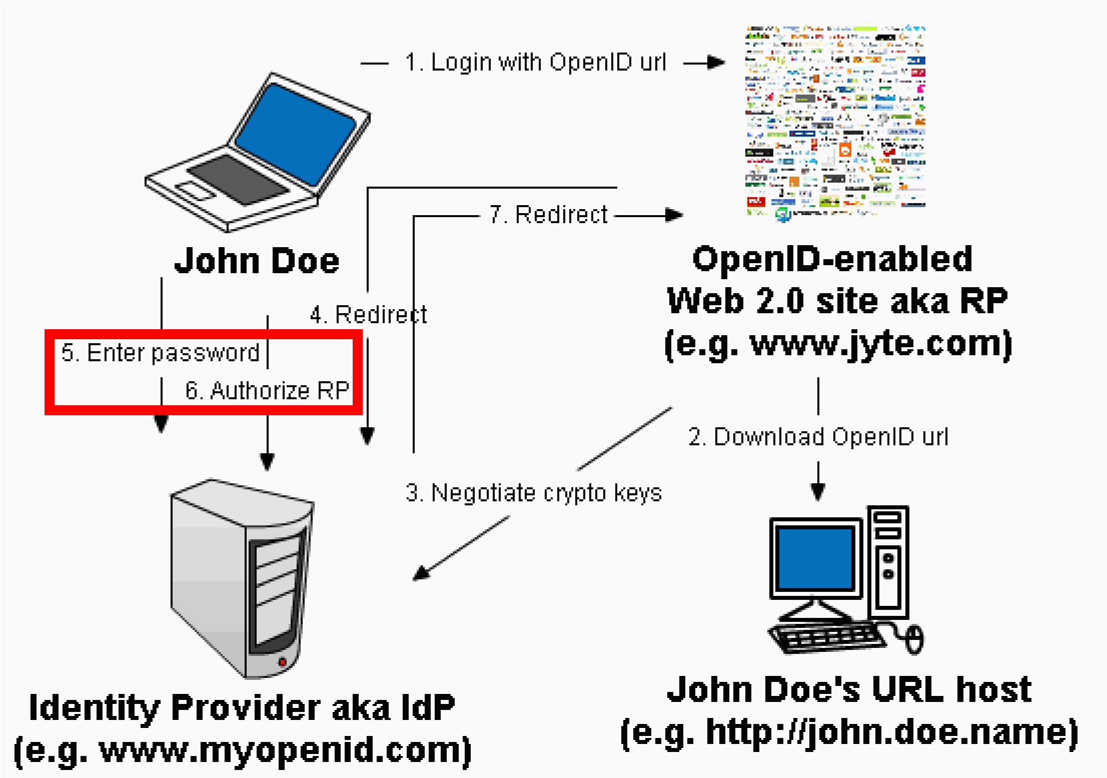


Lesson #4

Phishers 1 – OpenID 0

(or, why Johnny will never learn to read URLs)

Let me in!


1. Login with OpenID url
John Doe
7. Redirect
OpenID-enabled
Web 2.0 site aka RP
(e.g. www.jyte.com)
4. Redirect
5. Enter password
6. Authorize RP
2. Download OpenID url
3. Negotiate crypto keys
Identity Provider aka IdP
(e.g. www.myopenid.com)
John Doe's URL host
(e.g. http://john.doe.name)

Once signed in, you will no longer need to re-enter your password for other OpenID enabled sites

Convenient, eh?

In other words…

your identity provider receives and processes ALL your login requests on your behalf

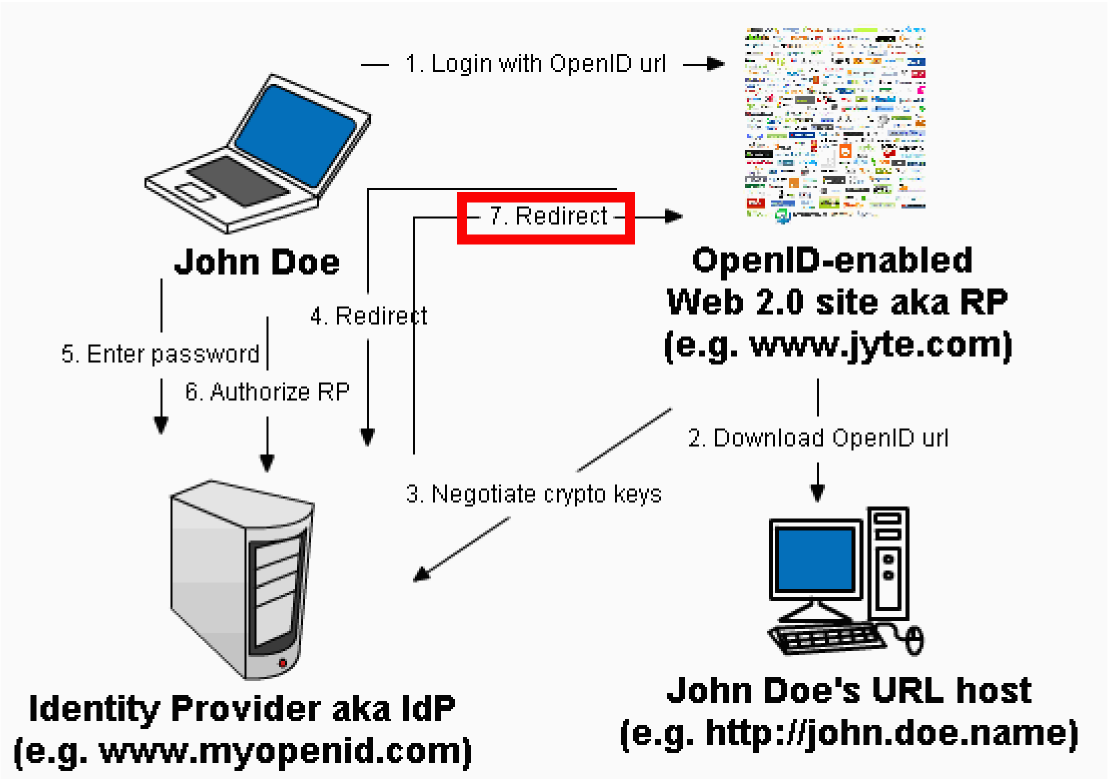
…privacy, anyone?

Lesson #5

OpenID makes privacy difficult

(or, why some paranoid users might want to use one OpenID login per site)

Not another redirect!



Attack #6 – Replay attack

Location: http://www.somesite.com/finish_auth.php?

openid.assoc_handle=%7BHMAC-HA1%7D%7B47bb..&

openid.identity=http%3A%2F%2Fjohn.doe.name%2F&

openid.mode=id_res&

openid.return_to=http%3A%2F%2www.somesite.com&

openid.sig=vbUyND6n39Ss8IkpKl19RT83O%2F4%3D&

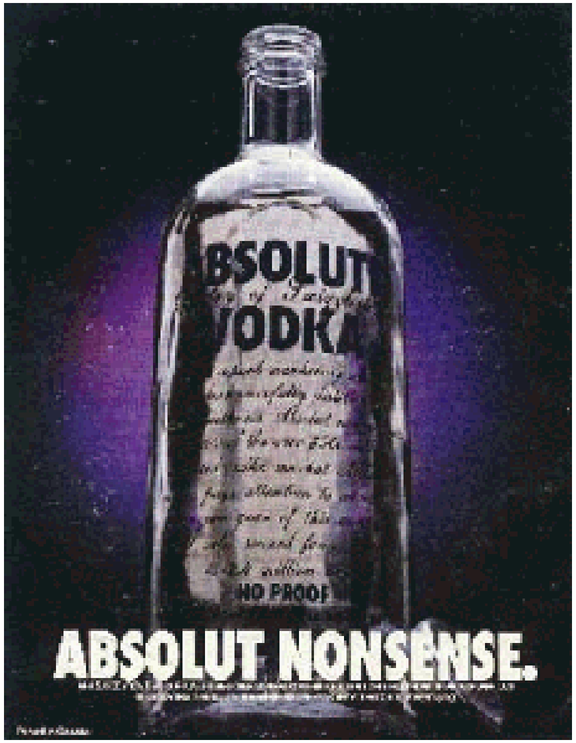
openid.signed=mode%2Cidentity%2Creturn_to&

nonce=wVso75KH

Problems with Nonces

a. Not part of the OpenID spec (v1)

b. Do not actually protect against active attackers!

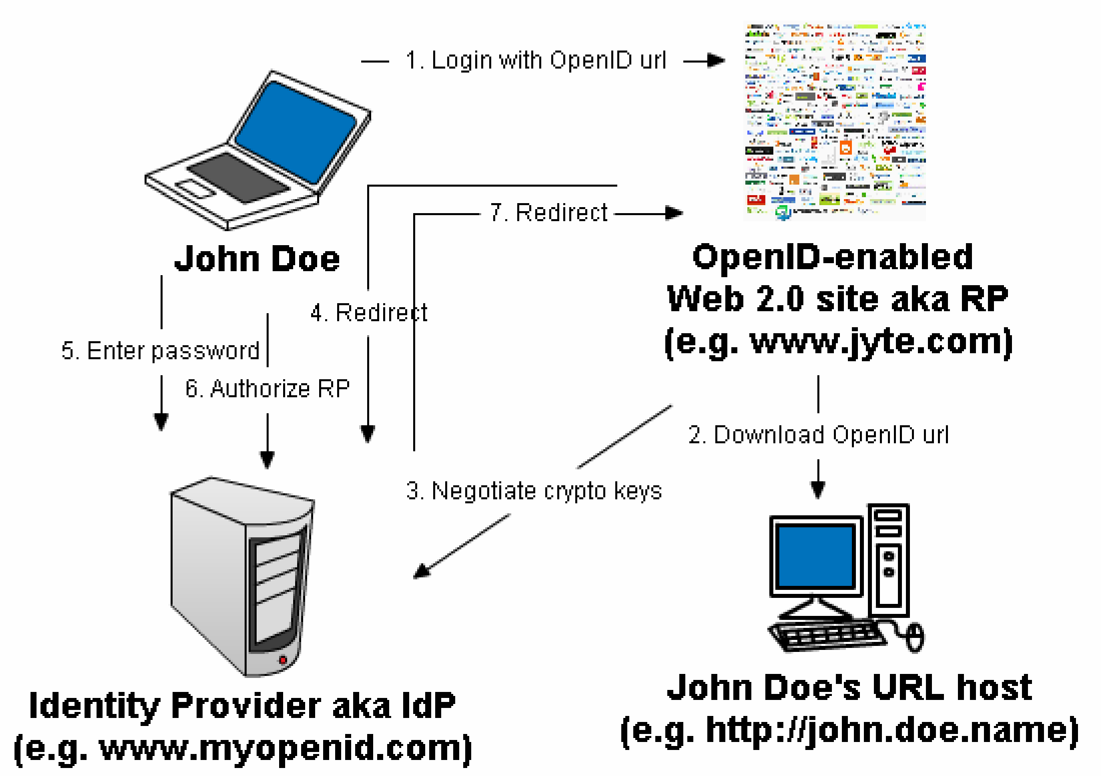


Lesson #6

Nonces are nonsense

(or, why you must be drinking absolut kool-aid if you believe nonces will protect you against an active attacker)

I am secure once I am logged in though, right?



Attack #7 – Cross-site request forgery

```
<html><body>

<iframe id="login"
src="http://bank.com/login?openid_url=john.doe.name" width="0"
height="0"></iframe>

<iframe id=“transfer"
src="http://bank.com/transfer_money?amount=100&to=attacker"
width="0" height="0"></iframe>

</body></html>
```

Lesson #7

OpenID robs you of control

(or IdP, not RP, makes the security decisions)

Is it really all that bad?!

No!

OpenID can make your logins far more secure than they are today!

How?!

Only one service to secure so we can afford to use

- Client-side certificates
- SecurID
- Smartcards

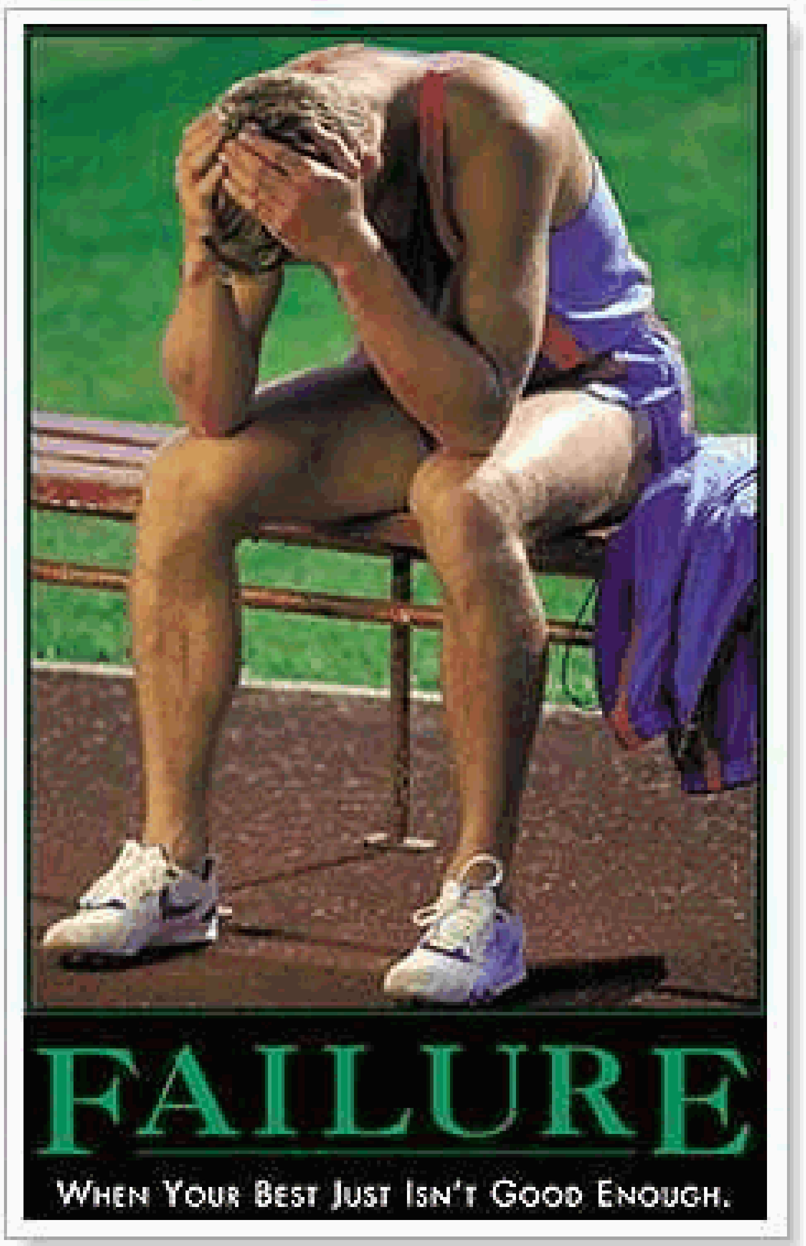
Lesson #8

There is only 1 front door with OpenID

(or, how I got over my privacy and learnt to love OpenID)

Lessons Learnt

1. Complexity breeds insecurity
2. Flexibility and security do not get along
3. Home brewed crypto is a no no
4. Phishers 1 – OpenID 0
5. OpenID makes privacy difficult
6. Nonces are nonsense
7. OpenID robs you of control
8. There is only 1 front door with OpenID



Is OpenID doomed?

Absolutely not

It’s a great system
solving a very real problem

But its security and
privacy concerns
need further thought

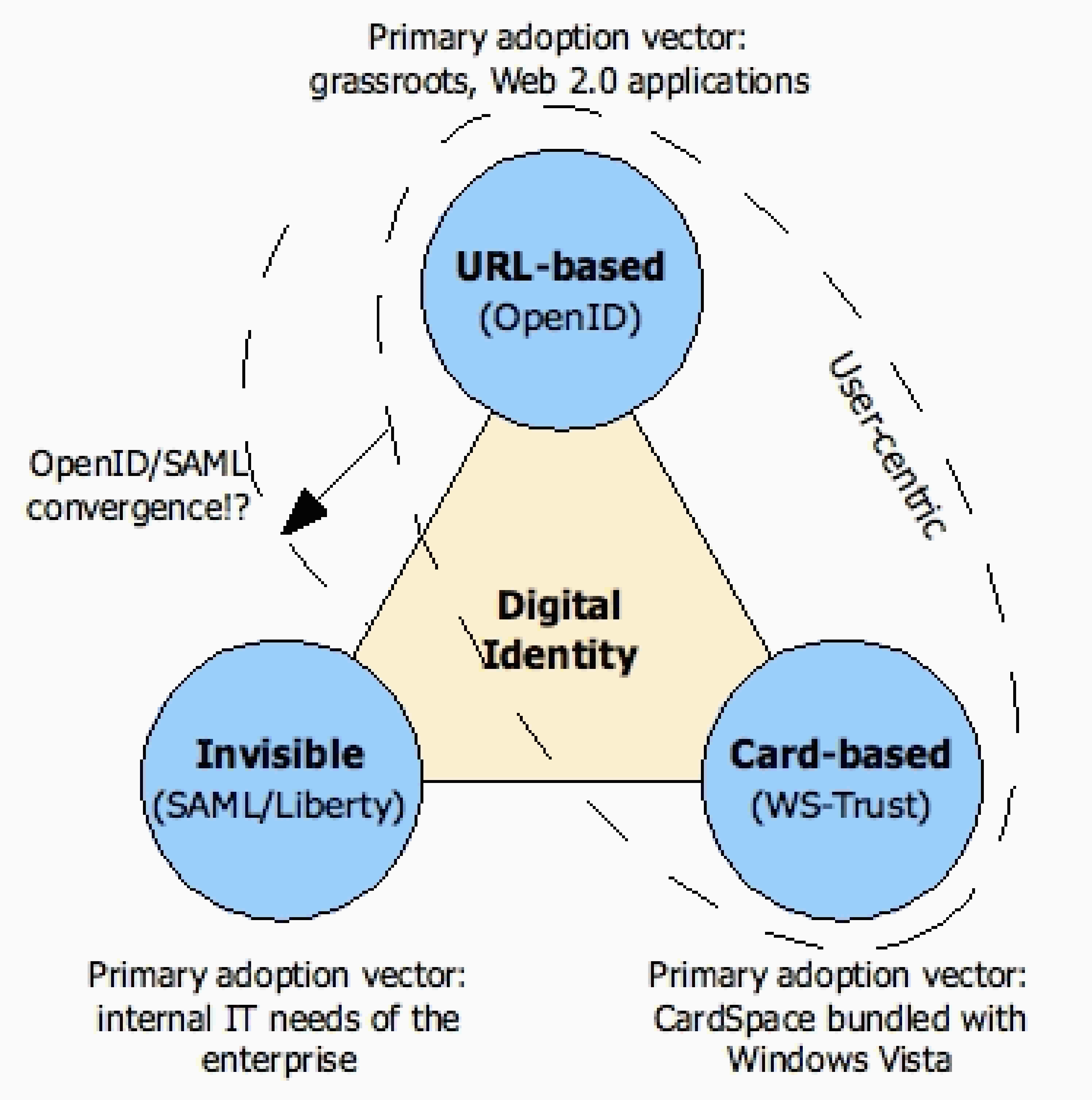
Thanks!

Try it today.

http://www.openid.net/

http://www.freeyourid.com/

eugene@tsyrklevich.name
vlad902@gmail.com


Primary adoption vector: grassroots, Web 2.0 applications
URL-based
(OpenID)
OpenID/SAML convergence!?
User-centric
Digital Identity
Invisible
(SAML/Liberty)
Card-based
(WS-Trust)
Primary adoption vector: internal IT needs of the enterprise
Primary adoption vector: CardSpace bundled with Windows Vista